Cisco IOS Security Command Reference: Commands S to Z

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

sa ipsec through sessions maximum

sa ipsec

To specify the IP security (IPsec) security association (SA) policy information to be used for a Group Domain of Interpretation (GDOI) group and to enter GDOI SA IPsec configuration mode, use the **sa ipsec** command in GDOI local server configuration mode. To remove the policy information that was specified, use the **no** form of this command.

sa ipsec *sequence-number*
no sa ipsec *sequence-number*

Syntax Description

sequence-number	Sequence number of the IPsec SA.

Command Default

None

Command Modes

GDOI local server configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

IPsec and SA policy information must be specified using this command if the traffic encryption key policy has to be defined.

Examples

The following example shows that three IPsec SA policy numbers (1, 2, and 3) have been specified:

```
sa ipsec 1
  profile gdoi-p
  match address ipv4 120
sa ipsec 2
  profile gdoi-q
  match address ipv4 121
sa ipsec 3
  profile gdoi-r
  match address ipv4 122
```

Related Commands

Command	Description
crypto gdoi group	Identifies a GDOI group and enters GDOI group configuration mode.
match address	Specifies an IP extended access list for a GDOI registration.
profile	Defines the IPsec SA policy for a GDOI group.
server local	Designates a device as a GDOI key server and enters GDOI local server configuration mode.

sa receive-only

To specify that an IP security (IPsec) security association (SA) is to be installed by a group member as "inbound only," use the **sa receive-only**command in GDOI local server configuration mode. To remove the inbound-only specification, use the **no** form of this command.

sa receive-only
no sa receive-only

Syntax Description

This command has no arguments or keywords.

Command Default

If this command is not configured, IPsec SAs are installed by group members as both inbound and outbound.

Command Modes

GDOI local server configuration (config-local-server)

Command History

Release	Modification
12.4(11)T	This command was introduced.
Cisco IOS XE Release 2.3	This command was implemented on the Cisco ASR 1000 series routers.

Usage Guidelines

This command is configured on a key server. The command may be used to ease in deployment.

Examples

The following example shows that the Group Domain of Interpretation (GDOI) group is instructed by the key server to install the IPsec SAs as "inbound only":

```
crypto gdoi group gdoi_group
 identity number 1234
server local
 sa receive-only
 sa ipsec 1
  profile gdoi-p
  match address ipv4 120
```

Related Commands

Command	Description
crypto gdoi gm	Allows group members to change the IPsec SA status.
crypto gdoi group	Identifies a GDOI group and enters GDOI group configuration mode.
server local	Designates a device as a GDOI key server and enters GDOI local server configuration mode.

sap mode-list (config-if-cts-dot1x)

To select the Security Association Protocol (SAP) authentication and encryption modes (prioritized from highest to lowest) used to negotiate link encryption between two interfaces, use the **sap mode-list** command in CTS dot1x interface configuration mode. To remove a mode-list and revert to the default, use the **no** form of this command.

sap mode-list {**gcm-encrypt** | **gmac** | **no-encap** | **null**} [**gcm-encrypt** | **gmac** | **no-encap** | **null**]
no sap mode-list {**gcm-encrypt** | **gmac** | **no-encap** | **null**} [**gcm-encrypt** | **gmac** | **no-encap** | **null**]

Syntax Description

gcm-encrypt	Specifies GMAC authentication, GCM encryption.
gmac	Specifies GMAC authentication only, no encryption.
no-encap	Specifies no encapsulation.
null	Specifies encapsulation present, no authentication, no encryption.

Command Default

The default encryption is **sap mode-list gcm-encrypt null**. When the peer interface does not support dot1x, 802.1AE MACsec, or 802.REV layer-2 link encryption, the default encryption is **null**.

Command Modes

CTS dot1x interface configuration (config-if-cts-dot1x)

Command History

Release	Modification
12.2(50) SY	This command was introduced on the Catalyst 6500 Series Switches.
IOS- XE 3.3.0 SG	This command was introduced on the Catalyst 4500 Series Switches.
15.0(1) SE	This command was introduced on the Catalyst 3000 Series Switches.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

Use the **sap mode-list** command to specify the authentication and encryption method to use during Dot1x authentication.

The Security Association Protocol (SAP) is an encryption key derivation and exchange protocol based on a draft version of the 802.11i IEEE protocol. SAP is used to establish and maintain the 802.1AE link-to-link encryption (MACsec) between interfaces that support MACsec.

Before the SAP exchange begins after a Dot1x authentication, both sides (supplicant and authenticator) have received the Pairwise Master Key (PMK) and the MAC address of the peer's port from the Cisco Secure Access Control Server (Cisco Secure ACS). If 802.1X authentication is not possible, SAP, and the PMK can be manually configured between two interfaces in CTS manual configuration mode.

If a device is running CTS-aware software but the hardware is not CTS-capable, disallow encapsulation with the **sap mode-list no-encap** command.

Use the **timer reauthentication** command to configure the reauthentication period to be applied to the CTS link in case the period is not available from the Cisco Secure ACS. The default reauthentication period is 86,400 seconds.

Note Because TrustSec NDAC and SAP are supported only on a switch-to-switch link, dot1x must be configured in multi-hosts mode. The authenticator PAE starts only when the **dot1x system-auth-control** command is enabled globally.

Examples

The following example specifies that SAP is to negotiate the use of CTS encapsulation with GCM cipher, or null-cipher as a second choice, but can accept no CTS encapsulation if the peer does not support CTS encapsulation in hardware.

```
Device(config-if-cts-dot1x)# sap mode-list gcm-encrypt null no-encap
```

Related Commands

Command	Description
cts dot1x	Enables Network Device Admission Control (NDAC) and configure NDAC authentication parameters.
propagate sgt (config-if-cts-dot1x)	Enables Security Group Tag (SGT) propagation on a Cisco TrustSec (CTS) 802.1X interface.
show cts interface	Displays CTS interface status and configurations.
show dot1x interface	Displays IEEE 802.1x configurations and statistics.
timer reauthentication (config-if-cts-dot1x)	Configures the reauthentication timer for a CTS device.

save-password

To save your extended authentication (Xauth) password locally on your PC, use the **save-password** command in Internet Security Association Key Management Protocol (ISAKMP) group configuration mode. To disable the Save-Password attribute, use the **no** form of this command.

save-password
no save-password

Syntax Description

This command has no arguments or keywords.

Command Default

Your Xauth password is not saved locally on your PC, and the Save-Password attribute is not added to the server group profile.

Command Modes

ISAKMP group configuration (config-isakmp-group)

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS 12.2SX family of releases. Support in a specific 12.2SX release is dependent on your feature set, platform, and platform hardware.

Usage Guidelines

Save password control allows you to save your Xauth password locally on your PC so that after you have initially entered the password, the Save-Password attribute is pushed from the server to the client. On subsequent authentications, you can activate the password by using the tick box on the software client or by adding the username and password to the Cisco IOS hardware client profile. The password setting remains until the Save-Password attribute is removed from the server group profile. After the password has been activated, the username and password are sent automatically to the server during Xauth without your intervention.

The save-password option is useful only if your password is static, that is, if it is not a one-time password such as one that is generated by a token.

The Save-Password attribute is configured on a Cisco IOS router or in the RADIUS profile.

To configure save password control, use the **save-password**command.

An example of an attribute-value (AV) pair for the Save-Password attribute is as follows:

```
ipsec:save-password=1
```

You must enable the **crypto isakmp client configuration group** command, which specifies group policy information that has to be defined or changed, before enabling the **save-password** command.

Note The Save-Password attribute can be applied only by a RADIUS user.

- The attribute can be applied on a per-user basis after the user has been authenticated.

- The attribute can override any similar group attributes.
- User-based attributes are available only if RADIUS is used as the database.

Examples

The following example shows that the Save-Password attribute has been configured:

```
crypto isakmp client configuration group cisco
 save-password
```

Related Commands

Command	Description
acl	Configures split tunneling.
crypto isakmp client configuration group	Specifies the DNS domain to which a group belongs.

scheme

To define the redundancy scheme that is used between two devices, use the **scheme**command in inter-device configuration mode. To disable the redundancy scheme, use the **no** form of this command.

scheme standby *standby-group-name*
no scheme standby *standby-group-name*

Syntax Description

standby	Redundancy scheme. Currently, the standby scheme is the only available scheme.
standby-group-name	Specifies the name of the standby group. This name must match the name that was specified via the **standby name** command. Also, the standby name should be the same on both the active and standby routers.

Command Default

A redundancy scheme is not specified.

Command Modes

Inter-device configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

Only the active or standby state of the standby group is used for Stateful Switchover (SSO). The virtual IP (VIP) address of the standby group is not required or used by SSO. Also, the standby group does not have to be part of any crypto map configuration.

Examples

The following example shows how to enable SSO and define the standby scheme that is to be used by the active and standby devices:

```
redundancy inter-device
 scheme standby HA-in
!
!
ipc zone default
 association 1
  no shutdown
  protocol sctp
   local-port 5000
    local-ip 10.0.0.1
   remote-port 5000
    remote-ip 10.0.0.2
```

Related Commands

Command	Description
standby name	Configures the name of the standby group.

search-filter

To configure a search request sent by the Lightweight Directory Access Protocol (LDAP) client to the server in order to find the user's node in the Directory Information Tree (DIT), use the **search-filter** command in LDAP server configuration mode. To delete the search request from the LDAP server group, use the **no** form of this command.

search-filter user-object-type *string*
no search-filter user-object-type *string*

Syntax Description

user-object-type	Adds a user attribute to the search filter.
string	Name of the object class attribute.

Command Default

No default search requests are configured.

Command Modes

LDAP server configuration (config-ldap-server)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Usage Guidelines

You can add multiple search filter attributes by using the **search-filter** command. The search filter is a mandatory configuration for an LDAP server, because it is used to filter the exact user from the search results. Without this configuration, a user cannot be authenticated. The **search-filter** command helps you to filter the search results based on the attributes mentioned in the search filter.

Examples

The following example shows how to filter the search results for an LDAP server. After you have specified the search criteria as shown below, the search filter string appears in the "(&(objectclass=person) (&(cn=$userid)(cid=$contextid)))" format.

```
Router(config)# ldap server server1
Router(config-ldap-server)# search-filter user-object-type cn
Router(config-ldap-server)# search-filter user-object-type cid
Router(config-ldap-server)# search-filter user-object-type objectclass
```

Related Commands

Command	Description
ldap server	Defines an LDAP server and enters LDAP server configuration mode.

search-type nested

To configure nested-group search requests, use the **search-type nested** command in Lightweight Directory Access Protocol (LDAP) server configuration mode. To remove the configuration, use the **no** form of this command.

search-type nested
no search-type nested

Syntax Description

This command has no arguments or keywords.

Command Default

No nested-group search requests are configured.

Command Modes

LDAP server configuration (config-ldap-server)

Command History

Release	Modification
15.3(2)T	This command was introduced.

Usage Guidelines

Use the **search-type nested** command to configure nested-group search requests. The nested-group search filter allows you to retrieve the complete nested-user-group chain information of a user in a particular Microsoft Active Directory domain. This customized filter is sent in an LDAP query to the server.

The **search-type nested** command overrides the **search-filter object-type** command, which is used to conduct a top-level search to obtain direct user groups from an LDAP server.

Examples

The following example shows how to configure nested-group search requests.

```
ldap server ldap_dir_1
bind authenticate root-dn cn=administrator,cn=users,dc=nac-blr2,dc=example,dc=com password
 example123
search-type nested
base-dn dc=sns,dc=example,dc=com
```

Related Commands

Command	Description
ldap server	Defines an LDAP server and enters LDAP server configuration mode.
search-filter object-type	Configures a search request sent by an LDAP client to a server to find a user's node in the DIT.

sec-level minimum

To specify the minimum security level parameter value when Cryptographically Generated Address (CGA) options are used, use the **sec-level minimum** command in Neighbor Discovery (ND) inspection policy configuration mode. To disable this function, use the **no** form of this command.

sec-level minimum *value*
no sec-level minimum *value*

Syntax Description

value	Minimum security level, which is a value from 1 to 7. The default security level is 1. The most secure level is 3.

Command Default

The default security level is 1.

Command Modes

ND inspection policy configuration (config-nd-inspection)

RA guard policy configuration (config-ra-guard)

Command History

Release	Modification
12.2(50)SY	This command was introduced.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The **sec-level minimum** command specifies the minimum security level parameter value when CGA options are used. Use the **sec-level minimum** command after enabling ND inspection policy configuration mode using the **ipv6 nd inspection policy** command.

Examples

The following example defines an ND policy name as policy1, places the router in ND inspection policy configuration mode, and specifies 2 as the minimum CGA security level:

```
Router(config)# ipv6 nd inspection policy policy1
Router(config-nd-inspection)# sec-level minimum 2
```

Related Commands

Command	Description
ipv6 nd inspection policy	Defines the ND inspection policy name and enters ND inspection policy configuration mode.
ipv6 nd raguard policy	Defines the RA guard policy name and enters RA guard policy configuration mode.

secondary-color

To configure the color of the secondary title bars on the login and portal pages of a SSL VPN website, use the **secondary-color** command in webvpn context configuration mode. To remove the color from the WebVPN context configuration, use the **no** form of this command.

secondary-color *color*
no secondary-color *color*

Syntax Description

color	The value for the *color* argument is entered as a comma-separated red, green, blue (RGB) value, an HTML color value (beginning with a"#"), or the name of the color that is recognized in HTML (no spaces between words or characters). The value is limited to 32 characters. The value is parsed to ensure that it matches one of the following formats (using Perl regex notation): • \#/x{6} • \d{1,3},\d{1,3},\d{1,3} (and each number is from 1 to 255) • \w+ The default color is purple.

Command Default

The color purple is used if this command is not configured or if the **no** form is entered.

Command Modes

Webvpn context configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

Configuring a new color overrides the color of the preexisting color.

Examples

The following examples show the three forms in which the secondary color is configured:

```
Router(config-webvpn-context)# secondary-color darkseagreen

Router(config-webvpn-context)# secondary-color #8FBC8F

Router(config-webvpn-context)# secondary-color 143,188,143
```

Related Commands

Command	Description
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

secondary-text-color

To configure the color of the text on the secondary bars of an SSL VPN website, use the **secondary-text-color** command in webvpn context configuration mode. To revert to the default color, use the **no** form of this command.

secondary-text-color [{**black** | **white**}]
no secondary-text-color [{**black** | **white**}]

Syntax Description

black	(Optional) Color of the text is black. This is the default value.
white	(Optional) Color of the text is white.

Command Default

The color of the text on secondary bars is black if this command is not configured or if the **no** form is entered.

Command Modes

Webvpn context configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

The color of the text on the secondary bars must be aligned with the color of the text on the title bar.

Examples

The following example sets the secondary text color to white:

```
Router(config)#
webvpn context context1

Router(config-webvpn-context)#
secondary-text-color white

Router(config-webvpn-context)#
```

Related Commands

Command	Description
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

secret

To associate a CLI view or a superview with a password, use the **secret** command in view configuration mode. To remove the configured password, use the **no** form of this command.

secret {**0** *unencrypted-password* | **5** *encrypted-password* | *unencrypted-password*}
no secret {**0** *unencrypted-password* | **5** *encrypted-password* | *unencrypted-password*}

Syntax Description

0	Specifies that an unencrypted password follows.
unencrypted-password	Unencrypted password. A password that contains a combination of alphanumeric characters. The password is case sensitive. This password is encrypted by the message digest 5 (MD5) method.
5	Specifies that an encrypted password follows.
encrypted-password	Encrypted password that you enter or that is copied from another router configuration.

Command Default

A user cannot access a CLI view or superview.

Command Modes

View configuration (config-view)

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

Security threats, as well as the cryptographic technologies to help protect against them, are constantly changing. For more information about the latest Cisco cryptographic recommendations, see the Next Generation Encryption (NGE) white paper.

A user cannot access any commands within the CLI view or superview until the **secret** command has been issued.

Before CSCts50236, the password could only be overwritten and not removed. With CSCts50236, the password can be removed or overwritten. Use the **no secret** command in the view configuration (config-view) mode to remove the configured password.

Examples

The following examples show how to configure two CLI views, “first” and “second”, and associate each view with a password:

```
Device> enable
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

```
Device(config)# aaa new-model
Device(config)# enable secret cisco
Device(config)# exit
Device# enable view root
Password:
*Dec  9 00:50:51.283: %PARSER-6-VIEW_SWITCH: successfully set to view 'root'.
Device# show parser view
Current view is 'root'
Device# configure terminal
Device(config)# parser view first
Device(config-view)#
*Dec  9 05:20:03.039: %PARSER-6-VIEW_CREATED: view 'first' successfully created.
Device(config-view)# secret firstpassword
Device(config-view)# secret secondpassword
% Overwriting existing secret for the current view
Device(config-view)# secret 0 thirdpassword
% Overwriting existing secret for the current view
Device(config-view)# secret 5 $1$jj1e$vmYyRbmj5UoU96tT1x7eP1
% Overwriting existing secret for the current view
Device(config-view)# secret 5 invalidpassword
ERROR: The secret you entered is not a valid encrypted secret.
To enter an UNENCRYPTED secret, do not specify type 5 encryption.
When you properly enter an UNENCRYPTED secret, it will be encrypted.
Device(config-view)# command exec include show version
Device(config-view)# command exec include configure terminal
Device(config-view)# command configure include all ip
Device(config-view)# exit


Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# parser view second
Device(config-view)#
*Dec 30 06:11:52.915: %PARSER-6-VIEW_CREATED: view 'second' successfully created.
Device(config-view)# secret mypasswd
Device(config-view)# commands exec include ping
Device(config-view)# end
Device# show running-config | include parser view second

.
.
.
parser view second
 secret 5 $1$PWs8$lz3lSx6OqAnFrUx2hkI0w0
 commands exec include ping
!
.
.
.
```

The following is sample output from the **show running-config** command for a situation in which the **secret** command has been configured using a level-5 encrypted password:

```
Device# show running-config | include parser view first

.
.
.
parser view first
 secret 5 $1$jj1e$vmYyRbmj5UoU96tT1x7eP1
 commands configure include all ip
```

```
 commands exec include configure terminal
 commands exec include configure
 commands exec include show version
 commands exec include show
!
.
.
.
```

Related Commands

Command	Description
parser view	Creates or changes a CLI view and enters view configuration mode.

secret-key

To configure the policy server secret key that is used to secure authentication requests, use the **secret-key** command in webvpn sso server configuration mode. To remove the secret key, use the **no** form of this command.

secret-key *key-name*
no secret-key *key-name*

Syntax Description

key-name	Name of secret key.

Command Default

A policy server secret key is not configured.

Command Modes

Webvpn sso server configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Note A web agent URL and policy server secret key are required for a Single SignOn (SSO) server configuration. If the web agent URL and policy server secret key are not configured, a warning message is displayed. (See the secret-key section in the Examples section below.)

- This is the same secret key that should be configured on the Cisco SiteMinder plug-in.

Examples

The following example shows the policy server secret key is "example.123":

```
webvpn context context1
 sso-server test-sso-server
  secret-key example.123
```

Warning Message

If a web agent URL and policy server secret key are not configured, a message similar to the following is received:

```
Warning: must configure web agent URL for sso-server "example"
Warning: must configure SSO policy server secret key for sso-server "example"
Warning: invalid configuration. SSO for "example" being disabled
```

Related Commands

Command	Description
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

secure boot-config

To take a snapshot of the router running configuration and securely archive it in persistent storage, use the **secure boot-config** command in global configuration mode. To remove the secure configuration archive and disable configuration resilience, use the **no** form of this command.

secure boot-config [**restore** *filename*]
no secure boot-config

Syntax Description

restore *filename*	(Optional) Reproduces a copy of the secure configuration archive as the supplied filename.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

Without any parameters, this command takes a snapshot of the router running configuration and securely archives it in persistent storage. Like the image, the configuration archive is hidden and cannot be viewed or removed directly from the command-line interface (CLI) prompt . It is recommended that you run this command after the router has been fully configured to reach a steady state of operation and the running configuration is considered complete for a restoration, if required. A syslog message is printed on the console notifying the user of configuration resilience activation. The secure archive uses the time of creation as its filename. For example, .runcfg-20020616-081702.ar was created July 16 2002 at 8:17:02.

The restore option reproduces a copy of the secure configuration archive as the supplied filename (disk0:running-config, slot1:runcfg, and so on). The restore operation will work only if configuration resilience is enabled. The number of restored copies that can be created is unlimited.

The **no** form of this command removes the secure configuration archive and disables configuration resilience. An enable, disable, enable sequence has the effect of upgrading the configuration archive if any changes were made to the running configuration since the last time the feature was disabled.

The configuration upgrade scenario is similar to an image upgrade. The feature detects a different version of Cisco IOS and notifies the user of a version mismatch. The same command can be run to upgrade the configuration archive to a newer version after new configuration commands corresponding to features in the new image have been issued.

The correct sequence of steps to upgrade the configuration archive after an image upgrade is as follows:

- Configure new commands
- Issue the **secure boot-config** command

Examples

The following example shows the command used to securely archive a snapshot of the router running configuration:

```
secure boot-config
```

The following example shows the command used to restore an archived image to the file slot0:rescue-cfg:

```
Router(config)# secure boot-config restore slot0:rescue-cfg
ios resilience:configuration successfully restored as slot0:rescue-cfg
```

Related Commands

Command	Description
secure boot-image	Enables Cisco IOS image resilience.
show secure bootset	Displays the status of image and configuration resilience.

secure boot-image

To enable Cisco IOS image resilience, use the **secure boot-image** command in global configuration mode. To disable Cisco IOS image resilience and release the secured image so that it can be safely removed, use the **no** form of this command.

secure boot-image
no secure boot-image

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

This command enables or disables the securing of the running Cisco IOS image. The following two possible scenarios exist with this command.

- When turned on for the first time, the running image (as displayed in the **show version** command output) is secured, and a syslog entry is generated. This command will function properly only when the system is configured to run an image from a disk with an Advanced Technology Attachment (ATA) interface. Images booted from a TFTP server cannot be secured. Because this command has the effect of "hiding" the running image, the image file will not be included in any directory listing of the disk. The **no** form of this command releases the image so that it can be safely removed.
- If the router is configured to boot up with Cisco IOS resilience and an image with a different version of Cisco IOS is detected, a message similar to the following is displayed at bootup:

```
ios resilience :Archived image and configuration version 12.2 differs from running version
 12.3.
Run secure boot-config and image commands to upgrade archives to running version.
```

To upgrade the image archive to the new running image, reenter this command from the console. A message will be displayed about the upgraded image. The old image is released and will be visible in the **dir** command output.

Caution Be careful when copying new images to persistent storage because the existing secure image name might conflict with the new image. To verify the name of the secured archive, run the **show secure bootset** command and resolve any name conflicts with the currently secured hidden image.

Note After the Cisco IOS image is secured, the resilient configuration feature will deny any requests to copy, modify, or delete the secure archive and will even survive a disk format operation.

Examples

The following example shows the activation of image resilience.

```
Router(config)# secure boot-image
```

Related Commands

Command	Description
dir	Displays a list of files on a file system.
secure boot-config	Saves a secure copy of the router running configuration in persistent storage.
show secure bootset	Displays the status of image and configuration resilience.
show version	Displays the configuration of the system hardware, the software version, the names and sources of configuration files, and the boot images.

secure cipher

To specify the ciphersuite in case of secure connection, use the **secure cipher**command in Lightweight Directory Access Protocol (LDAP) server configuration mode. To disable the secure connection, use the **no**form of this command.

secure cipher {**3des-ede-cbc-sha** | **des-cbc-sha** | **rc4-128-md5** | **rc4-128-sha** | **null-md5**} [**3des-ede-cbc-sha**] [**des-cbc-sha**] [**rc4-128-md5**] [**rc4-128-sha**] [**null-md5**]
no secure cipher {**3des-ede-cbc-sha** | **des-cbc-sha** | **rc4-128-md5** | **rc4-128-sha**} [**3des-ede-cbc-sha**] [**des-cbc-sha**] [**rc4-128-md5**] [**rc4-128-sha**] [**null-md5**]

Syntax Description

3des-ede-cbc-sha	Specifies the encryption null MD5 ciphersuite.
des-cbc-sha	Specifies encryption ssl_rsa_with_rc4_128_md5 ciphersuite.
rc4-128-md5	Specifies encryption ssl_rsa_with_rc4_128_md5 ciphersuite.
rc4-128-sha	Specifies encryption ssl_rsa_with_rc4_128_sha ciphersuite.
null-md5	Encryption null MD5 ciphersuite.

Command Default

If no ciphersuite is specified, all ciphersuites are considered.

Command Modes

LDAP server configuration (config-ldap-server)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Usage Guidelines

Note Security threats, as well as the cryptographic technologies to help protect against them, are constantly changing. For more information about the latest Cisco cryptographic recommendations, see the Next Generation Encryption (NGE) white paper.

A ciphersuite is a set of authentication, encryption, and data integrity algorithms used for exchanging messages between network nodes. During a Secure Socket Layer (SSL) handshake, for example, the two nodes negotiate to see which cipher uite they will use when transmitting messages back and forth.

The **secure cipher** command specifies the crypto methods supported by the Lightweight Directory Access Protocol (LDAP) client in Cisco IOS software. This command is applicable only when the **mode secure** command is enabled.

Examples

The following example shows how to configure the crypto methods that are supported by LDAP in Cisco IOS software:

```
Router(config)# ldap server server1
Router(config-ldap-server)# secure cipher des-cbc-sha
```

Related Commands

Command	Description
ldap server	Defines an LDAP server and enters LDAP server configuration mode.
mode secure	Enables the security mode in LDAP server.

security (Diameter peer)

To configure the security protocol for the Diameter peer connection, use the **security** command in Diameter peer configuration mode. To disable the configured protocol, use the **no** form of this command.

security {**ipsec** | **tls**}
no security {**ipsec** | **tls**}

Syntax Description

ipsec	IP security protocol.
tls	Transport layer security.

Command Default

IP security (IPsec) is the default security protocol for Diameter peer connections.

Command Modes

Diameter peer configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

If you dynamically change the security protocol for a Diameter peer, the connection to that peer is broken. When you exit the Diameter peer configuration submode, the connection is reestablished.

Examples

The following example shows how to configure IPsec for a Diameter peer:

```
Router (config-dia-peer)# security ipsec
```

Related Commands

Command	Description
diameter peer	Configures a Diameter peer and enters Diameter peer configuration submode.
show diameter peer	Displays the Diameter peer configuration.

security authentication failure rate

To configure the number of allowable unsuccessful login attempts, use the **security authentication failure rate**command in global configuration mode. To disable this functionality, use the **no** form of this command.

security authentication failure rate *threshold-rate* **log**
no security authentication failure rate *threshold-rate* **log**

Syntax Description

threshold-rate	Number of allowable unsuccessful login attempts. The valid value range for the *threshold-rate* argument is 2 to 1024. The default is 10.
log	Syslog authentication failures if the rate exceeds the threshold.

Command Default

The default number of failed login attempts before a 15-second delay is 10.

Command Modes

Global configuration

Command History

Release	Modification
12.3(1)	This command was introduced.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.3(7)T	The range of the *threshold-rate* value was changed from 1 through 1024 to 2 through 1024.

Usage Guidelines

The **security authentication failure rate** command provides enhanced security access to the router by generating syslog messages after the number of unsuccessful login attempts exceeds the configured threshold rate. This command ensures that there are not any continuous failures to access the router.

Note Previous to the Cisco IOS software release 12.3(7)T the *threshold-rate* value range was 1 through 1024. Unsuccessful login attempts will not be logged if a value of 1 is configured. As of Cisco ISO release 12.3(7)T, use a value between 2 and 1024.

Examples

The following example shows how to configure your router to generate a syslog message after eight failed login attempts:

```
security authentication failure rate 8 log
```

Related Commands

Command	Description
security passwords min-length	Ensures that all configured passwords are at least a specified length.

security ipsec

To apply a previously configured IP Security (IPSec) profile to the redundancy group communications, use the **security ipsec**command in inter-device configuration mode. To remove the IPSec profile from the configuration, use the **no** form of this command.

security ipsec *profile-name*
no security [**ipsec** [*profile-name*]]

Syntax Description

profile-name	Profile name, which was specified via the **crypto ipsec profile** command.

Command Default

The redundancy group is not secured.

Command Modes

Inter-device configuration

Command History

Release	Modification
12.3(11)T	This command was introduced.

Usage Guidelines

The **security ipsec**command allows you to secure a redundancy group via a previously configured IPSec profile. If you are certain that the Stateful Switchover (SSO) traffic between the redundancy group runs on a physically secure interface, you do not have to configure this command.

Note If you configure SSO traffic protection via the **security ipsec** command, the active and standby devices must be directly connected to each other via Ethernet networks.

Examples

The following example shows how to configure SSO traffic protection:

```
crypto ipsec transform-set trans2 ah-md5-hmac esp-aes
!
crypto ipsec profile sso-secure
 set transform-set trans2
!
redundancy inter-device
 scheme standby HA-in
 security ipsec sso-secure
```

Related Commands

Command	Description
crypto ipsec profile	Defines the IPSec parameters that are to be used for IPSec encryption between two IPSec routers.
redundancy inter-device	Enters inter-device configuration mode.

security passwords min-length

To ensure that all configured passwords are at least a specified length, use the **security passwords min-length** command in global configuration mode. To disable this functionality, use the **no** form of this command.

security passwords min-length *length*
no security passwords min-length *length*

Syntax Description

length	Minimum length of a configured password. The default is six characters.

Command Default

The command is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(1)	This command was introduced.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.

Usage Guidelines

The **security passwords min-length** command provides enhanced security access to the device by allowing you to specify a minimum password length, eliminating common passwords that are prevalent on most networks, such as “lab” and “cisco.” This command affects user passwords, enable passwords and secrets, and line passwords. After this command is enabled, any password that is less than the specified length will not work.

Examples

The following example shows both how to specify a minimum password length of six characters and what happens when the password does not adhere to the minimum length:

```
security passwords min-length 6
enable password lab
% Password too short - must be at least 6 characters. Password not configured.
```

Related Commands

Command	Description
enable password	Sets a local password to control access to various privilege levels.
security authentication failure rate	Configures the number of allowable unsuccessful login attempts.

security-group

To specify the membership of security group for an object group, use the **security-group** command in object-group identity configuration mode. To remove the security group identification number from the object group, use the **no** form of this command.

security-group tag-id *number*
no security-group tag-id *number*

Syntax Description

tag-id *number*	Specifies the Security Group Tag (SGT) identification number from 1 to 65535.

Command Default

No security group SGT identification number is defined.

Command Modes

Object-group identity configuration (config-object-group)

Command History

Release	Modification
15.2(1)S	This command was introduced in Cisco IOS Release 15.2(1)S.
Cisco IOS XE Release 3.5	This command was introduced in Cisco IOS XE Release 3.5.

Usage Guidelines

A security group can be specified for the object group with an SGT ID. The SGT ID is used by a Security Group Access (SGA) Zone-Based Policy firewall (ZBPF) to apply an enforcement policy by filtering on this SGT ID. The **security-group** command is used in the class map configuration of the SGA ZBPF. Multiple security groups can be specified using this command.

Note A policy map must also be configured for the SGA ZBPF.

Examples

The following example shows how the **security-group** command is used in the class map configuration of the SGA ZBPF.

```
Router(config)# object-group security myobject1
Router(config-object-group)# security-group tag-id 1
Router(config-object-group)# end
Router(config)# class-map type inspect match-any myclass1
Router(config-cmap)# match group-object security source myobject1
Router(config-cmap)# end
```

Related Commands

Command	Description
debug object-group event	Enables debug messages for object-group events.
group-object	Specifies a nested reference to a type of user group.
match group-object security	Matches traffic from a user in the security group.

Command	Description
object-group security	Creates an object group to identify traffic coming from a specific user or endpoint.
show object-group	Displays the content of all user groups.

self-identity

To define the identity that the local Internet Key Exchange (IKE) uses to identify itself to the remote peer, use the **self-identity**command in ISAKMP profile configuration mode. To remove the Internet Security Association and Key Management Protocol (ISAKMP) identity that was defined for the IKE, use the **no** form of this command.

```
self-identity {{address|address ipv6}|fqdn|user-fqdn user-fqdn}
no self-identity {{address | address ipv6} | fqdn | user-fqdn user-fqdn}
```

Syntax Description

address	The IP address of the local endpoint.
address ipv6	The IPv6 address of the local endpoint.
fqdn	The fully qualified domain name (FQDN) of the host.
user-fqdn *user-fqdn*	The user FQDNthat is sent to the remote endpoint.

Command Default

If no ISAKMP identity is defined in the ISAKMP profile configuration, global configuration is the default.

Command Modes

ISAKMP
profile configuration (config-isa-prof)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.4(4)T	The **address ipv6** keyword was added.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Examples

The following example shows that the IKE identity is the user FQDN "user@vpn.com":

```
crypto isakmp profile vpnprofile
 self-identity user-fqdn user@vpn.com
```

Related Commands

Command	Description
crypto isakmp profile	Defines an ISAKMP profile and audits IPSec user sessions.

serial-number (cs-server)

To specify whether the router serial number should be included in the certificate request, use the **serial-number** command in certificate server configuration mode. To restore the default behavior, use the **no** form of this command.

serial-number [**none**]
no serial-number

Syntax Description

none	(Optional) Specifies that a serial number is not included in the certificate request.

Command Default

Not configured. You are prompted for the serial number during certificate enrollment.

Command Modes

Certificate server configuration (cs-server)

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

You must configure the **crypto pki server** command with the name of the certificate server in order to enter certificate server configuration mode and configure this command.

Use this command to specify the router serial number in the certificate request, or use the **none** keyword to specify that a serial number should not be included in the certificate request.

Related Commands

Command	Description
auto-rollover	Enables the automated CA certificate rollover functionality.
cdp-url	Specifies a CDP to be used in certificates that are issued by the certificate server.
crl (cs-server)	Specifies the CRL PKI CS.
crypto pki server	Enables a CS and enters certificate server configuration mode, or immediately generates shadow CA credentials
database archive	Specifies the CA certificate and CA key archive format--and the password--to encrypt this CA certificate and CA key archive file.
database level	Controls what type of data is stored in the certificate enrollment database.

Command	Description
database url	Specifies the location where database entries for the CS is stored or published.
database username	Specifies the requirement of a username or password to be issued when accessing the primary database location.
default (cs-server)	Resets the value of the CS configuration command to its default.
grant auto rollover	Enables automatic granting of certificate reenrollment requests for a Cisco IOS subordinate CA server or RA mode CA.
grant auto trustpoint	Specifies the CA trustpoint of another vendor from which the Cisco IOS certificate server automatically grants certificate enrollment requests.
grant none	Specifies all certificate requests to be rejected.
grant ra-auto	Specifies that all enrollment requests from an RA be granted automatically.
hash (cs-server)	Specifies the cryptographic hash function the Cisco IOS certificate server uses to sign certificates issued by the CA.
issuer-name	Specifies the DN as the CA issuer name for the CS.
lifetime (cs-server)	Specifies the lifetime of the CA or a certificate.
mode ra	Enters the PKI server into RA certificate server mode.
mode sub-cs	Enters the PKI server into sub-certificate server mode
redundancy (cs-server)	Specifies that the active CS is synchronized to the standby CS.
show (cs-server)	Displays the PKI CS configuration.

Command	Description
shutdown (cs-server)	Allows a CS to be disabled without removing the configuration.

serial-number (ca-trustpoint)

To specify whether the router serial number should be included in the certificate request, use the **serial-number** command in ca-trustpoint configuration mode. To restore the default behavior, use the **no** form of this command.

serial-number [**none**]
no serial-number

Syntax Description

none	(Optional) Specifies that a serial number will not be included in the certificate request.

Command Default

Not configured. You will be prompted for the serial number during certificate enrollment.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.4(24)T	Support for IPv6 Secure Neighbor Discovery (SeND) command was introduced.

Usage Guidelines

Before you can issue the serial-number command, you must enable the **crypto ca trustpoint**command, which declares the certification authority (CA) that your router should use and enters ca-trustpoint configuration mode.

Use this command to specify the router serial number in the certificate request, or use the none keyword to specify that a serial number should not be included in the certificate request.

Examples

The following example shows how to omit a serial number from the "root" certificate request:

```
crypto ca trustpoint root
 enrollment url http://10.3.0.7:80
 ip-address none
 fqdn none
 serial-number none
 subject-name CN=jack, OU=PKI, O=Cisco Systems, C=US

crypto ca trustpoint root
 enrollment url http://10.3.0.7:80
 serial-number
```

Related Commands

Command	Description
crypto ca trustpoint	Declares the CA that your router should use.

serial-number (pubkey)

To define the serial number for the Rivest, Shamir, and Adelman (RSA) manual key to be used for encryption or signatures during Internet Key Exchange (IKE) authentication, use the **serial-number** command in pubkey configuration mode. To remove the manual key that was defined, use the **no** form of this command.

serial-number *serial-number*
no serial-number *serial-number*

Syntax Description

serial-number	Device serial number. The value is from 0 through infinity.

Command Default

No default behavior or values

Command Modes

Pubkey configuration (config-pubkey-key)

Command History

Release	Modification
12.2(15)T	This command was introduced.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Examples

The following example shows that the public key of an IP Security (IPSec) peer has been specified:

```
Router(config)# crypto keyring vpnkeyring
Router(conf-keyring)# rsa-pubkey name host.vpn.com
Router(config-pubkey-key)# address 10.5.5.1
Router(config-pubkey-key)# serial-number 1000000
Router(config-pubkey)# key-string
Router(config-pubkey)# 00302017 4A7D385B 1234EF29 335FC973
Router(config-pubkey)# 2DD50A37 C4F4B0FD 9DADE748 429618D5
Router(config-pubkey)# 18242BA3 2EDFBDD3 4296142A DDF7D3D8
Router(config-pubkey)# 08407685 2F2190A0 0B43F1BD 9A8A26DB
Router(config-pubkey)# 07953829 791FCDE9 A98420F0 6A82045B
Router(config-pubkey)# 90288A26 DBC64468 7789F76E EE21
Router(config-pubkey)# quit
Router(config-pubkey-key)# exit
Router(conf-keyring)# exit
```

Related Commands

Command	Description
address	Specifies the IP address of the remote RSA public key of the remote peer that you will manually configure.
key-string (IKE)	Specifies the RSA public key of a remote peer.

server (application firewall policy)

To configure a set of Domain Name System (DNS) servers for which the specified instant messenger application will be interacting, use the **server** command in the appropriate configuration mode. To change or remove a configured set of DNS servers, use the **no** form of this command.

server {**permit** | **deny**} {**name** *string* | **ip-address** {*ip-address* | **range** *ip-address-start ip-address-end*}}
no server {**permit** | **deny**} {**name** *string* | **ip-address** {*ip-address* | **range** *ip-address-start ip-address-end*}}

Syntax Description

permit	Inspects all traffic destined for a specified server, and the applicable policy is enforced.
deny	Blocks all traffic destined for a specified, denied server. TCP connections are denied by dropping all packets bound to the specified server.
name *string*	Name of DNS server for which traffic will be permitted (and inspected) or denied. The same server name cannot appear under two different instant messenger applications; however, the same name can appear under two different policies within the same instant messenger application. Each entry will accept only one DNS name.
ip-address	Indicates that at least one IP address will be listed.
ip-address	IP address of the DNS server for which traffic will be permitted (and inspected) or denied.
range *ip-address-start ip-address-end*	Range of DNS server IP addresses for which traffic will be permitted (and inspected) or denied.

Command Default

If this command is not issued, instant messenger application polices cannot be enforced.

Command Modes

cfg-appfw-policy-aim configuration

cfg-appfw-policy-ymsgr configuration

cfg-appfw-policy-msnmsgr configuration

Command History

Release	Modification
12.4(4)T	This command was introduced.

Usage Guidelines

The **server** command helps the instant messenger application engine to recognize the port-hopping instant messenger traffic and to enforce the security policy for that instant messenger application; thus, if this command is not issued, the security policy cannot be enforced if IM applications use port-hopping techniques.

To deploy IM traffic enforcement policies effectively, it is recommended that you issue the appropriate **server** command.

Note If a router cannot identify a packet as belonging to a particular instant messenger policy, the corresponding policy cannot be enforced.

To configure more than one set of servers, you can issue the **server** command multiple times within an instant messenger's application policy. Multiple entries are treated cumulatively.

The server name Command

The server command (with the **name** keyword) internally resolves the DNS name of the server. This command sends DNS queries multiple times to gather all possible IP addresses for the IM servers, which return different IP addresses at different times in response to DNS queries of the same names. It uses the Time to Live (TTL) field found in DNS responses to refresh its cache. After a certain period, the DNS cache in IM applications stabilize. It is recommended that you allow a couple of minutes for the DNS cache to populate with the IM server IP addresses before the IM traffic reaches the Cisco IOS firewall. All existing IM application connections are not subjected to IM policy enforcement.

Denying Access to a Particular Instant Messenger Application

You can deny traffic to a particular instant messenger application in one of the following ways:

- Issue the **server deny** command and list all the server names and IP addresses to which you want to deny access.

Note The first option is the preferred method because it performs slightly better than the second option.

- Issue the **server permit** command and list all the server names and IP addresses that you want inspected; thereafter, issue the **service default reset**command, which will deny access to all services.
- Issue **server deny** command to block access to any site given its DNS name. For example, to block all access to a gambling site, you can configure **server deny name www.noaccess.com**.

Examples

The following example shows to configure application policy "my-im-policy," which allows text-chat for Yahoo! instant messenger users and blocks instant messenger traffic for all other users:

```
appfw policy-name my-im-policy
 application http
  port-misuse im reset
!
 application im yahoo
  server permit name scs.msg.yahoo.com
  server permit name scsa.msg.yahoo.com
  server permit name scsb.msg.yahoo.com
  server permit name scsc.msg.yahoo.com
  service text-chat action allow
  service default action reset
!
 application im aol
  server deny name login.cat.aol.com
!
```

```
 application im msn
  server deny name messenger.hotmail.com
!
ip inspect name test appfw my-im-policy
interface FastEthernet0/0
 description Inside interface
 ip inspect test in
```

Related Commands

Command	Description
service	Specifies an action when a specific service is detected in the instant messenger traffic.

server (CWS)

To configure the Cloud Web Security server for content scanning, use the **server** command in parameter-map type inspect configuration mode. To disable content scanning on the Cloud Web Security server, use the **no** form of this command.

server {**on-failure** {**allow-all** | **block-all**} | {**primary** | **secondary**} {**ipv4** *ip-address* | **name** *domain-name*} **port http** *port-number* **https** *port-number*}
no server {**primary** | **secondary**} {**ipv4** *ip-address* | **name** *domain-name*} **port http** *port-number* **https** *port-number*

Syntax Description

on-failure	Specifies that there is a communication failure with Cloud Web Security server.
allow-all	Allows traffic to flow directly to the Cloud Web Security web server.
block-all	Blocks the traffic to the Cloud Web Security web server.
primary	Specifies the primary Cloud Web Security server.
secondary	Specifies the secondary Cloud Web Security server.
ipv4 *ip-address*	Specifies the IPv4 address of the Cloud Web Security server.
name *domain-name*	Specifies the domain name of the Cloud Web Security server.
port	Specifies the listening port number.
http *port-number*	Specifies the HTTP port and port number. Valid values for the *port-number* argument are from 1 to 65535.
https *port-number*	Specifies the secure HTTP (HTTPS) port and port number. Valid values for the *port-number* argument are from 1 to 65535.

Command Default

The Cloud Web Security server is not configured for content scanning.

Command Modes

Parameter-map type inspect configuration (config-profile)

Command History

Release	Modification
15.4(2)T	This command was introduced. This command replaces the **server scansafe** command.

Usage Guidelines

Use the **server** command to configure different ports for HTTP and secure HTTP (HTTPS). However, the default port for the proxied HTTP and HTTPS traffic is 8080 for Cloud Web Security. In case the name or the IP address of the Cloud Web Security server is not configured correctly, the default web page from the configured server will be sent for all the web requests from the endpoints.

If both the primary and secondary Cloud Web Security servers are unreachable, the traffic is dropped if you have configured the **server on-failure block-all** command or, if you have configured the **server on-failure allow-all** command, the traffic is allowed to the actual web server without redirecting.

Examples

The following example shows how to configure the Cloud Web Security server for content scanning:

```
Device(config)# parameter-map type cws global
Device(config-profile)# server primary ipv4 10.1.1.1 port http 81 https 101
```

Related Commands

Command	Description
parameter-map type cws global	Configures a global Cloud Web Security parameter map and enters parameter-map type inspect configuration mode.

server_(Diameter)

To associate a Diameter server with a Diameter authentication, authorization, and accounting (AAA) server group, use the **server** command in Diameter server group configuration submode. To remove a server from the server group, enter the **no** form of this command.

server *name*
no server *name*

Syntax Description

name	Character string used to name the Diameter server. **Note** The name specified for this command should match the name of a Diameter peer defined using the **diameter peer** command.

Command Default

No server is associated with a Diameter AAA server group.

Command Modes

Diameter server group configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

The **server** command allows you to associate a Diameter server with a Diameter server group.

Examples

The following example shows how to associate a Diameter server with a Diameter server group:

```
Router (config-sg-diameter)# server
 dia_peer_1
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes.
aaa authentication login	Set AAA authentication at login.
aaa authorization	Sets parameters that restrict user access to a network.
aaa group server diameter	Configures a server group for Diameter.

server (ldap)

To associate a particular Lightweight Directory Access Protocol (LDAP) server with a AAA server group, use the **server** command in LDAP server group configuration mode. To delete a server name from the LDAP server, use the **no** form of this command.

server *name*
no server *name*

Syntax Description

name	LDAP server name.

Command Default

No server name is configured in the LDAP server.

Command Modes

LDAP server group configuration (config-ldap-server)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Examples

The following example shows how to associate an LDAP server named server1 with a AAA server group:

```
Router(config)# aaa group server ldap name1
Router(config-ldap-sg)# server server1
```

Related Commands

Command	Description
ldap server	Defines an LDAP server and enters LDAP server configuration mode.

server (parameter-map)

To configure a set of Domain Name System (DNS) servers with which a given instant messenger application interacts, use the **server** command in parameter-map configuration mode. To disable the configuration, use the **no** form of this command.

server {**name** *string* [**snoop**] | **ip** {*ip-address* | **range** *ip-address-start ip-address-end*}}
no server {**name** *string* [**snoop**] | **ip** {*ip-address* | **range** *ip-address-start ip-address-end*}}

Syntax Description

name *string*	Specifies the name of the DNS server for which traffic will be permitted (and inspected) or denied.
snoop	(Optional) Enables DNS snooping.
ip	Indicates that at least one IP address will be listed.
ip-address	IP address of the DNS server for which traffic will be permitted (and inspected) or denied. **Note** You cannot configure network addresses that are reserved for special purposes as the server IP address. For example, IP addresses such as 0.0.0.0, 127.0.0.0, and 127.0.0.1 cannot be configured as the server IP address.
range *ip-address-start ip-address-end*	Specifies the range of DNS server IP addresses for which traffic will be permitted (and inspected) or denied.

Command Default

At least one server instance should be configured for the configured instant messenger policy to be enforced; otherwise, the parameter map will not have any definitions to enforce.

Command Modes

Parameter-map configuration (config-profile)

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.4(20)T	This command was modified. The **snoop** keyword was added. Support for the I Seek You (ICQ) and Windows Messenger IM Protocols was added.

Usage Guidelines

The **server** command helps the instant messenger application engine to recognize traffic from an instant messenger and to enforce the configured policy for that instant messenger application.

Before you can issue the **server** command, you must issue the **parameter-map type** command, which allows you to specify parameters that control the behavior of actions and match criteria specified under a policy map and a class map, respectively.

Note To enable name resolution, you must also enable the **ip domain name** and **ip name-server** commands.

To configure more than one set of servers, you can configure the **server** command multiple times within an instant messenger's parameter map. Multiple entries are treated cumulatively.

DNS Snooping

In Cisco IOS Release 12.4(20)T, users can enable DNS snooping on an access router to easily obtain address names. When DNS snooping is enabled, the Cisco IOS firewall that is running on the access router can "snoop" the DNS responses that are going through the router. The firewall can obtain the necessary addresses from the DNS responses because the DNS inspection engine decodes the DNS response packets and returns a list of addresses to the address database.

When using DNS snooping, network administrators no longer have to give a complete address, such as abcd.example1.example.com; instead, they can specify a partial address with a "wildcard character," such as *.example1.example.com.

Examples

The following example shows how to configure an IM-based firewall policy. In this example, all Yahoo Messenger and AOL traffic is allowed to pass through, while all MSN Messenger traffic is blocked. Also, parameter maps are defined to control all Yahoo Messenger and AOL traffic on a more granular level.

```
! Define Layer 7 class-maps.
class-map type inspect ymsgr match-any l7-cmap-ymsgr
 match service text-chat
!
class-map type inspect aol match-any l7-cmap-aol
 match service text-chat
 match service any
!
! Define Layer 7 policy-maps.
policy-map type inspect im l7-pmap-ymsgr
 class-type inspect ymsgr l7-cmap-ymsgr
  allow
  alarm
!
!
policy-map type inspect im l7-pmap-aol
 class-type inspect aol l7-cmap-aol
  allow
  alarm
!
!
! Define parameter map.
parameter-map type protocol-info ymsgr
 server name sdsc.msg.yahoo.com
 server ip 10.1.1.1
!
parameter-map type protocol-info aol
 server name sdsc.msg.aol.com
 server ip 172.16.1.1.
```

The following example shows how to configure an access router to block ICQ and Yahoo IM applications while allowing only text chat with Windows Messenger. In this example, snooping is enabled to obtain addressess for all IM applications.

```
! Define the servers for ICQ.
parameter-map type protocol-info icq-servers
 server name *.icq.com snoop
 server name oam-d09a.blue.aol.com
! Define the servers for Windows Messenger.
```

```
parameter-map type protocol-info winmsgr-servers
 server name messenger.msn.com snoop

! Define servers for yahoo.
parameter-map type protocol-info yahoo-servers
 server name scs*.msg.yahoo.com snoop
 server name c*.msg.yahoo.com snoop

! Define class-map to match ICQ traffic.
class-map type inspect icq-traffic
 match protocol icq icq-servers

! Define class-map to match windows Messenger traffic.
class-map type inspect winmsgr-traffic
 match protocol winmsgr winmsgr-servers
!

! Define class-map to match text-chat for windows messenger.
class-map type inspect winmsgr winmsgr-textchat
 match service text-chat
!

Define class-map to match default service
class-map type inspect winmsgr winmsgr-defaultservice
 match service any
!

! Define a Layer 7 IM policy-map to permit text-chat and block everything else.
policy-map type inspect im im-policy
 class type inspect winmsgr winmsgr-textchat
  allow
  !
 class type inspect winmsgr winmsgr-defaultservice
  reset
  !
!

! Define the Layer 4 policy to block ICQ and Yahoo Messenger and allow yahoo text-chat !
with Windows Messenger
policy-map type inspect firewall-policy
 class type inspect winmsgr-traffic
  inspect
  service-policy type inspect im im-policy
  !
 class type inspect icq-traffic
  drop
  !
 class type inspect yahoo-traffic
  drop
```

Related Commands

Command	Description
ip domain lookup	Enables the IP DNS-based hostname-to-address translation.
ip domain name	Defines a default domain name that the Cisco IOS software uses to complete unqualified hostnames (names without a dotted-decimal domain name).
ip name-server	Specifies the address of one or more name servers to be used for name and address resolution.
parameter-map type	Creates or modifies a parameter map.

server (RADIUS)

To configure the IP address of the RADIUS server for the group server, use the **server**command in server-group configuration mode. To remove the associated server from the authentication, authorization, and accounting (AAA) group server, use the **no** form of this command.

server *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*]
no server *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*]

Syntax Description

ip-address	IP address of the RADIUS server host.
auth-port *port-number*	(Optional) Specifies the User Datagram Protocol (UDP) destination port for authentication requests. The port-number argument specifies the port number for authentication requests. The host is not used for authentication if this value is set to 0.
acct-port *port-number*	(Optional) Specifies the UDP destination port for accounting requests. The port number argument specifies the port number for accounting requests. The host is not used for accounting services if this value is set to 0.

Command Default

If no port attributes are defined, the defaults are as follows:

- Authentication port: 1645
- Accounting port: 1646

Command Modes

Server-group configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(7)T	The following new keywords/arguments were added: • **auth-port** *port-number* • **acct-port** *port-number*
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **server** command to associate a particular server with a defined group server. There are two different ways in which you can identify a server, depending on the way you want to offer AAA services. You can identify the server simply by using its IP address, or you can identify multiple host instances or entries using the optional **auth-port** and **acct-port** keywords.

When you use the optional keywords, the network access server identifies RADIUS security servers and host instances associated with a group server on the basis of their IP address and specific UDP port numbers. The combination of the IP address and UDP port number creates a unique identifier, allowing different ports to be individually defined as RADIUS host entries providing a specific AAA service. If two different host entries on the same RADIUS server are configured for the same service--for example, accounting--the second host entry configured acts as failover backup to the first one. Using this example, if the first host entry fails to provide accounting services, the network access server will try the second host entry configured on the same device for accounting services. (The RADIUS host entries will be tried in the order they are configured.)

Examples

Configuring Multiple Entries for the Same Server IP Address

The following example shows the network access server configured to recognize several RADIUS host entries with the same IP address. Two different host entries on the same RADIUS server are configured for the same services--authentication and accounting. The second host entry configured acts as fail-over backup to the first one. (The RADIUS host entries are tried in the order in which they are configured.)

```
! This command enables AAA.
aaa new-model
! The next command configures default RADIUS parameters.
aaa authentication ppp default radius
! The next set of commands configures multiple host entries for the same IP address.
radius-server host 172.20.0.1 auth-port 1000 acct-port 1001
radius-server host 172.20.0.1 auth-port 2000 acct-port 2000
```

Configuring Multiple Entries Using AAA Group Servers

In this example, the network access server is configured to recognize two different RADIUS group servers. One of these groups, group1, has two different host entries on the same RADIUS server configured for the same services. The second host entry configured acts as failover backup to the first one.

```
! This command enables AAA.
aaa new-model
! The next command configures default RADIUS parameters.
aaa authentication ppp default group group1
! The following commands define the group1 RADIUS group server and associates servers
! with it.
aaa group server radius group1
   server 172.20.0.1 auth-port 1000 acct-port 1001
! The following commands define the group2 RADIUS group server and associates servers
! with it.
aaa group server radius group2
   server 172.20.0.1 auth-port 2000 acct-port 2001
! The following set of commands configures the RADIUS attributes for each host entry
! associated with one of the defined group servers.
radius-server host 172.20.0.1 auth-port 1000 acct-port 1001
radius-server host 172.20.0.1 auth-port 1000 acct-port 1001
radius-server host 172.31.0.1 auth-port 1645 acct-port 1646
```

Related Commands

Command	Description
aaa group server	Groups different server hosts into distinct lists and distinct methods.

Command	Description
aaa new-mode l	Enables the AAA access control model.
radius-server host	Specifies a RADIUS server host.

server (TACACS+)

To configure the IP address of the TACACS+ server for the group server, use the **server** command in TACACS+ group server configuration mode. To remove the IP address of the RADIUS server, use the **no** form of this command.

server *ip-address*
no server *ip-address*

Syntax Description

ip-address	IP address of the selected server.

Command Default

No default behavior or values.

Command Modes

TACACS+ group server configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

You must configure the aaa group server tacacs command before configuring this command.

Enter the **server** command to specify the IP address of the TACACS+ server. Also configure a matching **tacacs-server host** entry in the global list. If there is no response from the first host entry, the next host entry is tried.

Examples

The following example shows server host entries configured for the RADIUS server:

```
aaa new-model
aaa authentication ppp default group g1
aaa group server tacacs+ g1
 server 10.0.0.1
 server 10.2.0.1
tacacs-server host 10.0.0.1
tacacs-server host 10.2.0.1
```

Related Commands

Command	Description
aaa new-model	Enables the AAA access control model.
aaa server group	Groups different server hosts into distinct lists and distinct methods.
tacacs-server host	Specifies a RADIUS server host.

server address ipv4

To specify the address of the server that a Group Domain of Interpretation (GDOI) group is trying to reach, use the **server address ipv4** command in GDOI group configuration mode. To disable the address, use the **no** form of this command.

server address ipv4 {*addresshostname*}
no server address ipv4 {*addresshostname*}

Syntax Description

address	IP address of the server.
hostname	Hostname of the server.

Command Default

None

Command Modes

GDOI group configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

The **server address ipv4** command can be used only on a group member. This command must be specified or the group configuration on the group member is not complete.

Examples

The following example shows that the GDOI group is trying to reach the server with the IP address "10.34.255.57":

```
server address ipv4 10.34.255.57
```

Related Commands

Command	Description
crypto gdoi group	Identifies a GDOI group and enters GDOI group configuration mode.
server local	Designates a device as a GDOI key server and enters GDOI local server configuration mode.

server ip

To add a server to an Intelligent Services Gateway (ISG) Layer 4 redirect server group, use the **server ip** command in Layer 4 redirect server group configuration mode. To remove a server from a redirect server group, use the **no** form of this command.

server ip *ip-address* [**port** *port*]
no server ip *ip-address* [**port** *port*]

Syntax Description

ip *ip-address*	IP address of the server to be added to the redirect server group.
port *port*	(Optional) TCP port of the server to be added to the redirect server group.

Command Default

A server is not added to the redirect server group.

Command Modes

Layer 4 redirect server group configuration

Command History

Release	Modification
12.2(28)SB	This command was introduced.
Cisco IOS XE Release 3.5S	This command was modified. The *ip-address* argument accepts IPv6 addresses.

Usage Guidelines

Use the **server ip** command in Layer 4 redirect server group configuration mode to add a server, defined by its IP address and TCP port, to a redirect server group. The **server ip** command can be entered more than once to add multiple servers to the server group.

ISG Layer 4 redirection provides nonauthorized users with access to controlled services. Packets sent upstream from an unauthenticated user are forwarded to the server group, which deals with the packets in a suitable manner, such as routing them to a logon page. You can also use captive portals to handle requests from authorized users who request access to services to which they are not logged in.

Examples

The following example adds a server at IP address 10.0.0.0 and TCP port 8080 and a server at IP address 10.1.2.3 and TCP port 8081 to a redirect server group named “ADVT-SERVER”:

```
redirect server-group ADVT-SERVER
 server ip 10.0.0.0 port 8080
 server ip 10.1.2.3 port 8081
```

Related Commands

Command	Description
redirect server-group	Defines a group of one or more servers that make up a named ISG Layer 4 redirect server group.
redirect to (ISG)	Redirects ISG Layer 4 traffic to a specified server or server group.
show redirect group	Displays information about ISG Layer 4 redirect server groups.

Command	Description
show redirect translations	Displays information about the ISG Layer 4 redirect mappings for subscriber sessions.

server local

To designate a device as a Group Domain of Interpretation (GDOI) key server and enter GDOI local server configuration mode, use the **server local** command in GDOI group configuration mode. To remove a device as a key server, use the **no** form of this command.

server local
no server local

Syntax Description

This command has no arguments or keywords.

Command Default

A device is not designated as a GDOI key server.

Command Modes

GDOI group configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

This command is used on the key server to specify the key server policy that will be downloaded to the group members that are registered with the key server.

Examples

The following example shows that the device has been designated as a GDOI key server:

```
server local
```

Related Commands

Command	Description
crypto gdoi group	Identifies a GDOI group and enters GDOI group configuration mode.

server name (IPv6 TACACS+)

To specify an IPv6 TACACS+ server, use the **server name**command in TACACS+ group server configuration mode. To remove the IPv6 TACACS+ server from configuration, use the **no** form of this command.

server name *server-name*
no server name *server-name*

Syntax Description

server-name	The IPv6 TACACS+ server to be used.

Command Default

No server name is specified.

Command Modes

TACACS+ group server configuration (config-sg-tacacs+)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.

Usage Guidelines

You must configure the **aaa group server tacacs** command before configuring this command.

Enter the **server name** command to specify an IPv6 TACACS+ server.

Examples

The following example shows how to specify an IPv6 TACACS+ server named server1:

```
Router(config)# aaa group server tacacs+
Router(config-sg-tacacs+)# server name server1
```

Related Commands

Command	Description
aaa group server tacacs	Configures the TACACS+ server for IPv6 or IPv4 and enters TACACS+ server configuration mode.

server scansafe

Note Effective with Cisco IOS Release 15.4(2)T, the **server scansafe** command is replaced by the **server (CWS)** command. See the **server (CWS)** command for more information.

To configure the Cloud Web Security server for content scanning, use the **server scansafe** command in parameter-map type inspect configuration mode. To disable the Cloud Web Security server for content scanning, use the **no** form of this command.

server scansafe {**on-failure** {**allow-all** | **block-all**} | {**primary** | **secondary**} {**ipv4** *ip-address* | **name** *domain-name*} **port http** *port-number* **https** *port-number*}
no server scansafe {**primary** | **secondary**} {**ipv4** *ip-address* | **name** *domain-name*} **port http** *port-number* **https** *port-number*

Syntax Description

on-failure	Specifies that there is a communication failure with ScanSafe.
allow-all	Allows traffic to flow directly to the web server.
block-all	Blocks the traffic to the web server.
primary	Specifies the primary security as a service (SaaS) server.
secondary	Specifies the secondary SaaS server.
ipv4 *ip-address*	Specifies the IPv4 address of the server.
name *domain-name*	Specifies the domain name of the server.
port	Specifies the SaaS listening port number.
http *port-number*	Specifies the HTTP port and port number. Valid values for the *port-number* argument are from 1 to 65535.
https *port-number*	Specifies the secure HTTP (HTTPS) port and port number. Valid values for the *port-number* argument are from 1 to 65535.

Command Default

The Cloud Web Security server is not configured for content scanning.

Command Modes

Parameter-map type inspect configuration (config-profile)

Command History

Release	Modification
15.2(1)T1	This command was introduced.
15.4(2)T	This command was replaced by the **server (CWS)** command.

Usage Guidelines

Use the **server scansafe** command to configure different ports for HTTP and secure HTTP (HTTPS). However, the default port for the proxied HTTP and HTTPS traffic is 8080 for Cloud Web Security. In case the name

or the IP address of the Cloud Web Security server is not configured correctly, the default web page from the configured server will be sent for all the web requests from the endpoints.

If both the primary and secondary towers are unreachable, the traffic is dropped if you have configured the **server scansafe on-failure block-all** command or, if you have configured the **server scansafe on-failure allow-all** command, the traffic is allowed to the actual web server without redirecting.

Examples

The following example shows how to configure the Cloud Web Security server for content scanning:

```
Device(config)# parameter-map type content-scan global
Device(config-profile)# server scan-safe primary ipv4 10.1.1.1 port http 81 https 101
```

Related Commands

Command	Description
parameter-map type content-scan global	Configures a global content-scan parameter map and enters parameter-map type inspect configuration mode.

server vendor

To specify the URL filtering server, use the **server vendor** command in URL parameter-map configuration mode. To remove a server from the configuration, use the **no** form of this command.

server vendor {**n2h2** | **websense**} {*ip-addresshostname*} [**outside**] [**port** *port-number*] [**retrans** *retransmission-count*] [**timeout** *seconds*]
no server vendor {**n2h2** | **websense**} {*ip-addresshostname*} [**outside**] [**port** *port-number*] [**retrans** *retransmission-count*] [**timeout** *seconds*]

Syntax Description

n2h2	Specifies the N2H2 server.
websense	Specifies the Websense server.
ip-address	IP address of the URL filtering server that you want to configure.
hostname	Hostname of the URL filtering server that you want to configure.
outside	(Optional) Specifies that the vendor server is on the outside network.
port *port-number*	(Optional) Specifies the port number on which the vendor server listens. The range is from 1 to 65535. The default port for the Websense vendor is 15868 and the N2H2 vendor is 4005.
retrans *retransmission-count*	(Optional) Specifies the number of times the Cisco IOS firewall will retransmit the request when a response does not arrive for the request. The range is from 1 to 10. The default value is 2.
timeout *seconds*	(Optional) Specifies the length of time, in seconds, that the Cisco IOS firewall will wait for a response from the vendor server. The range is from 1 to 300. The default value is 6.

Command Default

No URL filtering is performed.

Command Modes

URL parameter-map configuration (config-profile)

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

Use the **server vendor** command to specify the URL filtering server. If there is no server, there can be no URL filtering.

When you are creating a URL filter parameter map, you can use the **server vendor** command after entering the **parameter-map type urlfilter** command. For more detailed information about creating a parameter map, see the **parameter-map type urlfilter** command.

Use the **server vendor** command to configure a Websense or N2H2 server, which will interact with the Cisco IOS firewall to filter HTTP requests on the basis of a specified policy--global filtering, user- or group-based filtering, keyword-based filtering, category-based filtering, or customized filtering.

If the firewall has not received a response from the vendor server within the time specified in the **timeout** *seconds* keyword and argument, the firewall checks the **retrans** *retransmission-count* keyword and argument configured for the vendor server. If the firewall has not exceeded the maximum retransmit tries allowed, it resends the HTTP lookup request. If the firewall has exceeded the maximum retransmit tries allowed, it deletes the outstanding request from the queue and checks the value specified in the **allow-mode** command. The firewall forwards the request if the allow mode is on; otherwise, it drops the request.

By default, URL lookup requests that are made to the vendor server contain nonnatted client IP addresses because the vendor server is deployed on the inside network. The **outside** keyword allows the vendor server to be deployed on the outside network. Cisco IOS software sends, in the URL lookup request, the client's IP address that has undergone network address translation (NAT).

Primary and Secondary Servers

When you configure multiple vendor servers, the Cisco IOS firewall uses only one server at a time--the primary server; all other servers are called secondary servers. When the primary server becomes unavailable for any reason, it becomes a secondary server and one of the secondary servers becomes the primary server.

A firewall marks a primary server as down when sending a request to or receiving a response from the server fails. When a primary server goes down, the system goes to the beginning of the configured servers list and tries to activate the first server on the list. If the first server on the list is unavailable, it tries the second server on the list; the system keeps trying to activate a server until it is successful or until it reaches the end of the server list. If the system reaches the end of the server list, it sets a flag indicating that all of the servers are down, and it enters allow mode. When allow mode is on, HTTP traffic is permitted.

Examples

The following example shows how to specify the N2H2 vendor server for URL filtering:

```
parameter-map type urlfilter u1
 server vendor n2h2 10.193.64.22 port 3128 outside
```

Related Commands

Command	Description
allow-mode	Turns the default mode of the filtering algorithm on or off.
ip urlfilter server vendor	Configures a vendor server for URL filtering.
max-request	Specifies the maximum number of outstanding requests that can exist at any given time.
parameter-map type urlfilter	Creates a parameter map that will hold parameters pertaining to the URL filter.

server-private (RADIUS)

To configure the IP address of the private RADIUS server for the group server, use the **server-private** command in RADIUS server-group configuration mode. To remove the associated private server from the authentication, authorization, and accounting (AAA) group server, use the **no** form of this command.

server-private *ip-address* [{**auth-port** *port-number* | **acct-port** *port-number*}] [**non-standard**] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]
no server-private *ip-address* [{**auth-port** *port-number* | **acct-port** *port-number*}] [**non-standard**] [**timeout** *seconds*] [**retransmit** *retries*] [**key** *string*]

Syntax Description

ip-address	IP address of the private RADIUS server host.
auth-port *port-number*	(Optional) User Datagram Protocol (UDP) destination port for authentication requests. The default value is 1645.
acct-port *port-number*	Optional) UDP destination port for accounting requests. The default value is 1646.
non-standard	(Optional) RADIUS server is using vendor-proprietary RADIUS attributes.
timeout *seconds*	(Optional) Time interval (in seconds) that the router waits for the RADIUS server to reply before retransmitting. This setting overrides the global value of the **radius-server timeout** command. If no timeout value is specified, the global value is used.
retransmit *retries*	(Optional) Number of times a RADIUS request is resent to a server, if that server is not responding or responding slowly. This setting overrides the global setting of the **radius-server retransmit** command.
key *string*	(Optional) Authentication and encryption key used between the router and the RADIUS daemon running on the RADIUS server. This key overrides the global setting of the **radius-server key** command. If no key string is specified, the global value is used. The *string* can be **0** (specifies that an unencrypted key follows), **6** (specifies that an advanced encryption scheme [AES] encrypted key follows), **7** (specifies that a hidden key follows), or a line specifying the unencrypted (clear-text) server key.

Command Default

If server-private parameters are not specified, global configurations will be used; if global configurations are not specified, default values will be used.

Command Modes

RADIUS server-group configuration (config-sg-radius)

Command History

Release	Modification
12.2(1)DX	This command was introduced on the Cisco 7200 series and Cisco 7401ASR.
12.2(2)DD	This command was integrated into Cisco IOS Release 12.2(2)DD.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.

Release	Modification
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
15.4(1)T	This command was modified. The **6** keyword was added.

Usage Guidelines

Use the **server-private** command to associate a particular private server with a defined server group. To prevent possible overlapping of private addresses between virtual route forwarding (VRF) instances, private servers (servers with private addresses) can be defined within the server group and remain hidden from other groups, while the servers in the global pool (default "radius" server group) can still be referred to by IP addresses and port numbers. Thus, the list of servers in server groups includes references to the hosts in the global configuration and the definitions of private servers.

Note If the **radius-server directed-request** command is configured, then a private RADIUS server cannot be used as the group server by configuring the **server-private** (RADIUS) command.

Use the **password encryption aes** command to configure type 6 AES encrypted keys.

Examples

The following example shows how to define the sg_water RADIUS group server and associate private servers with it:

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa group server radius sg_water
Device(config-sg-radius)# server-private 10.1.1.1 timeout 5 retransmit 3 key xyz
Device(config-sg-radius)# server-private 10.2.2.2 timeout 5 retransmit 3 key xyz
```

Related Commands

Command	Description
aaa group server	Groups different server hosts into distinct lists and distinct methods.
aaa new-model	Enables the AAA access control model.
password encryption aes	Enables a type 6 encrypted preshared key.
radius-server host	Specifies a RADIUS server host.
radius-server directed-request	Allows users to log in to a Cisco NAS and select a RADIUS server for authentication.

server-private (TACACS+)

To configure the IPv4 or IPv6 address of the private TACACS+ server for the group server, use the **server-private** command in TACACS+ server-group configuration mode. To remove the associated private server from the authentication, authorization, and accounting (AAA) group server, use the **no** form of this command.

server-private {*ip-address name ipv6-address*} [**nat**] [**single-connection**] [**port** *port-number*] [**timeout** *seconds*] [**key** [{**0** | **6** | **7**}] *string*]
no server-private

Syntax Description

ip-address	IP address of the private RADIUS or TACACS+ server host.
name	Name of the private RADIUS or TACACS+ server host.
ipv6-address	IPv6 address of the private RADIUS or TACACS+ server host.
nat	(Optional) Specifies the port Network Address Translation (NAT) address of the remote device. This address is sent to the TACACS+ server.
single-connection	(Optional) Maintains a single open connection between the router and the TACACS+ server.
port *port-number*	(Optional) Specifies a server port number. This option overrides the default, which is port 49.
timeout *seconds*	(Optional) Specifies a timeout value. This value overrides the global timeout value set with the **tacacs-server timeout** command for this server only.
key [**0** | **6** | **7**]	(Optional) Specifies an authentication and encryption key. This key must match the key used by the TACACS+ daemon. Specifying this key overrides the key set by the global **tacacs-server key** command for this server only. • If no number or 0 is entered, the string that is entered is considered to be plain text. If 6 is entered, the string that is entered is considered to be an advanced encryption scheme [AES] encrypted text. If 7 is entered, the string that is entered is considered to be hidden text.
string	(Optional) Character string specifying the authentication and encryption key.

Command Default

If server-private parameters are not specified, global configurations are used; if global configurations are not specified, default values are used.

Command Modes

TACACS+ server-group configuration (config-sg-tacacs+)

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(33)SRA1	This command was integrated into Cisco IOS Release 12.2(33)SRA1.

Release	Modification
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
12.2(54)SG	This command was integrated into Cisco IOS Release 12.2(54)SG.
Cisco IOS XE Release 3.2S	This command was modified. The *ipv6-address* argument was added.
15.4(1)T	This command was modified. The **6** keyword was added.

Usage Guidelines

Use the **server-private** command to associate a particular private server with a defined server group. To prevent possible overlapping of private addresses between virtual route forwardings (VRFs), private servers (servers with private addresses) can be defined within the server group and remain hidden from other groups, while the servers in the global pool (default "TACACS+" server group) can still be referred to by IP addresses and port numbers. Thus, the list of servers in server groups includes references to the hosts in the global configuration and the definitions of private servers.

Use the **password encryption aes** command to configure type 6 AES encrypted keys.

Examples

The following example shows how to define the tacacs1 TACACS+ group server and associate private servers with it:

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa group server tacacs+ tacacs1
Device(config-sg-tacacs+)# server-private 10.1.1.1 port 19 key cisco
Device(config-sg-tacacs+)# exit
Device(config)# ip vrf cisco
Device(config-vrf)# rd 100:1
Device(config-vrf)# exit
Device(config)# interface Loopback0
Device(config-if)# ip address 10.0.0.2 255.0.0.0
Device(config-if)# ip vrf forwarding cisco
Device(config-if)# exit
```

Related Commands

Command	Description
aaa group server	Groups different server hosts into distinct lists and distinct methods.
aaa new-model	Enables the AAA access control model.
ip tacacs source-interface	Uses the IP address of a specified interface for all outgoing TACACS+ packets.
ip vrf forwarding (server-group)	Configures the VRF reference of an AAA RADIUS or TACACS+ server group.
password encryption aes	Enables a type 6 encrypted preshared key.
tacacs-server host	Specifies a TACACS+ server host.

server-key

To configure the RADIUS key to be shared between a device and RADIUS clients, use the **server-key** command in dynamic authorization local server configuration mode. To remove this configuration, use the **no** form of this command.

server-key [{**0** | **7**}] *word*
no server-key [{**0** | **7**}] *word*

Syntax Description

0	(Optional) An unencrypted key will follow.
7	(Optional) A hidden key will follow.
word	Unencrypted server key.

Command Default

A server key is not configured.

Command Modes

Dynamic authorization local server configuration (config-locsvr-da-radius)

Command History

Release	Modification
12.2(28)SB	This command was introduced.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

A device (such as a router) can be configured to allow an external policy server to dynamically send updates to the router. This functionality is facilitated by the CoA RADIUS extension. CoA introduced peer-to-peer capability to RADIUS, enabling a router and external policy server each to act as a RADIUS client and server. Use the **server-key** command to configure the key to be shared between the Intelligent Services Gateway (ISG) and RADIUS clients.

Examples

The following example configures “cisco” as the shared server key:

```
aaa server radius dynamic-author
 client 10.0.0.1
 server-key cisco
```

Related Commands

Command	Description
aaa server radius dynamic-author	Configures a device as a AAA server to facilitate interaction with an external policy server.

service action

To specify an action when a specific service is detected in the instant messenger traffic, use the **service action**command in the appropriate configuration mode. To disable or change a specified action, use the **no** form of this command.

service {**default** | **text-chat**} **action** {**allow** [**alarm**] | **reset** [**alarm**] | **alarm**}
no service {**default** | **text-chat**} **action** {**allow** [**alarm**] | **reset** [**alarm**] | **alarm**}

Syntax Description

default	Matches all services that are not explicitly configured under the application. **Note** It is recommended that when an IM application is allowed, always specify the default option for an IM application.
text-chat	Controls the text-based chat service that is provided by instant messenger applications.
action	Indicates that a specific action is to follow.
allow	Allows a specific service.
reset	Blocks the service specified in the configuration. If the **default** option is being used, only services for which a specific action has been identified are allowed; all other services are denied.
alarm	Generates an alarm message when the specified service is encountered over the connection.

Command Default

If the command is not configured, the default is **service default action reset**.

Command Modes

cfg-appfw-policy-aim configuration

cfg-appfw-policy-ymsgr configuration

cfg-appfw-policy-msnmsgr configuration

Command History

Release	Modification
12.4(4)T	This command was introduced.

Usage Guidelines

When the **reset** keyword is used, the connection is reset if TCP is used, and the packet is dropped if UDP is used. When dropping a packet from a UDP connection, the session will not be immediately deleted; instead, the session will time out to prevent additional sessions from being immediately created.

The **alarm** keyword can be specified alone or with the **allow** or **reset** keywords; however, the **allow** or **reset** keywords are mutually exclusive.

Examples

The following example shows to configure application policy "my-im-policy," which allows text-chat for Yahoo! instant messenger users and blocks instant messenger traffic for all other users:

```
appfw policy-name my-im-policy
 application http
  port-misuse im reset
!
 application im yahoo
  server permit name scs.msg.yahoo.com
  server permit name scsa.msg.yahoo.com
  server permit name scsb.msg.yahoo.com
  server permit name scsc.msg.yahoo.com
  service text-chat action allow
  service default action reset
!
 application im aol
  server deny name login.user1.aol.com
!
 application im msn
  server deny name messenger.hotmail.com
!
ip inspect name test appfw my-im-policy
interface FastEthernet0/0
 description Inside interface
 ip inspect test in
```

service password-encryption

To automatically convert unencrypted passwords to encrypted passwords, use the **service password-encryption** command in global configuration mode. To restore the default, use the **no** form of this command.

service password-encryption
no service password-encryption

Syntax Description

This command has no arguments or keywords.

Command Default

No passwords are encrypted.

Command Modes

Global configuration

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB.

Usage Guidelines

The actual encryption process occurs when the current configuration is written or when a password is configured. Password encryption is applied to all passwords, including username passwords, authentication key passwords, the privileged command password, console and virtual terminal line access passwords, and Border Gateway Protocol neighbor passwords. This command is primarily useful for keeping unauthorized individuals from viewing your password in your configuration file.

When password encryption is enabled, the encrypted form of the passwords is displayed when a **more system:running-config** command is entered.

Caution This command does not provide a high level of network security. If you use this command, you should also take additional network security measures.

Note You cannot recover a lost encrypted password. You must clear NVRAM and set a new password.

Examples

The following example causes password encryption to take place:

```
service password-encryption
```

Related Commands

Command	Description
enable password	Sets a local password to control access to various privilege levels.
key-string (authentication)	Specifies the authentication string for a key.
neighbor password	Enables MD5 authentication on a TCP connection between two BGP peers.

service password-recovery

To enable password recovery capability, use the **service password-recovery** command in global configuration mode. To disable password recovery capability, use the **no service password-recovery [strict]** command.

service password-recovery
no service password-recovery[strict]

Syntax Description

[strict]	(Optional) Restricts device recovery.

Command Default

Password recovery capability is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)YA	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
Cisco IOS XE Release 3.10S	This command was integrated into Cisco IOS XE Release 3.10S. The **strict** keyword was added to the **no** form of this command.

Usage Guidelines

Note This command is not available on all platforms. Use Feature Navigator to ensure that it is available on your platform.

If you plan to disable the password recovery capability with the **no service password-recovery** command, we recommend that you save a copy of the system configuration file in a location away from the device. If you are using a device that is operating in VTP transparent mode, we recommend that you also save a copy of the vlan.dat file in a location away from the device.

Caution Entering the no **service password-recovery** command at the command line disables password recovery. Always disable this command before downgrading to an image that does not support password recovery capability, because you cannot recover the password after the downgrade.

The configuration register boot bit must be enabled so that there is no way to break into ROMMON when this command is configured. Cisco IOS software should prevent the user from configuring the boot field in the config register.

Bit 6, which ignores the startup configuration, and bit 8, which enables a break should be set.

The Break key should be disabled while the router is booting up and disabled in Cisco IOS software when this feature is enabled.

It may be necessary to use the **config-register** global configuration command to set the configuration register to autoboot *before* entering the **no service password-recovery** command. The last line of the **show version** EXEC command displays the configuration register setting. Use the **show version** EXEC command to obtain the current configuration register value, configure the router to autoboot with the **config-register** command if necessary, then enter the **no service password-recovery** command.

Once disabled, the following configuration register values are *invalid* for the **no service password-recovery** command:

- 0x0
- 0x2002 (bit 8 restriction)
- 0x0040 (bit 6)
- 0x8000 (bit 15)

The **no service password-recoverystrict** command does not allow device recovery and prevents the **send break** command, which is used to recover a device from the no service password-recovery feature, from having any effect during bootup.

The **strict** keyword is supported on the Cisco ASR 1000 Series platform, effective from Cisco IOS XE Release 3.10.

Note Since the **strict** keyword makes the router unrecoverable, before you use the keyword, ensure that you configure the password and configuration register, set up the autoboot image, save the configuration and reboot the router. Only if the correct image is autobooted and the enable password works, should you add the **no service password-recovery strict** command to the configuration. If the enable password is lost, the router should be shipped back to the Cisco support center to fix it.

Catalyst Switch Operation

Use the **service password-recovery** command to reenable the password-recovery mechanism (the default). This mechanism allows a user with physical access to the switch to hold down the **Mode** button and interrupt the boot process while the switch is powering up and to assign a new password. Use the **no** form of this command to disable the password-recovery capability.

When the password-recovery mechanism is disabled, interrupting the boot process is allowed only if the user agrees to set the system back to the default configuration. Use the **show version** EXEC command to verify if password recovery is enabled or disabled on a switch.

The **service password-recovery** command is valid only on Catalyst 3550 Fast Ethernet switches; it is not available for Gigabit Ethernet switches.

Router Configuration Examples

The following example shows how to obtain the configuration register setting (which in this example is set to autoboot), disable the password-recovery capability, and then verify that the configuration persists through a system reload. The **noconfirm** keyword prevents a confirmation prompt from interrupting the booting process.

```
Router# show version
Cisco Internetwork Operating System Software
IOS (tm) 5300 Software (C7200-P-M), Version 12.3(8)YA, RELEASE SOFTWARE (fc1)
TAC Support: http://www.cisco.com/tac
Copyright (c) 1986-2004 by Cisco Systems, Inc.
Compiled Wed 05-Mar-03 10:16 by xxx
Image text-base: 0x60008954, data-base: 0x61964000
ROM: System Bootstrap, Version 12.3(8)YA, RELEASE SOFTWARE (fc1)
BOOTLDR: 7200 Software (C7200-KBOOT-M), Version 12.3(8)YA, RELEASE SOFTWARE (fc1)
Router uptime is 10 minutes
System returned to ROM by reload at 16:28:11 UTC Thu Mar 6 2003
.
.
.
125440K bytes of ATA PCMCIA card at slot 0 (Sector size 512 bytes).
8192K bytes of Flash internal SIMM (Sector size 256K).
Configuration register is 0x2012
Router# configure terminal
Router(config)# no service password-recovery noconfirm
WARNING:
Executing this command will disable the password recovery mechanism.
Do not execute this command without another plan for password recovery.
Are you sure you want to continue? [yes/no]: yes
.
.
.
Router(config)# exit
Router#
Router# reload
Proceed with reload? [confirm] yes
00:01:54: %SYS-5-RELOAD: Reload requested
System Bootstrap, 12.3(8)YA...
Copyright (c) 1994-2004 by cisco Systems, Inc.
C7400 platform with 262144 Kbytes of main memory
PASSWORD RECOVERY FUNCTIONALITY IS DISABLED
.
.
.
```

The following example shows what happens when a break is confirmed and when a break is not confirmed.

Confirmed Break

```
PASSWORD RECOVERY FUNCTIONALITY IS DISABLED
program load complete, entry point: 0x80013000, size: 0x8396a8
Self decompressing the image :
########################################################################################################################
 [OK] !The 5-second window starts.
telnet> send break
             Restricted Rights Legend
Use, duplication, or disclosure by the Government is subject to restrictions as set forth
in subparagraph (c) of the Commercial Computer Software - Restricted Rights clause at FAR
sec. 52.227-19 and subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706
Cisco IOS Software, C831 Software (C831-K9O3SY6-M), Version 12.3(8)YA
Copyright (c) 1986-2004 by Cisco Systems, Inc.
```

```
Compiled Fri 13-Aug-04 03:21
Image text-base: 0x80013200, data-base: 0x81020514
PASSWORD RECOVERY IS DISABLED.
Do you want to reset the router to factory default configuration and proceed [y/n]?
!The user enters "y" here.
Reset router configuration to factory default.
This product contains cryptographic features and is subject to United States and local
country laws governing import, export, transfer and use. Delivery of Cisco cryptographic
products does not imply third-party authority to import, export, distribute or use encryption.
 Importers, exporters, distributors and users are responsible for compliance with U.S. and
 local country laws. By using this product you agree to comply with applicable laws and
regulations. If you are unable to comply with U.S. and local laws, return this product
immediately.
A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html
If you require further assistance please contact us by sending email to export@cisco.com.
Cisco C831 (MPC857DSL) processor (revision 0x00) with 46695K/2457K bytes of memory.
Processor board ID 0000 (1314672220), with hardware revision 0000 CPU rev number 7
3 Ethernet interfaces
4 FastEthernet interfaces
128K bytes of NVRAM
24576K bytes of processor board System flash (Read/Write)
2048K bytes of processor board Web flash (Read/Write)
         --- System Configuration Dialog ---
Would you like to enter the initial configuration dialog? [yes/no]: no
!Start up config is erased.
SETUP: new interface FastEthernet1 placed in "up" state
SETUP: new interface FastEthernet2 placed in "up" state
SETUP: new interface FastEthernet3 placed in "up" state
SETUP: new interface FastEthernet4 placed in "up" state
Press RETURN to get started!
Router> enable
Router# show startup configuration
startup-config is not present
Router# show running-config | incl service
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption !The "no service password-recovery" is disabled.
==========================================================================================
```

Unconfirmed Break

```
PASSWORD RECOVERY FUNCTIONALITY IS DISABLED
telnet> send break
program load complete, entry point: 0x80013000, size: 0x8396a8
Self decompressing the image :
##############################################################################################################
 [OK]
telnet> send break
              Restricted Rights Legend
Use, duplication, or disclosure by the Government is subject to restrictions as set forth
in subparagraph (c) of the Commercial Computer Software - Restricted Rights clause at FAR
sec. 52.227-19 and subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, California 95134-1706
Cisco IOS Software, C831 Software (C831-K9O3SY6-M), Version 12.3(8)YA
Copyright (c) 1986-2004 by Cisco Systems, Inc.
Compiled Fri 13-Aug-04 03:21
```

```
Image text-base: 0x80013200, data-base: 0x81020514
PASSWORD RECOVERY IS DISABLED.
Do you want to reset the router to factory default configuration and proceed [y/n]?
!The user enters "n" here.
This product contains cryptographic features and is subject to United States and local
country laws governing import, export, transfer and use. Delivery of Cisco cryptographic
products does not imply third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for compliance with U.S. and
local country laws. By using this product you agree to comply with applicable laws and
regulations. If you are unable to comply with U.S. and local laws, return this product
immediately.
A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html
If you require further assistance please contact us by sending email to export@cisco.com.
Cisco C831 (MPC857DSL) processor (revision 0x00) with 46695K/2457K bytes of memory.
Processor board ID 0000 (1314672220), with hardware revision 0000 CPU rev number 7
3 Ethernet interfaces
4 FastEthernet interfaces
128K bytes of NVRAM
24576K bytes of processor board System flash (Read/Write)
2048K bytes of processor board Web flash (Read/Write)
Press RETURN to get started! !The Cisco IOS software boots as if it is not interrupted.
Router> enable
Router# show startup configuration
Using 984 out of 131072 bytes
!
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
no service password-recovery
!
hostname Router
!
boot-start-marker
boot-end-marker
!
memory-size iomem 5
!
no aaa new-model
ip subnet-zero
!
ip ips po max-events 100
no ftp-server write-enable
!
interface Ethernet0
 no ip address
 shutdown
!
interface Ethernet1
 no ip address
 shutdown
 duplex auto
!
interface Ethernet2
 no ip address
 shutdown
!
interface FastEthernet1
 no ip address
 duplex auto
 speed auto
!
```

```
interface FastEthernet2
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet3
 no ip address
 duplex auto
 speed auto
!
interface FastEthernet4
 no ip address
 duplex auto
 speed auto
!
ip classless
!
ip http server
no ip http secure-server
!
control-plane
!
line con 0
 no modem enable
 transport preferred all
 transport output all
line aux 0
line vty 0 4
!
scheduler max-task-time 5000
end
Router# show running-configuration | incl service
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
no service password-recovery
```

Configuration Register Messages Example

The **no service password-recovery** command expects the router configuration register to be configured to autoboot. If the configuration register is set to something other than to autoboot *before* the **no service password-recovery** command is entered, a prompt like the one shown in the following example asking you to use the **config-register** global configuration command to change the setting.

```
Router(config)# no service password-recovery
Please setup auto boot using config-register first.
```

Note To avoid any unintended result due to the behavior of this command, use the **show version** command to obtain the current configuration register value. If not set to autoboot, then the router needs to be configured to autoboot with the **config-register** command before entering the **no service password-recovery** command.

Once password recovery is disabled, you cannot set the bit pattern value to 0x40, 0x8000, or 0x0 (disables autoboot). The following example shows the messages displayed when invalid configuration register settings are attempted on a router with password recovery disabled.

```
Router(config)# config-register 0x2143
Password recovery is disabled, cannot enable diag or ignore configuration.
```

The command resets the invalid bit pattern and continue to allow modification of nonrelated bit patterns. The configuration register value resets to 0x3 at the next system reload, which can be verified by checking the last line of the **show version** command output:

```
Configuration register is 0x2012 (will be 0x3 at next reload)
```

Catalyst Switch Example

The following example shows how to disable password recovery on a switch so that a user can only reset a password by agreeing to return to the default configuration:

```
Switch(config)# no service-password recovery
Switch(config)# exit
```

To use the password-recovery procedure, a user with physical access to the switch holds down the **Mode** button while the unit powers up and for a second or two after the LED above port 1X goes off. When the button is released, the system continues with initialization. If the password-recovery mechanism is disabled, the following message is displayed:

```
The password-recovery mechanism has been triggered, but is currently disabled. Access to
the boot loader prompt through the password-recovery mechanism is disallowed at this point.
 However, if you agree to let the system be reset back to the default system configuration,
 access to the boot loader prompt can still be allowed.
Would you like to reset the system back to the default configuration (y/n)?
```

If you choose not to reset the system back to the default configuration, the normal boot process continues, as if the **Mode** button had not been pressed. If you choose to reset the system back to the default configuration, the configuration file in flash memory is deleted and the VLAN database file, flash:vlan.dat (if present), is deleted.

The following is sample output from the **show version** command on a device when password recovery is disabled:

```
Switch# show version
Cisco Internetwork Operating System Software
IOS (tm) C3550 Software (C3550-I9Q3L2-M), Version 12.3(8)YA, RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2004 by cisco Systems, Inc.
Compiled Wed 24-Oct-01 06:20 by xxx
Image text-base: 0x00003000, data-base: 0x004C1864
ROM: Bootstrap program is C3550 boot loader
flam-1-6 uptime is 1 week, 6 days, 3 hours, 59 minutes
System returned to ROM by power-on
Cisco WS-C3550-48 (PowerPC) processor with 65526K/8192K bytes of memory.
Last reset from warm-reset
Running Layer2 Switching Only Image
Ethernet-controller 1 has 12 Fast Ethernet/IEEE 802.3 interfaces
Ethernet-controller 2 has 12 Fast Ethernet/IEEE 802.3 interfaces
Ethernet-controller 3 has 12 Fast Ethernet/IEEE 802.3 interfaces
Ethernet-controller 4 has 12 Fast Ethernet/IEEE 802.3 interfaces
Ethernet-controller 5 has 1 Gigabit Ethernet/IEEE 802.3 interface
Ethernet-controller 6 has 1 Gigabit Ethernet/IEEE 802.3 interface
48 FastEthernet/IEEE 802.3 interface(s)
2 Gigabit Ethernet/IEEE 802.3 interface(s)
The password-recovery mechanism is disabled.
```

```
32K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address: AA:00:0B:2B:02:00
Configuration register is 0x10F
```

Disabling Password Recovery Example

The following example shows how to disable password recovery capability using the **no service password-recovery strict** command:

```
Router# configure terminal
Router(config)# no service password-recovery strict
WARNING:
Executing this command will disable the password recovery mechanism.
Do not execute this command without another plan for password recovery.
Are you sure you want to continue? [yes]: yes
.
.
```

Related Commands

Command	Description
config-register	Changes the configuration register settings.
show version	Displays version information for the hardware and firmware.

service-module ids bootmode

To enter failsafe or normal boot mode for a Cisco Intrusion Prevention System (IPS) network module (also referred to as the Cisco Intrusion Detection System [IDS] network module and as the NME-IPS), use the **service-module ids bootmode** command in privileged EXEC mode.

service-module ids *slot/port* **bootmode**
{**failsafe** | **normal**}

Syntax Description

slot /	Number of the router chassis slot for the network module. The slash mark (/) is required between the *slot* argument and the *port*argument.
port	Port number of the network module. For Cisco IPS network modules, always use 0.
failsafe	Enters IDS failsafe boot mode on a Cisco IPS network module.
normal	Enters IDS normal boot mode on a Cisco IPS network module.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(15)XY	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

If a confirmation prompt is displayed, press **Enter** to confirm the action, or press **n** to cancel.

Examples

The following example enters the IDS failsafe boot mode on the Cisco IPS network module in slot 1:

```
Router# service-module ids 1/0 bootmode failsafe
```

The following example enters the IDS failsafe boot mode on the Cisco IPS network module in slot 1:

```
Router# service-module ids 1/0 bootmode normal
```

Related Commands

Command	Description
ids-service-module monitoring	Enables IDS monitoring on a specified interface.

service-module ids heartbeat-reset

To prevent the Cisco IOS software from rebooting the Cisco Intrusion Prevention System (IPS) network module (also referred to as the Cisco Intrusion Detection System [IDS] network module and as the NME-IPS), when the heartbeat is lost, use the **service-module ids heartbeat-reset** command in privileged EXEC mode.

service-module ids *slot/port* **heartbeat-reset**
{**enable** | **disable**}

Syntax Description

slot **/**	Number of the router chassis slot for the network module. The slash mark (/) is required between the *slot* argument and the *port*argument.
port	Port number of the network module. For Cisco IPS network modules, always use 0.
enable	Enables IDS heartbeat on a Cisco IPS network module.
disable	Disables IDS heartbeat on a Cisco IPS network module.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(15)XY	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

When the Cisco IPS network module, or NME-IPS, is booted in failsafe mode or is undergoing an upgrade, the **service-module ids heartbeat-reset** command does not permit a reboot during the process.

When the NME-IPS heartbeat is lost, the router applies a fail-open or fail-close configuration option to the NME-IPS and stops sending traffic to the NME-IPS, and sets the NME-IPS to error state. The router performs a hardware reset on the NME-IPS and monitors the NME-IPS until the heartbeat is reestablished.

Examples

The following example disables the IDS heartbeat on the Cisco IPS network module in slot 1:

```
Router# service-module ids 1/0 heartbeat-reset disable
```

The following example enables the IDS heartbeat on the Cisco IPS network module in slot 1:

```
Router# service-module ids 1/0 heartbeat-reset enable
```

The status of the heartbeat-reset is displayed by using the **service-module ids** *slot* **/** *port* **status**command:

```
Router# service-module ids 0/0 status
Service Module is Cisco IDS-Sensor 0/0
```

```
Service Module supports session via TTY line 194
Service Module heartbeat-reset is enabled <=====
```

Related Commands

Command	Description
ids-service-module monitoring	Enables IDS monitoring on a specified interface.

service-policy (policy-map)

Note Effective with Cisco IOS Release 12.4(20)T, the **service-policy (policy-map)** command replaces the **service-policy inspect** command.

To attach a Layer 7 policy map to the top-level Layer 3 or Layer 4 policy map, use the **service-policy** command in policy-map-class configuration mode. To disable the attachment, use the **no** form of this command.

service-policy *protocol-name policy-map*
no service-policy *protocol-name policy-map*

Syntax Description

protocol-name	Layer 7 application-specific service policy. The supported protocols are as follows: • **h323** —Associates the class with an H.323 protocol Deep Packet Inspection (DPI). • **gtpv0**—General Packet Radio Service (GPRS) Tunnel Protocol version 0 (GTPv0). • **gtpv1**—GTP version 1 (GTPv1). • **http** —Associates the class with an HTTP DPI. • **im** —Associates the class with an Instant Messenger (IM) protocol DPI. • **imap** —Associates the class with an Internet Message Access Protocol (IMAP) DPI. • **p2p** —Associates the class with a P2P protocol DPI. • **pop3** —Associates the class with a Post Office Protocol, Version 3 (POP3) DPI. • **sip** —Associates the class with a Session Initiation Protocol (SIP) DPI. • **smtp** —Associates the class with an Simple Mail Transfer Protocol (SMTP) DPI. • **sunrpc** —Associates the class with a SUN Remote Procedure Call (SUNRPC) DPI. • **urlfilter** —Associates the class with a **URL filter DPI**.
policy-name	Name of the Layer 7 policy map.

Command Default

Attachments are disabled.

Command Modes

Policy-map-class configuration (config-pmap-c)

Command History

Release	Modification
12.4(20)T	This command was introduced. This command replaces the **service policy-inspect** command.
Cisco IOS XE Release 3.4S	This command was modified. Support for General Packet Radio Service (GPRS) Tunneling Protocol (GTP) was added.

Usage Guidelines

The **service-policy (policy-map)** command attaches a Layer 7 policy-map to the top-level Layer 3 or Layer 4 policy map. The Layer 7 policy is a nested policy of the top-level policy, and it is called a child policy.

Examples

The following example creates a Layer 3 or Layer 4 policy called test, attaches a Layer 7 policy called p11 to that policy, and inspects H.323 traffic:

```
!
class-map type inspect match-all test
 match protocol h323
class-map type inspect h323 match-any c1
 match  message setup
!
policy-map type inspect h323 p11
 class type inspect h323 c1
  log
  rate-limit 15
policy-map type inspect test
 class type inspect test
  inspect
  service-policy h323 p11
 class class-default
  drop
!
```

Related Commands

Command	Description
class-map type inspect	Creates a Layer 3 and Layer 4 or a Layer 7 (application-specific) inspect type class map.
class type inspect	Specifies the traffic (class) on which an action is to be performed.
inspect	Enables Cisco IOS stateful packet inspection.
log (policy-map)	Generates a log of messages.
match message	Configures the match criterion for a class map on the basis of H.323 protocol messages.
match protocol (zone)	Configures the match criterion for a class map on the basis of the specified protocol.
policy-map type inspect	Creates a Layer 3, Layer 4 inspect type policy map or a Layer 7 application-specific inspect type policy map.
rate-limit	Limits the number of Layer 7 Session Initiation Protocol (SIP) or H.323 protocol messages that strike the Cisco IOS firewall every second.

service-policy (zones)

To attach a Layer 7 policy map to a top-level policy map, use the **service-policy** command in zone-pair configuration mode. To delete a Layer 7 policy map from a top-level policy map, use the **no** form of this command.

service-policy *policy-map-name*
no service-policy *policy-map-name*

Syntax Description

policy-map-name	Name of the Layer 7 policy map to be attached to a top-level policy map.

Command Default

None

Command Modes

Zone-pair configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

You can enter the **service-policy** (zones) command after entering the **zone-pair**command.

Examples

The following example attaches a Layer 7 policy map to a top-level policy map:

```
policy-map type inspect p1
 class type inspect c1
  inspect
  service-policy http myhttppolicy
```

Related Commands

Command	Description
zone-pair	Creates a zone-pair.

service-policy inspect

Note Effective with Cisco IOS Release 12.4(20)T, the **service-policy inspect command** command is replaced by the **service-policy (policy-map)** command. See the **service-policy (policy-map)**command for more information.

To attach a Layer 7 policy map to the top-level Layer 3 or Layer 4 policy map, use the **service-policy inspect**command in policy-map-class configuration mode. To disable the attachment, use the **no** form of this command.

service-policy inspect {**http** | **imap** | **pop3** | **smtp** | **sunrpc**} *policy-map*
no service-policy inspect {**http** | **imap** | **pop3** | **smtp** | **sunrpc**} *policy-map*

Syntax Description

http	Associates the class with an HTTP deep inspection policy (DPI).
imap	Associates the class with an Internet Message Access Protocol (IMAP) DPI.
pop3	Associates the class with a Post Office Protocol, Version 3 (POP3) DPI.
smtp	Associates the class with an Simple Mail Transfer Protocol (SMTP) DPI.
sunrpc	Associates the class with a SUN Remote Procedure Call (SUNRPC) DPI.
policy-map	Name of the Layer 7 policy map.

Command Default

Disabled.

Command Modes

Policy-map-class configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.4(20)T	This command was replaced by the service-policy (policy-map) command.

Usage Guidelines

The **service-policy inspect**command attaches a Layer 7 policy-map to the top-level Layer 3 or Layer 4 policy map. The Layer 7 policy is considered to be a nested policy of the top-level policy, and it is called a child policy.

Examples

```
The following example creates a Layer 3 or Layer 4 policy map p1, attaches a Layer 7 policy
 called p11 to that policy, and inspects HTTP traffic.
policy-map type inspect p1
 class type inspect c1
  service-policy inspect http p11
```

service-policy type inspect

To attach a firewall policy map to a zone-pair, use the **service-policy type inspect** command in zone-pair configuration mode. To disable this attachment to a zone-pair, use the **no** form of this command.

service-policy type inspect *policy-map-name*
no service-policy type inspect *policy-map-name*

Syntax Description

policy-map-name	Name of the policy map. The name can be a maximum of 40 alphanumeric characters.

Command Default

None

Command Modes

Zone-pair configuration (config-sec-zone-pair)

Command History

Release	Modification
12.4(6)T	This command was introduced.
15.1(2)T	Support for IPv6 was added.

Usage Guidelines

Use the **service-policy type inspect**command to attach a policy-map and its associated actions to a zone-pair.

Enter the command after entering the **zone-pair security**command.

Examples

The following example defines zone-pair z1-z2 and attaches the service policy p1 to the zone-pair:

```
!
zone security z1
zone security z2
!
class-map type inspect match-all c1
 match protocol tcp
policy-map type inspect p1
 class type inspect c1
  inspect
!
zone-pair security zp source z1 destination z2
 service-policy type inspect p1
!
```

Related Commands

Command	Description
zone-pair security	Creates a zone-pair.

session packet

To configure the number of simultaneous traffic packets that can be configured per session, use the **session packet** command in parameter-map type inspect configuration mode. To remove the configured limit, use the **no** form of this command

session packet *number-of-simultaneous-packets*
no session packet *number-of-simultaneous-packets*

Syntax Description

number-of-simultaneous-packets	Number of simultaneous packets per session. The range is from 25 to 100. The default is 25.

Command Default

25 simultaneous packets can be configured per session.

Command Modes

Parameter-map type inspect configuration (config-profile)

Command History

Release	Modification
Cisco IOS XE Release 3.11S	This command was introduced.

Usage Guidelines

All packets that exceed the configured limit are dropped by the zone-based policy firewall.

You must configure either the **parameter-map type inspect** or the **parameter-map type inspect global** command before configuring the **session packet** command.

The session packet limit configured under the **parameter-map type inspect** command has precedence over the limit configured under the **parameter-map type inspect global** command.

Examples

The following example shows how to configure the number of simultaneous packets per flow under the **parameter-map type inspect** command:

```
Device(config)# parameter-map type inspect inspect-pmap
Device(config-profile)# session packet 35
```

The following example shows how to configure the number of simultaneous packets per flow under the **parameter-map type inspect global** command:

```
Device(config)# parameter-map type inspect inspect global
Device(config-profile)# session packet 55
```

Related Commands

Command	Description
parameter-map type inspect	Configures an inspect-type parameter map for connecting thresholds, timeouts, and other parameters pertaining to the **inspect** action.
parameter-map type inspect global	Defines a global inspect parameter map and enter parameter-map type inspect configuration mode.
show parameter-map type inspect	Displays user-configured or default inspect-type parameter maps.

sessions maximum

To set the maximum number of allowed sessions that can exist on a zone pair, use the **sessions maximum**command in parameter-map configuration mode. To change the number of allowed sessions, use the **no** form of this command.

sessions maximum *sessions*
no sessions maximum

Syntax Description

sessions	Maximum number of allowed sessions. Range: 1 to 2147483647.

Command Default

Default value is unlimited.

Command Modes

Parameter-map configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.
15.1(2)T	Support for IPv6 was added.

Usage Guidelines

Use the **sessions maximum** command to limit the number of inspect sessions that match a certain class. Session limiting is activated when this parameter is configured.

This command is available only within an inspect type parameter map and takes effect only when the parameter map is associated with an inspect action in a policy.

If the **sessions maximum** command is configured, the number of established sessions on the router can be shown via the **show policy-map type inspect zone-pair** command.

Examples

The following example shows how to limit the maximum number of allowed sessions to 200 and how verify the number of established sessions:

```
parameter map type inspect abc
 sessions maximum 200
Router# show policy-map type inspect zone-pair
 Zone-pair: zp
  Service-policy inspect : test-udp
    Class-map: check-udp (match-all)
      Match: protocol udp
      Inspect
        Packet inspection statistics [process switch:fast switch]
        udp packets: [3:4454]
        Session creations since subsystem startup or last reset 92
        Current session counts (estab/half-open/terminating) [5:33:0]<---
        Maxever session counts (estab/half-open/terminating) [5:59:0]
        Last session created 00:00:06
        Last statistic reset never
        Last session creation rate 61
        Last half-open session total 33
      Police
```

```
    rate 8000 bps,1000 limit
    conformed 2327 packets, 139620 bytes; actions: transmit
    exceeded 36601 packets, 2196060 bytes; actions: drop
    conformed 6000 bps, exceed 61000 bps
  Class-map: class-default (match-any)
    Match: any
    Drop (default action)
      0 packets, 0 bytes
```

Related Commands

Command	Description
parameter map type	Creates or modifies a parameter map.

sessions rate

To specify a time duration for defining the session quota, use the **sessions rate** command in parameter-map type inspect configuration mode. To disable the specified time duration, use the **no** form of this command.

sessions rate {**high** *number-of-connections* | **low** *number-of-connections*} **time** *duration*
no sessions rate {**high** | **low**}

Syntax Description

high *number-of-connections*	Number of new unestablished sessions that will cause the system to start deleting half-open sessions.
low *number-of-connections*	Number of new unestablished sessions that will cause the system to stop deleting half-open sessions.
time	Specifies the time for which the session rate limit is applied.
duration	Time duration, in seconds, for which the session rate is limited. Range is from 1 to 2147483.

Command Default

The system does not start or stop deleting half-open sessions.

Command Modes

Parameter-map type inspect configuration (config-profile)

Command History

Release	Modification
Cisco IOS XE Release 2.4	This command was introduced.

Usage Guidelines

You can use the **one-minute** command to define session quota within one minute. You can use the **sessions rate** command to specify the time duration in which session quota can be defined. The **sessions rate** command and the **one-minute** command are mutually exclusive. If the **one-minute** command is configured in an inspect parameter map, the **sessions rate** command is rejected, and vice versa.

Examples

The following example shows how to configure a session rate of 25 seconds:

```
Router> enable
Router# configure terminal
Router(config)# parameter-type inspect type par1
Router(config-profile)# sessions-rate high 250 time 25
```

Related Commands

Command	Description
one-minute	Defines the number of new unestablished sessions that will cause the system to start deleting half-open sessions and stop deleting half-open sessions.
parameter-map type inspect	Configures an inspect type parameter map for connecting thresholds, timeouts, and other parameters pertaining to the inspect action.

server scansafe

Note Effective with Cisco IOS Release 15.4(2)T, the **server scansafe** command is replaced by the **server (CWS)** command. See the **server (CWS)** command for more information.

To configure the Cloud Web Security server for content scanning, use the **server scansafe** command in parameter-map type inspect configuration mode. To disable the Cloud Web Security server for content scanning, use the **no** form of this command.

server scansafe {**on-failure** {**allow-all** | **block-all**} | {**primary** | **secondary**} {**ipv4** *ip-address* | **name** *domain-name*} **port http** *port-number* **https** *port-number*}
no server scansafe {**primary** | **secondary**} {**ipv4** *ip-address* | **name** *domain-name*} **port http** *port-number* **https** *port-number*

Syntax Description

on-failure	Specifies that there is a communication failure with ScanSafe.
allow-all	Allows traffic to flow directly to the web server.
block-all	Blocks the traffic to the web server.
primary	Specifies the primary security as a service (SaaS) server.
secondary	Specifies the secondary SaaS server.
ipv4 *ip-address*	Specifies the IPv4 address of the server.
name *domain-name*	Specifies the domain name of the server.
port	Specifies the SaaS listening port number.
http *port-number*	Specifies the HTTP port and port number. Valid values for the *port-number* argument are from 1 to 65535.
https *port-number*	Specifies the secure HTTP (HTTPS) port and port number. Valid values for the *port-number* argument are from 1 to 65535.

Command Default

The Cloud Web Security server is not configured for content scanning.

Command Modes

Parameter-map type inspect configuration (config-profile)

Command History

Release	Modification
15.2(1)T1	This command was introduced.
15.4(2)T	This command was replaced by the **server (CWS)** command.

Usage Guidelines

Use the **server scansafe** command to configure different ports for HTTP and secure HTTP (HTTPS). However, the default port for the proxied HTTP and HTTPS traffic is 8080 for Cloud Web Security. In case the name

or the IP address of the Cloud Web Security server is not configured correctly, the default web page from the configured server will be sent for all the web requests from the endpoints.

If both the primary and secondary towers are unreachable, the traffic is dropped if you have configured the **server scansafe on-failure block-all** command or, if you have configured the **server scansafe on-failure allow-all** command, the traffic is allowed to the actual web server without redirecting.

Examples

The following example shows how to configure the Cloud Web Security server for content scanning:

```
Device(config)# parameter-map type content-scan global
Device(config-profile)# server scan-safe primary ipv4 10.1.1.1 port http 81 https 101
```

Related Commands

Command	Description
parameter-map type content-scan global	Configures a global content-scan parameter map and enters parameter-map type inspect configuration mode.

set aggressive-mode client-endpoint through show content-scan

set aggressive-mode client-endpoint

To specify the Tunnel-Client-Endpoint attribute within an Internet Security Association Key Management Protocol (ISAKMP) peer configuration, use the **set aggressive-mode client-endpoint** command in ISAKMP policy configuration mode. To remove this attribute from your configuration, use the **no** form of this command.

set aggressive-mode client-endpoint *client-endpoint*
no set aggressive-mode client-endpoint *client-endpoint*

Syntax Description

client-endpoint	One of the following identification types of the initiator end of the tunnel: • ID_IPV4 (IPV4 address) • ID_FQDN (fully qualified domain name, for example "green.cisco.com") • ID_USER_FQDN (e-mail address) The ID type is translated to the corresponding ID type in Internet Key Exchange (IKE).

Command Default

The Tunnel-Client-Endpoint attribute is not defined.

Command Modes

ISAKMP policy configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.4(4)T	Support for IPv6 was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

Before you can use this command, you must enable the **crypto isakmp peer** command.

To initiate an IKE aggressive mode negotiation and specify the RADIUS Tunnel-Client-Endpoint attribute, the **set aggressive-mode client-endpoint** command, along with the **set aggressive-mode password** command, must be configured in the ISAKMP peer policy. The Tunnel-Client-Endpoint attribute will be communicated to the server by encoding it in the appropriate IKE identity payload.

Examples

The following example shows how to initiate aggressive mode using RADIUS tunnel attributes:

```
crypto isakmp peer address 10.4.4.1
 set aggressive-mode client-endpoint user-fqdn user@cisco.com
 set aggressive-mode password cisco123
```

Related Commands

Command	Description
crypto isakmp peer	Enables an IPSec peer for IKE querying of AAA for tunnel attributes in aggressive mode.
set aggressive-mode password	Specifies the Tunnel-Password attribute within an ISAKMP peer configuration.

set aggressive-mode password

To specify the Tunnel-Password attribute within an Internet Security Association Key Management Protocol (ISAKMP) peer configuration, use the **set aggressive-mode password** command in ISAKMP policy configuration mode. To remove this attribute from your configuration, use the **no** form of this command.

set aggressive-mode password *password*
no set aggressive-mode password *password*

Syntax Description

password	Password that is used to authenticate the peer to a remote server. The tunnel password is used as the Internet Key Exchange (IKE) preshared key.

Command Default

The Tunnel-Password attribute is not defined.

Command Modes

ISAKMP policy configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.3(2)T	This command was modified so that output shows that the preshared key is either encrypted or unencrypted.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Before you can use this command, you must enable the **crypto isakmp peer** command.

To initiate an IKE aggressive mode negotiation, the **set aggressive-mode password**command, along with the **set aggressive-mode client-endpoint** command, must be configured in the ISAKMP peer policy. The Tunnel-Password attribute will be used as the IKE preshared key for the aggressive mode negotiation.

Output for the **set aggressive-mode password**command will show that the preshared key is either unencrypted or encrypted. An output example for an unencrypted preshared key would be as follows:

```
set aggressive-mode password test123
```

An output example for a type 6 encrypted preshared key would be as follows:

```
set aggressive-mode password 6 DV'P[aTVWWbcgKU]T\T\QhZAAB
```

Examples

The following example shows how to initiate aggressive mode using RADIUS tunnel attributes:

```
Router (config)# crypto isakmp peer address 10.4.4.1
Router (config-isakmp-peer)# set aggressive-mode client-endpoint user-fqdn user@cisco.com
Router (config-isakmp-peer)#
set aggressive-mode password cisco123
```

Related Commands

Command	Description
crypto isakmp peer	Enables an IPSec peer for IKE querying of AAA for tunnel attributes in aggressive mode.
set aggressive-mode client-endpoint	Specifies the Tunnel-Client-Endpoint attribute within an ISAKMP peer configuration.

set group

To set the Group Domain of Interpretation (GDOI) crypto map to the GDOI group that has already been defined, use the **set group** command in crypto map configuration mode. To remove the GDOI crypto map, use the **no** form of this command.

set group *group-name*
no set group *group-name*

Syntax Description

group-name	Name of the GDOI group.

Command Default

None

Command Modes

crypto map configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

This command must be configured for the GDOI crypto map to be complete.

Note This crypto map is specifically a GDOI crypto map, that is, the crypto map must be named as a GDOI crypto map, as in this example: **crypto map test 10 gdoi**

Examples

The following example shows that the group name is "hsrp-group":

```
set group hsrp-group
```

Related Commands

Command	Description
crypto map	Enters crypto map configuration mode and creates or modifies a crypto map entry, creates a crypto profile that provides a template for configuration of dynamically created crypto maps, indicates that the key management mechanism is GDOI, or configures a client accounting list.

set identity

To set the identity to the crypto map, use the **set identity** command in crypto map configuration mode.

set identity *name*

Syntax Description

name	Identity used to permit or restrict access for a host to a crypto map.

Command Default

If this command is not enabled, the encrypted connection does not have any restrictions other than the IP address of the encrypting peer.

Command Modes

Crypto map configuration

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.

Usage Guidelines

Use the **set identity** command to set the identity to the configured crypto maps. When this command is applied, only the hosts that match a configuration listed within the *name* argument can use that crypto map.

Examples

The following example shows how to configure two IP Security (IPSec) crypto maps and apply the identity to each crypto map. That is, the identity is set to "to-bigbiz" for the first crypto map and "to-little-com" for the second crypto map.

```
! The following is an IPSec crypto map (part of IPSec configuration). It can be used only
! by peers that have been authenticated by DN and if the certificate belongs to BigBiz.
crypto map map-to-bigbiz 10 ipsec-isakmp
 set peer 172.21.114.196
 set transform-set my-transformset
 match address 124
 set identity to-bigbiz
!
crypto identity to-bigbiz
 dn ou=BigBiz
!
!
! This crypto map can be used only by peers that have been authenticated by hostname
! and if the certificate belongs to little.com.
crypto map map-to-little-com 10 ipsec-isakmp
 set peer 172.21.115.119
 set transform-set my-transformset
 match address 125
 identity to-little-com
!
crypto identity to-little-com
 fqdn little.com
```

Related Commands

Command	Description
crypto identity	Configures the identity of the router with a given list of DNs in the certificate of the router.
crypto map (global IPSec)	Creates or modifies a crypto map entry and enters the crypto map configuration mode.
crypto mib ipsec flowmib history failure size	Associates the identity of the router with the DN in the certificate of the router.
fqdn	Associates the identity of the router with the hostname that the peer used to authenticate itself.

set ip access-group

To check a preencrypted or postdecrypted packet against an access control list (ACL) without having to use the outside physical interface ACL, use the **set ip access-group** command in crypto map configuration mode. To disable the check, use the **no** form of this command.

set ip access-group {*access-list-numberaccess-list-name*} {**in** | **out**}
no set ip access-group {*access-list-numberaccess-list-name*} {**in** | **out**}

Syntax Description

access-list-number	Number of an access list. Values 100 through 199 are used for IP access lists (extended). The values 2000 through 2699 are used for expanded access lists (extended).
access-list-name	Name of an access list.
in	Sets access control for inbound clear-text packets (after decryption).
out	Sets access control for outbound clear-text packets (prior to encryption).

Command Default

No crypto map access ACLs are defined to filter clear-text packets going through the IPSec tunnel.

Command Modes

Crypto map configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

The **set ip access-group** command is used after the crypto map has been configured.

Examples

The following example shows that a crypto map access ACL has been configured:

```
Router (config)# crypto map map vpn1 10
Router (config-crypto-map)# set ip access-group 151 in
```

Related Commands

Command	Description
crypto map	Assigns a previously defined crypto map set to an interface so that the interface can provide IPSec services.

set isakmp-profile

To set the Internet Security Association and Key Management Protocol (ISAKMP) profile name, use the **set isakmp-profile**command in crypto map configuration mode. To remove the ISAKMP profile name, use the **no** form of this command.

set isakmp-profile *profile-name*
no set isakmp-profile *profile-name*

Syntax Description

profile-name	Name of the ISAKMP profile.

Command Default

If the ISAKMP profile is not specified in the crypto map entry, the default is to the ISAKMP profile that is on the head. If there is no ISAKMP profile on the head, the default is "none."

Command Modes

Crypto map configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command describes the ISAKMP profile to use when you start the Internet Key Exchange (IKE) exchange.

Before configuring an ISAKMP profile on a crypto map, you should set up the ISAKMP profile.

Examples

The following example shows that an ISAKMP profile has been configured on a crypto map:

```
crypto map vpnmap 10 ipsec-isakmp
 set isakmp-profile vpnprofile
```

Related Commands

Command	Description
crypto ipsec transform-set	Defines a transform set, which is an acceptable combination of security protocols and algorithms.
crypto map (global)	Creates or modifies a crypto map entry.

set nat demux

To enable L2TP--IPSec support for NAT or PAT Windows clients, use the **set nat demux**command in crypto map configuration mode. To disable L2TP--IPSec support, use the **no** form of this command.

set nat demux
no set nat demux

Syntax Description

This command has no arguments or keywords.

Command Default

With this command disabled, Windows clients lose connection when another Windows client establishes an IP Security (IPSec) protected Cisco IOS Layer 2 Tunneling Protocol (L2TP) tunnel to the same Cisco IOS L2TP Network Server (LNS) when there is a network address translation (NAT) or port address translation (PAT) server between the Windows clients and the LNS.

Command Modes

Crypto map configuration

Command History

Release	Modification
12.3(11)T4	This command was introduced.
12.4(1)	This command was integrated into Release 12.4(1).

Usage Guidelines

Use this command if you have an environment with IPSec enabled and consisting of an LNS, and a network address translation (NAT) or port address translation (PAT) server between the Windows clients and the LNS.

This command has been tested only with Windows 2000 L2TP/IPsec clients running hotfix 818043.

You must enter the **crypto map** command if you are using static crypto maps or the **crypto dynamic-map** command if you are using dynamic crypto maps before issuing the **set nat demux** command.

Note If you do not have IPSec enabled, or you do not have a NAT or PAT server, you can have multiple Windows clients connect to a LNS without this command enabled.

Examples

The following example shows how to enable L2TP--IPSec support for NAT or PAT Windows clients for a dynamic crypto map:

```
.
.
.
!Enable virtual private networking.
vpdn enable
! Default L2TP VPDN group
vpdn-group 1
!
!Enables the LNS to accept dial in requests; specifies L2TP as the tunneling
protocol; specifies the number of the virtual templates used to clone
virtual-access interfaces; specifies an alternate IP address for a VPDN tunnel
```

```
accept-dialin.
  protocol l2tp
  virtual-template 1
  source-ip 10.0.0.1
!
!Disables Layer 2 Tunneling Protocol (L2TP) tunnel authentication.
no l2tp tunnel authentication
!
!Defines an Internet Key Exchange (IKE) policy and assigns priority 1.
crypto isakmp policy 1
 encr 3des
 group 2
!
crypto isakmp policy 2
 encr 3des
 authentication pre-share
 group 2
!
!Defines a transform set.
crypto ipsec transform-set vpn esp-3des esp-md5-hmac
 mode transport
crypto mib ipsec flowmib history tunnel size 2
crypto mib ipsec flowmib history failure size 2
!
!Names the dynamic crypto map entry to create (or modify) and enters crypto map configuration
 mode.
crypto dynamic-map dyn_map 1
!Specifies which transform sets can be used with the crypto map entry
 set transform-set vpn
!Enables L2TP--IPSec support.
 set nat demux
.
.
.
```

Related Commands

Command	Description
crypto dynamic-map	Names the dynamic crypto map entry to create (or modify) and enters crypto map configuration mode.
crypto map	Names the static crypto map entry to create (or modify) and enters crypto map configuration mode.
show crypto dynamic-map	Displays information about dynamic crypto maps.
show crypto ipsec sa	Displays the settings used by current SAs.
show crypto map	Displays information about static crypto maps.

set peer (IPsec)

To specify an IP Security (IPsec) peer in a crypto map entry, use the **set peer** command in crypto map configuration mode. To remove an IPsec peer from a crypto map entry, use the **no** form of this command.

set peer {*host-name* [**dynamic**] [**default**] | *ip-address* [**default**]}
no set peer {*host-name* [**dynamic**] [**default**] | *ip-address* [**default**]}

Syntax Description

host-name	Specifies the IPsec peer by its hostname. This is the peer's hostname concatenated with its domain name (for example, myhost.example.com).
dynamic	(Optional) The hostname of the IPsec peer will be resolved via a domain name server (DNS) lookup right before the router establishes the IPsec tunnel.
default	(Optional) If there are multiple IPsec peers, designates that the first peer is the default peer.
ip-address	Specifies the IPsec peer by its IP address.

Command Default

No peer is defined.

Command Modes

Crypto map configuration (config-crypto-map)

Command History

Release	Modification
11.2	This command was introduced.
12.3(4)T	The **dynamic** keyword was added.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.3(14)T	The **default** keyword was added.
12.2(33)SRA	The command was integrated into Cisco IOS Release 12.2(33)SRA

Usage Guidelines

Use this command to specify an IPsec peer for a crypto map.

This command is required for all static crypto maps. If you are defining a dynamic crypto map (with the **crypto dynamic-map** command), this command is not required, and in most cases is not used (because, in general, the peer is unknown).

For crypto map entries created with the **crypto map** *map-name seq-num* **ipsec-isakmp** command, you can specify multiple peers by repeating this command. The peer that packets are actually sent to is determined by the last peer that the router heard from (received either traffic or a negotiation request from) for a given data flow. If the attempt fails with the first peer, Internet Key Exchange (IKE) tries the next peer on the crypto map list.

For crypto map entries created with the **crypto map***map-name seq-num* **ipsec-manual** command , you can specify only one IPsec peer per crypto map. If you want to change the peer, you must first delete the old peer and then specify the new peer.

You can specify the remote IPsec peer by its hostname only if the hostname is mapped to the peer's IP address in a DNS or if you manually map the hostname to the IP address with the **ip host** command.

The dynamic Keyword

When specifying the hostname of a remote IPsec peer via the **set peer** command, you can also issue the **dynamic** keyword, which defers DNS resolution of the hostname until right before the IPsec tunnel has been established. Deferring resolution enables the Cisco IOS software to detect whether the IP address of the remote IPsec peer has changed. Thus, the software can contact the peer at the new IP address.

If the **dynamic** keyword is not issued, the hostname is resolved immediately after it is specified. So, the Cisco IOS software cannot detect an IP address change and, therefore, attempts to connect to the IP address that it previously resolved.

The default Keyword

If there are multiple peers and you specify the **default** keyword, the first peer is designated as the default peer.

If dead peer detection (DPD) detects a failure, the default peer is retried before there is an attempt to connect to the next peer in the peer list.

If the default peer is unresponsive, the next peer in the peer list becomes the new current peer. Future connections through the crypto map will try that peer.

Examples

The following example shows a crypto map configuration when IKE will be used to establish the security associations (SAs). In this example, an SA could be set up to either the IPsec peer at 10.0.0.1 or the peer at 10.0.0.2.

```
crypto map mymap 10 ipsec-isakmp
 match address 101
 set transform-set my_t_set1
 set peer 10.0.0.1
 set peer 10.0.0.2
```

The following example shows how to configure a router to perform real-time Domain Name System (DNS) resolution with a remote IPsec peer; that is, the hostname of peer is resolved via a DNS lookup right before the router establishes a connection (an IPsec tunnel) with the peer.

```
crypto map secure_b 10 ipsec-isakmp
  match address 140
  set peer b.cisco.com dynamic
  set transform-set xset
interface serial1
  ip address 10.30.0.1
  crypto map secure_b
access-list 140 permit ...
```

The following example shows that the first peer, at IP address 10.1.1.1, is the default peer:

```
crypto map tohub 1 ipsec-isakmp
 set peer 10.1.1.1 default
 set peer 10.2.2.2
```

The following example shows that the peer with the hostname user1 is the default peer.

```
crypto map tohub 2 ipsec-isakmp
 set peer user1 dynamic default
 set peer user2 dynamic
```

Related Commands

Command	Description
crypto dynamic-map	Creates a dynamic crypto map entry and enters the crypto map configuration command mode.
crypto map (global IPSec)	Creates or modifies a crypto map entry and enters the crypto map configuration mode.
crypto map (interface IPSec)	Applies a previously defined crypto map set to an interface.
crypto map local-address	Specifies and names an identifying interface to be used by the crypto map for IPsec traffic.
match address (IPSec)	Specifies an extended access list for a crypto map entry.
set pfs	Specifies that IPsec should ask for PFS when requesting new SAs for this crypto map entry, or that IPsec requires PFS when receiving requests for new SAs.
set security-association level per-host	Specifies that separate IPsec SAs should be requested for each source/destination host pair.
set security-association lifetime	Overrides (for a particular crypto map entry) the global lifetime value, which is used when negotiating IPsec SAs.
set session-key	Specifies the IPsec session keys within a crypto map entry.
set transform-set	Specifies which transform sets can be used with the crypto map entry.
show crypto map (IPSec)	Displays the crypto map configuration.

set pfs

To optionally specify that IP security (IPsec) requests the perfect forward secrecy (PFS) Diffie-Hellman (DH) prime modulus group identifier when requesting new security associations (SAs) for a crypto map entry or when IPsec requires PFS when receiving requests for new SAs, use the **set pfs** command in crypto m ap configuration mode. To specify that IPsec should not request PFS during the DH exchange, use the **no** form of this command.

set pfs {**group1** | **group2** | **group5** | **group14** | **group15** | **group16** | **group19** | **group20**}
no set pfs

Syntax Description

group1	Specifies the 768-bit DH identifier.
group2	Specifies the 1024-bit DH identifier.
group5	Specifies the 1536-bit DH identifier.
group14	Specifies the 2048-bit DH identifier.
group15	Specifies the 3072-bit DH identifier.
group16	Specifies the 4096-bit DH identifier.
group19	Specifies the 256-bit elliptic curve DH (ECDH) identifier.
group20	Specifies the 384-bit ECDH identifier.

Command Default

By default, PFS is not requested. If no group is specified with this command, the **group1** keyword is used as the default.

Command Modes

Crypto map configuration (config-crypto-map)

Command History

Release	Modification
11.3 T	This command was introduced.
12.1(1.3)T	Support was added for DH group 5.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	Support for IPv6 was added.
Cisco IOS XE Release 2.2	Support was added for DH groups 14, 15, and 16 on the Cisco ASR 1000 series routers.

Release	Modification
12.4(22)T	Support for DH groups 14, 15, and 16 on the Cisco ASR 1000 series routers was integrated into Cisco IOS Release 12.4(22)T.
15.1(2)T	This command was modified. DH groups 19 and 20 were added in Cisco IOS Release 15.1(2)T.

Usage Guidelines

This command is available for **ipsec-isakmp** crypto map entries and dynamic crypto map entries for both IKEv1 and IKEv2.

During negotiation, this command causes IPsec to request PFS when requesting new security associations for the crypto map entry. The default (**group1**) is sent if the **set pfs** statement does not specify a group. If the peer initiates the negotiation and the local configuration specifies PFS, the remote peer must perform a PFS exchange or the negotiation will fail. If the local configuration does not specify a group, a default of **group1** will be assumed, and an offer of either **group1** or **group2** will be accepted. If the local configuration specifies **group2**, that group *must* be part of the offer of the peer or the negotiation will fail. If the local configuration does not specify PFS, it will accept any offer of PFS from the peer.

PFS adds another level of security; if one key is ever cracked by an attacker, then only the data sent with that key will be compromised. Without PFS, data sent with other keys could be compromised also.

With PFS, every time a new security association is negotiated, a new DH exchange occurs. (This exchange requires additional processing time.)

The 1024-bit DH prime modulus group, **group2**, provides more security than **group1** but requires more processing time than **group1**.

The group chosen must be strong enough (have enough bits) to protect the IPsec keys during negotiation. While there is some disagreement regarding how many bits are necessary in the DH group to protect a specific key size, it is generally agreed that **group14** is good protection for 128-bit keys, **group15** is good protection for 192-bit keys, and **group16** is good protection for 256-bit keys.

Note **group5** may be used for 128-bit keys, but **group14** is better.

The ISAKMP group and the IPsec PFS group should be the same if PFS is used. If PFS is not used, a group is not configured in the IPsec crypto map.

Examples

The following example specifies that PFS should be used whenever a new security association is negotiated for the crypto map mymap 10:

```
crypto map mymap 10 ipsec-isakmp
 set pfs group2
```

Related Commands

Command	Description
crypto dynamic-map	Creates a dynamic crypto map entry and enters the crypto map configuration command mode.
crypto map (global IPsec)	Creates or modifies a crypto map entry and enters the crypto map configuration mode.

Command	Description
crypto map (interface IPsec)	Applies a previously defined crypto map set to an interface.
crypto map local-address	Specifies and names an identifying interface to be used by the crypto map for IPsec traffic.
match address (IPsec)	Specifies an extended access list for a crypto map entry.
set peer (IPsec)	Specifies an IPsec peer in a crypto map entry.
set security-association level per-host	Specifies that separate IPsec security associations should be requested for each source/destination host pair.
set security-association lifetime	Overrides (for a particular crypto map entry) the global lifetime value, which is used when negotiating IPsec security associations.
set transform-set	Specifies which transform sets can be used with the crypto map entry.
show crypto map (IPsec)	Displays the crypto map configuration.

set platform software trace forwarding-manager alg

To set the platform software trace levels for the forwarding manager application layer gateway (ALG), use the **set platform software trace forwarding-manager alg** command in privileged EXEC mode.

set platform software trace forwarding-manager {**F0** | **F1** | **FP** | **R0** | **R1** | **RP**} {**active** | **standby**} **alg** {**debug** | **emergency** | **error** | **info** | **noise** | **notice** | **verbose** | **warning**}

Syntax Description

F0	Specifies slot 0 of the Embedded Service Processor (ESP).
F1	Specifies slot 1 of the ESP.
FP	Specifies the ESP.
R0	Specifies slot 0 of the Route Processor (RP).
R1	Specifies slot 1 of the RP.
RP	Specifies the RP.
active	Specifies the active instance of the processor.
standby	Specifies the standby instance of the processor.
debug	Sets debug messages for ALGs.
emergency	Sets emergency messages for ALGs.
error	Sets error messages for ALGs.
info	Sets informational messages for ALGs.
noise	Sets the maximum message level for ALGs.
notice	Sets notice messages for ALGs.
verbose	Sets detailed debug messages for ALGs.
warning	Sets warning messages for ALGs.

Command Default

Trace levels are not set.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.11S	This command was introduced.

Usage Guidelines

Use this command to troubleshoot platform-specific ALG issues.

Examples

The following is example shows how to set platform-specific debug messages for ALGs:

```
Device# set platform software trace forwarding-manager FP active alg debug
```

Related Commands

alg sip blacklist	Configures a dynamic SIP ALG blacklist for destinations.
alg sip processor	Configures the maximum number of backlog messages that wait for shared resources.
alg sip timer	Configures a timer that SIP ALG uses to manage SIP calls.

set reverse-route

To define a distance metric for each static route or to tag a reverse route injection (RRI)-created route, use the **set reverse-route** command in crypto map configuration or IPsec profile configuration mode. To delete the tag or distance metric, use the **no** form of this command.

set reverse-route[{**distance** *number* | **tag** *tag-id* | **gateway** *next-hop*}]
no set reverse-route[{**distance** *number* | **tag** *tag-id* | **gateway** *next-hop*}]

Syntax Description

distance *number*	(Optional) Defines a distance metric for each static route. The range is from 1 to 255.
tag *tag-id*	(Optional) Creates a route and tags it. The tag value can be used as a match value for controlling redistribution using route maps.
gateway *next-hop*	(Optional) Defines the next-hop IP address of the preferred gateway through which encrypted traffic can be routed.

Command Default

The distance metric is 1 and the tag is 0.

Command Modes

Crypto map configuration (config-crypto-map)

IPsec profile configuration (config-crypto-profile)

Command History

Release	Modification
12.4(15)T	This command was introduced. This command replaced the **reverse-route tag** command.
Cisco IOS XE Release 3.2S	This command was modified. The **gateway** *next-hop* keyword and argument pair was added.

Usage Guidelines

This command can be applied on a per-crypto map basis or to a virtual tunnel interface (VTI) in a reverse route injection configuration.

RRI provides a scalable mechanism to dynamically learn and advertise the IP address and subnets that belong to a remote site that connects through an IPsec VPN tunnel.

When enabled in an IPsec crypto map, RRI learns all the subnets from any network that is defined in the crypto access control list (ACL) as the destination network. The learned routes are installed into the local routing table as static routes that point to the encrypted interface. When the IPsec tunnel is torn down, the associated static routes are removed. These static routes may then be redistributed into other dynamic routing protocols so that they can be advertised to other parts of the network (usually by redistributing RRI routes into dynamic routing protocols on the core side).

The **set reverse-route** command provides a way to configure a server so that a dynamically learned route can take precedence over static routes. The static routes are used only in the absence of the dynamically learned route.

Inserting an RRI in the remote peer through a gateway that is configured in the crypto IPsec profile ensures that the traffic to the remote peer is always routed through the configured gateway.

If you configure the RRI gateway when there are no sessions, then no changes occur. A route to the remote peer is added only when a new security association (SA) becomes active.

To change to a new gateway when there are active sessions, you must delete the active sessions. You cannot add, delete, or change a gateway configuration when there are active sessions.

The gateway configuration scenarios with respect to sessions are exhibited irrespective of whether Front Virtual Routing and Forwarding (FVRF) has been configured.

Examples

The following example shows how to set the value of the metric distance for each dynamic route to 20 in a crypto map situation. The configuration is on an Easy VPN server.

```
crypto dynamic-map mode 1
 set security-association lifetime seconds 300
 set transform-set 3dessha
 set isakmp-profile profile2
 set reverse-route distance 20
 reverse-route
```

The following example shows how to set the value of the metric distance for each dynamic route to 20 for a VTI. The configuration is on an Easy VPN server.

```
crypto isakmp profile profile1
 keyring mykeyring
 match identity group examplegroup
 client authentication list authenlist
 isakmp authorization list autholist
 client configuration address respond
 virtual-template 1
crypto ipsec profile vi
 set transform-set 3dessha
 set reverse-route distance 20
 set reverse-route gateway 10.0.0.1
 set isakmp-profile profile1
!
interface Virtual-Template1 type tunnel
 ip unnumbered
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile vi
```

Related Commands

Command	Description
debug crypto ipsec	Displays IPsec events.
reverse-route	Creates source proxy information for a crypto map entry.

set security-association dummy

To enable the generation and transmission of dummy packets for an IPsec traffic flow in a crypto map, use the **set security-association dummy** command in crypto map configuration mode. To disable this generation and transmission, use the **no** form of this command.

set security-association dummy {**pps** *rate* | **seconds** *seconds*}
no set security-association dummy

Syntax Description

pps *rate*	Packets per second rate. The range is 0 to 25.
seconds *seconds*	Delay, in seconds, between packets. The range is 1 to 3600.

Command Default

Generating and transmitting dummy packets is disabled.

Command Modes

Crypto map configuration (config-crypto-map)

Command History

Release	Modification
15.2(4)M3	This command was introduced.
Cisco IOS XE Release 3.10S	This command was integrated into Cisco IOS XE Release 3.10S.

Usage Guidelines

RFC 4303 specifies a method to hide packet data in an IPsec traffic flow by adding dummy packets to the flow. Use the **set security-association dummy** command to generate and transmit dummy packets to hide data in the IPsec traffic flow in a crypto map. The dummy packet is designated by setting the next header field in the Encapsulating Security Payload (ESP) packet to a value of 59. When a crypto engine receives such packets, it discards them.

Use the **pps** *rate* keyword/argument pair to specify a rate greater than one packet per second.

When using this command to generate dummy packets for a specific crypto map, dummy packets are generated for all flows created in the crypto map.

Examples

The following example generates dummy packets every five seconds in the traffic flow of a crypto map:

```
crypto map tohub 1 ipsec-isakmp
 set peer 10.1.1.1 default
 set peer 10.2.2.2
 set security-association dummy seconds 5
 set transform-set aes_sha2
 match address 101
```

Related Commands

Command	Description
crypto ipsec security-association dummy	Enables the generation and transmission of dummy packets in an IPsec traffic flow.

set security-association idle-time

To specify the maximum amount of time for which the current peer can be idle before the default peer is used, use the **set security-association idle-time** command in crypto map configuration mode. To disable this feature, use the **no** form of this command.

set security-association idle-time *seconds* [**default**]
no set security-association idle-time *seconds* [**default**]

Syntax Description

seconds	Number of seconds for which the current peer can be idle before the default peer is used. Although the command will accept values for *seconds* ranging from 60 to 86400 seconds, the configured value will be rounded up to the next multiple of 600 seconds (ten minutes).
default	(Optional) Specifies that the next connection is directed to the default peer. Default: If the **default** keyword is not specified and there is a connection timeout, the current peer remains unchanged.

Command Default

The default peer is not used if the current peer times out.

Command Modes

Crypto map configuration (config-crypto-map)

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)SRA	The command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

This command is optional. Use this command if you want the default peer to be used if the current peer times out. If there is a timeout to the current peer, the connection to that peer is closed. The next time a connection is initiated, it is directed to the default peer specified in the **set peer** command.

The configured value for *seconds* is rounded up to the next multiple of 600 seconds (ten minutes), and the rounded value becomes the polling interval for peer idle detection. Because the idle condition must be observed in two successive pollings, the period of inactivity may last up to twice the polling period before the connection to the idle peer can be closed.

Examples

In the following example, if the current peer is idle for at least 750 seconds, the default peer 10.1.1.1 (which was specified in the **set peer**command) is used for the next attempted connection:

```
crypto map tohub 1 ipsec-isakmp
 set peer 10.1.1.1 default
 set peer 10.2.2.2
 set security-association idle-time 750 default
```

In this example, the configured value of 750 seconds will be rounded up to 1200 seconds (the next multiple of 600), which becomes the idle polling interval. The connection to the idle peer will be closed after two successive idle pollings, resulting in an inactivity period of between 1200 and 2400 seconds before the connection is closed.

Related Commands

Command	Description
set peer (IPSec)	Specifies an IPsec peer in a crypto map entry.

set security-association level per-host

To specify that separate IP Security security associations should be requested for each source/destination host pair, use the **set security-association level per-host** command in cryp to map configuration mode. To specify that one security association should be requested for each crypto map access list **permit** entry, use the **no** form of this command.

set security-association level per-host
no set security-association level per-host

Syntax Description

This command has no arguments or keywords.

Command Default

For a given crypto map, all traffic between two IPSec peers matching a single crypto map access list **permit** entry will share the same security association.

Command Modes

Crypto map configuration

Command History

Release	Modification
11.3 T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is only available for **ipsec-isakmp** crypto map entries and is not supported for dynamic crypto map entries.

When you use this command, you need to specify that a separate security association should be used for each source/destination host pair.

Normally, within a given crypto map, IPSec will attempt to request security associations at the granularity specified by the access list entry. For example, if the access list entry permits IP protocol traffic between subnet A and subnet B, IPSec will attempt to request security associations between subnet A and subnet B (for any IP protocol), and unless finer-grained security associations are established (by a peer request), all IPSec-protected traffic between these two subnets would use the same security association.

This command causes IPSec to request separate security associations for each source/destination host pair. In this case, each host pairing (where one host was in subnet A and the other host was in subnet B) would cause IPSec to request a separate security association.

With this command, one security association would be requested to protect traffic between host A and host B, and a different security association would be requested to protect traffic between host A and host C.

The access list entry can specify local and remote subnets, or it can specify a host-and-subnet combination. If the access list entry specifies protocols and ports, these values are applied when establishing the unique security associations.

Use this command with care, as multiple streams between given subnets can rapidly consume system resources.

Examples

The following example shows what happens with an access list entry of **permit ip 10.1.1.0 0.0.0.255 10.2.2.0 0.0.0.255**and a per-host level:

- A packet from 10.1.1.1 to 10.2.2.1 will initiate a security association request, which would look like it originated via **permit ip host 10.1.1.1 host 10.2.2.1**.
- A packet from 10.1.1.1 to 10.2.2.2 will initiate a security association request, which would look like it originated via **permit ip host 10.1.1.1 host 10.2.2.2**.
- A packet from 10.1.1.2 to 10.2.2.1 will initiate a security association request, which would look like it originated via **permit ip host 10.1.1.2 host 10.2.2.1**

Without the per-host level, any of the above packets will initiate a single security association request originated via **permit ip 10.1.1.0 0.0.0.255 10.2.2.0 0.0.0.255**.

Related Commands

Command	Description
crypto dynamic-map	Creates a dynamic crypto map entry and enters the crypto map configuration command mode.
crypto map (global IPSec)	Creates or modifies a crypto map entry and enters the crypto map configuration mode.
crypto map (interface IPSec)	Applies a previously defined crypto map set to an interface.
crypto map local-address	Specifies and names an identifying interface to be used by the crypto map for IPSec traffic.
match address (IPSec)	Specifies an extended access list for a crypto map entry.
set peer (IPSec)	Specifies an IPSec peer in a crypto map entry.
set pfs	Specifies that IPSec should ask for PFS when requesting new security associations for this crypto map entry, or that IPSec requires PFS when receiving requests for new security associations.
set security-association lifetime	Overrides (for a particular crypto map entry) the global lifetime value, which is used when negotiating IPSec security associations.
set transform-set	Specifies which transform sets can be used with the crypto map entry.
show crypto map (IPSec)	Displays the crypto map configuration.

set security-association lifetime

To set the TEK lifetime for a specific crypto map entry or IPsec profile that is used when negotiating IPsec security associations (SAs), use the **set security-association lifetime** command in crypto map configuration mode or IPsec profile configuration mode. To reset a lifetime to the global value, use the **no** form of this command.

set security-association lifetime {**days** *number-of-days* | **kilobytes** {*number-of-kilobytes* | **disable**} | **seconds** *number-of-seconds*}
set security-association lifetime {**days** | **kilobytes** | **seconds**}

Syntax Description

days *number-of-days*	Lifetime in days. The range is 1 to 30.
kilobytes *number-of-kilobytes*	Volume of traffic (in kilobytes) that can pass between IPsec peers using an SA. The range is 2560 to 4294967295.
disable	Disables the SA rekey based on the traffic-volume lifetime.
seconds *number-of-seconds*	Lifetime in seconds. The range is 120 to 2592000. **Note** It is not recommended to use a lifetime value that is lower than 900 seconds in production routers.

Command Default

Global lifetime values are used.

Command Modes

Crypto map configuration (config-crypto-map)
IPsec profile configuration (ipsec-profile)

Command History

Release	Modification
11.3 T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	Support for IPv6 was added.
12.2(33)SXI	This command was modified. The **disable** keyword was added.
Cisco IOS XE Release 2.3	This command was integrated into Cisco IOS XE Release 2.3.
15.0(1)M	This command was modified. The **disable** keyword was added.
15.3(2)T	This command was modified. The **days** *number-of-days* keyword and argument pair was added, and the maximum value for the **seconds** *number-of-seconds* keyword and argument pair was extended from 86400 seconds to 2592000 seconds.

Release	Modification
Cisco IOS XE Release 3.9S	This command was integrated into Cisco IOS XE Release 3.9S.

Usage Guidelines

The TEK lifetime determines the lifetime of the SA. You enter this command on the key server (KS) or primary KS. This command sets the value for a specific crypto map entry or IPsec profile by overriding the global lifetime value. The SA and corresponding keys expire after the timed lifetime or traffic-volume lifetime is reached (whichever is first). This command is available only for **ipsec-isakmp** crypto map entries, dynamic crypto map entries, and IPsec profiles.

Note For Cisco Group Encrypted Transport (GET) VPN, you must use the command in IPsec profile configuration mode. This is because GET VPN uses the lifetime from the IPsec profile (not the crypto map).

If a specific crypto map entry or IPsec profile has lifetimes configured, when the router requests new SAs during SA negotiation, it specifies its crypto map or IPsec profile lifetime in the request to the peer; it uses this lifetime as the lifetime of the new SAs. When the router receives a negotiation request from a peer, it uses the smaller of the lifetimes proposed by the peer or by the locally configured lifetime.

A new SA is negotiated *before* the lifetime threshold of the existing SA is reached to ensure that a new SA is ready. The timed lifetime and the traffic volume lifetime each have a jitter mechanism to avoid SA rekey collisions. The new SA is negotiated either (30 plus a random number of) seconds before the **seconds** lifetime expires or when the traffic volume reaches (90 minus a random number of) the percent of the **kilobytes** lifetime (whichever occurs first).

SA rekey starts at 25 percent of the SA key's lifetime, which is earlier than the hard expiration, with a random jitter timing variation. During this time, the interval between SA soft and hard expiration should be more than 30 seconds but less than 200 seconds.

A lifetime change is not applied to existing SAs but is used in subsequent negotiations to establish SAs supported by this crypto map entry or IPsec profile. To enable the change sooner, you can clear all or part of the SA database by using the **clear crypto sa** command.

If no traffic has passed through the tunnel during the life of the SA, no new SA is negotiated when the lifetime expires. Instead, a new SA is negotiated only when IPsec sees a packet to be protected.

The lifetime values are ignored for manually established SAs (using an **ipsec-manual** crypto map entry).

Shorter lifetimes discourage a successful key recovery attack, because the attacker has less data encrypted under the same key to work with. However, shorter lifetimes need more CPU processing time.

Note For any configured lifetime longer than 24 hours, when ESP is used and the encryption algorithm is not NULL (esp-null or implicitly NULL such as with esp-gcm), the encryption algorithm must be AES-CBC (esp-aes) or AES-GCM (esp-gcm) with an AES key of 128 bits or stronger.

You should use a timed lifetime rather than a traffic-volume lifetime, because a small traffic-volume lifetime causes frequent SA rekeys. High throughput of encryption or decryption traffic can cause intermittent packet drops. The minimum traffic-volume lifetime threshold of 2560 kilobytes is *not* recommended on SAs that protect a medium-to-high throughput data link.

Disabling the traffic-volume lifetime affects only the router on which it is configured. It does not affect peer router behavior or the current router's time-based rekey. You should disable the traffic-volume lifetime when using high bandwidth (such as with 10-Gigabit Ethernet). This reduces packet loss in high traffic environments by preventing frequent rekeys when the volume lifetimes are reached.

You can also disable the traffic-volume lifetime by entering the **crypto ipsec security-association lifetime kilobytes disable** command.

On Cisco ASR 1000 Series Aggregation Services Routers, the values specified for this command in the global configuration mode might not be overridden by the values specified for this command under the IPsec profile configuration mode, unless the **shut** and **no shut** commands are specified for the values under IPsec profile. If the values are not specified under IPsec profile, then global values are applied.

Examples

The following example shows how to set the timed lifetime for a specific crypto map entry named map1 to 2700 seconds (45 minutes):

```
Device> enable
Device# configure terminal
Device(config)# crypto map map1 10 ipsec-isakmp
Device(config-crypto-map)# set security-association lifetime seconds 2700
Device(config-crypto-map)# end
```

The following example shows how to disable the traffic-volume lifetime for a specific crypto map entry named map2:

```
Device> enable
Device# configure terminal
Device(config)# crypto map map1 10 ipsec-isakmp
Device(config-crypto-map)# set security-association lifetime kilobytes disable
Device(config-crypto-map)# end
```

The following example shows how to set the timed lifetime to 3 days for an IPsec profile named profile1:

```
Device> enable
Device# configure terminal
Device(config)# crypto ipsec profile profile1
Device(ipsec-profile)# set security-association lifetime days 3
Device(ipsec-profile)# end
```

Related Commands

Command	Description
crypto dynamic-map	Creates a dynamic crypto map entry.
crypto ipsec security-association lifetime	Changes global lifetime values used when negotiating SAs.
crypto map (global IPsec)	Creates or modifies a crypto map entry.
crypto map (interface IPsec)	Applies a previously defined crypto map set to an interface.
crypto map local-address	Specifies and names an identifying interface to be used by the crypto map for IPsec traffic.
match address (IPsec)	Specifies an extended access list for a crypto map entry.

Command	Description
set peer (IPsec)	Specifies an IPsec peer in a crypto map entry.
set pfs	Specifies that IPsec should ask for PFS when requesting new SAs for this crypto map entry, or that IPsec requires PFS when receiving requests for new SAs.
set security-association level per-host	Specifies that separate SAs should be requested for each source/destination host pair.
set transform-set	Specifies the transform sets that can be used with the crypto map entry.
show crypto map (IPsec)	Displays the crypto map configuration.

set security-association replay disable

To disable anti-replay checking for a particular crypto map, dynamic crypto map, or crypto profile, use the **set security-association replay disable**command in crypto map configuration or crypto profile configuration mode. To enable anti-replay checking, use the **no** form of this command.

set security-association replay disable
no set security-association replay disable

Syntax Description

This command has no arguments or keywords.

Command Default

Anti-replay checking is enabled.

Command Modes

Crypto map configuration
Crypto profile configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(18)SXF6	This command was integrated into Cisco IOS Release 12.2(18)SXF6.

Examples

The following example shows that anti-replay checking has been disabled for the crypto map named "mymap."

```
crypto map mymap 30
set security-association replay disable
```

Related Commands

Command	Description
set security-association replay window-size	Controls the SAs that are created using the policy specified by a particular crypto map, dynamic crypto map, or crypto profile.

set security-association replay window-size

To control the security associations (SAs) that are created using the policy specified by a particular crypto map, dynamic crypto map, or crypto profile, use the **set security-association replay window-size**command in crypto map configuration or crypto profile configuration mode. To reset the crypto map to follow the global configuration that was specified by the **crypto ipsec security-association replay window-size** command, use the **no** form of this command.

set security-association replay window-size [*N*]
no set security-association replay window-size

Syntax Description

N	(Optional) Size of the window. The value can be 64, 128, 256, 512, or 1024. This value sets the window size for a particular crypto map, dynamic crypto map, or crypto profile.

Command Default

Window size is not set.

Command Modes

Crypto map configuration
Crypto profile configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(18)SXF6	This command was integrated into Cisco IOS Release 12.2(18)SXF6.

Examples

The following example shows that the SA window size has been set to 256 for the crypto map named "mymap":

```
crypto map mymap 10
set security-association replay window-size 256
```

Related Commands

Command	Description
set security-association replay disable	Disables anti-replay checking for a particular crypto map, dynamic crypto map, or crypto profile.

set security-policy limit

To define an upper limit to the number of flows that can be created for an individual virtual access interface, use the **set security-policy limit** command in IPsec profile configuration mode. To remove the limitation, use the **no** form of this command.

set security-policy limit *maximum-limit*
no set security-policy limit

Syntax Description

maximum-limit	The number of security policy entries that can be negotiated with the peer. The range is from 0 to 50000.

Command Default

The upper limit to the number of flows that can be created for an individual virtual access interface is not defined.

Command Modes

IPsec profile configuration (config-crypto-profile)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.
15.2(1)T	This command was integrated into Cisco IOS Release 15.2(1)T.

Usage Guidelines

The behavior of the **set security-policy limit** command is disabled by default. Any change to the maximum limit is applied to the existing session. If the maximum limit is set to 0, then no new IPsec security associations (SAs) are created.

Note Beginning in Cisco IOS Release 15.2(1)T, you can modify the maximum limit by using the **ipsec flow-limit** command.

Examples

The following example shows how to limit the number of flows that can be created for an individual virtual access interface to 5:

```
crypto ipsec profile ipsec-profile-1
 set security-policy limit 5
```

Related Commands

Command	Description
crypto ipsec profile	Defines the IPsec parameters that are to be used for IPsec encryption between two IPsec routers and enters IPsec profile configuration mode.
crypto isakmp profile	Defines an ISAKMP profile and IPsec user sessions.
interface virtual-template	Creates a virtual template interface that can be configured and applied dynamically when virtual access interfaces are created.

Command	Description
ipsec flow-limit	Specifies the maximum number of IPsec SAs that an IKev2 DVTI session can have on an IKev2 responder.

set session-key

To manually specify the IP Security session keys within a crypto map entry, use the **set session-key**command in crypto map configuration mode. This command is available only for **ipsec-manual** crypto map entries. To remove IPSec session keys from a crypto map entry, use the **no** form of this command.

Authentication Header (AH) Protocol Syntax
set session-key {**inbound** | **outbound**} **ah** *spi hex-key-string*
no set session-key {**inbound** | **outbound**} **ah**

Encapsulation Security Protocol (ESP) Syntax
set session-key {**inbound** | **outbound**} **esp** *spi cipher hex-key-string*
authenticator *hex-key-string*
no set session-key {**inbound** | **outbound**} **esp**

Syntax Description

inbound	Sets the inbound IPSec session key. (You must set both inbound and outbound keys.)
outbound	Sets the outbound IPSec session key. (You must set both inbound and outbound keys.)
ah	Sets the IPSec session key for the AH protocol. Use when the crypto map entry's transform set includes an AH transform.
esp	Sets the IPSec session key for ESP. Use when the crypto map entry's transform set includes an ESP transform.
spi	Specifies the security parameter index (SPI), a number that is used to uniquely identify a security association. The SPI is an arbitrary number you assign in the range of 256 to 4,294,967,295 (FFFF FFFF). You can assign the same SPI to both directions and both protocols. However, not all peers have the same flexibility in SPI assignment. For a given destination address/protocol combination, unique SPI values must be used. The destination address is that of the router if inbound, the peer if outbound.
hex-key-string	Specifies the session key; enter in hexadecimal format. This is an arbitrary hexadecimal string of 8, 16, or 20 bytes. If the crypto map's transform set includes a DES algorithm, specify at least 8 bytes per key. If the crypto map's transform set includes an MD5 algorithm, specify at least 16 bytes per key. If the crypto map's transform set includes an SHA algorithm, specify 20 bytes per key. Keys longer than the above sizes are simply truncated.
cipher	Indicates that the key string is to be used with the ESP encryption transform.
authenticator	(Optional) Indicates that the key string is to be used with the ESP authentication transform. This argument is required only when the crypto map entry's transform set includes an ESP authentication transform.

Command Default

No session keys are defined by default.

Command Modes

Crypto map configuration

Command History

Release	Modification
11.3 T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to define IPSec keys for security associations via **ipsec-manual** crypto map entries. (In the case of **ipsec-isakmp** crypto map entries, the security associations with their corresponding keys are automatically established via the IKE negotiation.)

If the crypto map's transform set includes an AH protocol, you must define IPSec keys for AH for both inbound and outbound traffic. If the crypto map's transform set includes an ESP encryption protocol, you must define IPSec keys for ESP encryption for both inbound and outbound traffic. If your transform set includes an ESP authentication protocol, you must define IPSec keys for ESP authentication for inbound and outbound traffic.

When you define multiple IPSec session keys within a single crypto map, you can assign the same security parameter index (SPI) number to all the keys. The SPI is used to identify the security association used with the crypto map. However, not all peers have the same flexibility in SPI assignment. You should coordinate SPI assignment with your peer's operator, making certain that the same SPI is not used more than once for the same destination address/protocol combination.

Security associations established via this command do not expire (unlike security associations established via IKE).

Session keys at one peer must match the session keys at the remote peer.

If you change a session key, the security association using the key will be deleted and reinitialized.

Examples

The following example shows a crypto map entry for manually established security associations. The transform set "t_set" includes only an AH protocol.

```
crypto ipsec transform-set t_set ah-sha-hmac
crypto map mymap 20 ipsec-manual
 match address 102
 set transform-set t_set
 set peer 10.0.0.21
 set session-key inbound ah 300 1111111111111111111111111111111111111111
 set session-key outbound ah 300 2222222222222222222222222222222222222222
```

The following example shows a crypto map entry for manually established security associations. The transform set "someset" includes both an AH and an ESP protocol, so session keys are configured for both AH and ESP for both inbound and outbound traffic. The transform set includes both encryption and authentication ESP transforms, so session keys are created for both using the **cipher** and **authenticator** keywords.

```
crypto ipsec transform-set someset ah-sha-hmac esp-des esp-sha-hmac
```

```
crypto map mymap 10 ipsec-manual
 match address 101
 set transform-set someset
 set peer 10.0.0.1
 set session-key inbound ah 300 9876543210987654321098765432109876543210
 set session-key outbound ah 300 fedcbafedcbafedcbafedcbafedcbafedcbafedc
 set session-key inbound esp 300 cipher 0123456789012345
  authenticator 00001111222233334444555566667777888899999
 set session-key outbound esp 300 cipher abcdefabcdefabcd
  authenticator 99998888777766665555444433332222111110000
```

Related Commands

Command	Description
crypto map (global IPSec)	Creates or modifies a crypto map entry and enters the crypto map configuration mode.
crypto map (interface IPSec)	Applies a previously defined crypto map set to an interface.
crypto map local-address	Specifies and names an identifying interface to be used by the crypto map for IPSec traffic.
match address (IPSec)	Specifies an extended access list for a crypto map entry.
set peer (IPSec)	Specifies an IPSec peer in a crypto map entry.
set transform-set	Specifies which transform sets can be used with the crypto map entry.
show crypto map (IPSec)	Displays the crypto map configuration.

set transform-set

To specify which transform sets can be used with the crypto map entry, use the **set transform-set**command in crypto map configuration mode. To remove all transform sets from a crypto map entry, use the **no** form of this command.

set transform-set *transform-set-name*
[*transform-set2...transform-set6*]
no set transform-set

Syntax Description

transform-set-name	Name of the transform set. For an **ipsec-manual** crypto map entry, you can specify only one transform set. For an **ipsec-isakmp** or dynamic crypto map entry, you can specify up to six transform sets.

Command Default

No transform sets are included by default.

Command Modes

Crypto map configuration

Command History

Release	Modification
11.3 T	This command was introduced.
12.4(4)T	Support for IPv6 was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
15.4(2)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

Usage Guidelines

This command is required for all static and dynamic crypto map entries.

Use this command to specify which transform sets to include in a crypto map entry.

For an **ipsec-isakmp** crypto map entry, you can list multiple transform sets with this command. List the higher priority transform sets first.

If the local router initiates the negotiation, the transform sets are presented to the peer in the order specified in the crypto map entry. If the peer initiates the negotiation, the local router accepts the first transform set that matches one of the transform sets specified in the crypto map entry.

The first matching transform set that is found at both peers is used for the security association. If no match is found, IPSec will not establish a security association. The traffic will be dropped because there is no security association to protect the traffic.

For an **ipsec-manual** crypto map entry, you can specify only one transform set. If the transform set does not match the transform set at the remote peer's crypto map, the two peers will fail to correctly communicate because the peers are using different rules to process the traffic.

If you want to change the list of transform sets, re-specify the new list of transform sets to replace the old list. This change is only applied to crypto map entries that reference this transform set. The change will not be applied to existing security associations, but will be used in subsequent negotiations to establish new security associations. If you want the new settings to take effect sooner, you can clear all or part of the security association database by using the **clear crypto sa** command.

Any transform sets included in a crypto map must previously have been defined using the **crypto ipsec transform-set** command.

Examples

The following example defines two transform sets and specifies that they can both be used within a crypto map entry. (This example applies only when IKE is used to establish security associations. With crypto maps used for manually established security associations, only one transform set can be included in a given crypto map entry.)

```
crypto ipsec transform-set my_t_set1 esp-des esp-sha-hmac
crypto ipsec transform-set my_t_set2 ah-sha-hmac esp-des esp-sha-hmac
crypto map mymap 10 ipsec-isakmp
 match address 101
 set transform-set my_t_set1 my_t_set2
 set peer 10.0.0.1
 set peer 10.0.0.2
```

In this example, when traffic matches access list 101, the security association can use either transform set "my_t_set1" (first priority) or "my_t_set2" (second priority) depending on which transform set matches the remote peer's transform sets.

sgbp aaa authentication

To enable a Stack Group Bidding Protocol (SGBP) authentication list, use the **sgbp aaa authentication** command in global configuration mode. To disable the SGBP authentication list, use the **no** form of this command.

sgbp aaa authentication list *list-name*
no sgbp aaa authentication list *list-name*

Syntax Description

list	*list-name*	Name of a list of methods of authentication to use.

Command Default

A SGBP authentication list is not enabled. You must use the same authentication, authorization and accounting (AAA) method list as PPP usersl.

Command Modes

Global configuration

Command History

Release	Modification
12.3(2)T	This command introduced.

Usage Guidelines

Use the **sgbp aaa authentication**command to create a list different from the AAA list that is used by PPP users.

Examples

The following example shows how to create the AAA list "SGBP" that is to be used by SGBP users:

```
Router(config)# sgbp aaa authentication list SGBP
```

Related Commands

Command	Description
aaa authentication ppp	Specifies one or more AAA authentication methods for use on serial interfaces that are running PPP.
aaa authentication sgbp	Specifies one or more AAA authentication methods for SGBP.
ppp authentication	Enables at least one PPP authentication protocol and to specifies the order in which the protocols are selected on the interface.

show (cs-server)

To display the public key infrastructure (PKI) certificate server configuration, use the **show** command in certificate server configuration mode.

show

Syntax Description

This command has no arguments or keywords.

Command Modes

Certificate server configuration (cs-server)

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

You must configure the **crypto pki server** command with the name of the certificate server in order to enter certificate server configuration mode and configure this command.

Related Commands

Command	Description
auto-rollover	Enables the automated CA certificate rollover functionality.
cdp-url	Specifies a CDP to be used in certificates that are issued by the certificate server.
crl (cs-server)	Specifies the CRL PKI CS.
crypto pki server	Enables a CS and enters certificate server configuration mode, or immediately generates shadow CA credentials
database archive	Specifies the CA certificate and CA key archive format--and the password--to encrypt this CA certificate and CA key archive file.
database level	Controls what type of data is stored in the certificate enrollment database.
database url	Specifies the location where database entries for the CS is stored or published.

Command	Description
database username	Specifies the requirement of a username or password to be issued when accessing the primary database location.
default (cs-server)	Resets the value of the CS configuration command to its default.
grant auto rollover	Enables automatic granting of certificate reenrollment requests for a Cisco IOS subordinate CA server or RA mode CA.
grant auto trustpoint	Specifies the CA trustpoint of another vendor from which the Cisco IOS certificate server automatically grants certificate enrollment requests.
grant none	Specifies all certificate requests to be rejected.
grant ra-auto	Specifies that all enrollment requests from an RA be granted automatically.
hash (cs-server)	Specifies the cryptographic hash function the Cisco IOS certificate server uses to sign certificates issued by the CA.
issuer-name	Specifies the DN as the CA issuer name for the CS.
lifetime (cs-server)	Specifies the lifetime of the CA or a certificate.
mode ra	Enters the PKI server into RA certificate server mode.
mode sub-cs	Enters the PKI server into sub-certificate server mode
redundancy (cs-server)	Specifies that the active CS is synchronized to the standby CS.
serial-number (cs-server)	Specifies whether the router serial number should be included in the certificate request.

Command	Description
shutdown (cs-server)	Allows a CS to be disabled without removing the configuration.

show (ca-trustpool)

To display the public key infrastructure (PKI) trustpool policy of the router, use the **show** command in ca-trustpool configuration mode.

show

Syntax Description

This command has no arguments or keywords.

Command Modes

Ca-trustpool configuration (ca-trustpool)

Command History

Release	Modification
15.2(2)T	This command was introduced.
15.1(1)SY	This command was integrated into Cisco IOS 15.1(1)SY.

Usage Guidelines

Before you can use this command, you must enable the **crypto pki trustpool policy** command, which enters ca-trustpool configuration mode.

Examples

```
Router(config)# crypto pki trustpool policy
Router(ca-trustpool)# show

 Chain validation will stop at the first CA certificate in the pool
   Trustpool CA certificates will expire 12:58:31 PST Apr 5 2012
   Trustpool policy revocation order:      crl
   Certficate matching is disabled
   Policy Overrides:
```

Related Commands

Command	Description
cabundle url	Configures the URL from which the PKI trustpool CA bundle is downloaded.
chain-validation	Enables chain validation from the peer's certificate to the root CA certificate in the PKI trustpool.
crl	Specifes the CRL query and cache options for the PKI trustpool.
crypto pki trustpool import	Manually imports (downloads) the CA bundle into the PKI trustpool to update or replace the existing CA bundle.
crypto pki trustpool policy	Configures PKI trustpool policy parameters.

Command	Description
default	Resets the value of a ca-trustpool configuration command to its default.
match	Enables the use of certificate maps for the PKI trustpool.
ocsp	Specifies OCSP settings for the PKI trustpool.
revocation-check	Disables revocation checking when the PKI trustpool policy is being used.
show crypto pki trustpool	Displays the PKI trustpool certificates of the router and optionally shows the PKI trustpool policy.
source interface	Specifies the source interface to be used for CRL retrieval, OCSP status, or the downloading of a CA certificate bundle for the PKI trustpool.
storage	Specifies a file system location where PKI trustpool certificates are stored on the router.
vrf	Specifies the VRF instance to be used for CRL retrieval.

show aaa attributes

To display the mapping between an authentication, authorization, and accounting (AAA) attribute number and the corresponding AAA attribute name, use the **show aaa attributes** command in EXEC configuration mode.

show aaa attributes [**protocol radius**]

Syntax Description

protocol radius	(Optional) Displays the mapping between a RADIUS attribute and a AAA attribute name and number.

Command Modes

EXEC

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(11)T	The **protocol radius**keyword was added.
12.3(14)T	T.38 fax relay call statistics were made available to Call Detail Records (CDRs) through Vendor-Specific Attributes (VSAs) and added to the call log.

Examples

The following example is sample output for the **show aaa attributes**command. In this example, all RADIUS attributes that have been enabled are displayed.

```
Router# show aaa attributes protocol radius
AAA ATTRIBUTE LIST:
    Type=1     Name=disc-cause-ext                Format=Enum
        Protocol:RADIUS
        Non-Standard  Type=195   Name=Ascend-Disconnect-Cau Format=Enum
        Cisco VSA     Type=1     Name=Cisco AVpair          Format=String
    Type=2     Name=Acct-Status-Type              Format=Enum
        Protocol:RADIUS
        IETF          Type=40    Name=Acct-Status-Type      Format=Enum
    Type=3     Name=acl                           Format=Ulong
        Protocol:RADIUS
        IETF          Type=11    Name=Filter-Id             Format=Binary
    Type=4     Name=addr                          Format=IPv4 Address
        Protocol:RADIUS
        IETF          Type=8     Name=Framed-IP-Address     Format=IPv4 Addre
    Type=5     Name=addr-pool                     Format=String
        Protocol:RADIUS
        Non-Standard  Type=218   Name=Ascend-IP-Pool        Format=Ulong
    Type=6     Name=asyncmap                      Format=Ulong
        Protocol:RADIUS
        Non-Standard  Type=212   Name=Ascend-Asyncmap       Format=Ulong
    Type=7     Name=Authentic                     Format=Enum
        Protocol:RADIUS
        IETF          Type=45    Name=Authentic             Format=Enum
    Type=8     Name=autocmd                       Format=String
```

The following example is sample output for the **show aaa attributes**command. In this example, all the T.38 fax relay statistics are displayed.

```
Router# show aaa attributes
!
 Type=485   Name=originating-line-info          Format=Ulong
    Type=486   Name=charge-number                  Format=String
    Type=487   Name=transmission-medium-req        Format=Ulong
    Type=488   Name=redirecting-number             Format=String
    Type=489   Name=backward-call-indicators       Format=String
    Type=490   Name=remote-media-udp-port          Format=Ulong
    Type=491   Name=remote-media-id                Format=String
    Type=492   Name=supp-svc-xfer-by               Format=String
    Type=493   Name=faxrelay-start-time            Format=String
    Type=494   Name=faxrelay-max-jit-buf-depth     Format=String
    Type=495   Name=faxrelay-jit-buf-ovflow        Format=String
    Type=496   Name=faxrelay-mr-hs-mod             Format=String
    Type=497   Name=faxrelay-init-hs-mod           Format=String
    Type=498   Name=faxrelay-num-pages             Format=String
    Type=499   Name=faxrelay-direction             Format=String
    Type=500   Name=faxrelay-ecm-in-use            Format=String
    Type=501   Name=faxrelay-encap-prot            Format=String
    Type=502   Name=faxrelay-nsf-country-code      Format=String
    Type=503   Name=faxrelay-nsf-manuf-code        Format=String
    Type=504   Name=faxrelay-fax-success           Format=String
    Type=505   Name=faxrelay-tx-packets            Format=String
    Type=506   Name=faxrelay-rx-packets            Format=String
```

The table below provides an alphabetical listing of the fields displayed in the output of the **show aaa attributes**command displaying T.38 statistics and a description of each field.

Table 1: show aaa attributes Field Descriptions

Field	Description
Format=Ulong	Format type is ULong.
Format=String	Format type is string.
Name=backward-call-indicators	Backward call indicator.
Name=charge-number	Charge number.
Name=faxrelay-direction	Direction of fax relay.
Name=faxrelay-ecm-in-use	Error correction mode in use for the fax relay.
Name=faxrelay-encap-prot	Encapsulation protocol for fax relay.
Name=faxrelay-fax-success	Fax relay success.
Name=faxrelay-init-hs-mod	Fax relay initial high-speed modulation.
Name=faxrelay-jit-buf-ovflow	Fax relay jitter buffer overflow.
Name=faxrelay-max-jit-buf-depth	Fax relay maximum jitter buffer depth.
Name=faxrelay-mr-hs-mod	Fax relay most recent high speed modulation.

Field	Description
Name=faxrelay-num-pages	Fax relay number of fax pages.
Name=faxrelay-nsf-country-code	Fax relay Nonstandard Facilities (NSF) country code.
Name=faxrelay-nsf-manuf-code	Fax relay NSF manufacturers code.
Name=faxrelay-rx-packets	Fax relay received packets
Name=faxrelay-start-time	Fax relay start time.
Name=faxrelay-tx-packets	Fax relay transmitted packets.
Name=originating-line-info	Originating line information.
Name=redirecting-number	Redirecting number.
Name=remote-media-id	Remote media ID.
Name=remote-media-udp-port	Remote media UDP port.
Name=supp-svc-xfer-by	Supplementary service transfer.
Name=transmission-medium-req	Transmission medium requirement.
Type=	Type of fax relay string.

Related Commands

Command	Description
debug voip aaa	Enables debugging messages for gateway authentication, authorization, and accounting (AAA) to be sent to the system console.

show aaa cache filterserver

To display the cache status, use the **show aaa cache filterserver** command in user EXEC or privileged EXEC mode.

show aaa cache filterserver {**acl** | **pending**}

Syntax Description

acl	Shows the contents of the access control cache at the last refresh.
pending	Shows the contents of the pending call cache, which references filters that have not received a response from the RADIUS server.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.4T	The **acl** and **pending** keywords were added.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

The **show aaa cache filterserver** command shows how many times a particular filter has been referenced or refreshed. This function may be used in administration to determine which filters are actually being used.

Examples

The following is sample output for the **show aaa cache filterserver** command using the **acl** and **pending**keywords:

```
Router# show aaa cache filterserver acl
Filter     Server          Age Expires Refresh Access-Control-Lists
-------------------------------------------------------------------------------
aol        10.2.3.4          0    1440     100 ip in icmp drop
                                               ip out icmp drop
                                               ip out forward tcp dstip 10.2.3.4
msn        10.2.3.4        N/A   Never       2 ip in tcp drop
msn2       10.2.3.4        N/A   Never       2 ip in tcp drop
vone       10.2.3.4        N/A   Never       0 ip in tcp drop
```

The following is sample output for the **show aaa cache filterserver** command using the **pending** keyword:

```
Router# show aaa cache filterserver pending

AAA pending cache:
Filter Age Expires Refresh
-------------------------------------------------------------------------------
myfilter N/A Never N/A call 0x501802D8 (00000085)
```

The table below describes the significant fields shown in the display.

Table 2: show aaa cache filterserver Field Descriptions

Field	Description
Filter	Filter name
Server	RADIUS server IP address
Age	When to expire a cache entry (in minutes)
Expires	Number of minutes in which a cache entry will expire
Refresh	Number of times a cache has been refreshed
Access-Control-Lists	Access control list (ACL) of the server

Related Commands

Command	Description
aaa authorization cache filterserver	Enables AAA authorization caches and the downloading of ACL configurations from a RADIUS filter server.

show aaa cache group

To display all the cache entries stored by the authentication, authorization, and accounting (AAA) cache, use the **show aaa cache group**command in privileged EXEC mode.

show aaa cache group *name* {**all** | **profile** *name*}

Syntax Description

name	Text string representing a cache server group.
all	Displays all server group profile details.
profile *name*	Displays the specified individual server group profile details.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.
Cisco IOS XE Release 2.3	This command was integrated into Cisco IOS XE Release 2.3.

Usage Guidelines

Use the **show aaa cache group** command to display all cache entries for a specific group.

Examples

The following example shows how to display all cache entries for a group. The fields are self-explanatory.

```
Router# show aaa cache group sg1
-----------------------------------------------------------
 Entries in Profile dB SG1 for exact match
-----------------------------------------------------------
Profile: .*user*
Updated: 00:00:33
Parse User: Y
Authen User: Y
     6462F2F0 0 00000001 service-type(253) 4 2
     6462F304 0 00000001 Framed-Protocol(66) 4 1
     6462F318 0 00000009 policy-directive(339) 29 apply service internet_bronze
Profile: .*internet*
Updated: 00:00:33
Parse User: Y
Authen User: Y
     64630088 0 00000001 service-type(253) 4 5
     6463009C 0 00000009 ssg-service-info(350) 16 IBronze Internet
```

```
     646300B0 0 00000001 timeout(313) 4 90(5A)
-------------------------------------------------------------
 Entries in Profile dB SG1 for regexp match
-------------------------------------------------------------
Profile: .*internet*,
Updated: 00:00:33
Parse User: Y
Authen User: Y
     64630088 0 00000001 service-type(253) 4 5
     6463009C 0 00000009 ssg-service-info(350) 16 IBronze Internet
     646300B0 0 00000001 timeout(313) 4 90(5A)
Profile: .*user*,
Updated: 00:00:34
Parse User: Y
Authen User: Y
     6462F2F0 0 00000001 service-type(253) 4 2
     6462F304 0 00000001 Framed-Protocol(66) 4 1
     6462F318 0 00000009 policy-directive(339) 29 apply service internet_bronze
```

Related Commands

Command	Description
clear aaa cache group	Clears individual entries or all entries in the cache.
debug aaa cache group	Debugs the caching mechanism and ensures that entries are being cached from AAA server responses and are being found when queried.

show aaa common-criteria policy

To display the common criteria security policy details, use the **show aaa common-criteria policy** command in privileged EXEC mode.

show aaa common-criteria policy {**name** *policy-name* | **all**}

Syntax Description

name *policy-name*	Specifies the password security details for a specific policy.
all	Specifies the password security details for all configured policies.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(2)SE	This command was introduced.

Usage Guidelines

Use the **show aaa common-criteria policy** command to display the security policy details for a specific policy or for all configured policies.

Examples

The following is sample output from the **show aaa common-criteria policy** command:

```
Device# show aaa common-criteria policy name policy1

Policy name: policy1
Minimum length: 1
Maximum length: 64
Upper Count: 20
Lower Count: 20
Numeric Count: 5
Special Count: 2
Number of character changes 4
Valid forever. User tied to this policy will not expire.
```

The following is sample output from the **show aaa common-criteria policy all** command:

```
Device# show aaa common-criteria policy all
==========================================================

Policy name: policy1
Minimum length: 1
Maximum length: 64
Upper Count: 20
Lower Count: 20
Numeric Count: 5
Special Count: 2
Number of character changes 4
Valid forever. User tied to this policy will not expire.
==========================================================
Policy name: policy2
Minimum length: 1
```

```
Maximum length: 34
Upper Count: 10
Lower Count: 5
Numeric Count: 4
Special Count: 2
Number of character changes 4
Valid forever. User tied to this policy will not expire.
=========================================================
```

The following table describes the significant fields shown in the display.

Table 3: show aaa common-criteria policy all Field Descriptions

Field	Description
Policy name	Name of the configured security policy.
Minimum length	Minimum length of the password.
Maximum length	Maximum length of the password.
Upper Count	Number of uppercase characters.
Lower Count	Number of lowercase characters.
Numeric Count	Number of numeric characters.
Special Count	Number of special characters.
Number of character changes	Number of changed characters between old and new passwords.

Related Commands

Command	Description
aaa common-criteria policy	Configures an authentication, authorization, and accounting (AAA) common criteria security policy.
debug aaa common-criteria	Enables debugging for AAA common criteria password security policies.

show aaa dead-criteria

To display dead-criteria detection information for an authentication, authorization, and accounting (AAA) server, use the **show aaa dead-criteria** command in privileged EXEC mode.

show aaa dead-criteria {**security-protocol** *ip-address*} [**auth-port** *port-number*] [**acct-port** *port-number*][*server-group-name*]

Syntax Description

security-protocol	Security protocol of the specified AAA server. Currently, the only protocol that is supported is RADIUS.
ip-address	IP address of the specified AAA server.
auth-port	(Optional) Authentication port for the RADIUS server that was specified.
port-number	(Optional) Number of the authentication port. The default is 1645 (for a RADIUS server).
acct-port	(Optional) Accounting port for the RADIUS server that was specified.
port-number	(Optional) Number of the accounting port. The default is 1646 (for a RADIUS server).
server-group-name	(Optional) Server group with which the specified server is associated. The default is "radius" (for a RADIUS server).

Command Default

Currently, the *port-number* argument for the **auth-port** keyword and the *port-number* argument for the **acct-port** keyword default to 1645 and 1646, respectively. The default for the *server-group-name* argument is radius.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(6)	This command was introduced.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.

Usage Guidelines

Multiple RADIUS servers having the same IP address can be configured on a router. The **auth-port** and **acct-port** keywords are used to differentiate the servers. The dead-detect interval of a server that is associated with a specified server group can be obtained by using the **server-group-name** keyword. (The dead-detect interval and retransmit values of a RADIUS server are set on the basis of the server group to which the server belongs. The same server can be part of multiple server groups.)

Examples

The following example shows that dead-criteria-detection information has been requested for a RADIUS server at the IP address 172.19.192.80:

```
Router# show aaa dead-criteria radius 172.19.192.80 radius
RADIUS Server Dead Critieria:
```

```
============================
Server Details:
    Address : 172.19.192.80
    Auth Port : 1645
    Acct Port : 1646
Server Group : radius
Dead Criteria Details:
    Configured Retransmits : 62
    Configured Timeout : 27
    Estimated Outstanding Transactions: 5
    Dead Detect Time : 25s
    Computed Retransmit Tries: 22
    Statistics Gathered Since Last Successful Transaction
=====================================================
Max Computed Outstanding Transactions: 5
Max Computed Dead Detect Time: 25s
Max Computed Retransmits : 22
```

The "Max Computed Dead Detect Time" is displayed in seconds. The other fields shown in the display are self-explanatory.

Related Commands

Command	Description
debug aaa dead-criteria transactions	Displays AAA dead-criteria transaction values.
radius-server dead-criteria	Forces one or both of the criteria--used to mark a RADIUS server as dead--to be the indicated constant.
show aaa server-private	Displays the status of all private RADIUS servers.
show aaa servers	Displays information about the number of packets sent to and received from AAA servers.

show aaa local user lockout

To display a list of all locked-out users, use the **show aaa local user lockout**command in privileged EXEC mode.

show aaa local user lockout

Syntax Description

This command has no arguments or keywords.

Command Default

Names of locked-out users are not displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

This command can be used only by users having root privilege.

Examples

The following output of the **show aaa local user lockout** command illustrates that user1 is locked out:

```
Router# show aaa local user lockout
               Local-user          Lock time
               user1                  04:28:49 UTC Sat Jun 19 2004
The fields in the output example are self-explanatory.
```

Related Commands

Command	Description
aaa local authentication attempts max-fail	Specifies the maximum number of unsuccessful authentication attempts before a user is locked out.
clear aaa local user fail-attempts	Clears the unsuccessful login attempts of a user.
clear aaa local user lockout	Unlocks the locked-out user.

show aaa memory

To display the output of the AAA data structure memory tracing information, use the **show aaa memory** command in user EXEC or privileged EXEC mode.

Note The command may cause high load on the device.

show aaa memory [{**detailed** [**component** [**line**]] | **stats** {**all** | **attr_list** | **cursor** | **event** | **request** | **summary**}}]

Syntax Description

detailed	(Optional) Displays information about the status of various AAA data structures actively used by AAA clients and statistics of data structure usage.
component	(Optional) Displays information about a specified component.
line	(Optional) Displays the substring to match in the component name.
stats	(Optional) Displays data-structure memory statistics.
all	(Optional) Displays memory statistics.
attr_list	(Optional) Displays the attribute list usage statistics.
cursor	(Optional) Displays the cursor usage statistics.
event	(Optional) Displays the event usage statistics.
request	(Optional) Displays the request usage statistics.
summary	(Optional) Displays the data-structure usage summary.

Command Modes

User EXEC (>)
Privileged EXEC (#

Command History

Release	Modification
12.4(24)T	This command was introduced in a release earlier than IOS Release 12.4(24)T.
12.2(33)SXI	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI. The **stats** keyword is not supported in this release.
12.2(33)SRC	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRC. The **stats** keyword is not supported in this release.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

Use the **show aaa memory** to display the status of various AAA data structures actively used by AAA clients and statistics of data structure usage.

Examples

The following is sample output from the **show aaa memory detailed**command:

```
Router# show aaa memory detailed
AAA (accounting)             In-use Asked-For/Allocated Count  Size  Cfg/Max
  ------------------------------------------------------------------------------
  aaa_acct_rec            :        --        --/--            --    72   --/--
  aaa_acct_rec_node       :        --        --/--            --    24   --/--
  AAA (attribute)              In-use Asked-For/Allocated Count  Size  Cfg/Max
  ------------------------------------------------------------------------------
  aaa_attr                :        --        --/--            --    16   --/--
  aaa_attr_list           :        --        --/--            --    20   --/--
  AAA (database)               In-use Asked-For/Allocated Count  Size  Cfg/Max
  ------------------------------------------------------------------------------
  hash_elt                :        --        --/--            --    64   --/--
  aaa_acct_db             :        --        --/--            --   160   --/--
  aaa_db_elt_chunk        :       128     61568/912           2    64 2048/0
  aaa_uid_hash_table_str  :      4096      4096/4148          1  4096   --/--
  Total                   :      4224     65664/5060          3    --   --/--
  AAA (misc)                   In-use Asked-For/Allocated Count  Size  Cfg/Max
  ------------------------------------------------------------------------------
  aaa_interface           :        --        --/--            --   280   --/--
  aaa_idb_name            :        --        --/--            --   232   --/--
  aaa_general_db          :        --        --/--            --   644   --/--
  aaa_chunks              :        --         0/0             --    28  200/0
  aaa_interface_struct    :       560       560/664           2   280   --/--
  Total                   :       560       560/664           2    --   --/--
  RADIUS                       In-use Asked-For/Allocated Count  Size  Cfg/Max
  ------------------------------------------------------------------------------
  Total allocated: 0.004 Mb, 5 Kb, 5724 bytes
AAA Low Memory Statistics:

_____________________________
  Authentication low-memory threshold      : 3%
  Accounting low-memory threshold          : 2%
  AAA Unique ID Failure                    : 0
  Local server  Packet dropped             : 0
  CoA  Packet dropped                      : 0
  PoD  Packet dropped                      : 0
```

The following is sample output from the **show aaa memory stats all**command:

```
Router# show aaa memory stats all
AAA Memory trace summary:
-------------------------------------------------------------------------------------
TYPE           mallocs        frees        failures        active      max-usage
-------------------------------------------------------------------------------------
AAA_ATTR_L          41           40               0             1              6
AAA_CURSOR          88           88               0             0              2
AAA_EVENT            5            5               0             0              1
AAA_REQUES           2            2               0             0              1
-------------------------------------------------------------------------------------
AAA_ATTR_LIST data-structure active allocations trace:
-----------------------------------------------------------------
  Allocator-PC            AAA API                 Active Mallocs
-----------------------------------------------------------------
 0x01956360     aaa_attr_list_alloc                        1
-----------------------------------------------------------------
AAA_CURSOR data-structure active allocations trace:
-----------------------------------------------------------------
```

```
  Allocator-PC            AAA API                 Active Mallocs
-----------------------------------------------------------------
-----------------------------------------------------------------
AAA_EVENT data-structure active allocations trace:
-----------------------------------------------------------------
  Allocator-PC            AAA API                 Active Mallocs
-----------------------------------------------------------------
-----------------------------------------------------------------
AAA_REQUEST data-structure active allocations trace:
-----------------------------------------------------------------
  Allocator-PC            AAA API                 Active Mallocs
-----------------------------------------------------------------
-----------------------------------------------------------------
```

The table below describes the significant fields in the display.

Table 4: show aaa memory stats all Field Descriptions

Field	Description
TYPE	AAA data structure type.
mallocs	Total number of data structures allocated.
frees	Total number of data structures freed.
failures	Total number of data structure allocations failed.
active	Total number of actively used data structures.
max-usage	Maximum number of active allocations of data structure at any point.

The following is sample output from the **show aaa memory stats**with the **attr_list**keyword:

```
Router# show aaa memory stats attr_list
AAA_ATTR_LIST data-structure active allocations trace:
-----------------------------------------------------------------
  Allocator-PC            AAA API                 Active Mallocs
-----------------------------------------------------------------
 0x01956360     aaa_attr_list_alloc                        1
-----------------------------------------------------------------
```

The table below describes the significant fields in the display.

Table 5: show aaa memory stats attr_list Field Descriptions

Field	Description
Allocator-PC	AAA client that allocated a active data structure
AAA API	AAA API called by the client for an actively allocated data structure.
Active Mallocs	Number of active allocations from a client PC.

The following is sample output from the **show aaa memory stats cursor**command:

```
Router# show aaa memory stats cursor
AAA_CURSOR data-structure active allocations trace:
-----------------------------------------------------------------
```

```
  Allocator-PC            AAA API                 Active Mallocs
-----------------------------------------------------------------
```

The following is sample output from the **show aaa memory stats event**command:

```
Router# show aaa memory stats event
AAA_EVENT data-structure active allocations trace:
-----------------------------------------------------------------
  Allocator-PC            AAA API                 Active Mallocs
-----------------------------------------------------------------
-----------------------------------------------------------------
```

The following is sample output from the **show aaa memory stats request**command:

```
Router# show aaa memory stats request
AAA_REQUEST data-structure active allocations trace:
-----------------------------------------------------------------
  Allocator-PC            AAA API                 Active Mallocs
-----------------------------------------------------------------
-----------------------------------------------------------------
```

show aaa method-lists

To display all the named method lists defined in the authentication, authorization, and accounting (AAA) subsystem, use the **show aaa method-lists**command in user EXEC or privileged EXEC mode.

show aaa method-lists {**accounting** | **all** | **authentication** | **authorization**}

Syntax Description

accounting	Displays method lists defined for accounting services.
all	Displays method lists defined for all services.
authentication	Displays method lists defined for authentication services.
authorization	Displays method lists defined for authorization services.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Examples

The following example shows how to display method lists for the accounting services:

```
Router# show aaa method-lists accounting

acct queue=AAA_ML_ACCT_SHELL
name=Permanent None valid=TRUE id=0 Action=NOT_SET :state=ALIVE
acct queue=AAA_ML_ACCT_AUTH_PROXY
  name=default valid=TRUE id=0 Action=START STOP :state=DEAD : SERVER_GROUP tac+
acct queue=AAA_ML_ACCT_NET
  name=methodtest valid=TRUE id=BA000002 Action=START STOP :state=DEAD :
  name=tunnel valid=TRUE id=48000003 Action=START STOP :state=DEAD : SERVER_GROs
  name=session valid=TRUE id=5C000004 Action=START STOP :state=DEAD : SERVER_GRs
acct queue=AAA_ML_ACCT_CONN
acct queue=AAA_ML_ACCT_SYSTEM
  name= valid=TRUE id=82000005 Action=START STOP :state=DEAD : SERVER_GROUP rads
acct queue=AAA_ML_ACCT_RESOURCE
acct queue=AAA_ML_ACCT_RM
permanent lists
The table below describes the significant fields shown in the display.
```

Table 6: show aaa method-lists accounting Field Descriptions

Field	Description
acct queue	Specifies the type of service for which the method lists are defined.
name	Name of the method list for the specified AAA service.
valid	Identifies the validity of the method-lists.
id	A unique identifier for the specified AAA method list.
Action	Specifies the type of action to be performed on accounting records. One of the following types of actions is displayed: Start-stop, Stop-only or None.
state	Describes the current state of the AAA server. There are two possible states: • DEAD--Indicates that the server is currently presumed dead and, in the case of failovers, this server will be skipped unless it is the last server in the group. • ALIVE--Indicates that the server is currently considered alive and attempts will be made to communicate with it.
SERVER_GROUP	Name of the server group, RADIUS hosts or TACTACS+ hosts.

The following example shows how to display method lists for authentication services.

The table below describes the significant fields shown in the display.

```
Router# show aaa method-lists authentication

authen queue=AAA_ML_AUTHEN_LOGIN
  name=default valid=TRUE id=0 :state=DEAD : SERVER_GROUP radius
authen queue=AAA_ML_AUTHEN_ENABLE
  name=default valid=TRUE id=0 :state=ALIVE : SERVER_GROUP tacacs+ ENABLE  NONE
authen queue=AAA_ML_AUTHEN_PPP
authen queue=AAA_ML_AUTHEN_SGBP
authen queue=AAA_ML_AUTHEN_ARAP
  name=default valid=TRUE id=0 :state=DEAD : SERVER_GROUP tacacs+
  name=MIS-access valid=TRUE id=FF000006 :state=DEAD : SERVER_GROUP tacacs+
authen queue=AAA_ML_AUTHEN_DOT1X
  name=default valid=TRUE id=0 :state=DEAD : SERVER_GROUP radius
authen queue=AAA_ML_AUTHEN_EAPOUDP
  name=default valid=TRUE id=0 :state=ALIVE : ENABLE  SERVER_GROUP radius
authen queue=AAA_ML_AUTHEN_8021X
permanent lists
  name=Permanent Enable None valid=TRUE id=0 :state=ALIVE : ENABLE  NONE
  name=Permanent Enable valid=TRUE id=0 :state=ALIVE : ENABLE
  name=Permanent None valid=TRUE id=0 :state=ALIVE : NONE
  name=Permanent Local valid=TRUE id=0 :state=ALIVE : LOCAL
```

The following example shows how to display method lists for authorization services. The table below describes the significant fields shown in the display.

```
Router# show aaa method-lists authorization

author queue=AAA_ML_AUTHOR_SHELL
author queue=AAA_ML_AUTHOR_NET
  name=method1 valid=TRUE id=12000001 :state=ALIVE : NONE
```

```
  name=mygroup valid=TRUE id=6D000007 :state=ALIVE : SERVER_GROUP radius LOCAL
  name=list11 valid=TRUE id=6C000009 :state=DEAD : SERVER_GROUP radius
author queue=AAA_ML_AUTHOR_CONN
  name=default valid=TRUE id=0 :state=ALIVE : SERVER_GROUP tacacs+
author queue=AAA_ML_AUTHOR_IPMOBILE
author queue=AAA_ML_AUTHOR_RM
author queue=AAA_ML_AUTHOR_CONFIG
author queue=AAA_ML_AUTHOR_AUTH_PROXY
  name=default valid=TRUE id=0 :state=ALIVE : SERVER_GROUP tacacs+
author queue=AAA_ML_AUTHOR_PREAUTH
author queue=AAA_ML_AUTHOR_FLTSV
  name=default valid=TRUE id=0 :state=DEAD : SERVER_GROUP grp1
name=group valid=TRUE id=48000008 :state=ALIVE : SERVER_GROUP tacacs+ NONE
permanent lists
  name=local-list valid=TRUE id=0 :state=ALIVE : LOCAL
```

The following example shows how to display method lists for all the services. The table below describes the significant fields shown in the display.

```
Router# show aaa method-lists all

authen queue=AAA_ML_AUTHEN_LOGIN
  name=default valid=TRUE id=0 :state=ALIVE : SERVER_GROUP tacacs+
authen queue=AAA_ML_AUTHEN_ENABLE
  name=default valid=TRUE id=0 :state=ALIVE : SERVER_GROUP tacacs+ ENABLE  NONE
authen queue=AAA_ML_AUTHEN_PPP
authen queue=AAA_ML_AUTHEN_SGBP
authen queue=AAA_ML_AUTHEN_ARAP
  name=default valid=TRUE id=0 :state=ALIVE : SERVER_GROUP tacacs+
  name=MIS-access valid=TRUE id=FF000006 :state=ALIVE : SERVER_GROUP tacacs+
authen queue=AAA_ML_AUTHEN_DOT1X
  name=default valid=TRUE id=0 :state=DEAD : SERVER_GROUP radius
authen queue=AAA_ML_AUTHEN_EAPOUDP
  name=default valid=TRUE id=0 :state=ALIVE : ENABLE  SERVER_GROUP radius
authen queue=AAA_ML_AUTHEN_8021X
permanent lists
  name=Permanent Enable None valid=TRUE id=0 :state=ALIVE : ENABLE  NONE
  name=Permanent Enable valid=TRUE id=0 :state=ALIVE : ENABLE
  name=Permanent None valid=TRUE id=0 :state=ALIVE : NONE
  name=Permanent Local valid=TRUE id=0 :state=ALIVE : LOCAL
author queue=AAA_ML_AUTHOR_SHELL
author queue=AAA_ML_AUTHOR_NET
  name=method1 valid=TRUE id=12000001 :state=ALIVE : NONE
  name=mygroup valid=TRUE id=6D000007 :state=ALIVE : SERVER_GROUP radius LOCAL
  name=list11 valid=TRUE id=6C000009 :state=DEAD : SERVER_GROUP radius
author queue=AAA_ML_AUTHOR_CONN
  name=default valid=TRUE id=0 :state=ALIVE : SERVER_GROUP tacacs+
author queue=AAA_ML_AUTHOR_IPMOBILE
author queue=AAA_ML_AUTHOR_RM
author queue=AAA_ML_AUTHOR_CONFIG
author queue=AAA_ML_AUTHOR_AUTH_PROXY
  name=default valid=TRUE id=0 :state=ALIVE : SERVER_GROUP tacacs+
author queue=AAA_ML_AUTHOR_PREAUTH
author queue=AAA_ML_AUTHOR_FLTSV
  name=default valid=TRUE id=0 :state=DEAD : SERVER_GROUP grp1
name=group valid=TRUE id=48000008 :state=ALIVE : SERVER_GROUP tacacs+ NONE
permanent lists
  name=local-list valid=TRUE id=0 :state=ALIVE : LOCAL
acct queue=AAA_ML_ACCT_SHELL
acct queue=AAA_ML_ACCT_AUTH_PROXY
  name=default valid=TRUE id=0 Action=START STOP :state=ALIVE : SERVER_GROUP ta+
acct queue=AAA_ML_ACCT_NET
  name=methodtest valid=TRUE id=BA000002 Action=START STOP :state=DEAD :
```

```
  name=tunnel valid=TRUE id=48000003 Action=START STOP :state=DEAD : SERVER_GROs
  name=session valid=TRUE id=5C000004 Action=START STOP :state=DEAD : SERVER_GRs
acct queue=AAA_ML_ACCT_CONN
acct queue=AAA_ML_ACCT_SYSTEM
  name= valid=TRUE id=82000005 Action=START STOP :state=DEAD : SERVER_GROUP rads
acct queue=AAA_ML_ACCT_RESOURCE
acct queue=AAA_ML_ACCT_RM
permanent lists
  name=Permanent None valid=TRUE id=0 Action=NOT_SET :state=ALIVE
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security purposes when you use RADIUS or TACACS+.
aaa authentication arap	Enables a AAA authentication method for ARA.
aaa authorization	Sets parameters that restricts user access to a network.

show aaa service-profiles

To display the service profiles downloaded and stored by an authentication, authorization, and accounting (AAA) session, use the **show aaa service-profiles**command in user EXEC or privileged EXEC mode.

show aaa service-profiles

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
15.0(1)S	This command was introduced.

Examples

The following is sample output from the **show aaa service-profiles**command. The field description is self-explantory.

```
Router# show aaa service-profiles
Service Name: example.com
```

Related Commands

Command	Description
aaa service-profiles	Configures the service profile parameters for a AAA session.

show aaa servers

To display the status and number of packets that are sent to and received from all public and private authentication, authorization, and accounting (AAA) RADIUS servers as interpreted by the AAA Server MIB, use the **show aaa servers** command in user EXEC or privileged EXEC mode.

show aaa servers [{**private** | **public**}]

Syntax Description

private	(Optional) Displays private AAA servers only, which are also displayed by the AAA Server MIB.
public	(Optional) Displays public AAA servers only, which are also displayed by the AAA Server MIB.

Command Modes

User EXEC (>)
privileged EXEC (#)

Command History

Release	Modification
12.2(6)T	This command was introduced.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
15.1(1)S	This command was modified. Support for private RADIUS servers in CISCO-AAA-SERVER-MIB was added.
15.1(4)M	This command was modified. Support for private RADIUS servers in CISCO-AAA-SERVER-MIB was added.
15.2(4)S1	This command was modified. Support for displaying the estimated outstanding and throttled transactions (access and accounting) in the command output was added.

Usage Guidelines

Only RADIUS servers are supported by the **show aaa servers** command.

The command displays information about packets sent and received for all AAA transaction types--authentication, authorization, and accounting.

Examples

The following is sample output from the **show aaa servers private** command. Only the first four lines of the display pertain to the status of private RADIUS servers, and the output fields in this part of the display are described in the table below.

```
Router# show aaa servers private

RADIUS: id 24, priority 1, host 172.31.164.120, auth-port 1645, acct-port 1646
     State: current UP, duration 375742s, previous duration 0s
     Dead: total time 0s, count 0
     Quarantined: No
     Authen: request 5, timeouts 1, failover 0, retransmission 1
             Response: accept 4, reject 0, challenge 0
             Response: unexpected 0, server error 0, incorrect 0, time 14ms
```

```
        Transaction: success 4, failure 0
        Throttled: transaction 0, timeout 0, failure 0
Author: request 0, timeouts 0, failover 0, retransmission 0
        Response: accept 0, reject 0, challenge 0
        Response: unexpected 0, server error 0, incorrect 0, time 0ms
        Transaction: success 0, failure 0
        Throttled: transaction 0, timeout 0, failure 0
Account: request 5, timeouts 0, failover 0, retransmission 0
        Request: start 3, interim 0, stop 2
        Response: start 3, interim 0, stop 2
        Response: unexpected 0, server error 0, incorrect 0, time 12ms
        Transaction: success 5, failure 0
        Throttled: transaction 0, timeout 0, failure 0
Elapsed time since counters last cleared: 4d8h22m
Estimated Outstanding Access Transactions: 0
Estimated Outstanding Accounting Transactions: 0
Estimated Throttled Access Transactions: 0
Estimated Throttled Accounting Transactions: 0
Maximum Throttled Transactions: access 0, accounting 0
Requests per minute past 24 hours:
        high - 8 hours, 22 minutes ago: 0
        low  - 8 hours, 22 minutes ago: 0
        average: 0
```

The table below describes the significant fields in the display.

Table 7: show aaa servers Field Descriptions

Field	Description
id	A unique identifier for all AAA servers defined on the router.
priority	Order of use for servers within a group.
host	IP address of the private RADIUS server host.
auth-port	UDP destination port on the AAA server that is used for authentication and authorization requests. The default value is 1645.
acct-port	UDP destination port on the AAA server that is used for accounting requests. The default value is 1646.
State	Describes the current state of the AAA server; the duration, in seconds, that the server has been in that state; and the duration, in seconds, that the server was in the previous state. The following states are possible: • DEAD--Indicates that the server is currently down and, in the case of failovers, this server will be omitted unless it is the last server in the group. • duration--Indicates the amount of time the server is assumed to be in the current state, either UP or DEAD. • previous duration--Indicates the amount of time the server was considered to be in the previous state. • UP--Indicates that the server is currently considered alive and attempts will be made to communicate with it.

Field	Description
Dead	Indicates the number of times that this server has been marked dead, and the cumulative amount of time, in seconds, that it spent in that state.

Authen	Provides information about authentication packets that were sent to and received from the server, and authentication transactions that were successful or that failed. The following information may be reported in this field:
	• request--Number of authentication requests that were sent to the AAA server.
	• timeouts--Number of timeouts (no responses) that were observed when a transmission was sent to this server.
	• Response--Provides statistics about responses that were observed from this server and includes the following reports:
	  • unexpected--Number of unexpected responses. A response is considered unexpected when it is received after the timeout period for the packet has expired. This may happen if the link to the server is severely congested, for example. An unexpected response can also be produced when a server generates a response for no apparent reason.
	  • server error--Number of server errors. This category is a “catchall” for error packets that do not fall into one of the previous categories.
	  • incorrect--Number of incorrect responses. A response is considered incorrect if it is of the wrong format than the one expected by the protocol. This frequently happens when an incorrect server key is configured on the router.
	  • time--Time (in milliseconds) taken to respond to an authentication packets.
	• Transaction: These fields provide information about authentication, authorization, and accounting transactions related to the server. A transaction is defined as a request for authentication, authorization, or accounting information that is sent by the AAA module, or by an AAA client (such as PPP) to an AAA protocol (RADIUS or TACACS+), which may involve multiple packet transmissions and retransmissions. Transactions may require packet retransmissions to one or more servers in a single server group, to verify success or failure. Success or failure is reported to AAA by the RADIUS and TACACS+ protocols as follows
	  • success--Incremented when a transaction is successful.
	  • failure--Incremented when a transaction fails; for example, packet retransmissions to another server in the server group failed or did not succeed. A negative response to an Access-Request, such as Access-Reject, is considered to be a successful transaction.

Author	The fields in this category are similar to those in the Authen: fields. An important difference, however, is that because authorization information is carried in authentication packets for the RADIUS protocol, these fields are not incremented when using RADIUS.
Account	The fields in this category are similar to those in the Authen: fields, but provide accounting transaction and packet statistics.
Elapsed time since counters last cleared	Displays the time in days, hours, and minutes that have passed since the counters were last cleared.

Note In case of Intelligent Services Gateway (ISG), the estimated outstanding accounting transactions will take some time to become zero. This is because there is a constant churn in the interim accounting requests.

The fields in the output of the **show aaa servers**command are mapped to Simple Network Management Protocol (SNMP) objects in the Cisco AAA-SERVER-MIB and are used in SNMP reporting. The first line of the sample output of the **show aaa servers**command (RADIUS: id 24, priority 1, host 172.31.164.120, auth-port 1645, acct-port 1646) is mapped to the Cisco AAA-SERVER-MIB as follows:

- id maps to casIndex
- priority maps to casPriority
- host maps to casAddress
- auth-port maps to casAuthenPort
- acct-port maps to casAcctPort

Mapping the following set of objects listed in the Cisco AAA-SERVER-MIB map to fields displayed by the **show aaa servers** command is more straightforward. For example, the casAuthenRequests field corresponds to the Authen: request portion of the report, casAuthenRequestTimeouts corresponds to the Authen: timeouts portion of the report, and so on.

- casAuthenRequests
- casAuthenRequestTimeouts
- casAuthenUnexpectedResponses
- casAuthenServerErrorResponses
- casAuthenIncorrectResponses
- casAuthenResponseTime
- casAuthenTransactionSuccesses
- casAuthenTransactionFailures
- casAuthorRequests
- casAuthorRequestTimeouts
- casAuthorUnexpectedResponses
- casAuthorServerErrorResponses
- casAuthorIncorrectResponses
- casAuthorResponseTime
- casAuthorTransactionSuccesses
- casAuthorTransactionFailures

- casAcctRequests
- casAcctRequestTimeouts
- casAcctUnexpectedResponses
- casAcctServerErrorResponses
- casAcctIncorrectResponses
- casAcctResponseTime
- casAcctTransactionSuccesses
- casAcctTransactionFailures
- casState
- casCurrentStateDuration
- casPreviousStateDuration
- casTotalDeadTime
- casDeadCount

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs.

Related Commands

Command	Description
radius-server dead-criteria	Forces one or both of the criteria--used to mark a RADIUS server as dead--to be the indicated constant.
server-private	Associates a particular private RADIUS server with a defined server group.

show aaa subscriber profile

To display all the subscriber profiles under the specified namestring in the authentication, authorization, and accounting (AAA) subsystem, use the **show aaa subscriber profile**command in user EXEC or privileged EXEC mode.

show aaa subscriber profile *profile-name*

Syntax Description

profile-name	The AAA subscriber profile name.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(31)SB1	This command was integrated into Cisco IOS Release 12.2(31)SB1.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

This command display all the subscriber profile CLIs under the specified namestring. If no namestring is specified, all the subscriber profiles in the subscriber profile database will be displayed.

Examples

The following example shows how to display subscriber profile information:

```
Router# show aaa subscriber profile db

-----------------------------------------------------------
 Entries in Profile dB subscribers for exact match
-----------------------------------------------------------
Profile: prof1
Updated: 00:00:55
Parse User: N
Authen User: N
Query Count: 4
     6897DBDC 0 0000000A service-name(381) 8 service1, service none, protocol ne
-----------------------------------------------------------
 Entries in Profile dB subscribers for regexp match
-----------------------------------------------------------
No entries found for regexp match
The table below describes the significant fields shown in the display.
```

Table 8: show aaa subscriber profile Descriptions

Field	Description
Profile	Indicates the subscriber profile specified.
Updated	Time elapsed since profile last updated.

Field	Description
Parse User	Identifies this entry as a regexp.
Authen User	Identifies if entry matches require authentication.
Query Count	Usage Counters. Indicates the number of times Profile dB successfully found an entry when queried for.

Related Commands

Command	Description
aaa authorization subscriber-service	Configures local subscriber profiles which are used after the existing methods are exhausted.
subscriber profile	Configures service-related information under a particular subscriber profile.

show aaa user

To display attributes related to an authentication, authorization, and accounting (AAA) session, use the **show aaa user**command in privileged EXEC mode.

show aaa user {**all***unique-id*}

Syntax Description

all	Displays information about all users of which AAA currently has knowledge.
unique-id	Displays information about this user only.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(31)ZV1	This command was modified to display the user name first and then the accounting data and was implemented on the Cisco 10000 series router for the PRE3.
Cisco IOS XE Release 2.4	This command was integrated into Cisco IOS XE Release 2.4.

Usage Guidelines

When a user logs into a Cisco router and uses AAA, a unique ID is assigned to the session. Throughout the life of the session, various attributes that are related to the session are collected and stored internally within a AAA database. These attributes can include the IP address of the user, the protocol being used to access the router (such as PPP or Serial Line Internet Protocol [SLIP]), the speed of the connection, and the number of packets or bytes that are received or transmitted.

The output of this command:

- Provides a snapshot of various subdatabases that are associated with a AAA unique ID. Some of the more important ones are listed in the table below.
- Shows various AAA call events that are associated with a particular session. For example, when a session comes up, the events generally recorded are CALL START, NET UP, and IP Control Protocol UP (IPCP UP).
- Provides a snapshot of the dynamic attributes that are associated with a particular session. (Dynamic attributes are those that keep changing values throughout the life of the session.) Some of the more important ones are listed in the table below.

The unique ID of a session can be obtained from the output of the **show aaa sessions** command.

Note This command does not provide information for all users who are logged into a device, but only for those who have been authenticated or authorized using AAA or only for those whose sessions are being accounted for by the AAA module.

Note When you use the **all** keyword, a large amount of output may be produced, depending on the number of users who are logged into the device at any time.

Examples

The following example shows that information is requested for all users:

```
Router# show aaa user all
```

The following example shows that information is requested for user 5:

```
Router# show aaa user 5
```

The following is sample output from the **show aaa user** command. The session information displayed is for a PPP over Ethernet over Ethernet (PPPoEoE) session.

```
Router# show aaa user 3
Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%
Time source is hardware calendar, *20:32:49.199 PST Wed Dec 17
2003
  Unique id 3 is currently in use.
  Accounting:
    log=0x20C201
    Events recorded :
      CALL START
      NET UP
      IPCP_PASS
      INTERIM START
      VPDN NET UP
  update method(s) :
    NONE
  update interval = 0
  Outstanding Stop Records : 0
  Dynamic attribute list:
    63CCF138 0 00000001 connect-progress(30) 4 LAN Ses Up
    63CCF14C 0 00000001 pre-session-time(239) 4 3(3)
    63CCF160 0 00000001 nas-tx-speed(337) 4 102400000(61A8000)
    63CCF174 0 00000001 nas-rx-speed(33) 4 102400000(61A8000)
    63CCF188 0 00000001 elapsed_time(296) 4 2205(89D)
    63CCF19C 0 00000001 bytes_in(97) 4 6072(17B8)
    63CCF1B0 0 00000001 bytes_out(223) 4 6072(17B8)
    63CCF1C4 0 00000001 pre-bytes-in(235) 4 86(56)
    63CCF1D8 0 00000001 pre-bytes-out(236) 4 90(5A)
    63CCF1EC 0 00000001 paks_in(98) 4 434(1B2)
    63CCF244 0 00000001 paks_out(224) 4 434(1B2)
    63CCF258 0 00000001 pre-paks-in(237) 4 7(7)
    63CCF26C 0 00000001 pre-paks-out(238) 4 9(9)
  No data for type EXEC
  No data for type CONN
  NET: Username=peer1
    Session Id=00000003 Unique Id=00000003
    Start Sent=1 Stop Only=N
    stop_has_been_sent=N
    Method List=63B4A10C : Name = default
    Attribute list:
    63CCF138 0 00000001 session-id(293) 4 3(3)
    63CCF14C 0 00000001 Framed-Protocol(62) 4 PPP
    63CCF160 0 00000001 protocol(241) 4 ip
    63CCF174 0 00000001 addr(5) 4 70.0.0.1
```

```
  No data for type CMD
  No data for type SYSTEM
  No data for type RM CALL
  No data for type RM VPDN
  No data for type AUTH PROXY
  No data for type IPSEC-TUNNEL
  No data for type RESOURCE
  No data for type 10
  No data for type CALL
Debg: No data available
Radi: 641AACAC
Interface:
  TTY Num = -1
  Stop Received = 0
  Byte/Packet Counts till Call Start:
    Start Bytes In = 106      Start Bytes Out = 168
    Start Paks    In = 3      Start Paks  Out = 4
  Byte/Packet Counts till Service Up:
    Pre Bytes In = 192      Pre Bytes Out = 258
    Pre Paks  In = 10      Pre Paks  Out = 13
  Cumulative Byte/Packet Counts :
    Bytes In = 6264      Bytes Out = 6330
    Paks  In = 444      Paks  Out = 447
  StartTime = 19:56:01 PST Dec 17 2003
  AuthenTime = 19:56:04 PST Dec 17 2003
  Component = PPoE
Authen: service=PPP type=CHAP method=RADIUS
Kerb: No data available
Meth: No data available
Preauth: No Preauth data.
General:
  Unique Id = 00000003
  Session Id = 00000003
  Attribute List:
    63CCF180 0 00000001 port-type(156) 4 PPP over Ethernet
    63CCF194 0 00000009 interface(152) 7 0/0/0/0
PerU: No data available
```

The table below lists the significant fields shown in the display.

Table 9: show aaa user Field Descriptions

Field	Description
EXEC	Exec-Accounting database.
NET	Network Accounting database.
CMD	Command Accounting database.
Pre Bytes In	Bytes that were received before the call was authenticated.
Pre Bytes Out	Bytes that were transmitted before the call was authenticated.
Pre Paks In	Packets that were received before the call was authenticated.
Pre Paks Out	Packets that were transmitted before the call was authenticated.
Bytes In	Bytes that were received after the call was authenticated.
Bytes Out	Bytes that were transmitted after the call was authenticated.

Field	Description
Paks In	Packets that were received after the call was authenticated.
Paks Out	Packets that were transmitted after the call was authenticated.
Authen	Authentication database.
General	General database.
PerU	Per-User database.

Related Commands

Command	Description
show aaa sessions	Displays information about AAA sessions as seen in the AAA Session MIB.

show access-group mode interface

To display the Access Contol List (ACL) configuration on a Layer 2 interface, use the **show access-group mode interface**command in privileged EXEC mode.

show access-group mode interface [*interface interface-number*]

Syntax Description

type	(Optional) Interface type; valid values are **fastethernet**, **gigabitethernet**, **tengigabitethernet**, and **port-channel**
number	(Optional) Interface number.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.

Usage Guidelines

The valid values for the port number depend on the chassis used.

Examples

This example shows how to display the ACL configuration mode on Fast Ethernet interface 6/1:

```
Router# show access-group mode interface fastethernet 6/1
Interface FastEthernet6/1:
   Access group mode is: merge
Router#
```

Related Commands

Command	Description
access-group mode	Specifies the override modes and the nonoverride modes.

show access-lists compiled

To display a table showing Turbo Access Control Lists (ACLs), use the show access-lists compiled command in user EXEC or privileged EXEC mode.

show access-lists compiled

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(6)S	This command was introduced.
12.1(1)E	This command was introduced for Cisco 7200 series routers.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.1(4)E	This command was implemented on the Cisco 7100 series routers.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.2	This command was integrated into Cisco IOS XE Release 2.2.

Usage Guidelines

This command is used to display the status and condition of the Turbo ACL tables associated with each access list. The Turbo ACL feature processes access lists more expediently, providing faster functionality for routers equipped with the feature. The Turbo ACL feature compiles the ACLs into a set of lookup tables, while maintaining the first match requirements. Packet headers are used to access these tables in a small, fixed number of lookups, independently of the existing number of ACL entries. The memory usage is displayed for each table; large and complex access lists may require substantial amounts of memory. If the memory usage is greater than the memory available, you can disable the Turbo ACL feature so that memory exhaustion does not occur, but the acceleration of the access lists is not then enabled.

Examples

The following is partial sample output from the show access-lists compiled command:

```
Router# show access-lists compiled
Compiled ACL statistics:
12 ACLs loaded, 12 compiled tables
 ACL         State      Tables  Entries  Config  Fragment  Redundant  Memory
1           Operational    1        2        1         0          0      1Kb
2           Operational    1        3        2         0          0      1Kb
3           Operational    1        4        3         0          0      1Kb
```

```
4           Operational    1        3        2         0          0      1Kb
5           Operational    1        5        4         0          0      1Kb
9           Operational    1        3        2         0          0      1Kb
20          Operational    1        9        8         0          0      1Kb
21          Operational    1        5        4         0          0      1Kb
101         Operational    1       15        9         7          2      1Kb
102         Operational    1       13        6         6          0      1Kb
120         Operational    1        2        1         0          0      1Kb
199         Operational    1        4        3         0          0      1Kb
First level lookup tables:
Block      Use              Rows       Columns   Memory used
  0   TOS/Protocol            6/16     12/16      66048
  1   IP Source (MS)         10/16     12/16      66048
  2   IP Source (LS)         27/32     12/16      132096
  3   IP Dest (MS)            3/16     12/16      66048
  4   IP Dest (LS)            9/16     12/16      66048
  5   TCP/UDP Src Port        1/16     12/16      66048
  6   TCP/UDP Dest Port       3/16     12/16      66048
  7   TCP Flags/Fragment      3/16     12/16      66048
```

The table below describes the significant fields shown in the display.

Table 10: show access-lists compiled Field Descriptions

Field	Description
State	Describes the state of each Turbo ACL table. Operational--The access list has been compiled by the Turbo ACL feature, and matching to this access list is performed through the Turbo ACL tables at high speed. Other possible values in the State field are as follows: • Unsuitable--The access list is not suitable for compiling, perhaps because it has time-range enabled entries, evaluate references, or dynamic entries. • Deleted--No entries are in this access list. • Building--The access list is being compiled. Depending on the size and complexity of the list, and the load on the router, the building process may take a few seconds. • Out of memory--An access list cannot be compiled because the router has exhausted its memory.
Entries	Number of ACL entries being used for the compilation. This number is effectively (Config + Fragment - Redundant).
Config	Number of ACL lines from the configuration itself.
Fragment	In order to handle IP fragments for entries that have Layer 4 information in them (for example, TCP port numbers), TurboACL generates extra ACL entries that match only IP fragments. These are used in the compilation, but do not appear in the configuration.
Redundant	Number of entries that are covered by an earlier entry, and therefore are redundant. These entries are not used in the compilation. Redundant entries come mainly from two sources; the config itself might contain redundant entries, often as a result of a poorly maintained, large ACL. More typically, when TurboACL adds extra entries for IP fragments, often these entries are redundant because other added fragment entries cover them.

Related Commands

Command	Description
access-list compiled	Enables the Turbo ACL feature.
access-list (extended)	Provides extended access lists that allow more detailed access lists.
access-list (standard)	Creates a standard access list.
clear access-list counters	Clears the counters of an access list.
clear access-temp	Manually clears a temporary access list entry from a dynamic access list.
ip access-list	Defines an IP access list by name.
show ip access-lists	Displays the contents of all current IP access lists.

show access-lists

To display the contents of current access lists, use the **show access-lists** command in user EXEC or privileged EXEC mode.

show access-lists [{*access-list-numberaccess-list-name*}]

Syntax Description

access-list-number	(Optional) Number of the access list to display. The system displays all access lists by default.
access-list-name	(Optional) Name of the IP access list to display.

Command Default

The system displays all access lists.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.0(6)S	The output was modified to identify the compiled ACLs.
12.1(1)E	This command was implemented on the Cisco 7200 series.
12.1(5)T	The command output was modified to identify compiled ACLs.
12.1(4)E	This command was implemented on the Cisco 7100 series.
12.2(2)T	The command output was modified to show information for IPv6 access lists.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The show access-lists command is used to display the current ACLs operating in the router. Each access list is flagged using the Compiled indication if it is operating as an accelerated ACL.

The display also shows how many packets have been matched against each entry in the ACLs, enabling the user to monitor the particular packets that have been permitted or denied. This command also indicates whether the access list is running as a compiled access list.

Examples

The following is sample output from the **show access-lists** command when access list 101 is specified:

```
Router# show access-lists 101
Extended IP access list 101
```

```
    permit tcp host 198.92.32.130 any established (4304 matches) check=5
    permit udp host 198.92.32.130 any eq domain (129 matches)
    permit icmp host 198.92.32.130 any
    permit tcp host 198.92.32.130 host 171.69.2.141 gt 1023
    permit tcp host 198.92.32.130 host 171.69.2.135 eq smtp (2 matches)
    permit tcp host 198.92.32.130 host 198.92.30.32 eq smtp
    permit tcp host 198.92.32.130 host 171.69.108.33 eq smtp
    permit udp host 198.92.32.130 host 171.68.225.190 eq syslog
    permit udp host 198.92.32.130 host 171.68.225.126 eq syslog
    deny   ip 150.136.0.0 0.0.255.255 224.0.0.0 15.255.255.255
    deny   ip 171.68.0.0 0.1.255.255 224.0.0.0 15.255.255.255 (2 matches) check=1
    deny   ip 172.24.24.0 0.0.1.255 224.0.0.0 15.255.255.255
    deny   ip 192.82.152.0 0.0.0.255 224.0.0.0 15.255.255.255
    deny   ip 192.122.173.0 0.0.0.255 224.0.0.0 15.255.255.255
    deny   ip 192.122.174.0 0.0.0.255 224.0.0.0 15.255.255.255
    deny   ip 192.135.239.0 0.0.0.255 224.0.0.0 15.255.255.255
    deny   ip 192.135.240.0 0.0.7.255 224.0.0.0 15.255.255.255
    deny   ip 192.135.248.0 0.0.3.255 224.0.0.0 15.255.255.255
```

An access list counter counts how many packets are allowed by each line of the access list. This number is displayed as the number of matches. Check denotes how many times a packet was compared to the access list but did not match.

The following is sample output from the show access-lists command when the Turbo Access Control List (ACL) feature is configured on all of the following access lists.

Note The permit and deny information displayed by the show access-lists command may not be in the same order as that entered using the access-list command.

```
Router# show access-lists
Standard IP access list 1 (Compiled)
    deny   any
Standard IP access list 2 (Compiled)
    deny   192.168.0.0, wildcard bits 0.0.0.255
    permit any
Standard IP access list 3 (Compiled)
    deny   0.0.0.0
    deny   192.168.0.1, wildcard bits 0.0.0.255
    permit any
Standard IP access list 4 (Compiled)
    permit 0.0.0.0
    permit 192.168.0.2, wildcard bits 0.0.0.255
```

The following is sample output from the **show access-lists** command that shows information for IPv6 access lists when IPv6 is configured on the network:

```
Router# show access-lists
IPv6 access list list2
     deny ipv6 FEC0:0:0:2::/64 any sequence 10
     permit ipv6 any any sequence 20
```

Related Commands

Command	Description
access-list (IP extended)	Defines an extended IP access list.
access-list (IP standard)	Defines a standard IP access list.

Command	Description
clear access-list counters	Clears the counters of an access list.
clear access-template	Clears a temporary access list entry from a dynamic access list manually.
ip access-list	Defines an IP access list by name.
show ip access-lists	Displays the contents of all current IP access lists.
show ipv6 access-list	Displays the contents of all current IPv6 access lists.

show access-session fqdn

To display the FQDN configurations, use the **show access-session fqdn** command in EXEC mode.

show access-session fqdn {**passthru-domain-list** | **list-domain** *list-domain* | **fqdn-maps**}

Syntax Description

passthru-domain-list	Displays the lists of domains for the access session.
list-domain *list-domain*	Displays all the domains in the list.
fqdn-maps	Displays mapping of FQDN ACL to the domain name list.

Command Default

None

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
	This command was introduced.

This example shows how to display the lists of domains for the access session:

```
# sh access-sess fqdn passthru-domain-list
Domain-name-lists
----------------------------
abc
```

This example shows how to display the domains in the list for the access session:

```
# sh access-sess fqdn  list-domain abc
Domain's associated with the list
----------------------------------------
abc
google
```

show accounting

The **show accounting** command is replaced by the **show aaa user**command. See the **show aaa user** command for more information.

show appfw

To display application firewall policy information, use the **show appfw**command in user EXEC or privileged EXEC mode.

show appfw {**configuration** | **dns** [**cache** [**policy** *policy-name*]] | **name** *appfw-name*}

Syntax Description

configuration	Displays configuration information for configured policies.
dns	Displays IP addresses resolved by the Domain Name System (DNS) server of the applicable instant messenger application.
cache	(Optional) Displays IP addresses related to the DNS server.
policy	(Optional) Displays information for the specified policy.
policy-name	Name of the policy.
name	Displays information about the specified application firewall.
appfw-name	Name of an application firewall.

Command Default

If no policies are specified, information for all policies is displayed.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(4)T	This command was modified. The **dns** and **cache**keywords were added to support instant messenger traffic inspection.
12.4(24)T	This command was modified in a release earlier than Cisco IOS Release 12.4(24)T. The **name** keyword and *appfw-name* argument were added.

Usage Guidelines

Use this command to display information regarding the application firewall policy configuration or the IP addresses of the DNS cache.

Use the **show appfw** command in conjunction with the **show ip inspect config** command to display the complete firewall configuration.

If you do not specify a policy using the **policy** *policy-name* option, the IP addresses gathered for all DNS names and policies are displayed.

Examples

This following output for the **show appfw configuration** command displays the configuration for the inspection rule "mypolicy," which is applied to all incoming HTTP traffic on FastEthernet interface 0/0. In this example, all available HTTP inspection parameters have been defined.

```
Router# show appfw configuration

Application Firewall Rule configuration
  Application Policy name mypolicy
    Application http
      strict-http action allow alarm
      content-length minimum 0 maximum 1 action allow alarm
      content-type-verification match-req-rsp action allow alarm
      max-header-length request length 1 response length 1 action allow alarm
      max-uri-length 1 action allow alarm
      port-misuse default action allow alarm
      request-method rfc default action allow alarm
      request-method extension default action allow alarm
      transfer-encoding default action allow alarm
```

The table below describes the significant fields shown in the display.

Table 11: show appfw configuration Field Descriptions

Field	Description
Application Policy name	Name of the application policy.
strict-http action allow alarm	Allows HTTP messages to pass through the firewall.
content-length minimum 0 maximum 1 action allow alarm	Allows HTTP traffic having the maximum message size of 1 to pass through the firewall.
content-type-verification match-req-rsp action allow alarm	Allows HTTP traffic after verifying the content type of the HTTP response against the accept field of the HTTP request.
max-header-length request length 1 response length 1 action allow alarm	Allows the alarm to pass through the firewall if both the maximum header length request and the response is 1.
max-uri-length 1 action allow alarm	Allows HTTP traffic if the uniform resource identifier (URI) length in the request message is 1.
port-misuse default action allow alarm	Allows HTTP traffic through the firewall for all the default applications in the HTTP message.
request-method rfc default action allow alarm	Allows HTTP traffic for RFC 2616 supported methods.
request-method extension default action allow alarm	Allows HTTP traffic for all the extension methods.
transfer-encoding default action allow alarm	Allows HTTP traffic for all types of transfer encoded messages.

Related Commands

Command	Description
show ip inspect config	Displays firewall configuration and session information.

show ase

Note Effective with Cisco IOS Release 12.4(24), the **show ase** command is not available in Cisco IOS software.

To display the Automatic Signature Extraction (ASE) run-time status or detected signatures, use the **show ase** command in privileged EXEC mode.

show ase [{**dispersion-table** *num-entries-to-display* | **prevalence-table** *num-entries-to-display* | **signatures** | **special-case-table** *num-entries-to-display* | **statistics**}]

Syntax Description

dispersion-table	(Optional) Displays the dispersion table.
num-entries-to-display	(Optional) The number of table entries to be displayed. The range is from 0 to 4294967295.
prevalence-table	(Optional) Displays the prevalence table.
signatures	(Optional) Displays the detected ASE signatures.
special-case-table	(Optional) Displays the special case table.
statistics	(Optional) Displays the address description table staistics.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(15)T	This command was introduced.
12.4(24)	This command was removed.

Usage Guidelines

Use the **show ase** command without any keywords to display the run-time status. Use the **show ase**command with the **signatures** keyword to display the detected ASE signatures.

This command is used on the Cisco 1800, 2800, and 7200 series routers, Cisco 7301 router, and Integrated Services Routers (ISRs) as ASE sensors.

Examples

The following example output displays the ASE run-time status:

Note The ASE collector must be started in order for the ASE run-time status information to be displayed.

```
Router# show ase
ASE Information:
Collector IP: 10.10.10.3
```

```
TIDP Group  : 10
Status      : Online
Packets inspected: 1105071
Address Dispersion Threshold: 20
Prevalence Threshold: 10
Sampling set to: 1 in 64
Address Dispersion Inactivity Timer: 3600s
Prevalence Table Refresh Time: 60s
```

The table below describes the significant fields shown in the display.

Table 12: show ase Field Descriptions

Field	Description
Collector IP	The IP address of the ASE collector.
TIDP Group	Threat Information Distribution Protocol (TIDP) group used for exchange between the ASE sensor and ASE collector.
Status	The four states are: • **Connected** --The ASE sensor has connected with the ASE collector, but it has not completed initialization. • **Enabled** --The ASE feature is enabled in global configuration mode, but the ASE sensor has not connected with the ASE collector. • **Not Enabled** --The ASE feature is not enabled in global configuration mode. • **Online** --The ASE is ready for inspecting traffic.
Packets inspected	Total number of packets inspected on this ASE collector.
Address Dispersion Threshold	Number of IP address occurrences that are permitted by the ASE sensor before this signature is considered an anomaly. **Note** The Address Dispersion Threshold is configured on the ASE collector. This information is shown on the ASE sensor (this router) for informational purposes.
Prevalence Threshold	The number of signature occurrences that are permitted before this signature is considered an anomaly. The default threshold is 10 seconds.
Sampling set to	A sampling value that sets the chance for which a signature is being inspected. For example, 1 in 64 is less than 1 in 32 chances.
Address Dispersion Inactivity Timer	Number of seconds that a signature does not occur. After this interval elapses, the signature is purged from the Address Dispersion table.
Prevalence Table Refresh Time	Number of seconds that the ASE sensor has before it clears the occurrence table. If a signature does not occur for the Prevalence Threshold during a refresh, then the Prevalence Threshold is not considered.

The following example output displays the detected ASE signatures:

```
Router# show ase signature
Automatic Signature Extraction Detected Signatures
==================================================
Signature Hash: 0x1E4A2076AAEA19B1, Offset: 54, Dest Port: TCP 135,
Signature: 05 00 00 03 10 00 00 00 F0 00 10 00 01 00 00 00 B8 00 00 00 00 00 03 00 01 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00
Signature Hash: 0x24EC60FB1CF9A800, Offset: 72, Dest Port: TCP 445,
Signature: 00 00 00 00 00 00 00 00 00 00 00 00 FF FE 00 00 00 00 00 62 00 02 50 43 20 4E
45 54 57 4F 52 4B 20 50 52 4F 47 52 41 4D
Signature Hash: 0x0B0275535FFF480C, Offset: 54, Dest Port: TCP 445,
Signature: 00 00 00 85 FF 53 4D 42 72 00 00 00 00 18 53 C8 00 00 00 00 00 00 00 00 00 00
00 00 00 00 FF FE 00 00 00 00 00 62 00 02
```

Related Commands

Command	Description
ase collector	Enters the ASE collector server IP address so that the ASE sensor has IP connectivity to the ASE collector.
ase group	Identifies the TIDP group number for the ASE feature.
ase enable	Enables the ASE feature on a specified interface.
ase signature extraction	Enables the ASE feature globally on the router.
clear ase signature	Clears ASE signatures that were detected on the router.
debug ase	Provides error, log, messaging, reporting, status, and timer information.

show audit

To display the contents of an audit file, use the **show audit**command in privileged EXEC mode.

show audit [**filestat**]

Syntax Description

filestat	(Optional) Displays the rollover counter for the circular buffer and the number of messages that are received. The rollover counter, which indicates the number of times circular buffer has been overwritten, is reset when the audit filesize is changed (via the **audit filesize** command).

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)S	This command was introduced.
12.0(27)S	This feature was integrated into Cisco IOS Release 12.0(27)S.
12.2(25)S	The **filestat** keyword was added.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The audit file is a fixed file size in the disk file system. The audit file contains syslog messages (also known as hashes), which monitor changes that are made to your router. A separate hash is maintained for each of the following areas: running version, running configuration, startup configuration, file system, and hardware configuration. The **show audit**command will display any changes that are made to any of these areas.

Note Audit logs are enabled by default and cannot be disabled.

Examples

The following example is sample output from the **show audit** command:

```
Router# show audit
```

*Sep 14 18:37:31.535:%AUDIT-1-RUN_VERSION:Hash:

24D98B13B87D106E7E6A7E5D1B3CE0AD User:

```
*Sep 14 18:37:31.583:%AUDIT-1-RUN_CONFIG:Hash:
4AC2D776AA6FCA8FD7653CEB8969B695 User:
*Sep 14 18:37:31.595:%AUDIT-1-STARTUP_CONFIG:Hash:
95DD497B1BB61AB33A629124CBFEC0FC User:
*Sep 14 18:37:32.107:%AUDIT-1-FILESYSTEM:Hash:
```

```
330E7111F2B526F0B850C24ED5774EDE User:
*Sep 14 18:37:32.107:%AUDIT-1-HARDWARE_CONFIG:Hash:
32F66463DDA802CC9171AF6386663D20 User:
```

The table below describes the significant fields shown in the display.

Table 13: show audit Field Descriptions

Field	Description
`AUDIT-1-RUN_VERSION:Hash: 24D98B13B87D106E7E6A7E5D1B3CE0AD User:`	Running version, which is a hash of the information that is provided in the output of the **show version** command: running version, ROM information, BOOTLDR information, system image file, system and processor information, and configuration register contents.
`AUDIT-1-RUN_CONFIG:Hash: 4AC2D776AA6FCA8FD7653CEB8969B695 User:`	Running configuration, which is a hash of the running configuration.
`AUDIT-1-STARTUP_CONFIG:Hash: 95DD497B1BB61AB33A629124CBFEC0FC User:`	Startup configuration, which is a hash of the contents of the files on NVRAM, which includes the startup-config, private-config, underlying-config, and persistent-data.
`AUDIT-1-FILESYSTEM:Hash: 330E7111F2B526F0B850C24ED5774EDE User:`	File system, which is a hash of the dir information on all of the flash file systems, which includes bootflash and any other flash file systems on the router.
`AUDIT-1-HARDWARE_CONFIG:Hash:32F66463DDA802CC9171AF6386663D20 User:`	Hardware configuration, which is a hash of platform-specific information that is generally provided in the output of the **show diag**command.

Related Commands

Command	Description
audit filesize	Changes the size of the audit file.
audit interval	Changes the time interval that is used for calculating hashes.

show authentication interface

To display information about the Auth Manager for a given interface, use the **show authentication interface**command in privileged EXEC mode.

show authentication interface *type number*

Syntax Description

type	Interface type. For more information, use the question mark (?) online help function.
number	Interface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SXI	This command was introduced.
15.2(2)T	This command was integrated into Cisco IOS Release 15.2(2)T.

Usage Guidelines

Use the **show authentication interface** command to display information about the Auth Manager for a given interface.

Examples

The following is sample output from the **show authentication interface** command:

```
Switch# show authentication interface g1/0/23
Client list:
  MAC Address     Domain   Status         Handle      Interface
  000e.84af.59bd  DATA     Authz Success  0xE0000000  GigabitEthernet1/0/23
Available methods list:
  Handle  Priority  Name
  3        0        dot1x
Runnable methods list:
  Handle  Priority  Name
  3        0        dot1x
```

The table below describes the significant fields shown in the display. Other fields are self-explanatory.

Table 14: show authentication interface Field Descriptions

Field	Description
MAC Address	The MAC address of the client.
Domain	The domain of the client--either DATA or voice.

Field	Description
Status	The status of the authentication session. The possible values are: • Authc Failed--an authentication method has run for this session and authentication failed. • Authc Success--an authentication method has run for this session and authentication was successful. • Authz Failed--a feature has failed and the session has terminated. • Authz Success--all features have been applied to the session and the session is active. • Idle--this session has been initialized but no authentication methods have run. This is an intermediate state. • No methods--no authentication method has provided a result for this session. • Running--an authentication method is running for this session.
Interface	The type and number of the authentication interface.
Available methods list	Summary information for the authentication methods available on the interface.
Runnable methods list	Summary information for the authentication methods that can run on the interface.

Related Commands

Command	Description
show authentication registrations	Displays information about the authentication methods that are registered with the Auth Manager.
show authentication sessions	Displays information about the current Auth Manager sessions.

show authentication registrations

To display information about the authentication methods that are registered with the Auth Manager, use the **show authentication registrations**command in privileged EXEC mode.

show authentication registrations

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SXI	This command was introduced.
15.2(2)T	This command was integrated into Cisco IOS Release 15.2(2)T.

Usage Guidelines

Use the **show authentication re gistrations** command to display information about all methods registered with the Auth Manager.

Examples

The following is sample output for the show authentication registrations command:

```
Switch# show authentication registrations
Auth Methods registered with the Auth Manager:
   Handle   Priority   Name
     3         0       dot1x
     2         1       mab
     1         2       webauth
```

The table below describes the significant fields shown in the display.

Table 15: show authentication registrations Field Descriptions

Field	Description
Priority	The priority of the method. If the priority for authentication methods has not been configured with the **authentication priority** command, then the default priority is displayed. The default from highest to lowest is dot1x, mab, and webauth.
Name	The name of the authentication method. The values can be dot1x, mab, or webauth.

Related Commands

Command	Description
show authentication interface	Displays information about the Auth Manager for a given interface.
show authentication sessions	Displays information about current Auth Manager sessions.

show authentication sessions

To display information about current Auth Manager sessions, use the **show authentication sessions** command in privileged EXEC mode.

Note Effective with Cisco IOS Release 12.2(33)SXI, the **show dot1x** command is supplemented by the **show authentication sessions** command. The **show dot1x** command is reserved for displaying output specific to the use of the 802.1X authentication method. The **show authentication sessions** command displays information for all authentication methods and authorization features.

Cisco IOS XE Release 3SE and Later Releases
show authentication sessions [{[**database**] | [{**handle** *handle-number* | **interface** *type number* | **mac** *mac-address* | **method** *method-name* [**interface** *type number*] | **session-id** *session-id*}]}] [**details**]

All Other Releases
show authentication sessions [{**handle** *handle-number* | **interface** *type number* | **mac** *mac-address* | **method** *method-name* **interface** *type number* | **session-id** *session-id*}]

Syntax Description

database	(Optional) Displays session data stored in the session database. This keyword allows you to see information like the VLAN ID, which is not cached internally. A warning message displays if data stored in the session database does not match the internally cached data.
handle *handle-id*	(Optional) Specifies the particular handle for which to display Auth Manager information.
interface *type number*	(Optional) Specifies a particular interface type and number for which Auth Manager information is to be displayed. To display the valid keywords and arguments for interfaces, use the question mark (?) online help function.
mac *mac-address*	(Optional) Specifies the particular MAC address for which you want to display information.
method *method-name*	(Optional) Specifies the particular authentication method for which to display Auth Manager information. Valid methods are one of the following: • **dot1x**—IEEE 802.1X authentication method. • **mab**—MAC authentication bypass (MAB) method. • **webauth**—Web authentication method. If you specify a method, you can also specify an interface.

session-id *session-id*	(Optional) Specifies the particular session for which to display Auth Manager information.
details	(Optional) Displays detailed information for each session instead of displaying a single-line summary for sessions.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SXH	Support for this command was introduced.
12.2(33)SXI	This command was changed to add the **handle** *handle* keyword and argument and add information to the output.
15.2(2)T	This command was integrated into Cisco IOS Release 15.2(2)T.
Cisco IOS XE Release 3.2SE	This command was modified. The **database** and **details** keywords were added.

Usage Guidelines

Use the **show authentication sessions** command to display information about all current Auth Manager sessions. To display information about specific Auth Manager sessions, use one or more of the keywords.

Examples

The following example shows how to display all authentication sessions on the switch:

```
Device# show authentication sessions

Interface  MAC Address     Method   Domain   Status         Session ID
Gi1/48     0015.63b0.f676  dot1x    DATA     Authz Success  0A3462B1000000102983C05C
Gi1/5      000f.23c4.a401  mab      DATA     Authz Success  0A3462B10000000D24F80B58
Gi1/5      0014.bf5d.d26d  dot1x    DATA     Authz Success  0A3462B10000000E29811B94
```

The following example shows how to display all authentication sessions on an interface:

```
Device# show authentication sessions interface GigabitEthernet3/0/2 details

            Interface:  GigabitEthernet3/0/2
              IIF-ID:  0x1055240000001F6
         MAC Address:  0010.0010.0001
        IPv6 Address:  Unknown
        IPv4 Address:  192.0.2.1
           User-Name:  auto601
              Status:  Authorized
              Domain:  DATA
      Oper host mode:  single-host
     Oper control dir:  both
      Session timeout:  N/A
    Common Session ID:  AC14FC0A0000101200E28D62
      Acct Session ID:  Unknown
              Handle:  0xDB003227
       Current Policy:  dot1x_dvlan_reauth_hm

Local Policies:
             Template: CRITICAL_VLAN (priority 150)
           Vlan Group:  Vlan: 130
```

```
Method status list:
       Method           State
       dot1x            Authc Failed
```

The following example shows how to display the authentication session for a specified session ID:

```
Device# show authentication sessions session-id 0B0101C70000004F2ED55218

            Interface:  GigabitEthernet9/2
          MAC Address:  0000.0000.0011
           IP Address:  192.0.2.254
             Username:  johndoe
               Status:  Authz Success
               Domain:  DATA
       Oper host mode:  multi-host
     Oper control dir:  both
        Authorized By:  Critical Auth
          Vlan policy:  N/A
      Session timeout:  N/A
         Idle timeout:  N/A
    Common Session ID:  0B0101C70000004F2ED55218
      Acct Session ID:  0x00000003
               Handle:  0x91000001
Runnable methods list:
       Method   State
       mab      Authc Success
       dot1x    Not run
```

The following examples show how to display all clients authorized by the specified authentication method:

```
Device# show authentication sessions method mab

No Auth Manager contexts match supplied criteria

Device# show authentication sessions method dot1x

Interface  MAC Address     Domain   Status         Session ID
Gi9/2      0000.0000.0011  DATA     Authz Success  0B0101C70000004F2ED55218
```

The table below describes the significant fields shown in the displays.

Table 16: show authentication sessions Field Descriptions

Field	Description
Interface	The type and number of the authentication interface.
MAC Address	The MAC address of the client.
Domain	The name of the domain, either DATA or VOICE.

Field	Description
Status	The status of the authentication session. The possible values are: • Authc Failed—An authentication method has run for this session and authentication failed. • Authc Success—An authentication method has run for this session and authentication was successful. • Authz Failed—A feature has failed and the session has terminated. • Authz Success—All features have been applied to the session and the session is active. • Idle—This session has been initialized but no authentication methods have run. This is an intermediate state. • No methods—No authentication method has provided a result for this session. • Running—An authentication method is running for this session.
Handle	The context handle.
State	The operating states for the reported authentication sessions. The possible values are: • Not run—The method has not run for this session. • Running—The method is running for this session. • Failed over—The method has failed and the next method is expected to provide a result. • Success—The method has provided a successful authentication result for the session. • Authc Failed—The method has provided a failed authentication result for the session.

Related Commands

Command	Description
show access-sessions	Displays information about session aware networking sessions.
show authentication registrations	Displays information about the authentication methods that are registered with the Auth Manager.
show authentication statistics	Displays statistics for Auth Manager sessions.
show dot1x	Displays details for an identity profile specific to the use of the 802.1X authentication method.

show auto secure config

To display AutoSecure configurations, use the **show auto secure config**command in privileged EXEC mode.

show auto secure config

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(1)	This command was introduced.
12.3(15)	Autosecure disables the configuration of the autosec_iana_reserved_block, autosec_private_block, or autosec_complete_bogon access control lists (acls), and application-to-edge interfaces. Output for these acls is no longer shown in the show output.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.

Examples

The following sample output from the **show auto secure config** command shows what has been enabled and disabled via the **auto secure** command:

```
Router# show auto secure config
no service finger
no service pad
no service udp-small-servers
no service tcp-small-servers
service password-encryption
service tcp-keepalives-in
service tcp-keepalives-out
no cdp run
no ip bootp server
no ip http server
no ip finger
no ip source-route
no ip gratuitous-arps
no ip identd
security passwords min-length 6
security authentication failure rate 10 log
enable secret 5 $1$CZ6G$GkGOnHdNJCO3CjNHHyTUA.
aaa new-model
aaa authentication login local_auth local
line console 0
 login authentication local_auth
 exec-timeout 5 0
 transport output telnet
line aux 0
 login authentication local_auth
 exec-timeout 10 0
 transport output telnet
line vty 0 4
 login authentication local_auth
 transport input telnet
```

```
ip domain-name cisco.com
crypto key generate rsa general-keys modulus 1024
ip ssh time-out 60
ip ssh authentication-retries 2
line vty 0 4
 transport input ssh telnet
service timestamps debug datetime localtime show-timezone msec
service timestamps log datetime localtime show-timezone msec
logging facility local2
logging trap debugging
service sequence-numbers
logging console critical
logging buffered
interface FastEthernet0/1
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled
!
interface FastEthernet1/0
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled
!
interface FastEthernet1/1
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled
!
interface FastEthernet0/0
 no ip redirects
 no ip proxy-arp
 no ip unreachables
 no ip directed-broadcast
 no ip mask-reply
 no mop enabled
!
ip cef
interface FastEthernet0/0
 ip verify unicast reverse-path
ip inspect audit-trail
ip inspect dns-timeout 7
ip inspect tcp idle-time 14400
ip inspect udp idle-time 1800
ip inspect name autosec_inspect cuseeme timeout 3600
ip inspect name autosec_inspect ftp timeout 3600
ip inspect name autosec_inspect http timeout 3600
ip inspect name autosec_inspect rcmd timeout 3600
ip inspect name autosec_inspect realaudio timeout 3600
ip inspect name autosec_inspect smtp timeout 3600
ip inspect name autosec_inspect tftp timeout 30
ip inspect name autosec_inspect udp timeout 15
ip inspect name autosec_inspect tcp timeout 3600
access-list 100 deny ip any any
interface FastEthernet0/0
```

```
ip inspect autosec_inspect out
ip access-group 100 in
```

Related Commands

Command	Description
auto secure	Secures the management and forwarding planes of the router.

show call admission statistics

To monitor the global Call Admission Control (CAC) configuration parameters and the behavior of CAC, use the **show call admission statistics**command in user EXEC or privileged EXEC mode.

show call admission statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.2(18)SXD1	This command was integrated into Cisco IOS Release 12.2(18)SXD1.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Examples

The following is sample output from the **show call admission statistics** command:

```
Router# show call admission statistics

Total Call admission charges: 0, limit 25
Total calls rejected 12, accepted 51
Load metric: charge 0, unscaled 0
```

The table below describes the significant fields shown in the display.

Table 17: show call admission statistics Field Descriptions

Field	Description
Total call admission charges	Percentage of system resources being charged to the system. If you configured a resource limit, SA requests are dropped when this field is equal to that limit.
limit	Maximum allowed number of total call admission charges. Valid values are 0 to 100000.
Total calls rejected	Number of SA requests that were not accepted.
accepted	Number of SA requests that were accepted.
unscaled	Not related to IKE. This value always is 0.

Related Commands

Command	Description
call admission limit	Instructs IKE to drop calls when a specified percentage of system resources are being consumed.
crypto call admission limit	Specifies the maximum number of IKE SA requests allowed before IKE begins rejecting new IKE SA requests.

show class-map type inspect

To display Layer 3 and Layer 4 or Layer 7 (application-specific) inspect type class maps and their matching criteria, use the **show class-map type inspect** command in privileged EXEC mode.

show class-map type inspect [*protocol-name*] [*class-map-name*]

Syntax Description

protocol-name	(Optional) Layer 7 application-specific class map. The supported protocols are as follows: • **aol** --America Online Instant Messenger (IM) • **edonkey** --eDonkey peer-to-peer (P2P) • **fasttrack** --FastTrack traffic P2P • **gnutella** --Gnutella Version 2 traffic P2P • **h323** --H323 protocol • **http** --HTTP • **icq** --I Seek You (ICQ) IM • **imap** --Internet Message Access Protocol (IMAP) • **kazaa2** --Kazaa Version 2 P2P • **msnmsgr** --MSN Messenger IM protocol • **pop3** --Post Office Protocol, Version 3 (POP 3) • **sip** --SMDS Interface Protocol (SIP) • **smtp** --Simple Mail Transfer Protocol (SMTP) • **sunrpc** --SUN Remote Procedure Call (SUNRPC) • **winmsgr** --Windows IM • **ymsgr** --Yahoo IM
class-map-name	(Optional) Name of the inspect type class map. The name can be a maximum of 40 alphanumeric characters.

Command Default

Information for all inspect type class maps is displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.4(9)T	This command was modified. The following keywords were added: **edonkey**, **fasttrack**, **gnutella**, **kazaa2**, **aol**, **msnmsgr**, **ymsgr**.

Release	Modification
12.4(20)T	This command was modified. The following keywords were added: **icq**and **winmsgr**.
Cisco IOS XE Release 2.1	This command was modified. It was integrated into Cisco IOS XE Release 2.1. The *protocol-name*argument is not supported.

Usage Guidelines

Use the **show class-map type inspect**command to display class maps for a particular inspect type class map.

Examples

The following is sample output from the **show class-map type inspect** command with all class maps:

```
Router# show class-map type inspect
Class Map type inspect match-all classe0 (id 7)
   Match access-group  34
 Class Map type inspect match-all c1 (id 5)
   Match access-group  101
   Match protocol http
 Class Map type inspect match-all class1 (id 1)
   Match none
```

The following is sample output from the **show class-map type inspect** with the class map classe0 specified:

```
Router# show class-map type inspect classe0
 Class Map type inspect match-all classe0 (id 7)
   Match access-group  34
```

The table below describes the significant fields shown in the display.

Table 18: show class-map type inspect Field Descriptions

Field	Description
Class Map	Inspect type class maps being displayed. Output is displayed for each configured class map. The choice for implementing class matches (for example, match-all) appears next to the traffic class.
Match	Match criteria specified for the class map. For inspect type class maps without any protocols specified, the criteria are **access-group**, **class-map**, **protocol**, and **user-group**. For inspect type class maps with protocols specified, the criteria are **no**and **service**.

Related Commands

Command	Description
show class-map type port-filter	Displays port-filter class maps and their matching criteria.

show class-map type urlfilter

To display URL filter class maps and their matching criteria, use the **show class-map type urlfilter** command in privileged EXEC mode.

show class-map type urlfilter [{**trend** | **n2h2** | **websense**}] [*class-map-name*]

Syntax Description

trend	(Optional) Specifies Trend Micro class maps.
n2h2	(Optional) Specifies SmartFilter class maps.
websense	(Optional) Specifies Websense class maps.
class-map-name	(Optional) Name of the URL filter class map.

Command Default

Information for all local URL filter class maps is displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(15)XZ	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use the **show class-map type urlfilter**command to display all local URL filter class maps and their matching criteria. To display class maps for a particular URL filtering server type--Trend Micro, SmartFilter or Websense--include the appropriate keyword. To display the matching criteria for a particular class map, specify the class map name.

Examples

The following is sample output from the **show class-map type urlfilter**command when three local URL filtering class maps have been configured:

```
Router# show class-map type urlfilter

 Class Map type urlfilter match-any untrusted-domain-class (id 1)
  Match server-domain urlf-glob untrusted-domain-param

 Class Map type urlfilter match-any trusted-domain-class (id 2)
  Match server-domain urlf-glob trusted-domain-param

 Class Map type urlfilter match-any keyword-class (id 4)
  Match url-keyword urlf-glob keyword-param
```

The following is sample output from the **show class-map type urlfilter trend**command when one Trend Micro URL filtering class map has been configured:

```
Router# show class-map type urlfilter trend
 Class Map type urlfilter trend match-any drop-category (id 3)
  Match url category Adult-Mature-Content
```

```
  Match url category Gambling
  Match url category Personals-Dating
```

The following is sample output from the **show class-map type urlfilter websense**command:

```
Router# show class-map type urlfilter websense
 Class Map type urlfilter websense match-any websense-map (id 5)
  Match server-response any
```

The table below describes the significant fields shown in the display.

Table 19: show class-map type urlfilter Field Descriptions

Field	Description
Class Map	URL filtering class map being displayed. Output is displayed for each configured class map of the type of URL filtering specified--**trend**, **n2h2**, or **websense**. The default URL filtering type is **local**. The choice for implementing class matches (for example, match-any) appears next to the traffic class.
Match	Match criteria specified for the class map. For local URL filtering class maps, the criteria are **server-domain urlf-glob** parameter maps and the **url-keyword urlf-glob** parameter map. For Trend-Micro URL filtering class maps, the criteria are **url-category** and **url-reputation**. For SmartFilter and Websense class maps, the match criterion is **server-response any**.

show clock detail

To display the clock details for Cisco IOS public key infrastructure (PKI), use the **show clock detail** command in EXEC mode.

show clock detail

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.1	This command was introduced.

Examples

The following example is sample output for the **show clock detail** command:

```
Router # show clock detail
07:07:35.514 IST Sun Jun 3 2018
Time source is user configuration
```

show content-scan

Note Effective with Cisco IOS Release 15.4(2)T, the **show content-scan** command is replaced by the **show cws** command. See the **show cws** command for more information.

To display content scan information, use the **show content-scan** command in user EXEC or privileged EXEC mode.

show content-scan {**session** {**active** [{**detail** | **egress-vrf** *vrf-number* | **ingress-vrf** *vrf-number* | **ip-addr** *ip-address* [{**all**}]}] | **history** *sessions*} | **statistics** [{**all** | **detailed** | **failures** | **memory-usage**}] | **summary**}

Syntax Description

session	Displays content-scan session information.
active	Displays active sessions.
detail	(Optional) Displays content-scan session details.
egress-vrf	(Optional) Displays information about the virtual routing and forwarding (VRF) instance at the egress interface.
vrf-number	(Optional) Egress or ingress VRF ID. Valid values are from 0 to 1024.
igress-vrf	(Optional) Displays information about the VRF instance at the ingress interface.
ip-addr *ip-address*	(Optional) Displays information about the specified IP address.
all	(Optional) Displays information about all sessions.
history	Displays information about terminated sessions.
sessions	Number of sessions. Valid values are from 1 to 512.
statistics	Displays statistics of the content scanned.
detailed	(Optional) Displays detailed statistics of the content scanned.
failures	(Optional) Displays content-scan failure statistics.
memory-usage	(Optional) Displays content-scan memory usage statistics.
summary	Displays a summary of the content scan information.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
15.2(1)T1	This command was introduced.
15.2(4)M	This command was modified. The **detailed**, **failures**, and **memory-usage** keywords were added.
15.4(1)T	This command was modified. The **detail**, **egress-vrf**, **ingress-vrf**, **ip-addr**, and **all** keywords and the *vrf-number* and *ip-address* arguments were added.
15.4(2)T	This command was replaced by the **show cws** command.

Usage Guidelines

Cloud Web Security provides content scanning of HTTP and secure HTTP (HTTPS) traffic and malware protection services to web traffic. The content-scanning process redirects client web traffic to the cloud web security servers. These servers scan the web traffic content and allow or block traffic based on compliance with the configured policies and thus protect clients from malware. Content scanning is enabled on an Internet-facing WAN interface to protect the web traffic that goes out. Use the **show content-scan** command to view content-scan information.

The **show content-scan session history** command displays information about a maximum of 512 terminated sessions.

Examples

The following is sample output from the **show content-scan session history** command:

```
Device# show content-scan session history 6

 Protocol  Source             Destination           Bytes         URI                 Time

 HTTP      192.168.100.2:1347 209.165.201.104:80    (102:45)       www.google.com
00:01:13
 HTTP      192.168.100.2:1326 209.165.201.106:80    (206:11431)    www.google.com
00:12:55
 HTTP      192.168.100.2:1324 209.165.201.105:80    (206:11449)    www.google.com
00:15:20
 HTTP      192.168.100.2:1318 209.165.201.105:80    (206:11449)    www.google.com
00:17:43
 HTTP      192.168.100.2:1316 209.165.201.104:80    (206:11449)    www.google.com
00:20:04
 HTTP      192.168.100.2:1315 10.254.145.107:80     (575:1547)     alert.scansafe.net
00:21:32
```

The following table describes the significant fields shown in the display.

Table 20: show content-scan session history Field Descriptions

Field	Description
Protocol	Protocol used for content scanning.
Source	IP address of the source with the port number.
Destination	IP address of the destination with the port number.
URI	Uniform Resource Identifier (URI) that identifies a name or a resource on the Internet.

Field	Description
Time	Duration of time when a session was terminated.

The following is sample output from the **show content-scan statistics** command:

```
Device# show content-scan statistics

 Current HTTP sessions: 3
 Current HTTPS sessions: 0
 Total HTTP sessions: 11
 Total HTTPS sessions: 0
 White-listed sessions: 0
 Time of last reset: 00:01:58
```

The following table describes the fields shown in the display.

Table 21: show content-scan statistics Field Descriptions

Field	Description
Current HTTP sessions	Number of current HTTP sessions.
Current HTTPS sessions	Number of current secure HTTP (HTTPS) sessions.
Total HTTP sessions	Total number of HTTP sessions.
Total HTTPS sessions	Total number of HTTPS sessions.
White-listed sessions	Number of sessions that are on the allowed list. An allowed list is an approved list of entities that are provided a particular privilege, service, mobility, access, or recognition. Allowed listing means to grant access.
Time of last reset	Duration of time since sessions were last reset.

The following is sample output from the **show content-scan statistics failures** command:

```
Device# show content-scan statistics failures

Reset during proxy Mode:                0
HTTPS reconnect failures:               0
Buffer enqueue failures:                0
Buffer length exceeded:                 0
Particle coalesce failures:             0
L4F failures:                           0
Lookup failures:                        0
Memory failures:                        0
Tower unreachable:                      0
Resets sent:                            0
```

The following table describes the significant fields shown in the display.

Table 22: show content-scan statistics failures Field Descriptions

Field	Description
Reset during proxy Mode	Reset messages that are received when content scan is in proxy mode.
HTTPS reconnect failures	Connection failures while reconnecting to HTTPS.
Buffer enqueue failures	Buffering queue failures. When a packet fails to reach its destination, the packet is buffered in a queue for a retry. This queue to which packets are buffered can fail, and this failure is added to the statistics.
Buffer length exceeded	Packets that exceed the buffer length.
Particle coalesce failures	Packet defragmentation failures. When content scan receives packet fragments, these fragments are joined together or coalesced, and any failures during the coalescing are added to the statistics.
L4F failures	Layer 4 Forwarding (L4F) failures. When content scan and L4F is out of sync with each other, the statistics are incremented. **Note** We recommend that you inform TAC, if this counter increments rapidly.
Lookup failures	Content-scan entry lookup failures. During normal packet flows, content scan entries are checked at certain points. When such a lookup fails (when it was not expected to fail), it is added to the statistics.
Memory failures	Memory failures in the content scan subsystem (can be malloc, chunk_malloc, list, and so on).
Tower unreachable	Content-scan tower unreachable during packet flows.
Resets sent	Packet processing errors. During packet processing, if errors are encountered, reset messages are sent to end hosts.

The following sample output from the **show content-scan session active egress-vrf** command:

```
Device# show content-scan session active egress-vrf 1

Protocol      Source          Destination     Bytes             Time
HTTP [0]:     10.1.1.1:25176   10.2.2.1:80    (262:10495)       00:00:00
        URI: 10.2.2.1
        Username/usergroup(s): /
```

Related Commands

Command	Description
content-scan out	Enables content scanning on an egress interface.
debug content-scan	Enables content-scan debugging.

show crypto ace redundancy through show cts sxp

show crypto ace redundancy

To display information about a Blade Failure Group, use the **show crypto ace redundancy** command in privileged EXEC mode.

show crypto ace redundancy

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)SXE2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example shows information about a Blade Failure Group that has a group ID of 1 and consists of two IPSec VPN SPAs--one IPSec VPN SPA is in slot 3, subslot 0 and one IPSec VPN SPA is in slot 5, subslot 0:

```
Router# show crypto ace redundancy
-------------------------------------
LC Redundancy Group ID            :1
Pending Configuration Transactions:0
Current State                     :OPERATIONAL
Number of blades in the group     :2
Slots
-------------------------------------
Slot:3 Subslot:0
Slot state:0x36
Booted
Received partner config
Completed Bulk Synchronization
Crypto Engine in Service
Rebooted 22 times
Initialization Timer not running
Slot:5 Subslot:0
Slot state:0x36
Booted
Received partner config
Completed Bulk Synchronization
Crypto Engine in Service
Rebooted 24 times
Initialization Timer not running
ACE B2B Group State:OPERATIONAL Event:BULK DONE
ACE B2B Group State:CREATED Event:CONFIG_DOWNLOAD_DONE
ACE B2B Group State:DELETED Event:CONFIG_DELETE
ACE B2B Group State:OPERATIONAL Event:BULK DONE
ACE B2B Group State:CREATED Event:CONFIG_DOWNLOAD_DONE
ACE B2B Group State:DELETED Event:CONFIG_DELETE
```

```
ACE B2B Group State:OPERATIONAL Event:CONFIG_DOWNLOAD_DONE
ACE B2B Group State:DELETED Event:CONFIG_ADD
ACE B2B Group State:CREATED Event:UNDEFINED B2B HA EVENT
ACE B2B Group State:CREATED Event:CONFIG_DOWNLOAD_DONE
```

Related Commands

Command	Description
linecard-group feature card	Assigns a group ID to a Blade Failure Group.
redundancy	Enters redundancy configuration mode.
show redundancy linecard-group	Displays the components of a Blade Failure Group.

show crypto ca certificates

Note This command was replaced by the **show crypto pki certificates** command effective with Cisco IOS Release 12.3(7)T.

To display information about your certificate, the certification authority certificate, and any registration authority certificates, use the **show crypto ca certificates** command in EXEC mode.

show crypto ca certificates

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.3 T	This command was introduced.

Usage Guidelines

This command shows information about the following certificates:

- Your certificate, if you have requested one from the CA (see the **crypto pki enroll** command)
- The certificate of the CA, if you have received the CA's certificate (see the **crypto pki authenticate** command)
- RA certificates, if you have received RA certificates (see the **crypto pki authenticate** command)

Examples

The following is sample output from the **show crypto ca certificates** command after you authenticated the CA by requesting the CA's certificate and public key with the **crypto pki authenticate** command:

```
CA Certificate
  Status: Available
  Certificate Serial Number: 3051DF7123BEE31B8341DFE4B3A338E5F
  Key Usage: Not Set
```

The CA certificate might show Key Usage as "Not Set."

The following is sample output from the **show crypto ca certificates** command, and shows the router's certificate and the CA's certificate. In this example, a single, general purpose RSA key pair was previously generated, and a certificate was requested but not received for that key pair.

```
Certificate
  Subject Name
    Name: myrouter.example.com
    IP Address: 10.0.0.1
    Serial Number: 04806682
  Status: Pending
  Key Usage: General Purpose
    Fingerprint: 428125BD A3419600 3F6C7831 6CD8FA95 00000000
```

```
CA Certificate
  Status: Available
  Certificate Serial Number: 3051DF7123BEE31B8341DFE4B3A338E5F
  Key Usage: Not Set
```

Note that in the previous sample, the router's certificate Status shows "Pending." After the router receives its certificate from the CA, the Status field changes to "Available" in the **show** output.

The following is sample output from the **show crypto ca certificates** command, and shows two router's certificates and the CA's certificate. In this example, special usage RSA key pairs were previously generated, and a certificate was requested and received for each key pair.

```
Certificate
  Subject Name
    Name: myrouter.example.com
    IP Address: 10.0.0.1
  Status: Available
  Certificate Serial Number: 428125BDA34196003F6C78316CD8FA95
  Key Usage: Signature

Certificate
  Subject Name
    Name: myrouter.example.com
    IP Address: 10.0.0.1
  Status: Available
  Certificate Serial Number: AB352356AFCD0395E333CCFD7CD33897
  Key Usage: Encryption

CA Certificate
  Status: Available
  Certificate Serial Number: 3051DF7123BEE31B8341DFE4B3A338E5F
  Key Usage: Not Set
```

The following is sample output from the **show crypto ca certificates** command when the CA supports an RA. In this example, the CA and RA certificates were previously requested with the **crypto ca authenticate** command.

```
CA Certificate
  Status: Available
  Certificate Serial Number: 3051DF7123BEE31B8341DFE4B3A338E5F
  Key Usage: Not Set
RA Signature Certificate
  Status: Available
  Certificate Serial Number: 34BCF8A0
  Key Usage: Signature

RA KeyEncipher Certificate
  Status: Available
  Certificate Serial Number: 34BCF89F
  Key Usage: Encryption
```

Related Commands

Command	Description
crypto pki authenticate	Authenticates the CA (by obtaining the certificate of the CA).
crypto pki enroll	Obtains the certificates of your router from the CA.
debug crypto pki messages	Displays debug messages for the details of the interaction (message dump) between the CA and the route.

Command	Description
debug crypto pki transactions	Displays debug messages for the trace of interaction (message type) between the CA and the router.

show crypto ca crls

Note This command was replaced by the **show crypto pki crls** command effective with Cisco IOS Release 12.3(7)T.

To display the current certificate revocation list (CRL) on router, use the **show crypto ca crls** command in EXEC mode.

show crypto ca crls

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
12.1	This command was introduced.

Examples

The following is sample output of the **show crypto ca crls**command:

```
Router# show crypto ca crls

          CRL Issuer Name:
              OU = sjvpn, O = cisco, C = us
              LastUpdate: 16:17:34 PST Jan 10 2002
              NextUpdate: 17:17:34 PST Jan 11 2002
              Retrieved from CRL Distribution Point:
                LDAP: CN = CRL1, OU = sjvpn, O = cisco, C = us
```

Related Commands

Command	Description
crypto pki crl request	Requests that a new CRL be obtained immediately from the CA.

show crypto ca roots

The **show crypto ca roots**command is replaced by the **show crypto ca trustpoints** command. See the **show crypto ca trustpoints**command for more information.

show crypto ca timers

Note This command was replaced by the **show crypto pki timers** command effective with Cisco IOS Release 12.3(8)T.

To display the status of the managed timers that are maintained by Cisco IOS for public key infrastructure (PKI), use the **show crypto ca timers**command in EXEC mode.

show crypto ca timers

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.

Usage Guidelines

For each timer, this command displays the time remaining before the timer expires. It also associates trustpoint certification authorities (CAs), except for certificate revocation list (CRL) timers, by displaying the CRL distribution point.

Examples

The following example is sample output for the **show crypto ca timers** command:

```
Router# show crypto ca timers
PKI Timers
| 4d15:13:33.144
 | 4d15:13:33.144  CRL http://msca-root.cisco.com/CertEnroll/msca-root.crl
 |328d11:56:48.372  RENEW msroot
 | 6:43.201  POLL verisign
```

Related Commands

Command	Description
auto-enroll	Enables autoenrollment.
crypto pki trustpoint	Declares the CA that your router should use.

show crypto ca trustpoints

Note This command was replaced by the **show crypto pki trustpoints** command effective with Cisco IOS Release 12.3(7)T and 12.2(18)SXD.

To display the trustpoints that are configured in the router, use the **show crypto pki trustpoints**command in privileged EXEC or user EXEC mode.

show crypto ca trustpoints

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC
User EXEC

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

This command replaces the show crypto ca roots command. If you enter the show crypto ca roots command, the output will be written back as the show crypto pki trustpoints command.

Examples

The following is sample output from the **show crypto ca trustpoints** command:

```
Router# show crypto ca trustpoints
Trustpoint bo:
    Subject Name:
    CN = bomborra Certificate Manager
     O = cisco.com
     C = US
          Serial Number:01
    Certificate configured.
    CEP URL:http://bomborra
    CRL query url:ldap://bomborra
```

Related Commands

Command	Description
crypto pki trustpoint	Declares the CA that your router should use.

show crypto call admission statistics

To monitor Crypto Call Admission Control (CAC) statistics, use the **show crypto call admission statistics** command in user EXEC or privileged EXEC mode.

show crypto call admission statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.2(18)SXD1	This command was integrated into Cisco IOS Release 12.2(18)SXD1.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
15.1(3)T	This command was modified. The output of this command was updated to display information about IPsec SAs.

Usage Guidelines

You can use this command to display information about Crypto CAC configuration parameters and their history, including statistics regarding the current security association (SA) count, one or more SA being negotiated, total new SA requests, the number of Internet Key Exchange (IKE) and IPsec SA requests accepted and rejected, and details regarding rejected SA requests.

Examples

The following is sample output from the **show crypto call admission statistics** command:

```
Router# show crypto call admission statistics

----------------------------------------------------------------------
              Crypto Call Admission Control Statistics
----------------------------------------------------------------------
System Resource Limit:      111 Max IKE SAs:     0 Max in nego:  1000
Total IKE SA Count:           0 active:          0 negotiating:     0
Incoming IKE Requests:        0 accepted:        0 rejected:        0
Outgoing IKE Requests:        0 accepted:        0 rejected:        0
Rejected IKE Requests:        0 rsrc low:        0 Active SA limit: 0
                                                   In-neg SA limit: 0
IKE packets dropped at dispatch:        0
Max IPSEC SAs:   111
Total IPSEC SA Count:           0 active:          0 negotiating:     0
Incoming IPSEC Requests:        0 accepted:        0 rejected:        0
Outgoing IPSEC Requests:        0 accepted:        0 rejected:        0
Phase1.5 SAs under negotiation:         0
```

The table below shows significant fields shown in the display.

Table 23: show crypto call admission statistics Field Descriptions

Field	Description
System Resource Limit	Percentage of system resources that a router is using before IKE starts dropping all SA requests.
Max IKE SAs	Number of active IKE SA requests allowed on the router.
Total IKE SA Count	Number of IKE SAs.
active	Number of active SAs.
negotiating	Number of SA requests being negotiated.
Incoming IKE Requests	Number of incoming IKE SA requests.
Incoming IKE Requests accepted	Number of accepted IKE SA requests.
Incoming IKE Requests rejected	Number of rejected incoming IKE SA requests.
Outgoing IKE Requests	Number of outgoing IKE SA requests.
Outgoing IKE requests accepted	Number of accepted outgoing IKE SA requests.
Outgoing IKE requests rejected	Number of rejected outgoing IKE SA requests.
Rejected IKE Requests	Number of IKE requests that were rejected.
rsrc low	Number of IKE requests that were rejected because system resources were low or the preconfigured system resource limit was exceeded.
SA limit	Number of IKE SA requests that were rejected because the SA limit has been reached.
Incoming IPSEC Requests	Number of incoming IPsec SA requests.
Incoming IPSEC Requests accepted	Number of accepted IPsec SA requests.
Incoming IPSEC Requests rejected	Number of rejected incoming IPsec SA requests.
Outgoing IPSEC Requests	Number of outgoing IPsec SA requests.
Outgoing IPSEC requests accepted	Number of accepted outgoing IPsec SA requests.
Outgoing IPSEC requests rejected	Number of rejected outgoing IPsec SA requests.
Phase1.5 SAs	Number of negotiations in XAUTH or configuration exchange mode.

Related Commands

Command	Description
clear crypto call admission statistics	Clears counters that track the number of accepted and rejected IKE SA requests.

show crypto ctcp

To display information about a Cisco Tunnel Control Protocol (cTCP) session, use the **show crypto ctcp**command in privileged EXEC mode.

show crypto ctcp [**peer** *ip-address*] [**detail**]

Syntax Description

peer	(Optional) Displays information about a specific peer.
ip-address	(Optional) IP address of the specific peer.
detail	(Optional) Displays information about the local TCP sequence number and the TCP sequence number of the packets for the peer.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(9)T	This command was introduced.

Examples

The following **show** command output displays detailed information about a specific peer:

```
Router# show crypto ctcp peer 10.76.235.21 detail
    Remote                Local                VRF                  Status
    10.76.235.21:3519     10.76.248.239:10000                       CTCP_ACK_R
                          LocalSeq#6807392F    RemoteSeq#010116C7
```

The table below provides information about significant fields in the display.

Table 24: show crypto ctcp Field Descriptions

Field	Description
Remote	IP address of the remote peer with which this cTCP session is set up.
Local	IP address of the server to which the cTCP packets are addressed.
VRF	Name of the Virtual Private Network routing and forwarding (VRF) instance to which this session belongs. If the VRF is blank, the global routing table is used.
Status	Status of the cTCP session. CTCP_ACK_R is a successful cTCP setup. Any other state indicates that cTCP is not yet set up or failed to be set up.
LocalSeq	Sequence number of the last Transmission Control Protocol (TCP) packet sent by the server on this connection.
RemoteSeq	Sequence number of the last TCP packet that was received by the peer on this connection.

Related Commands

Command	Description
crypto ctcp	Configures cTCP encapsulation for Easy VPN.

show crypto datapath

To display the counters that help troubleshoot an encrypted data path, use the **show crypto datapath**command in privileged EXEC mode.

show crypto datapath {**ipv4** | **ipv6**} {**realtime** | **snapshot**} {**all** | **non-zero**} [{**error** | **internal** | **punt** | **success**}]

Syntax Description

ipv4	Designate IPv4 is used in the network.
ipv6	Designate IPv6 is used in the network.
realtime	Displays the counters that capture traffic statistics as they occur.
snapshot	Displays the counters that capture traffic statistics as of a single point in time.
all	Display all counters.
non-zero	Display all counters that have at least one event recorded.
error	(Optional) Display the packet processing and dropped packet errors.
internal	(Optional) Track the movement of a packet from end to end across an encrypted data path.
punt	(Optional) Display the instances when the configured processing method failed, and an alternative was used.
success	(Optional) Display the interfaces where packets were successfully processed.

Command Default

The command defaults are:

- IP version: **ipv4**
- Counters: **all**
- Display time: **realtime**

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

Use the **show crypto datapath counters command to troubleshoot an encrypted data path.**

Note Cisco recommends use of this command only for troubleshooting under the guidance of a Cisco TAC engineer.

You must specify the IP version used in the network. You can display all counters, only the counters that have recorded events, or one of these specific counters:

- Error counters track packet processing errors and associated packet drops. When a packet encounters an error, the first 64 bytes of that packet are stored in a buffer, to facilitate troubleshooting.
- Internal counters show the detailed movement of a packet, end to end, across an encrypted data path.
- Punt counters track instances when the configured packet processing method failed, and an alternative method was used. Because such instances might indicate a problem, it is useful to track them.
- Success counters help diagnose network performance problems. Frequently, although a network is configured for fast switching or CEF, packets are using a slower path. Success counters record the interfaces in the data path where packets were successfully processed and reveal the actual processing path.

You must also choose the display timeframe for the counters:

- The **realtime** option captures traffic statistics as they occur, and results in significant discrepancies between the first data reports and later data, because the counters increment with the traffic flow. This is the default option.
- The **snapshot** option captures traffic statistics as of a specific point in time, and results in a close match among all counts, because the counters do not increment with the continuing traffic flow.

Examples

The following example shows output from the **show crypto datapath command**. In this example, the **snapshot** option is specified for the timeframe, and only counters that have recorded events are displayed. The output of this command is intended for use by Cisco TAC engineers.

```
Router# show crypto datapath ipv4 snapshot non-zero

Success Statistics: Snapshot at 21:34:30 PST Mar 4 2006
  crypto check input core
    2nd round ok:            245      1st round ok:            118
  post crypto ip encrypt
    post encrypt ipflowok:   230
  crypto ceal post encrypt switch
    post encrypt ipflowok-2: 230
Error Statistics: Snapshot at 21:34:30 PST Mar 4 2006
Punt Statistics: Snapshot at 21:34:30 PST Mar 4 2006
  crypto ceal post decrypt switch
    fs to ps:                245
Internal Statistics: Snapshot at 21:34:30 PST Mar 4 2006
  crypto check input
    check input core not con 378      check input core consume 623
  crypto check input core
    came back from ce:       245      deny pak:                15
  crypto ipsec les fs
    not esp or ah:           1113
  post crypto ip decrypt
    decrypt switch:          245
  crypto decrypt ipsec sa check
    check ident success:     245
  crypto ceal post decrypt switch
    fs:                      245
  crypto ceal post decrypt fs
    les ip turbo fs:         245      tunnel ip les fs:        245
  crypto ceal post decrypt ps
```

```
  proc inline:             245
crypto ceal punt to process inline
  coalesce:                245      simple enq:              245
crypto ceal post encrypt switch
  ps:                      230
crypto ceal post encrypt ps
  ps coalesce:             230      simple enq:              230
crypto engine ps vec
  ip encrypt:              230
crypto send epa packets
  ucast next hop:          230      ip ps send:              230
```

Related Commands

Command	Description
show monitor event-trace	Displays contents of error history buffers.

show crypto debug-condition

To display crypto debug conditions that have already been enabled in the router, use the **show crypto debug-condition**command in privileged EXEC mode.

show crypto debug-condition [**peer**] [**connid**] [**spi**] [**fvrf**] [**gdoi-group** *groupname*] [**isakmp profile** *profile-name*] [**ivrf**] [**local** *ip-address*] [**unmatched**] [**username** *username*]

Syntax Description

peer	(Optional) Displays debug conditions related to the peer. Possible conditions can include peer IP address, subnet mask, hostname, username, and group key.
connid	(Optional) Displays debug conditions related to the connection ID.
spi	(Optional) Displays debug conditions related to the security parameter index (SPI).
fvrf	(Optional) Displays debug conditions related to the front-door virtual private network (VPN) routing and forwarding (FVRF) instance.
gdoi-group *groupname*	(Optional) Displays debug conditions related to the Group Domain of Interpretation (GDOI) group filter. • The *groupname*value is the name of the GDOI group.
isakmp profile *profile-name*	(Optional) Displays debug conditions related to the Internet Security Association Key Management Protocol (ISAKMP) profile filter. • The *profile-name*value is the name of the profile filter.
ivrf	(Optional) Displays debug conditions related to the inside VRF (IVRF) instance.
local *ip-address*	(Optional) Displays debug conditions related to the local address debug condition filters. • The *ip-address* is the IP address of the local crypto endpoint.
unmatched	(Optional) Displays debug messages related to the Internet Key Exchange (IKE), IP Security (IPsec), or the crypto engine, depending on what was specified via the **debug crypto condition unmatched** [**engine** | **gdoi-group**| **ipsec** | **isakmp**] command.
username *username*	(Optional) Displays debug messages related to the AAA Authentication (Xauth) or public key infrastructure (PKI) and authentication, authorization, and accounting (AAA) username filter.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(2)T	This command was introduced.

Release	Modification
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(11)T	The **gdoi-group** *groupname* **, isakmp profile** *profile-name* **, local** *ip-address* **,**and **username** *username* keywords and arguments were added.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

You can specify as many filter values as specified via the **debug crypto condition** command. (You cannot specify a filter value that you did not use in the **debug crypto condition** command.)

Examples

The following example shows how to display debug messages when the peer IP address is 10.1.1.1, 10.1.1.2, or 10.1.1.3 and when the connection ID 2000 of crypto engine 0 is used. This example also shows how to enable global debug crypto CLIs and enable the **show crypto debug-condition** command to verify conditional settings.

```
Router#
debug crypto condition connid 2000 engine-id 1
Router#
debug crypto condition peer ipv4 10.1.1.1
Router#
debug crypto condition peer ipv4 10.1.1.2
Router#
debug crypto condition peer ipv4 10.1.1.3
Router#
debug crypto condition unmatched
! Verify crypto conditional settings.
Router#
show crypto debug-condition
Crypto conditional debug currently is turned ON
IKE debug context unmatched flag:ON
IPsec debug context unmatched flag:ON
Crypto Engine debug context unmatched flag:ON
IKE peer IP address filters:
10.1.1.1  10.1.1.2   10.1.1.3
Connection-id filters:[connid:engine_id]2000:1,
! Enable global crypto CLIs to start conditional debugging.
Router#
debug crypto isakmp
Router#
debug crypto ipsec
Router#
debug crypto engine
```

The following example shows how to disable all crypto conditional settings via the **reset** keyword:

```
Router#
debug crypto condition reset
! Verify that all crypto conditional settings have been disabled.
Router#
show crypto debug-condition
Crypto conditional debug currently is turned OFF
IKE debug context unmatched flag:OFF
```

```
IPsec debug context unmatched flag:OFF
Crypto Engine debug context unmatched flag:OFF
```

Related Commands

Command	Description
debug crypto condition	Defines conditional debug filters.
debug crypto condition unmatched	Displays crypto conditional debug messages when context information is unavailable to check against debug conditions.

show crypto dynamic-map

To display a dynamic crypto map set, use the **show crypto dynamic-map** command in EXEC mode.

show crypto dynamic-map [**tag** *map-name*]

Syntax Description

tag *map-name*	(Optional) Displays only the crypto dynamic map set with the specified *map-name*.

Command Modes

EXEC

Command History

Release	Modification
11.3 T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **show crypto dynamic-map** command to view a dynamic crypto map set.

Examples

The following is sample output for the **show crypto dynamic-map** command:

```
Router# show crypto dynamic-map
Crypto Map Template"vpn1" 1
        ISAKMP Profile: vpn1-ra
        No matching address list set.
        Security association lifetime: 4608000 kilobytes/3600 seconds
        PFS (Y/N): N
        Transform sets={
                vpn1,
```

The following partial configuration was in effect when the above **show crypto dynamic-map** command was issued:

```
crypto dynamic-map vpn1 1
 set transform-set vpn1
 set isakmp-profile vpn1-ra
 reverse-route
```

Related Commands

Command	Description
show crypto map	Views the crypto map configuration.

show crypto eli

To display how many IKE security associations (SAs) and IPsec sessions are active and how many Diffie-Hellman (DH) keys are in use for each hardware crypto engine, use the **show crypto eli** in user EXEC or privileged EXEC mode.

show crypto eli

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
12.1(5)E	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS release 12.2(33)SXH.

Usage Guidelines

Use this command to obtain a snapshot of how many Internet Key Exchange (IKE) and IPsec sessions are active and how many DH keys are in use for each hardware crypto engine. The **show crypto eli** command also allows you to see how far an Integrated Service Adapter (ISA) is from reaching its maximum limit. The ELI component of the command calls the Encryption Layer Interface.

Note IKE is a key management protocol standard that is used in conjunction with the IPsec standard. IPsec can be configured without IKE. However, IKE enhances IPsec by providing additional features, flexibility, and ease of configuration for the IPsec standard. When IKE is used with IPsec, IKE automatically negotiates the IPsec SAs.

Examples

The following is sample output for the **show crypto eli** command:

```
Device# show crypto eli

Encryption Layer :  ACTIVE
 Number of crypto engines = 2.
 Slot-3 crypto engine details.
 Capability-IPSec :No-IPPCP, 3DES, NoRSA
 IKE-Session   :    0 active,  2029 max, 0 failed
 DH-Key        :    0 active,  1014 max, 0 failed
 IPSec-Session :    0 active,  4059 max, 0 failed
 Slot-5 crypto engine details.
 Capability-IPSec :No-IPPCP, 3DES, NoRSA
 IKE-Session   :    0 active,  2029 max, 0 failed
 DH-Key        :    0 active,  1014 max, 0 failed
 IPSec-Session :    0 active,  4059 max, 0 failed
```

The following is sample output for the **show crypto eli** command for the IPSec VPN SPA:

```
Device# show crypto eli

Hardware Encryption : ACTIVE
 Number of hardware crypto engines = 2

 CryptoEngine SPA-IPSEC-2G[3/0] details: state = Active
 Capability      :
     IPSEC: DES, 3DES, AES, RSA

 IKE-Session   :     0 active, 16383 max, 0 failed
 DH            :     0 active,  9999 max, 0 failed
 IPSec-Session :     0 active, 65534 max, 0 failed

 CryptoEngine SPA-IPSEC-2G[3/1] details: state = Active
 Capability      :
     IPSEC: DES, 3DES, AES, RSA

 IKE-Session   :     1 active, 16383 max, 0 failed
 DH            :     0 active,  9999 max, 0 failed
 IPSec-Session :     2 active, 65534 max, 0 failed
```

The table below describes significant fields shown in the display.

Table 25: show crypto eli summary Field Descriptions

Field	Description
active	The number of sessions that are active on a given hardware crypto engine.
max	The maximum number of sessions allowed for any given IKE, DH, or IPsec entry.
failed	The number of times that Cisco IOS software attempted to create more sessions than the number specified in “max.”

show crypto eng qos

To monitor and maintain low latency queueing (LLQ) for IPSec encryption engines, use the show crypto eng qos command in privileged EXEC mode.

show crypto eng qos

Syntax Description

This command has no keywords or arguments.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(13)T	This command was introduced in Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **show crypto eng qos** command to determine if QoS is enabled on LLQ for IPSec encryption engines.

Examples

The following example shows how to determine if LLQ for IPSec encryption engines is enabled:

```
Router# show crypto eng qos
crypto engine name: Multi-ISA Using VAM2
        crypto engine type: hardware
                      slot: 5
                  queuing: enabled
         visible bandwidth: 30000 kbps
                  llq size: 0
    default queue size/max: 0/64
      interface table size: 32
  FastEthernet0/0 (3), iftype 1, ctable size 16, input filter:ip
precedence 5
    class voice (1/3), match ip precedence 5
          bandwidth 500 kbps, max token 100000
          IN  match pkt/byte 0/0, police drop 0
          OUT match pkt/byte 0/0, police drop 0
  class default, match pkt/byte 0/0, qdrop 0
  crypto engine bandwidth:total 30000 kbps, allocated 500 kbps
```

The field descriptions in the above display are self-explanatory.

show crypto engine

To display a summary of the configuration information for the crypto engines, use the **show crypto engine** command in privileged EXEC mode.

show crypto engine {**accelerator** {**statistic** | **ring** {**control** | **packet** | **pool**}} | **brief** | **configuration** | **connections** {**active** | **dh** | **dropped-packet** | **flow**} | **qos** | **token** [**detail**]}

Syntax Description

accelerator	Displays crypto accelerator information.
statistic	Displays crypto accelerator statistic information.
ring	Displays crypto accelerator ring information.
control	Displays control ring information.
packet	Displays packet ring information.
pool	Displays pool ring information.
brief	Displays a summary of the configuration information for the crypto engine.
configuration	Displays the version and configuration information for the crypto engine.
connections	Displays information about the crypto engine connections.
active	Displays all active crypto engine connections.
dh	Displays crypto engine Diffie-Hellman table entries.
dropped-packet	Displays crypto engine dropped packets.
flow	Displays crypto engine flow table entries.
qos	Displays quality of service (QoS) information. • This keyword has a null output if any advanced integration module (AIM) except AIM-VPN/SSL-1 is used. The command-line interface (CLI) will accept the command, but there will be no output.
token	Displays the crypto token engine information.
detail	(Optional) Displays the detailed information of the crypto token engine.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.2	This command was introduced on the Cisco 7200, RSP7000, and 7500 series routers.

Release	Modification
12.2(15)ZJ	This command was implemented for the AIM-VPN/BPII on the following platforms: Cisco 2610XM, Cisco 2611XM, Cisco 2620XM, Cisco 2621XM, Cisco 2650XM, and Cisco 2651XM.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.4(4)T	IPv6 address information was added to command output.
12.4(9)T	AIM-VPN/SSL-3 encryption module information was added to command output.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(22)T	The **token** and **detail**keywords were added.
Cisco IOS XE Release 2.2	This command was integrated into Cisco IOS XE Release 2.2. The **accelerator**, **control, packet, pool, ring**, and **static** keywords were added.

Usage Guidelines

This command displays all crypto engines and displays the AIM-VPN product name.

If a hardware crypto engine does not support native Group Domain of Interpretation (GDOI) header preservation, the **show crypto engine connections active** output for Group Encrypted Transport VPN (GET VPN) IP security (IPsec) connections displays a disallowed IP address of 0.0.0.0 (see the **show crypto engine connections active**"Examples" section).

Examples

The following is sample output from the **show crypto engine brief**command shows typical crypto engine summary information:

```
Router# show crypto engine brief
crypto engine name:  Virtual Private Network (VPN) Module
        crypto engine type:  hardware
                     State:  Enabled
                  Location:  aim 0
 VPN Module in slot:  0
       Product Name:  AIM-VPN/SSL-3
  Software Serial #:  55AA
          Device ID:  001F - revision 0000
          Vendor ID:  0000
        Revision No:  0x001F0000
       VSK revision:  0
       Boot version:  255
        DPU version:  0
        HSP version:  3.3(18) (PRODUCTION)
       Time running:  23:39:30
               Compression:  Yes
                       DES:  Yes
                   3 DES:  Yes
                 AES CBC:  Yes (128,192,256)
                AES CNTR:  No
    Maximum buffer length:  4096
         Maximum DH index:  3500
         Maximum SA index:  3500
```

```
      Maximum Flow index:  7000
    Maximum RSA key size:  2048
      crypto engine name:  Cisco VPN Software Implementation
      crypto engine type:  software
           serial number:  CAD4FCE1
     crypto engine state:  installed
  crypto engine in slot:  N/A
```

The table below describes the significant fields shown in the display.

Table 26: show crypto engine brief Field Descriptions

Field	Description
crypto engine name	Name of the crypto engine as assigned with the *key-name* argument in the **crypto key generate dss** command.
crypto engine type	If "software" is listed, the crypto engine resides in either the Route Switch Processor (RSP) (the Cisco IOS crypto engine) or in a second-generation Versatile Interface Processor (VIP2). If "crypto card" or "Encryption Service Adapter" (ESA) is listed, the crypto engine is associated with an ESA.
crypto engine state	The state "installed" indicates that a crypto engine is located in the given slot, but it is not configured for encryption. The state "dss key generated" indicates the crypto engine found in that slot has Digital Signature Standard (DSS) keys already generated.
crypto engine in slot	Chassis slot number of the crypto engine. For the Cisco IOS crypto engine, this is the chassis slot number of the RSP.

The following is sample output from **show crypto engine**command shows IPv6 information:

```
Router# show crypto engine connections
    ID Interface  Type  Algorithm           Encrypt  Decrypt IP-Address
     1 Et2/0      IPsec MD5                       0       46 FE80::A8BB:CCFF:FE01:2C02
     2 Et2/0      IPsec MD5                      41        0 FE80::A8BB:CCFF:FE01:2C02
     5 Tu0        IPsec SHA+DES                   0        0 3FFE:2002::A8BB:CCFF:FE01:2C02

     6 Tu0        IPsec SHA+DES                   0        0 3FFE:2002::A8BB:CCFF:FE01:2C02

  1001 Tu0        IKE   SHA+DES                   0        0 3FFE:2002::A8BB:CCFF:FE01:2C02
```

The following **show crypto engine** command output displays information for a situation in which a hardware crypto engine does not support native GDOI:

```
Router# show crypto engine connections active
Crypto Engine Connections
ID Interface     Type  Algorithm           Encrypt  Decrypt IP-Address
1079 Se0/0/0.10  IPsec AES+SHA                 0        0 0.0.0.0
1080 Se0/0/0.10  IPsec AES+SHA                 0        0 0.0.0.0
4364 <none>      IKE   SHA+3DES                0        0
4381 <none>      IKE   SHA+3DES                0        0
```

Related Commands

Command	Description
crypto engine accelerator	Enables the use of the onboard hardware accelerator for IPSec encryption.

show crypto engine accelerator sa-database

To display active (in-use) entries in the platform-specific virtual private network (VPN) module database, use the **show crypto engine accelerator sa-database** command in privileged EXEC mode.

show crypto engine accelerator sa-database

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(1)XC	This command was introduced on the Cisco 1720 and Cisco 1750 platforms.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines

Use this command when encrypted traffic is sent to the router and a problem with the encryption module is suspected.

Note The **show crypto engine accelerator sa-database** command is intended only for Cisco Systems TAC personnel to collect debugging information.

Examples

The following is sample output for the **show crypto engine accelerator sa-database** command:

```
Router# show crypto engine accelerator sa-database
Flow Summary
        Index   Algorithms
        005      tunnel inbound  esp-md5-hmac esp-des ah-sha-hmac
        006      tunnel outbound esp-md5-hmac esp-des ah-sha-hmac
        007      tunnel inbound  esp-md5-hmac esp-des ah-sha-hmac
        008      tunnel outbound esp-md5-hmac esp-des ah-sha-hmac
        009      tunnel inbound  esp-md5-hmac esp-des ah-sha-hmac
        010      tunnel outbound esp-md5-hmac esp-des ah-sha-hmac
SA Summary:
        Index   DH-Index        Algorithms
        003     001(deleted)    DES SHA
        004     002(deleted)    DES SHA
DH Summary
        Index Group Config
```

Related Commands

Command	Description
debug crypto engine acclerator logs	Enables logging of commands and associated parameters sent from the VPN module driver to the VPN module hardware using a debug flag.

show crypto engine accelerator ring

To display the contents and status of the control command, transmit packets, and receive packet rings used by the hardware accelerator crypto engine, use the **show crypto engine accelerator ring** command in privileged EXEC mode.

show crypto engine accelerator ring [{**control** | **packet** | **pool**}]

Syntax Description

control	(Optional) Number of control commands that are queued for execution by the hardware accelerator crypto engine are displayed.
packet	(Optional) Contents and status information for the transmit packet rings that are used by the hardware accelerator crypto engine are displayed.
pool	(Optional) Contents and status information for the receive packet rings that are used by the hardware accelerator crypto engine are displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(3)XL	This command was introduced for the Cisco uBR905 cable access router.
12.2(2)XA	Support was added for the Cisco uBR925 cable access router.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T and implemented for the AIM-VPN/EPII and AIM-VPN/HPII on the following platforms: Cisco 2691, Cisco 3660, Cisco 3725, and Cisco 3745.
12.2(15)ZJ	This command was implemented for the AIM-VPN/BPII on the following platforms: Cisco 2610XM, Cisco 2611XM, Cisco 2620XM, Cisco 2621XM, Cisco 2650XM, and Cisco 2651XM.
12.3(4)T	The AIM-VPN/BPII was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2610XM, Cisco 2611XM, Cisco 2620XM, Cisco 2621XM, Cisco 2650XM, and Cisco 2651XM.

Usage Guidelines

This command displays the command ring information.

If there were valid data in any of the rings, the ring entry would be printed.

Examples

The following example shows the command ring information:

```
Router# show crypto engine accelerator ring packet
PPQ RING:
cmd ring:head = 10 tail =10
result ring:head = 10 tail =10
destination ring:head = 10 tail =10
source ring:head = 10 tail =10
free ring:head = 0 tail =255
        00000000  071A96C5
```

```
        00000000  071A96C5
        00000001  071A9465
        00000001  071A9465
        00000002  071A9205
        00000002  071A9205
.
.
.
```

Related Commands

Command	Description
clear crypto engine accelerator counter	Resets the statistical and error counters for the hardware accelerator to zero.
crypto ca	Defines the parameters for the certification authority used for a session.
crypto cisco	Defines the encryption algorithms and other parameters for a session.
crypto dynamic-map	Creates a dynamic map crypto configuration for a session.
crypto engine accelerator	Enables the use of the onboard hardware accelerator for IPSec encryption.
crypto ipsec	Defines the IPSec SAs and transformation sets.
crypto isakmp	Enables and defines the IKE protocol and its parameters.
crypto key	Generates and exchanges keys for a cryptographic session.
crypto map	Creates and modifies a crypto map for a session.
debug crypto engine accelerator control	Displays each control command as it is given to the crypto engine.
debug crypto engine accelerator packet	Displays information about each packet sent for encryption and decryption.
show crypto engine accelerator sa-database	Displays the active (in-use) entries in the crypto engine SA database.
show crypto engine accelerator statistic	Displays the current run-time statistics and error counters for the crypto engine.
show crypto engine brief	Displays a summary of the configuration information for the crypto engine.
show crypto engine configuration	Displays the version and configuration information for the crypto engine.
show crypto engine connections	Displays a list of the current connections maintained by the crypto engine.

show crypto engine accelerator logs

To display information about the last 32 CryptoGraphics eXtensions (CGX) Library packet processing commands and associated parameters sent from the VPN module driver to the VPN module hardware, use the **show crypto engine accelerator logs** command in privileged EXEC mode.

show crypto engine accelerator logs

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(1)XC	This command was introduced on the Cisco 1720 and Cisco 1750 platforms.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines

Use this command when encrypted traffic is sent to the router and a problem with the encryption module is suspected. Use the **debug crypto engine accelerator logs** command to enable command logging before using this command.

Note The **show crypto engine accelerator logs** command is intended only for Cisco Systems TAC personnel to collect debugging information.

Examples

The following is sample output for the **show crypto engine accelerator logs** command:

```
Router# show crypto engine accelerator logs
Contents of packet log (current index = 20):
tag = 0x5B02, cmd = 0x5000
param[0] = 0x000E, param[1] = 0x57E8
param[2] = 0x0008, param[3] = 0x0000
param[4] = 0x0078, param[5] = 0x0004
param[6] = 0x142C, param[7] = 0x142C
param[8] = 0x0078, param[9] = 0x000C
tag = 0x5B03, cmd = 0x4100
param[0] = 0x000E, param[1] = 0x583C
param[2] = 0x0034, param[3] = 0x0040
param[4] = 0x00B0, param[5] = 0x0004
param[6] = 0x1400, param[7] = 0x1400
param[8] = 0x0020, param[9] = 0x000C
tag = 0x5C00, cmd = 0x4100
param[0] = 0x000E, param[1] = 0x57BC
param[2] = 0x0034, param[3] = 0x0040
param[4] = 0x00B0, param[5] = 0x0004
param[6] = 0x1400, param[7] = 0x1400
param[8] = 0x0020, param[9] = 0x000C
.
.
.
```

```
tag = 0x5A01, cmd = 0x4100
param[0] = 0x000E, param[1] = 0x593C
param[2] = 0x0034, param[3] = 0x0040
param[4] = 0x00B0, param[5] = 0x0004
param[6] = 0x1400, param[7] = 0x1400
param[8] = 0x0020, param[9] = 0x000C
Contents of cgx log (current index = 12):
cmd = 0x0074 ret = 0x0000
param[0] = 0x0010, param[1] = 0x028E
param[2] = 0x0039, param[3] = 0x0D1E
param[4] = 0x0100, param[5] = 0x0000
param[6] = 0x0000, param[7] = 0x0000
param[8] = 0x0000, param[9] = 0x0000
cmd = 0x0062 ret = 0x0000
param[0] = 0x0035, param[1] = 0x1BE0
param[2] = 0x0100, param[3] = 0x0222
param[4] = 0x0258, param[5] = 0x0000
param[6] = 0x0000, param[7] = 0x0000
param[8] = 0x0000, param[9] = 0x0000
cmd = 0x0063 ret = 0x0000
param[0] = 0x0222, param[1] = 0x0258
param[2] = 0x0000, param[3] = 0x0000
param[4] = 0x0000, param[5] = 0x0000
param[6] = 0x0000, param[7] = 0x020A
param[8] = 0x002D, param[9] = 0x0000
.
.
.
cmd = 0x0065 ret = 0x0000
param[0] = 0x0222, param[1] = 0x0258
param[2] = 0x0010, param[3] = 0x028E
param[4] = 0x00A0, param[5] = 0x0008
param[6] = 0x0001, param[7] = 0x0000
param[8] = 0x0000, param[9] = 0x0000
```

Related Commands

Command	Description
debug crypto engine acclerator logs	Enables logging of commands and associated parameters sent from the VPN module driver to the VPN module hardware using a debug flag.

show crypto engine accelerator statistic

To display IP Security (IPsec) encryption statistics and error counters for the onboard hardware accelerator of a device, the IPsec VPN shared port adapter (SPA) or a Cisco VPN Internal Service Module (ISM), use the **show crypto engine accelerator statistic** command in privileged EXEC mode.

show crypto engine accelerator statistic

Cisco ASR 1000 Series Aggregation Services Routers
show crypto engine accelerator statistic[{**platform**}]

IPsec VPN SPA (SPA-IPSEC-2G) and VSPA (WS-IPSEC-3G)
show crypto engine accelerator statistic[{**slot** *slot/subslot* | **all**}] [{**coreutil** | **detail**}]

Syntax Description

platform	(Optional) Displays platform statistics and information required for debugging.
slot *slot/subslot*	(Optional) Specifies the chassis slot number and secondary slot number on the SPA Interface Processor (SIP), where the SPA is installed. Displays platform statistics for the corresponding SPA.
all	(Optional) Displays platform statistics for all IPsec VPN SPAs or VPN Services Port Adapter (VSPA) on the device.
coreutil	(Optional) Displays VPN core utilization statistics.
detail	(Optional) Displays SPA platform statistics and network interface controller statistics. The controller statistics contain Layer 2 counters.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.1(1)XC	This command was introduced in the Cisco 1700 Series Modular Access Routers and other Cisco devices that support hardware accelerators for IPsec encryption.
12.1(3)XL	This command was modified. This command was implemented in Cisco uBR905 Cable Access Routers.
12.2(2)XA	This command was modified. Support was added for Cisco uBR925 Cable Access Routers.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T and implemented for the AIM-VPN/EPII and AIM-VPN/HPII on the following platforms: Cisco 2691, Cisco 3660, Cisco 3725, and Cisco 3745. In addition, the output was enhanced to display compression statistics.
12.2(15)ZJ	This command was modified. This command was implemented for the AIM-VPN/BPII on the following platforms: Cisco 2610XM, Cisco 2611XM, Cisco 2620XM, Cisco 2621XM, Cisco 2650XM, and Cisco 2651XM.

Release	Modification
12.3(4)T	The AIM-VPN/BPII was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2610XM, Cisco 2611XM, Cisco 2620XM, Cisco 2621XM, Cisco 2650XM, and Cisco 2651XM.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA to support the IPsec VPN SPA on Cisco 7600 Series Routers.
12.4(9)T	This command was modified. Output was added for the AIM-VPN Secure Sockets Layer (SSL) encryption module.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH to support the IPsec VPN SPA on Cisco Catalyst 6500 Series Switches.
12.2(33)SXI	This command was modified. The **coreutil** keyword was added for VSPA, and the output was added to display the percentage utilization with other utilization statistics in the crypto engine.
12.4(24)T	This command was modified. The output was enhanced to display reassembly and fragmentation drop counters for VPN Service Adapter (VSA) traffic statistics.
Cisco IOS XE Release 3.7S	This command was integrated into Cisco IOS XE Release 3.7S. The **platform** keyword was added. The output was also enhanced to display platform statistics and debugging information for the crypto engine.
15.3(2)T	This command was modified. The output of this command was enhanced to display statistical information about the Cisco VPN ISM.
Cisco IOS XE Fuji 16.8.1	Supported added for Cisco ISR4300 Series platforms.

Usage Guidelines

No specific usage guidelines apply to hardware accelerators.

The **show crypto engine accelerator statistic platform** command displays the output from a series of **show** commands. The specific commands depend on the platform on which the command is executed. This is indicated in the command output.

Note Refer to the appropriate hardware manual for slot information. For SIPs, refer to the platform-specific *SPA Hardware Installation Guide* or the corresponding "Identifying Slots and Subslots for SIPs and SPAs" module in the platform-specific *SPA Software Configuration Guide*.

IPsec VPN SPA and VSPA

Use the **slot** keyword to display platform statistics for the corresponding SPA. The output with this keyword will not include network interface controller statistics.

Use the **all** keyword to display platform statistics for all IPsec VPN SPAs and VSPAs on the device. The output with this keyword will not include network interface controller statistics.

Use the **detail** keyword to display platform statistics for the SPA and network interface controller statistics. The controller statistics contain Layer 2 counters.

VSPA

Use the **coreutil** keyword to display VPN core utilization statistics. The output with this keyword will not include network interface controller statistics.

Tip You can add a time stamp to **show** commands by using the **exec prompt timestamp** command in line configuration mode.

Examples

Hardware VPN Module

The following example displays compression statistics for an onboard hardware accelerator of a device:

```
Device# show crypto engine accelerator statistic

Device:   AIM-VPN/SSL-3
Location: AIM Slot: 0
Virtual Private Network (VPN) Module in slot : 0
Statistics for Hardware VPN Module since the last clear of counters 85319 seconds ago
            560 packets in                          560 packets out
          95600 bytes in                         124720 bytes out
              0 paks/sec in                           0 paks/sec out
              0 Kbits/sec in                          0 Kbits/sec out
              0 packets decrypted                   560 packets encrypted
              0 bytes before decrypt             124720 bytes encrypted
              0 bytes decrypted                   95600 bytes after encrypt
              0 packets decompressed                  0 packets compressed
              0 bytes before decomp                   0 bytes before comp
              0 bytes after decomp                    0 bytes after comp
              0 packets bypass decompr                0 packets bypass compres
              0 bytes bypass decompres                0 bytes bypass compressi
              0 packets not decompress                0 packets not compressed
              0 bytes not decompressed                0 bytes not compressed
                 1.0:1 compression ratio                 1.0:1 overall
          10426 commands out                      10426 commands acknowledged
Last 5 minutes:
              0 packets in                            0 packets out
              0 paks/sec in                           0 paks/sec out
              0 bits/sec in                           0 bits/sec out
              0 bytes decrypted                       0 bytes encrypted
              0 Kbits/sec decrypted                   0 Kbits/sec encrypted
                 1.0:1 compression ratio                 1.0:1 overall
Errors:
    ppq full errors         :        0   ppq rx errors           :        0
    cmdq full errors        :        0   cmdq rx errors          :        0
    ppq down errors         :        0   cmdq down errors        :        0
    no buffer               :        0   replay errors           :        0
    dest overflow           :        0   authentication errors   :        0
    Other error             :        0   Raw Input Underrun      :        0
    IPSEC Unsupported Option:        0   IPV4 Header Length      :        0
    ESP Pad Length          :        0   IPSEC Decompression     :        0
    AH ESP seq mismatch     :        0   AH Header Length        :        0
    AH ICV Incorrect        :        0   IPCOMP CPI Mismatch     :        0
    IPSEC ESP Modulo        :        0   Unexpected IPV6 Extension:       0
    Unexpected Protocol     :        0   Dest Buf overflow       :        0
    IPSEC Pkt is fragment   :        0   IPSEC Pkt src count     :        0
    Invalid IP Version      :        0   Unwrappable             :        0
    SSL Output overrun      :        0   SSL Decompress failure  :        0
    SSL BAD Decomp History  :        0   SSL Version Mismatch    :        0
```

```
    SSL Input overrun       :        0   SSL Conn Modulo          :        0
    SSL Input Underrun      :        0   SSL Connection closed    :        0
    SSL Unrecognised content:        0   SSL record header length :        0
    PPTP Duplicate packet   :        0   PPTP Exceed max missed p :        0
    RNG self test fail      :        0   DF Bit set               :        0
    Hash Miscompare         :        0   Unwrappable object       :        0
    Missing attribute       :        0   Invalid attribute value  :        0
    Bad Attribute           :        0   Verification Fail        :        0
    Decrypt Failure         :        0   Invalid Packet           :        0
    Invalid Key             :        0   Input Overrun            :        0
    Input Underrun          :        0   Output buffer overrun    :        0
    Bad handle value        :        0   Invalid parameter        :        0
    Bad function code       :        0   Out of handles           :        0
    Access denied           :        0   Out of memory            :        0
    NR overflow             :        0   pkts dropped             :        0
Warnings:
    sessions_expired        :        0   packets_fragmented       :        0
    general:                :        0
HSP details:
    hsp_operations          :    10441   hsp_session
```

The following table describes the significant fields shown in the display.

Table 27: show crypto engine accelerator statistic Field Descriptions

Field	Description
packets decompressed	Packets that were decompressed by the interface.
packets compressed	Packets that were compressed by the interface.
bytes before decomp	Compressed bytes that were presented to the compression algorithm from the input interface on decryption.
bytes before comp	Uncompressed bytes (payload) that were presented to the compression algorithm from Cisco software on encryption.
bytes after decomp	Decompressed bytes that were sent to Cisco software by the compression algorithm on decryption.
bytes after comp	Compressed bytes that were forwarded to Cisco software by the algorithm on encryption.
packets bypass compres	Packets that were not compressed because they were too small (less than 128 bytes).
packets not compressed	Packets that were not compressed because the packets were expanded rather than compressed.
compression ratio	Ratio of compression and decompression of packets presented to the compression algorithm that were successfully compressed or decompressed. This statistic measures the efficiency of the algorithm for all packets that were compressed or decompressed.

Field	Description
overall	Ratio of compression and decompression of packets presented to the compression algorithm, including packets that were not compressed because they were expanded or very small in size. This ratio indicates whether data traffic on this interface is suitable for compression. A ratio of 1:1 would imply that no successful compression is being performed on this data traffic.

Cisco 7200 Router with VSA

The following is sample output from a Cisco 7200 router with a VSA:

```
Device# show crypto engine accelerator statistic 1/0

Inbound rate: 0pps 0kb/s  Outbound rate: 0pps 0kb/s
    TRAFFIC                     Transmitted                  Received
 ------------------------------------------------------------------------------
  Message  Count:                         5                         5
  Message  Byte Count:                 1212                       256
  Message  Overflow:                      0
  Outbound Count:                        54                       154
  Outbound Byte Count:                12472                     30332
  Outbound Overflow:                      0
  Inbound  Count:                       153                       153
  Inbound  Byte Count:                26304                     19864
  Inbound  Overflow:                      0
  Reassembled Pkt:                        0
  Fragments Dropped:                      0
     IPPE:                                0
     EPPE:                                0
     FIFO:                                0
     RAE:                                 0
Inbound Traffic:
 ------------------------------------------------------------------------------
  Decrypted Pkt:                        150
  Passthrough Pkt:                        3
  IKE Pkt:                                0
  SPI Error:                              0
  Policy Violation:                       0
Outbound Traffic:            Route cache                  Processor
 ------------------------------------------------------------------------------
  Encrypted Pkt:                        150                       0
  Passthrough Pkt:                        0                       4
  Policy Violation:                       0
Queue Depth:
 ------------------------------------------------------------------------------
TXRing Current Queue Depth:
    High Priority   :                   0.0 %
    Medium Priority :                   0.0 %
    Low Priority    :                   0.0 %
VSA RX Exception statistics:
   Invalid SA              :          0   Enc Dec mismatch        :          0
   Next Header mismatch    :          0   Pad mismatch            :          0
   MAC mismatch            :          0   Anti replay failed      :          0
   Enc Seq num overflow    :          0   Dec IPver mismatch      :          0
   Enc IPver mismatch      :          0   TTL Decr                :          0
   Selector checks         :          0   UDP mismatch            :          0
   IP Parse error          :          0   Fragmentation Error     :          0
   IB Selector check       :          0   TimeBased Replay Err    :          0
   Misc. Exceptions        :          0
```

The following table describes the significant fields shown in the display.

Table 28: show crypto engine accelerator statistic Field Descriptions for a Cisco 7200 Router with the VSA

Field	Description
Message Count	Number of messages sent to the VSA.
Message Byte Count	Byte count for messages.
Message Overflow	Number of messages that could not be sent because there was no space in the transmission ring.
Outbound Count	Number of outbound packets sent to the VSA either for classification, encryption, or both (includes packets for encryption or passthrough).
Outbound Byte Count	Byte count of packets.
Outbound Overflow	Number of outbound packets that could not be sent.
Inbound Count	Number of inbound packets sent to the VSA either for classification, decryption, or both.
Inbound Byte Count	Byte count for packets.
Inbound Overflow	Number of inbound packets that could not be sent because the transmission ring was full.
Reassembled Pkt	Number of reassembled packets.
Fragments Dropped	Number of fragments dropped.
IPPE	Number of inbound fragments dropped by the Ingress Packet Processing Engine (IPPE).
EPPE	Number of outbound fragments dropped by the Egress Packet Processing Engine (EPPE).
FIFO	Number of fragments dropped by the FIFO fragment queue.
RAE	Number of fragments dropped by the Reassembly Engine (RAE).
Inbound Traffic	Inbound fragments.
Decrypted Pkt	Number of decrypted packets.
Passthrough Pkt	Number of clear packets in the inbound direction.
IKE Pkt	Number of Internet Key Exchange (IKE) packets that were received.
SPI Error	Number of received packets that have an invalid security parameter index (SPI).

Field	Description
Policy Violation	Number of clear packets that the VSA received that should have come encrypted as per the policy.
Outbound Traffic	Outbound fragments.
Encrypted Pkt	Number of encrypted packets.
Passthrough Pkt	Number of outbound clear packets.
Policy Violation	Number outbound security association (SA) to encrypt the packet.
Queue Depth	Number of packets in queue.
TXRing Current Queue Depth	Current queue depth of the three transmitting rings, which are High, Medium, and Low Priority.
VSA RX Exception statistics	Errors from the crypto chip.
Invalid SA	Specified SA does not exist.
Enc Dec mismatch	Packet on the wrong SA type.
Next Header mismatch	Wrong next header field found in the packet.
Pad mismatch	Wrong pad found in the packet.
MAC mismatch	Authentication check failed.
Anti replay failed	Antireplay error.
Enc Seq num overflow	Sequence number reached the maximum specified for the SA.
Dec IPver mismatch	Wrong IP version for the packet to be decrypted. For example, an IPv4 packet came in for an IPv6 SA.
Enc IPver mismatch	Wrong IP version for the packet to be encrypted.
TTL Decr	Time to Live (TTL) decremented to 0 (zero).
Selector checks	Decrypted packet failed the policy check.
UDP mismatch	UDP packet failed the sanity check.
IP Parse error	Error in IP packet parsing.
Fragmentation Error	Could not fragment; Don’t Fragment (DF) bit set.
IB Selector check	Decrypted packet failed the policy check (for Group Encrypted Transport VPN (GET VPN)).
TimeBased Replay Err	Time-based anti-replay failed for GET VPN.

Field	Description
Misc. Exceptions	Errors not classified as any of the above.

IPsec VPN SPA and VSPA

The following example shows platform statistics for the IPsec VPN SPA in slot 1 subslot 0 and also displays network interface controller statistics (this sample output is from a Catalyst 6500 Series Switch installed with IPsec VPN SPA):

```
Device# show crypto engine accelerator statistic slot 1/0 detail

1/0 detail
VPN module in slot 1/0
Decryption Side Data Path Statistics
====================================
Packets RX..............: 454260
Packets TX..............: 452480
IPSec Transport Mode.....: 0
IPSec Tunnel Mode........: 452470
AH Packets..............: 0
ESP Packets.............: 452470
GRE Decapsulations.......: 0
NAT-T Decapsulations.....: 0
Clear...................: 8
ICMP....................: 0
Packets Drop............: 193
Authentication Errors....: 0
Decryption Errors........: 0
Replay Check Failed......: 0
Policy Check Failed......: 0
Illegal Clear Packet.....: 0
GRE Errors..............: 0
SPD Errors..............: 0
HA Standby Drop..........: 0
Hard Life Drop..........: 0
Invalid SA..............: 191
SPI No Match............: 0
Destination No Match.....: 0
Protocol No Match........: 0
Reassembly Frag RX.......: 0
IPSec Fragments..........: 0
IPSec Reasm Done.........: 0
Clear Fragments..........: 0
Clear Reasm Done.........: 0
Datagrams Drop..........: 0
Fragments Drop..........: 0
Decryption Side Controller Statistics
=====================================
Frames RX...............: 756088
Bytes RX................: 63535848
Mcast/Bcast Frames RX....: 2341
RX Less 128Bytes.........: 756025
RX Less 512Bytes.........: 58
RX Less 1KBytes..........: 2
RX Less 9KBytes..........: 3
RX Frames Drop..........: 0
Frames TX...............: 452365
Bytes TX................: 38001544
Mcast/Bcast Frames TX....: 9
TX Less 128Bytes.........: 452343
TX Less 512Bytes.........: 22
```

```
TX Less 1KBytes..........: 0
TX Less 9KBytes..........: 0
Encryption Side Data Path Statistics
====================================
Packets RX...............: 756344
Packets TX...............: 753880
IPSec Transport Mode.....: 0
IPSec Tunnel Mode........: 753869
GRE Encapsulations.......: 0
NAT-T Encapsulations.....: 0
LAF prefragmented........: 0
Fragmented...............: 0
Clear....................: 753904
ICMP.....................: 0
Packets Drop.............: 123
IKE/TED Drop.............: 27
Authentication Errors....: 0
Encryption Errors........: 0
HA Standby Drop..........: 0
Hard Life Drop...........: 0
Invalid SA...............: 191
Reassembly Frag RX.......: 0
Clear Fragments..........: 0
Clear Reasm Done.........: 0
Datagrams Drop...........: 0
Fragments Drop...........: 0
Encryption Side Controller Statistics
=====================================
Frames RX................: 454065
Bytes RX.................: 6168274
Mcast/Bcast Frames RX....: 1586
RX Less 128Bytes.........: 1562
RX Less 512Bytes.........: 452503
RX Less 1KBytes..........: 0
RX Less 9KBytes..........: 0
RX Frames Drop...........: 0
Frames TX................: 753558
Bytes TX.................: 100977246
Mcast/Bcast Frames TX....: 2
TX Less 128Bytes.........: 3
TX Less 512Bytes.........: 753555
TX Less 1KBytes..........: 0
TX Less 9KBytes..........: 0
```

The following table describes the significant fields shown in the display.

Table 29: show crypto engine accelerator statistic Field Descriptions for IPsec VPN SPA Statistics

Field	Description
Decryption Side Data Path Statistics	Information about packets received on the decryption side of IPsec VPN SPA.
Packets RX	Number of packets received on the decryption side of IPsec VPN SPA.
Packets TX	Number of packets transmitted by IPsec VPN SPA in the decryption direction.
IPSec Transport Mode	Number of packets in IPsec Transport Mode.

Field	Description
IPSec Tunnel Mode	Number of packets in IPsec Tunnel Mode.
AH Packets	Number of packets with Authentication Headers (AHs).
ESP Packets	Number of packets with Encapsulating Security Payload (ESP) headers.
GRE Decapsulations	Number of packets that were generic routing encapsulation (GRE) decapsulated.
NAT-T Decapsulations	Number of packets that were Network Address Translation-Traversal (NAT-T) decapsulated.
Clear	Number of clear packets received.
ICMP	Number of Internet Control Message Protocol (ICMP) packets received.
Packets Drop	Number of packets dropped. **Note** This does not represent the sum of the individual drop subtotals displayed (does not include bridge protocol data unit (BPDU), Cisco Discovery Protocol, or Maintenance Operation Protocol (MOP) packets drops).
Authentication Errors	Number of authentication errors.
Decryption Errors	Number of decryption errors.
Replay Check Failed	Number of replay check errors.
Policy Check Failed	Number of policy check errors.
Illegal Clear Packet	Number of illegal clear packets.

Field	Description
GRE Errors	Number of GRE errors due to invalid packets or invalid SAs. **Note** These errors correspond to the sum of the following GRE errors in the output from the **show stats icpu** command: "GRE Packet Errors," "GRE SA No Match," and "Invalid GRE SA." These errors include the number of GRE packets that are RFC compliant but use a format not supported by the VPN module, the number of GRE packets in which the SA lookup results is a no match, and the number of GRE packets in which the SA lookup matches an entry marked as invalid.
SPD Errors	Number of security policy database (SPD) errors. **Note** These errors correspond to the sum of the following SPD errors in the output from the **show stats icpu** command: "SPD Lookup Failed," "SPD Invalid," and "SPD ID No Match."
HA Standby Drop	Number of packet drops on a High Availability (HA) standby IPsec VPN SPA. **Note** The standby IPsec VPN SA is not supposed to receive packets.
Hard Life Drop	Number of packet drops due to SA hard life expiration. **Note** These packets are dropped during rekeying after the SA volume lifetime has been reached.
Invalid SA	Number of packet drops due to an invalid SA.
SPI No Match	Number of packet drops due to a Security Parameter Index (SPI) mismatch.
Destination No Match	Number of packet drops due to an error in matching the destination.
Protocol No Match	Number of packet drops due to an error in matching the protocol.
Reassembly Frag RX	Number of packets that required reassembly during processing.
IPsec Fragments	Number of IPsec fragments.

Field	Description
IPsec Reasm Done	Number of IPsec fragments reassembled.
Clear Fragments	Number of clear fragments.
Clear Reasm Done	Number of clear fragments reassembled.
Datagrams Drop	Number of reassembled datagrams that were dropped.
Fragments Drop	Number of fragments that were dropped.
Decryption Side Controller Statistics	Information about packets received on the decryption side controller.
Frames RX	Number of frames received.
Bytes RX	Number of bytes received.
Mcast/Bcast Frames RX	Number of multicast or broadcast frames received.
RX Less 128Bytes	Number of frames less than 128 bytes in size.
RX Less 512Bytes	Number of frames greater than or equal to 128 bytes and less than 512 bytes in size.
RX Less 1KBytes	Number of frames greater than or equal to 512 bytes and less than 1 kilobyte (KB) in size.
RX Less 9KBytes	Number of frames greater than or equal to 1 KB and less than 9 KB in size.
RX Frames Drop	Number of frames dropped.
Frames TX	Number of frames transmitted.
Bytes TX	Number of bytes transmitted.
Mcast/Bcast Frames TX	Number of multicast or broadcast frames transmitted.
TX Less 128Bytes	Number of frames less than 128 bytes in size.
TX Less 512Bytes	Number of frames greater than or equal to 128 bytes and less than 512 bytes in size.
TX Less 1KBytes	Number of frames greater than or equal to 512 bytes and less than 1 KB in size.
TX Less 9KBytes	Number of frames greater than or equal to 1 KB and less than 9 KBs in size.
Encryption Side Data Path Statistics	Information about packets received on the encryption side of IPsec VPN SPA.
Packets RX	Number of packets received on the encryption side of the IPsec VPN SPA.

Field	Description
Packets TX	Number of packets transmitted by the IPsec VPN SPA in the encryption direction.
IPsec Transport Mode	Number of packets in IPsec Transport Mode.
IPsec Tunnel Mode	Number of packets in IPsec Tunnel Mode.
GRE Encapsulations	Number of packets that were GRE encapsulated.
NAT-T Encapsulations	Number of packets that were NAT-T encapsulated.
LAF prefragmented	Number of packets with prefragmented look-ahead fragmentation (LAF) set.
Fragmented	Number of packets fragmented.
Clear	Number of clear packets.
ICMP	Number of ICMP packets.
Packets Drop	Number of packet drops. **Note** This does not represent the sum of the individual drop subtotals displayed (does not include BPDU, Cisco Discovery Protocol, or MOP packets drops).
IKE/TED Drop	Number of packet drops because the SA has not been set up.
Authentication Errors	Number of authentication errors.
Encryption Errors	Number of encryption errors.
HA Standby Drop	Number of packet drops on an HA standby IPsec VPN SPA. **Note** The standby IPsec VPN SPA is not supposed to receive packets.
Hard Life Drop	Number of packet drops due to SA hard-life expiration. **Note** These packets are dropped during rekeying after the SA volume lifetime has been reached.
Invalid SA	Number of packet drops due to an invalid SA.
Reassembly Frag RX	Number of packets that required reassembly processing.
Clear Fragments	Number of clear fragments.

Field	Description
Clear Reasm Done	Number of clear fragments reassembled.
Datagrams Drop	Number of reassembled datagrams dropped.
Fragments Drop	Number of fragments dropped.
Encryption Side Controller Statistics	Information about packets received on the decryption side controller.
Frames RX	Number of frames received.
Bytes RX	Number of bytes received.
Mcast/Bcast Frames RX	Number of multicast or broadcast frames received.
RX Less 128Bytes	Number of frames less than 128 bytes in size.
RX Less 512Bytes	Number of frames greater than or equal to 128 bytes and less than 512 bytes in size.
RX Less 1KBytes	Number of frames greater than or equal to 512 bytes and less than 1 KB in size.
RX Less 9KBytes	Number of frames greater than or equal to 1 KB and less than 9 KB in size.
RX Frames Drop	Number of frames dropped.
Frames TX	Number of frames transmitted.
Bytes TX	Number of bytes transmitted.
Mcast/Bcast Frames TX	Number of multicast or broadcast frames transmitted.
TX Less 128Bytes	Number of frames less than 128 bytes in size.
TX Less 512Bytes	Number of frames greater than or equal to 128 bytes and less than 512 bytes in size.
TX Less 1KBytes	Number of frames greater than or equal to 512 bytes and less than 1 KB in size.
TX Less 9KBytes	Number of frames greater than or equal to 1 KB and less than 9 KB in size.

VSPA

The following is sample output when the **coreutil** keyword is used with the VSPA and Cisco Catalyst 6500 Series Switches that use Cisco IOS Release 12.2(33)SXI and later releases:

```
Device# show crypto engine accelerator statistic slot 2/0 coreutil

Utilization Percentages for VPN blade in slot 2/0
Blade Utilization Percentages
```

```
==========================
Last 5 seconds ---------------------
Slowpath ..................... 35 %
Inbound ...................... 24 %
Outbound ..................... 32 %
QoS .......................... 44 %
Last 1 minute ----------------------
Slowpath ..................... 12 %
Inbound ...................... 11 %
Outbound ..................... 15 %
QoS .......................... 23 %
Last 5 minutes ---------------------
Slowpath ...................... 8 %
Inbound ...................... 11 %
Outbound ..................... 11 %
QoS .......................... 10 %

Device# show crypto engine accelerator statistic all coreutil

Utilization Percentages for VPN blade in slot 2/0
Blade Utilization Percentages
==========================
Last 5 seconds ---------------------
Slowpath ..................... 35 %
Inbound ...................... 24 %
Outbound ..................... 32 %
QoS .......................... 44 %
Last 1 minute ----------------------
Slowpath ..................... 12 %
Inbound ...................... 11 %
Outbound ..................... 15 %
QoS .......................... 23 %
Last 5 minutes ---------------------
Slowpath ...................... 8 %
Inbound ...................... 11 %
Outbound ..................... 11 %
QoS .......................... 10 %
Utilization Percentages for VPN blade in slot 2/1
Blade Utilization Percentages
==========================
Last 5 seconds ---------------------
Slowpath ..................... 88 %
Inbound ...................... 78 %
Outbound ..................... 79 %
QoS .......................... 32 %
Last 1 minute ----------------------
Slowpath ..................... 76 %
Inbound ...................... 80 %
Outbound ..................... 80 %
QoS .......................... 13 %
Last 5 minutes ---------------------
Slowpath ..................... 75 %
Inbound ...................... 65 %
Outbound ..................... 70 %
QoS .......................... 12 %
```

The following table describes the significant fields shown in the display.

Table 30: show crypto engine accelerator statistic coreutil Field Descriptions

Field	Description
Slowpath	Utilization of slowpath traffic capacity.

Field	Description
Inbound	Utilization of inbound traffic capacity.
Outbound	Utilization of outbound traffic capacity.
QoS	Utilization of quality of service (QoS) traffic capacity.

Related Commands

Command	Description
clear crypto engine accelerator counter	Resets statistical error counters for the hardware accelerator.
crypto ca	Defines parameters for the certification authority.
crypto cisco	Defines encryption algorithms and other parameters.
crypto dynamic-map	Creates a dynamic map crypto configuration.
crypto engine accelerator	Enables the use of the onboard hardware accelerator of the Cisco uBR905 and Cisco uBR925 routers for IPsec encryption.
crypto ipsec	Defines IPsec SAs and transformation sets.
crypto isakmp	Enables and defines the IKE protocol.
crypto key	Generates and exchanges keys for a cryptographic session.
crypto map	Creates and modifies a crypto map for a session.
debug crypto engine accelerator control	Displays each control command as sent to the crypto engine.
debug crypto engine accelerator packet	Displays information about each packet sent for encryption and decryption.
show crypto engine accelerator ring	Displays the contents of command and transmit rings for the crypto engine.
show crypto engine accelerator sa-database	Displays the active (in-use) entries in the crypto engine SA database.
show crypto engine brief	Displays a summary of the configuration information for the crypto engine.
show crypto engine configuration	Displays the version and configuration information for the crypto engine.
show crypto engine connections	Displays a list of the current connections maintained by the crypto engine.

show crypto gdoi

To display information about a Group Domain of Interpretation (GDOI) configuration, use the **show crypto gdoi** command in privileged EXEC mode.

```
show crypto gdoi [debug-condition
| [[group group-name] [{feature {gm-removal|policy-replace|gdoi-mib|
ipv6-crypto-path|suite-b|cts-sgt|long-sa-lifetime}|gm [{acl [{download|
local}]|identifier [detail]|pubkey|rekey sa [detail]|replay}]|ks [{acl|coop
[identifier [detail] | version]|identifier [detail]|members [ip-address]|policy
|rekey|replay}]|ipsec sa}]]]
```

Syntax Description

debug-condition	(Optional) Displays GDOI debug conditional filters.
group *group-name*	(Optional) Displays information about the group specified.
feature	(Optional) Displays the version of the GET VPN software running on each key server (KS) and group member (GM) in the GET VPN network and displays whether each device is running a version that supports the specified feature.
gm-removal	(Optional) Displays whether GM removal is supported.
policy-replace	(Optional) Displays whether the rekeying and policy replacement feature is supported.
gdoi-mib	(Optional) Displays whether the GDOI MIB is supported.
ipv6-crypto-path	(Optional) Displays whether devices in the GET VPN network support IPv6 encryption and decryption (and thus can be added to an IPv6 group).
suite-b	(Optional) Displays whether Suite B cryptography is supported.
cts-sgt	(Optional) Displays whether IPsec inline tagging for Cisco TrustSec is supported.
long-sa-lifetime	(Optional) Displays whether long security association (SA) lifetimes are supported.
gm	(Optional) Displays information about GMs. This keyword must be entered on a GM.
acl	(Optional) Displays the access control list (ACL) that has been applied to the GDOI group.
download	(Optional) Displays the ACL downloaded from the KS.
local	(Optional) Displays the locally-configured ACL.
identifier [**detail**]	(Optional) Displays Suite B sender identifier (SID) information. The **detail** keyword displays detailed information.
pubkey	(Optional) Displays public keys downloaded from the KS.
rekey sa [**detail**]	(Optional) Displays all existing GDOI rekey security associations (SAs), whether in an active or standby state. The **detail** keyword displays detailed information.
replay	(Optional) Displays group information for time-based anti-replay.

ks	(Optional) Displays information about KSs. This keyword must be entered on a KS.
coop	(Optional) Displays information about the cooperative KSs.
version	(Optional) Displays information about the cooperative KS and client versions.
members *ip-address*	(Optional) Displays information about registered GMs. You can specify the IPv4 address of a specific GM.
policy	(Optional) Displays KS policy information.
ipsec sa	(Optional) Displays information about the IP security (IPsec) security associations (SAs) for all GMs.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.4(11)T	This command was modified. The **group** *group-name* keyword and argument combination and the **gm**, **acl**, **rekey**, **replay**, **ks**, **coop** [**version**], **members**, **policy**, and **ipsec sa** keywords were added.
Cisco IOS XE Release 2.3	This command was integrated into Cisco IOS XE Release 2.3.
15.1(3)T	This command was modified. The **debug-condition** keyword was added.
15.2(1)T	This command was modified. The **feature**, **gm-removal**, **policy-replace**, and **gdoi-mib** keywords were added.
15.2(3)T	This command was modified. Output was added that displays information about whether the GET VPN data plane is in IPv4 or IPv6 (whether there are group policies defined in IPv4 or IPv6) and whether the control paths for groups are in IPv4 or IPv6), and the **ipv6-crypto-path** keyword was added.
15.2(4)M	This command was modified. The **suite-b** keyword was added, and the **identifier** and **detail** keyword combination for Suite B cryptography was added.
Cisco IOS XE Release 3.8S	This command was modified. The **feature**, **gm-removal**, **policy-replace**, and **gdoi-mib** keywords were added.

Release	Modification
15.3(2)T	This command was modified. The **cts-sgt** and **long-sa-lifetime** keywords were added. The output was enhanced for the following forms of the command: • **show crypto gdoi**: Shows the traffic encryption keys (TEKs) that a GM last received from the KS and shows the time until the next rekey. • **show crypto gdoi gm replay**: Shows information about the last 50 time-based antireplay errors. • **show crypto gdoi ks rekey**: Shows the number of rekey retransmissions, the current retransmit period, and the time until the next retransmission. • **show crypto gdoi ks policy**: Shows the time until the next rekey.
Cisco IOS XE Release 3.9S	This command was integrated into Cisco IOS XE Release 3.9S.
Cisco IOS XE Release 3.11S	This command was modified. The **rekey** keyword was renamed to **rekey sa**.

Usage Guidelines

Because the **show running-config** command does not display enabled **debug** commands, the **debug-condition** keyword is useful for displaying GDOI debug conditional filters that are enabled.

Examples

The following example shows how to display GET VPN group information for all groups. In this example, the command was entered on a KS:

```
Device# show crypto gdoi

GROUP INFORMATION

    Group Name               : GETV6 (Unicast)
    Group Identity           : 1111
    Crypto Path              : ipv6
    Key Management Path      : ipv4
    Group Members            : 2
    IPSec SA Direction       : Both
    Redundancy               : Configured
        Local Address        : 192.0.2.1
        Local Priority       : 100
        Local KS Status      : Alive
        Local KS Role        : Primary
        Local KS Version     : 1.0.4
    Group Rekey Lifetime     : 86400 secs
    Group Rekey
        Remaining Lifetime   : 86127 secs
    Rekey Retransmit Period  : 10 secs
    Rekey Retransmit Attempts: 2
    Group Retransmit
        Remaining Lifetime   : 0 secs

      IPSec SA Number        : 1
      IPSec SA Rekey Lifetime: 3600 secs
      Profile Name           : IPSEC_PROF_GETV6
```

```
      Replay method          : Time Based
      Replay Window Size     : 10
      SA Rekey
         Remaining Lifetime  : 3328 secs
      ACL Configured         : access-list ACL_GETV6_MIX

     Group Server list       : Local


GROUP INFORMATION

    Group Name               : GETV4 (Unicast)
    Group Identity           : 2222
    Crypto Path              : ipv4
    Key Management Path      : ipv4
    Group Members            : 2
    IPSec SA Direction       : Both
    Redundancy               : Configured
        Local Address        : 192.0.2.1
        Local Priority       : 90
        Local KS Status      : Alive
        Local KS Role        : Secondary
        Local KS Version     : 1.0.4
    Group Rekey Lifetime     : 86400 secs
    Group Rekey
        Remaining Lifetime   : 86127 secs
    Rekey Retransmit Period  : 10 secs
    Rekey Retransmit Attempts: 2
    Group Retransmit
        Remaining Lifetime   : 0 secs

      IPSec SA Number        : 1
      IPSec SA Rekey Lifetime: 3600 secs
      Profile Name           : IPSEC_PROF_GETV6
      Replay method          : Count Based
      Replay Window Size     : 64
      SA Rekey
         Remaining Lifetime  : 3328 secs
      ACL Configured         : access-list ACL_GETV4_HOST

     Group Server list       : Local
```

The following example shows how to enter the command on a GM to display GET VPN group information for all groups of which it is a member:

```
Device# show crypto gdoi

GROUP INFORMATION

    Group Name               : GETV6
    Group Identity           : 1111
    Crypto Path              : ipv6
    Key Management Path      : ipv4
    Rekeys received          : 0
    IPSec SA Direction       : Both

     Group Server list       : 192.0.2.1
                               192.0.2.11

    Group member             : 192.0.2.2          vrf: None
       Version               : 1.0.4
```

```
        Registration status   : Registered
        Registered with       : 192.0.2.1
        Re-registers in       : 3116 sec
        Succeeded registration: 1
        Attempted registration: 1
        Last rekey from       : 192.0.2.254
        Last rekey seq num    : 0
        Unicast rekey received: 0
        Rekey ACKs sent       : 0
        Rekey Received        : never
        allowable rekey cipher: any
        allowable rekey hash  : any
        allowable transformtag: any ESP

     Rekeys cumulative
        Total received        : 0
        After latest register : 0
        Rekey Acks sents      : 0

 ACL Downloaded From KS 192.0.2.1:
   access-list   deny tcp host 2001:DB8:1::1 eq 0 host 2001:DB8:0:ABCD::1 eq 0 sequence 1
   access-list   permit ipv6 host 2001:DB8:1::1 host 2001:DB8:0:ABCD::1 sequence 2
   access-list   permit ipv6 host 2001:DB8:0:ABCD::1 host 2001:DB8:1::1 sequence 3
   access-list   deny udp 2001:DB8:0001::/48 eq 0 2001:DB8:0002::/48 eq 0 sequence 4
   access-list   deny udp 2001:DB8:0002::/48 eq 0 2001:DB8:0001::/48 eq 0 sequence 5
   access-list   permit icmp 2001:DB8:0001::/48 2001:DB8:0002::/48 sequence 6
   access-list   permit icmp 2001:DB8:0002::/48 2001:DB8:0001::/48 sequence 7

KEK POLICY:
    Rekey Transport Type     : Unicast
    Lifetime (secs)          : 86013
    Encrypt Algorithm        : AES
    Key Size                 : 128
    Sig Hash Algorithm       : HMAC_AUTH_SHA
    Sig Key Length (bits)    : 1024

TEK POLICY for the current KS-Policy ACEs Downloaded:
  Ethernet2/0:
    IPsec SA:
        spi: 0x627E4B84(1652444036)
        transform: esp-aes
        sa timing:remaining key lifetime (sec): (3214)
        Anti-Replay(Time Based) : 10 sec interval
        tag method : cts sgt
        alg key size: 24 (bytes)
        sig key size: 20 (bytes)
        encaps: ENCAPS_TUNNEL



GROUP INFORMATION

    Group Name               : GETV4
    Group Identity           : 2222
    Crypto Path              : ipv4
    Key Management Path      : ipv4
    Rekeys received          : 0
    IPSec SA Direction       : Both

     Group Server list       : 192.0.2.1

    Group member             : 192.0.2.2          vrf: None
       Version               : 1.0.4
       Registration status   : Registered
```

```
       Registered with       : 192.0.2.1
       Re-registers in       : 3058 sec
       Succeeded registration: 1
       Attempted registration: 1
       Last rekey from       : 192.0.2.254
       Last rekey seq num    : 0
       Unicast rekey received: 0
       Rekey ACKs sent       : 0
       Rekey Received        : never
       allowable rekey cipher: any
       allowable rekey hash  : any
       allowable transformtag: any ESP

    Rekeys cumulative
       Total received        : 0
       After latest register : 0
       Rekey Acks sents      : 0

 ACL Downloaded From KS 192.0.2.1:
   access-list   permit icmp host 192.0.2.2 host 192.0.2.3
   access-list   permit icmp host 192.0.2.3 host 192.0.2.2

KEK POLICY:
    Rekey Transport Type     : Unicast
    Lifetime (secs)          : 86013
    Encrypt Algorithm        : 3DES
    Key Size                 : 192
    Sig Hash Algorithm       : HMAC_AUTH_SHA
    Sig Key Length (bits)    : 1024

TEK POLICY for the current KS-Policy ACEs Downloaded:
  Ethernet2/0:
    IPsec SA:
        spi: 0xF6E6B597(4142314903)
        transform: esp-aes
        sa timing:remaining key lifetime (sec): (3214)
        Anti-Replay : Disabled
        tag method : cts sgt
        alg key size: 24 (bytes)
        sig key size: 20 (bytes)
        encaps: ENCAPS_TUNNEL
```

The following example shows how to enter the command on a GM to display GET VPN group information for all groups of which it is a member. This is an example in which Suite B is configured; it shows that when you are using GCM or GMAC, the TEK POLICY section includes a separate IPsec SA with a unique security parameter index (SPI) for each ACL entry downloaded:

```
Device# show crypto gdoi

GROUP INFORMATION

    Group Name               : diffint
    Group Identity           : 1234
    Crypto Path              : ipv4
    Key Management Path      : ipv4
    Rekeys received          : 0
    IPSec SA Direction       : Both

     Group Server list       : 10.0.8.1

    Group member             : 10.0.3.1         vrf: None
       Version               : 1.0.4
```

```
       Registration status   : Registered
       Registered with       : 10.0.8.1
.
.
.
ACL Downloaded From KS 10.0.8.1:
   access-list   permit ip host 10.0.1.1 host 239.0.1.1
   access-list   permit ip host 10.0.100.2 host 238.0.1.1
   access-list   permit ip host 10.0.1.1 host 10.0.100.2
   access-list   permit ip host 10.0.100.2 host 10.0.1.1

KEK POLICY:
    Rekey Transport Type     : Unicast
    Lifetime (secs)          : 85740
    Encrypt Algorithm        : 3DES
    Key Size                 : 192
    Sig Hash Algorithm       : HMAC_AUTH_SHA256
    Sig Key Length (bits)    : 1024

TEK POLICY for the current KS-Policy ACEs Downloaded:
  Ethernet3/0:
    IPsec SA:
        spi: 0x318846DE(831014622)
        transform: esp-gcm
        sa timing:remaining key lifetime (sec): (86350)
        Anti-Replay(Counter Based) : 64
        tag method : disabled
        alg key size: 24 (bytes)
        sig key size: 20 (bytes)
        encaps: ENCAPS_TUNNEL

    IPsec SA:
        spi: 0xF367AEA0(4083658400)
        transform: esp-gcm
        sa timing:remaining key lifetime (sec): (86350)
        Anti-Replay(Counter Based) : 64
        tag method : disabled
        alg key size: 24 (bytes)
        sig key size: 20 (bytes)
        encaps: ENCAPS_TUNNEL

    IPsec SA:
        spi: 0xE583A3F5(3850609653)
        transform: esp-gcm
        sa timing:remaining key lifetime (sec): (86350)
        Anti-Replay(Counter Based) : 64
        tag method : disabled
        alg key size: 24 (bytes)
        sig key size: 20 (bytes)
        encaps: ENCAPS_TUNNEL

    IPsec SA:
        spi: 0xE9AC04C(245022796)
        transform: esp-gcm
        sa timing:remaining key lifetime (sec): (86350)
        Anti-Replay(Counter Based) : 64
        tag method : disabled
        alg key size: 24 (bytes)
        sig key size: 20 (bytes)
        encaps: ENCAPS_TUNNEL
```

The following example shows how to enter the command on a KS to display GET VPN group information for a specific group:

```
Device# show crypto gdoi group diffint

GROUP INFORMATION

    Group Name               : diffint (Multicast)
    Group Identity           : 3333
    Group Members            : 1
    IPSec SA Direction       : Both
    Group Rekey Lifetime     : 300 secs
    Group Rekey
        Remaining Lifetime   : 260 secs
    Rekey Retransmit Period  : 10 secs
    Rekey Retransmit Attempts: 2
    Group Retransmit
        Remaining Lifetime   : 0 secs

      IPSec SA Number        : 1
      IPSec SA Rekey Lifetime: 300 secs
      Profile Name           : gdoi-p
      Replay method          : Count Based
      Replay Window Size     : 64
      SA Rekey
         Remaining Lifetime  : 261 secs
      ACL Configured         : access-list 120

      IPSec SA Number        : 2
      IPSec SA Rekey Lifetime: 300 secs
      Profile Name           : gdoi-p
      Replay method          : Count Based
      Replay Window Size     : 64
      SA Rekey
         Remaining Lifetime  : 261 secs
      ACL Configured         : access-list 122

     Group Server list       : Local
```

The following example shows how to enter the command on a KS to display basic KS status and parameters:

```
Device# show crypto gdoi ks

Total group members registered to this box: 2

Key Server Information For Group diffint:
    Group Name               : diffint
    Group Identity           : 3333
    Group Members            : 2
    IPSec SA Direction       : Both
    Data Path                : IPv6
    Control Path             : IPv4
    ACL Configured           : access-list 120
```

The following example shows how to enter the command on a KS to display KS policy information. This is an example in which Suite B is configured; it shows the Selector field, which matches the IPsec SA SPI with the ACL that it downloaded:

```
Device# show crypto gdoi ks policy

Key Server Policy:
For group diffint (handle: 2147483650) server 10.0.8.1 (handle: 2147483650):

  # of teks : 5  Seq num : 0
.
.
.
  TEK POLICY (encaps : ENCAPS_TUNNEL)
    spi                : 0xE7994585
    access-list        : gcm-acl
    Selector           : permit ip host 10.0.1.1 host 239.0.1.1
    transform          : esp-gcm
    alg key size       : 16            sig key size          : 0
    orig life(sec)     : 900           remaining life(sec)   : 676
    tek life(sec)      : 900           elapsed time(sec)     : 224
    override life (sec): 0             antireplay window size: 64


  TEK POLICY (encaps : ENCAPS_TUNNEL)
    spi                : 0x87CB1FA3
    access-list        : gcm-acl
    Selector           : permit ip host 10.0.100.2 host 238.0.1.1
    transform          : esp-gcm
    alg key size       : 16            sig key size          : 0
    orig life(sec)     : 900           remaining life(sec)   : 676
    tek life(sec)      : 900           elapsed time(sec)     : 224
    override life (sec): 0             antireplay window size: 64
```

The following example shows how to enter the command on a KS to display the encryption ACLs for groups. This example displays a numbered encryption ACL, which means that it is an IPv4 ACL (because IPv6 allows only named ACLs):

```
Device# show crypto gdoi ks acl

    Group Name              : diffint
    Configured ACL          : access-list 101 permit gre any any
```

The following example shows how to enter the command on a KS to display the encryption ACLs for groups. This example displays named encryption ACLs for two groups (an IPv4 group and an IPv6 group):

```
Device# show crypto gdoi ks acl

Group Name: GETV6
 Configured ACL:
   access-list ACL_GETV6_MIX  deny tcp host 2001:DB8:1::1 host 2001:DB8:0:ABCD::1 sequence
 10
  access-list ACL_GETV6_MIX  permit ipv6 host 2001:DB8:1::1 host 2001:DB8:0:ABCD::1 sequence
 20
  access-list ACL_GETV6_MIX  permit ipv6 host 2001:DB8:0:ABCD::1 host 2001:DB8:1::1 sequence
 30
   access-list ACL_GETV6_MIX  deny udp 2001:DB8:0001::/48 2001:DB8:0002::/48 sequence 40
   access-list ACL_GETV6_MIX  deny udp 2001:DB8:0002::/48 2001:DB8:0001::/48 sequence 50
   access-list ACL_GETV6_MIX  permit icmp 2001:DB8:0001::/48 2001:DB8:0002::/48 sequence
60
   access-list ACL_GETV6_MIX  permit icmp 2001:DB8:0002::/48 2001:DB8:0001::/48 sequence
70
```

```
Group Name: GETV4
 Configured ACL:
   access-list ACL_GETV4_HOST  permit icmp host 192.0.2.2 host 192.0.2.3
   access-list ACL_GETV4_HOST  permit icmp host 192.0.2.3 host 192.0.2.2
```

The following example shows how to enter the command on a GM to display the encryption ACLs for the groups to which it belongs. Even though a GM can be in any combination of IPv4 and IPv6 groups, this example shows that the GM is a member of only one group (in this case, an IPv6 group):

```
Device# show crypto gdoi gm acl

    Group Name: GETV6
    ACL Downloaded From KS 192.0.2.1:
     access-list  permit ipv6 2001:DB8:0001::/48 2001:DB8:0002::/48 sequence 1
     access-list  permit ipv6 2001:DB8:0002::/48 2001:DB8:0001::/48 sequence 2
```

The following example shows how to enter the command on a GM to display the encryption ACLs for the groups to which it belongs. In this case, the GM belongs to two groups (an IPv4 group and an IPv6 group):

```
Device# show crypto gdoi gm acl

Group Name: GETV6
 ACL Downloaded From KS 192.0.2.1:
   access-list   deny tcp host 2001:DB8:1::1 eq 0 host 2001:DB8:0:ABCD::1 eq 0 sequence 1
   access-list   permit ipv6 host 2001:DB8:1::1 host 2001:DB8:0:ABCD::1 sequence 2
   access-list   permit ipv6 host 2001:DB8:0:ABCD::1 host 2001:DB8:1::1 sequence 3
   access-list   deny udp 2001:DB8:0001::/48 eq 0 2001:DB8:0002::/48 eq 0 sequence 4
   access-list   deny udp 2001:DB8:0002::/48 eq 0 2001:DB8:0001::/48 eq 0 sequence 5
   access-list   permit icmp 2001:DB8:0001::/48 2001:DB8:0002::/48 sequence 6
   access-list   permit icmp 2001:DB8:0002::/48 2001:DB8:0001::/48 sequence 7
 ACL Configured Locally:

Group Name: GETV4
 ACL Downloaded From KS 192.0.2.1:
   access-list   permit icmp host 192.0.2.2 host 192.0.2.3
   access-list   permit icmp host 192.0.2.3 host 192.0.2.2
 ACL Configured Locally:
```

The following example shows how to enter the command on a KS to display KS sender ID (KSSID) information (for Suite B):

```
Device# show crypto gdoi ks identifier

KS Sender ID (KSSID) Information for Group GETVPN:

    Transform Mode           : Counter (Suite-B)
    Re-initializing          : Yes
    SID Length (Group Size)  : 24 bits (MEDIUM)
    Current KSSID In-Use     : 25
    Last GMSID Used          : 108

KS Sender ID (KSSID) Information for Group GETVPN-NO-GCM:

    Transform Mode           : Non-Counter (Non-Suite-B)
```

If this KS is a secondary cooperative KS, the configured group size (which you can view by using the **show running-config** command) might differ from the size in the SID Length (Group Size) field above if the primary cooperative KS has not yet switched to using the new group size. (If the group size is being changed, all secondary cooperative KSs must first configure the new group size, and then the primary cooperative KS must configure the new group size before it is used by all cooperative KSs.)

The following example shows how to enter the command on a KS to display detailed KSSID information (for Suite B):

```
Device# show crypto gdoi ks identifier detail

KS Sender ID (KSSID) Information for Group GETVPN:

    Transform Mode           : Counter (Suite-B)
    Re-initializing          : Yes
    SID Length (Group Size)  : 24 bits (MEDIUM)
    Current KSSID In-Use     : 25
    Last GMSID Used          : 108

    KSSID(s) Assigned        : 0, 10, 22-36, 95-103
    KSSID(s) Used            : 26-32
    KSSID(s) Used (Old)      : 0, 10, 22-25
    Available KSSID(s)       : 33-36, 95-103

KS Sender ID (KSSID) Information for Group GETVPN-NO-GCM:

    Transform Mode           : Non-Counter (Non-Suite-B)
```

If no KSSIDs are in a set, the corresponding fields display a value of none:

```
    KSSID(s) Assigned        : none
    KSSID(s) Used            : none
    KSSID(s) Used (Old)      : none
    Available KSSID(s)       : none
```

The following example shows how to enter the command on a primary cooperative KS to display KSSID information for cooperative KSs (for Suite B):

```
Device# show crypto gdoi ks coop identifier

COOP-KS Sender ID (SID) Information for Group GETVPN:

    Local KS Role: Primary , Local KS Status: Alive
        Local Address               : 10.0.5.2
        Next SID Client Operation   : NOTIFY
        Re-initializing             : No
        KSSID Overlap               : No
        SID Length (Group Size) Cfg  : 24 bits (MEDIUM)
        SID Length (Group Size) Used : 24 bits (MEDIUM)
        Current KSSID In-Use        : 4
        KSSID(s) Assigned           : 0-4, 10
        KSSID(s) Used               : 2-4
        Old KSSID(s) Used           : none
```

The following example shows how to enter the command on a primary cooperative KS to display detailed KSSID information for cooperative KSs (for Suite B):

```
Device# show crypto gdoi ks coop identifier detail

COOP-KS Sender ID (SID) Information for Group GETVPN:

    Local KS Role: Primary , Local KS Status: Alive
        Local Address               : 10.0.5.2
        Next SID Client Operation   : NOTIFY
        Re-initializing             : No
        KSSID Overlap               : No
        SID Length (Group Size) Cfg  : 24 bits (MEDIUM)
        SID Length (Group Size) Used : 24 bits (MEDIUM)
        Current KSSID In-Use        : 4
        KSSID(s) Assigned           : 0-4, 10
        KSSID(s) Used               : 2-4
        Old KSSID(s) Used           : none

    Peer KS Role: Secondary , Peer KS Status: Alive
        Peer Address                : 10.0.6.2
        Next SID Client Operation   : NOTIFY
        Re-initializing             : No
        KSSID Overlap               : No
        SID Length (Group Size) Cfg  : 32 bits (LARGE)
        SID Length (Group Size) Used : 24 bits (MEDIUM)
        Current KSSID In-Use        : 6
        KSSID(s) Assigned           : 5-9
        KSSID(s) Used               : 5-6
        Old KSSID(s) Used           : none

    Peer KS Role: Secondary , Peer KS Status: Dead
        Peer Address                : 10.0.7.2
        Next SID Client Operation   : NOTIFY
        Re-initializing             : No
        KSSID Overlap               : No
        SID Length (Group Size) Cfg  : 24 bits (MEDIUM)
        SID Length (Group Size) Used : 24 bits (MEDIUM)
        Current KSSID In-Use        : 109
        KSSID(s) Assigned           : 100-110
        KSSID(s) Used               : 100-109
        Old KSSID(s) Used           : none
```

Only the primary cooperative KS has information for all peer cooperative KSs. The secondary KS has the SID information only for itself and for the primary KS.

Note that with the SID Length (Group Size) fields, when changing the group size for S1 to S2 (for any group size), all secondaries must be configured with S2 first, and then the primary can configure S2. Only after the primary configures S2 will the primary and secondaries begin to use S2. Therefore, when a secondary has configured the new group size S2, the local **show** command still shows the old group size S1 being used, because S2 is not yet in use (until the primary changes to S2). However, the **show** command when used on the cooperative KS will show that S2 is configured.

The following example shows how to enter the command on a secondary cooperative KS to display KSSID information for cooperative KSs (for Suite B):

```
Device# show crypto gdoi ks coop identifier

COOP-KS Sender ID (SID) Information for Group GETVPN:

    Local KS Role: Secondary , Local KS Status: Alive
        Local Address               : 10.0.6.2
        Next SID Client Operation   : NOTIFY
```

```
        Re-initializing              : No
        KSSID Overlap                : No
        SID Length (Group Size) Cfg  : 32 bits (LARGE)
        SID Length (Group Size) Used : 24 bits (MEDIUM)
        Current KSSID In-Use         : 6
        KSSIDs Assigned              : 5-9
        KSSIDs Used                  : 5-6
        Old KSSIDs Used              : none
```

The following example shows how to enter the command on a secondary cooperative KS to display detailed KSSID information for cooperative KSs (for Suite B):

```
Device# show crypto gdoi ks coop identifier detail

COOP-KS Sender ID (SID) Information for Group GETVPN:

    Local KS Role: Secondary , Local KS Status: Alive
        Local Address                : 10.0.6.2
        Next SID Client Operation    : NOTIFY
        Re-initializing              : No
        KSSID Overlap                : No
        SID Length (Group Size) Cfg  : 32 bits (LARGE)
        SID Length (Group Size) Used : 24 bits (MEDIUM)
        Current KSSID In-Use         : 6
        KSSIDs Assigned              : 5-9
        KSSIDs Used                  : 5-6
        Old KSSIDs Used              : none

    Peer KS Role: Primary , Peer KS Status: Alive
        Peer Address                 : 10.0.5.2
        Next SID Client Operation    : NOTIFY
        Re-initializing              : No
        KSSID Overlap                : No
        SID Length (Group Size) Cfg  : 24 bits (MEDIUM)
        SID Length (Group Size) Used : 24 bits (MEDIUM)
        Current KSSID In-Use         : 4
        KSSIDs Assigned              : 0-4, 10
        KSSIDs Used                  : 2-4
        Old KSSIDs Used              : none
```

The following example shows how to enter the command on a KS to display cooperative KS and client GET VPN software versions:

```
Device# show crypto gdoi ks coop version

Cooperative key server infra Version : 1.0.2

Client : KS_POLICY_CLIENT        Version : 1.0.1
Client : GROUP_MEMBER_CLIENT     Version : 1.0.1
Client : SID_CLIENT              Version : 1.0.1
```

The following example shows how to enter the command on a GM to display the SID information for each registered GM in the group to which the GM belongs (for Suite B):

```
Device# show crypto gdoi gm identifier

GM Sender ID (SID) Information for Group diffint:

  Group Member: 10.0.1.2         vrf: None
```

```
    Transform Mode                  : Counter (Suite-B)
    # of SIDs Last Requested        : 2

    CURRENT SIDs:
      SID Length (Group Size)       : 24 bits (MEDIUM)
      # of SIDs Downloaded          : 2
      First SID Downloaded          : 0x00000D
      Last SID Downloaded           : 0x00000E

  Group Member: 10.0.3.1         vrf: None
    Transform Mode                  : Counter (Suite-B)
    # of SIDs Last Requested        : 2

    CURRENT SIDs:
      SID Length (Group Size)       : 24 bits (MEDIUM)
      # of SIDs Downloaded          : 2
      First SID Downloaded          : 0x00000F
      Last SID Downloaded           : 0x000010
```

The following example shows how to enter the command on a GM to display detailed SID information for each registered GM in the group to which the GM belongs (for Suite B):

```
Device# show crypto gdoi gm identifier detail

GM Sender ID (SID) Information for Group diffint:

  Group Member: 10.0.1.2         vrf: None
    Transform Mode                  : Counter (Suite-B)
    # of SIDs Last Requested        : 2

    CURRENT SIDs:
      SID Length (Group Size)       : 24 bits (MEDIUM)
      # of SIDs Downloaded          : 2
      First SID Downloaded          : 0x00000D
      Last SID Downloaded           : 0x00000E

      CM Interface    Bandwidth (Kbps)  MTU (Bytes)  # SIDs
      ============    ================  ===========  ======
      Gi0/1           10000             1500         1
      Gi0/2           10000             1000         1

    OLD SIDs:
      SID Length (Group Size)       : 24 bits (MEDIUM)
      # of SIDs Downloaded          : 2
      First SID Downloaded          : 0x00000B
      Last SID Downloaded           : 0x00000C

    NEXT SID REQUEST:
      TEK Lifetime                  : 7200 sec
      SID Length (Group Size)       : 24 bits (MEDIUM)


  Group Member: 10.0.3.1         vrf: None
    Transform Mode                  : Counter (Suite-B)
    # of SIDs Last Requested        : 2

    CURRENT SIDs:
      SID Length (Group Size)       : 24 bits (MEDIUM)
      # of SIDs Downloaded          : 2
      First SID Downloaded          : 0x00000F
      Last SID Downloaded           : 0x000010
```

```
      CM Interface    Bandwidth (Kbps)  MTU (Bytes)  # SIDs
      ============    ================  ===========  ======
      Gi1/0           10000             1500         1
      Gi1/1           10000             1000         1

    OLD SIDs: none

    NEXT SID REQUEST:
      TEK Lifetime                  : 7200 sec
      SID Length (Group Size)       : 24 bits (MEDIUM)
```

The following example shows how to enter the command on a KS to display KS status and parameters for a specific GDOI group:

```
Device# show crypto gdoi group diffint ks

Group Information
   Group Name                  : diffint
   Group Identity              : 3333
   Group Members Registered    : 1
   Group Server                : Local
   Group Rekey Lifetime        : 300 secs
   Group Rekey
       Remaining Lifetime      : 84 secs
   IPSec SA Number             : 1
     IPSec SA Rekey Lifetime   : 120 secs
     Profile Name              : gdoi-p
   SA Rekey
       Remaining Lifetime      : 64 secs
   access-list 120 permit ip host 10.0.1.1 host 192.168.1.1
   access-list 120 permit ip host 10.0.100.2 host 192.168.1.1
   Group Member List for Group diffint :
   Member ID                   : 10.0.3.1
   Group Name                  : test
   Group Identity              : 4444
   Group Members Registered    : 0
   Group Server                : Local
   Group Rekey Lifetime        : 600 secs
   IPSec SA Number             : 1
     IPSec SA Rekey Lifetime   : 120 secs
     Profile Name              : gdoi-p
   access-list 120 permit ip host 10.0.1.1 host 192.168.1.1
   access-list 120 permit ip host 10.0.100.2 host 192.168.1.1
```

The following example shows how to enter the command on a GM to display brief status information for a specific GDOI group:

```
Device# show crypto gdoi group diffint gm

Group Member Information For Group diffint:
    IPSec SA Direction       : Both
    ACL Received From KS     : gdoi_group_diffint_temp_acl

    Group member             : 10.0.3.1         vrf: None
       Version               : 1.0.2
       Registration status   : Registered
       Registered with       : 10.0.5.2
       Re-registers in       : 77 sec
       Succeeded registration: 1
       Attempted registration: 1
       Last rekey from       : 10.0.5.2
```

```
        Last rekey seq num    : 0
        Multicast rekey rcvd  : 9
```

The following example shows how to enter the command on a KS to display KS information for registered GMs:

```
Device# show crypto gdoi ks members

Group Member Information :
Detail :
Number of rekeys sent for group diffint : 10
Group Member ID   : 10.0.0.1
Group ID          : 3333
Group Name        : diffint
Key Server ID     : 192.0.2.253
Rekeys sent       : 10
Rekeys retries    : 0
Rekey Acks Rcvd   : 10
Rekey Acks missed : 0
Sent seq num :    2    3    1    2
Rcvd seq num :    2    3    1    2
Group Member ID   : 192.0.2.251
Group ID          : 3333
Group Name        : diffint
Key Server ID     : 192.0.2.252
Rekeys sent       : 10
Rekeys retries    : 0
Rekey Acks Rcvd   : 10
Rekey Acks missed : 0
Sent seq num :    2    3    1    2
Rcvd seq num :    2    0    0    0
```

The following example shows how to enter the command on a GM to verify the RSA public key that is downloaded from the KS:

```
Device# show crypto gdoi gm pubkey

GDOI Group: diffint
    KS IP Address: 10.0.9.1
    conn-id: 1020    my-cookie:BFC164DB    his-cookie:3F2C75D9
    Key Data:
      305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00B508E9 EDD36AE1
      B7AFEB96 74AAD793 4AAA549B 91809707 25AE59E7 E7359CB3 6C938C82 5ED17AC3
      9E1B1611 DF3791DD FBAC8C4B EEEDC4F5 46C4472A BAAE0870 69020301 0001
```

For RSA public keys, the KS sends the GM the RSA public key when the GM registers. When the KS sends a rekey, it signs it using the RSA private key. After the GM receives this rekey, it verifies the signature using the public key that it downloaded from the KS (therefore, the GM knows that it received the rekey from the KS).

The following example shows how to use the command on a GM to display information about the IPsec SA for each group to which the GM belongs (this command cannot be used on a KS):

```
Device# show crypto gdoi ipsec sa

SA created for group GETV6:
  Ethernet2/0:
    protocol = ip
```

```
      local ident  = 2001:DB8:0001::/48, port = 0
      remote ident = 2001:DB8:0002::/48, port = 0
      direction: Both, replay(method/window): Time/6 sec
    protocol = ip
      local ident  = 2001:DB8:0002::/48, port = 0
      remote ident = 2001:DB8:0001::/48, port = 0
      direction: Both, replay(method/window): Time/6 sec
```

The following example shows how to use the GET VPN software versioning command on the KS (or primary KS) to check whether all the devices in the GET VPN network support the GM removal feature:

```
Device# show crypto gdoi feature gm-removal

Group Name: GET
 Key Server ID       Version   Feature Supported
    10.0.8.1         1.0.2          Yes
    10.0.9.1         1.0.2          Yes
    10.0.10.1        1.0.2          Yes
    10.0.11.1        1.0.2          Yes
 Group Member ID     Version   Feature Supported
    10.0.0.2         1.0.2          Yes
    10.0.0.3         1.0.1          No
```

The following example shows how enter the command on the KS (or primary KS) to find only those devices that do *not* support GM removal:

```
Device# show crypto gdoi feature gm-removal | include No

    10.0.0.3         1.0.1          No
```

The above example shows that the GM with IP address 10.0.0.3 is running older software version 1.0.1 (which does not support GM removal) and should be upgraded. You can also enter the above command on a GM.

The following example shows how to use the GET VPN software versioning command on a GM to check whether it supports the GM removal feature:

```
Device# show crypto gdoi feature gm-removal

 Version   Feature Supported
 1.0.2           Yes
```

The following example shows how to use the GET VPN software versioning command on the KS (or primary KS) to check whether devices in the GET VPN network support rekey triggering after KS policy replacement:

```
Device# show crypto gdoi feature policy-replace

Group Name: GET
 Key Server ID     Version  Feature Supported
  10.0.8.1         1.0.2          Yes
  10.0.9.1         1.0.2          Yes
  10.0.10.1        1.0.2          Yes
  10.0.11.1        1.0.2          Yes
 Group Member ID   Version  Feature Supported
```

```
  192.0.2.2          1.0.2          Yes
  10.0.0.3         1.0.1          No
```

You can also enter the above command on a GM.

The following example shows how to enter the command on the KS (or primary KS) to find only those devices that do *not* support rekey triggering after policy replacement:

```
Device# show crypto gdoi feature policy-replace  | include No

   10.0.0.3        1.0.1          No
```

For these devices, the primary KS sends only the triggered rekey without instructions for policy replacement. Therefore, when a GM receives the rekey, it installs the new SAs but does not shorten the lifetimes of the old SAs. This behavior is the same as the old rekey method and ensures backward compatibility. You can also enter the above command on a GM.

The following example shows how to use the GET VPN software versioning command on the KS (or primary KS) to check whether all the devices in the GET VPN network support the GDOI MIB:

```
Device# show crypto gdoi feature gdoi-mib

Group Name: GET
 Key Server ID       Version   Feature Supported
    10.0.8.1         1.0.2          Yes
    10.0.9.1         1.0.2          Yes
    10.0.10.1        1.0.2          Yes
    10.0.11.1        1.0.2          Yes
 Group Member ID     Version   Feature Supported
    192.0.2.2          1.0.2          Yes
    10.0.0.3         1.0.1          No
```

You can also enter the above command on a GM.

The following example shows how to enter the command on the KS (or primary KS) to find only those devices that do *not* support the GDOI MIB:

```
Device# show crypto gdoi feature gdoi-mib | include No

    10.0.0.3         1.0.1          No
```

You can also enter the above command on a GM.

The following example shows how to use the GET VPN software versioning command on the KS (or primary KS) to check whether all the devices in each group support GET VPN for IPv6 in the Data Plane (and thus can be added to an IPv6 group):

```
Device# show crypto gdoi feature ipv6-crypto-path

Group Name: GET
 Key Server ID       Version   Feature Supported
    10.0.8.1         1.0.3          Yes
    10.0.9.1         1.0.3          Yes
    10.0.10.1        1.0.3          Yes
    10.0.11.1        1.0.3          Yes
 Group Member ID     Version   Feature Supported
    192.0.2.2          1.0.3          Yes
```

```
    10.0.0.3         1.0.1          No
```

You can also enter the above command on a GM (which will display the information for the GM but not for the KS or other GMs).

The following example shows how to enter the command on the KS (or primary KS) to find only those devices in the GET VPN network that do *not* support GET VPN for IPv6 in the Data Plane:

```
Device# show crypto gdoi feature ipv6-crypto-path | include No

    10.0.0.3         1.0.1          No
```

All devices in the same GDOI group (including the KS, cooperative KSs, and GMs) must support the GET VPN for IPv6 in the Data Plane feature before the group's KS can enable the feature. To enable the feature for a group, you must ensure that all devices in the group are running compatible versions of the GET VPN software.

You can also enter the above command on a GM (which will display the information for the GM but not for the KS or other GMs).

The following example shows how to use the GET VPN software versioning command on the KS (or primary KS) to check whether all the devices in each group support Suite B cryptography:

```
Device# show crypto gdoi feature suite-b

Group Name: GETVPN
    Key Server ID       Version   Feature Supported
        10.0.5.2         1.0.4          Yes
        10.0.6.2         1.0.4          Yes
        10.0.7.2         1.0.3          No
        10.0.8.2         1.0.2          No

    Group Member ID     Version   Feature Supported
        10.0.1.2         1.0.2          No
        10.0.2.5         1.0.3          No
        10.0.3.1         1.0.4          Yes
        10.0.3.2         1.0.4          Yes
```

You can also enter the above command on a GM (which will display the information for the GM but not for the KS or other GMs).

The following example shows how to enter the command on the KS (or primary KS) to find only those devices in the GET VPN network that do *not* support Suite B:

```
Device# show crypto gdoi feature suite-b | include No

        10.0.7.2         1.0.3          No
        10.0.8.2         1.0.2          No
        10.0.1.2         1.0.2          No
        10.0.2.5         1.0.3          No
```

All devices in the same GDOI group (including the KS, cooperative KSs, and GMs) must support the Suite B feature before the group's KS can enable the feature. To enable the feature for a group, you must ensure that all devices in the group are running compatible versions of the GET VPN software.

You can also enter the above command on a GM (which will display the information for the GM but not for the KS or other GMs).

The following example shows how to use the GET VPN software versioning command on the KS (or primary KS) to check whether all the devices in each group support IPsec inline tagging for Cisco TrustSec:

```
Device# show crypto gdoi feature cts-sgt

Group Name: GETVPN
    Key Server ID       Version   Feature Supported
        10.0.5.2         1.0.5          Yes
        10.0.6.2         1.0.5          Yes
        10.0.7.2         1.0.3          No
        10.0.8.2         1.0.2          No

    Group Member ID     Version   Feature Supported
        10.0.1.2         1.0.2          No
        10.0.2.5         1.0.3          No
        10.0.3.1         1.0.5          Yes
        10.0.3.2         1.0.5          Yes
```

You can also enter the above command on a GM (which will display the information for the GM but not for the KS or other GMs).

The following example shows how to enter the command on the KS (or primary KS) to find only those devices in the GET VPN network that do *not* support IPsec inline tagging for Cisco TrustSec:

```
Device# show crypto gdoi feature cts-sgt | include No

        10.0.7.2         1.0.3          No
        10.0.8.2         1.0.2          No
        10.0.1.2         1.0.2          No
        10.0.2.5         1.0.3          No
```

All devices in the same GDOI group (including the KS, cooperative KSs, and GMs) must support the IPsec inline tagging for Cisco TrustSec feature before the group's KS can enable the feature. To enable the feature for a group, you must ensure that all devices in the group are running compatible versions of the GET VPN software.

You can also enter the above command on a GM (which will display the information for the GM but not for the KS or other GMs).

The following example shows how to use the GET VPN software versioning command on the KS (or primary KS) to check whether all the devices in each group support long SA lifetimes (from 24 hours to 30 days):

```
Device# show crypto gdoi feature long-sa-lifetime

Group Name: GETVPN
    Key Server ID       Version   Feature Supported
        10.0.5.2         1.0.5          Yes
        10.0.6.2         1.0.5          Yes
        10.0.7.2         1.0.3          No
        10.0.8.2         1.0.2          No

    Group Member ID     Version   Feature Supported
        10.0.1.2         1.0.2          No
```

```
        10.0.2.5        1.0.3          No
        10.0.3.1        1.0.5          Yes
        10.0.3.2        1.0.5          Yes
```

You can also enter the above command on a GM (which will display the information for the GM but not for the KS or other GMs).

The following example shows how to enter the command on the KS (or primary KS) to find only those devices in the GET VPN network that do *not* support long SA lifetimes:

```
Device# show crypto gdoi feature long-sa-lifetime | include No

        10.0.7.2        1.0.3          No
        10.0.8.2        1.0.2          No
        10.0.1.2        1.0.2          No
        10.0.2.5        1.0.3          No
```

All devices in the same GDOI group (including the KS, cooperative KSs, and GMs) must support long SA lifetimes before the group's KS can enable the feature. To enable the feature for a group, you must ensure that all devices in the group are running compatible versions of the GET VPN software.

You can also enter the above command on a GM (which will display the information for the GM but not for the KS or other GMs).

The following sample output shows detailed information about the SAs:

```
Router# show crypto gdoi rekey sa detail
KEK SA DB STATS:
    num_active = 2
    num_malloc = 46014
    num_free = 46011

  KEK POLICY (transport type : Unicast)
   Local addr/port : 1.2.20.32/848
   Remote addr/port : 10.1.2.1/848
    spi : 0x72C3C67E7B15BF701C30A0C22E1A1A7E
    management alg     : disabled    encrypt alg       : 3DES
    crypto iv length   : 8           key size          : 24
    orig life(sec)     : 0
    sig hash algorithm : enabled     sig key length    : 94
    sig size           : 64          conn_id           : 33957
    seq num            : 0           prev seq num      : 0
    handle             : 80009EFE    Interface         : GigabitEthernet
    group name         : gdoi-group1

  KEK POLICY (transport type : Unicast)
   Local addr/port : 1.2.20.32/848
   Remote addr/port : 10.1.2.1/848
    spi : 0xFCD0DD8333235B1652FA922BE85FAD65
    management alg     : disabled    encrypt alg       : 3DES
    crypto iv length   : 8           key size          : 24
    orig life(sec)     : 0
    sig hash algorithm : enabled     sig key length    : 94
    sig size           : 64          conn_id           : 33956
    seq num            : 0           prev seq num      : 0
    handle             : 80009E4D    Interface         : GigabitEthernet
    group name         : gdoi-group1
```

The table below describes the significant fields shown in the displays.

Table 31: show crypto gdoi Field Descriptions

Field	Description
Group Name	Name of the GDOI group.
Group Identity	GDOI group identity number or address.
Crypto Path	IP version for the data plane. IPv6 shows that group policies are defined in IPv6.
Key Management Path	IP version for the control plane. IPv4 shows that the control path for this group is in IPv4.
Group Members	Number of GMs that are registered to the KS.
IPSec SA Direction	Direction of the IPsec SA. Direction can be inbound (Receive Only) or bidirectional (Both).
Redundancy	Indicates whether KS redundancy is configured (meaning whether there are cooperative KSs).
Local Address	IP address of the local KS.
Local Priority	Priority of the local KS among the group of cooperative KSs.
Local KS Status	Indicates whether the local KS is active (alive).
Local KS Role	Indicates whether the local KS is the primary KS or a cooperative KS.
Local KS Version	Version of the GET VPN software running on the local KS.
Group Rekey Lifetime	Time between rekeys that is configured for the group.
Group Rekey Remaining Lifetime	Remaining time before the next rekey for the group.
Rekey Retransmit Period	Period between retransmissions of the rekey (in seconds).
Rekey Retransmit Attempts	Number of rekey retransmission attempts.
Group Retransmit Remaining Lifetime	Number of seconds until the next rekey retransmission.
IPSec SA Number	Number of the IPsec SA.
IPSec SA Rekey Lifetime	Lifetime that is configured for group IPSec SAs (rekey SAs).
Profile Name	IPsec profile that is defined for the group.
Replay method	Type of anti-replay that is configured (Count Based or Time Based).
Replay Window Size	Window size for the replay counter.
SA Rekey Remaining Lifetime	Remaining lifetime of the current group IPSec SA (rekey SA).

Field	Description
ACL Configured	Name of the ACL that is configured for the group.
Group Server list	Location of the list of group servers (Local if the command is issued on a KS or a list of IP addresses if issued on a GM).
Rekeys received	Number of rekeys received by the group.
Group member	IP address of the local GM.
vrf	Indicates whether virtual routing and forwarding (VRF) is configured on the GM.
Version	Version of the GET VPN software running on the GM.
Registration status	Indicates whether the GM is registered with a KS.
Registered with	IP address of the KS to which the GM is registered.
Re-registers in	Number of seconds until the GM reregisters with a KS.
Succeeded registration	Indicates whether the GM successfully registered with the KS.
Attempted registration	Number of times the GM attempted to register with the KS.
Last rekey from	IP address of the KS from which the GM received its last rekey.
Last rekey seq num	Anti-replay sequence number of the last rekey the GM received from the KS.
Unicast rekey received	Number of unicast rekeys received by the GM.
Rekey ACKs sent	Number of rekey acknowledgments sent by the GM to the KS.
Rekey Received	Indicates whether the GM has received a rekey from the KS.
allowable rekey cipher	Type of cipher that is acceptable for a rekey.
allowable rekey hash	Type of hash algorithm that is acceptable for a rekey.
allowable transformtag	Type of transform set that is acceptable for a rekey.
Rekeys cumulative	List of statistics for cumulative rekeys for the GM.
Total received	Total number of rekeys received by the GM.
After latest register	Total number of rekeys received by the GM since the most recent registration.
Rekey Acks sents	Total number of rekey acknowledgments sent by the GM.
ACL Downloaded From KS	List of ACLs that the GM has downloaded from the KS.
access-list	ACL configuration (policy) or configurations (policies) for the GMs.

Field	Description
KEK POLICY	List of details for the KEK policy.
Rekey Transport Type	Type of transport for rekey messages (Unicast or Multicast).
Lifetime (secs)	Lifetime of the rekey (in seconds).
Encrypt Algorithm	Encryption algorithm of the KEK policy.
Key Size	Encryption key size (in bits).
Sig Hash Algorithm	Type of algorithm for the signature key (hash).
Sig Key Length (bits)	Key length (in bits) for the signature key (hash).
TEK POLICY for the current KS-Policy ACEs Downloaded	List of details for the TEK policy for the current KS policy ACEs that were downloaded.
IPsec SA	List of details for the IPsec SA.
spi	Security parameter index (SPI) ID that is associated with the TEK.
transform	Transform set for the IPsec SA for the GM.
sa timing:remaining key lifetime (sec)	Remaining lifetime of the TEK (in seconds).
Anti-Replay(Time Based)	Interval duration for time-based anti-replay.
tag method	Method used for GET VPN inline tagging. The possible values are cts sgt (for Cisco TrustSec security group tags) or disabled.
alg key size	Length of the key (in bytes) for the encryption algorithm that is configured in the TEK policy. The possible key lengths are as follows: • 16 (AES) • 24 (AES-192) • 32 (AES-256) • 8 (DES) • 24 (3DES) • 16 (GCM) • 24 (GCM-192) • 32 (GCM-256) • 16 (GMAC) • 24 (GMAC-192) • 32 (GMAC-256)

Field	Description
sig key size	Length of the key (in bytes) for the signature that is configured in the TEK policy. The possible key lengths are as follows: • 16 (MD5) • 20 (SHA) • 32 (SHA-256) • 48 (SHA-384) • 64 (SHA-512)
encaps	Type of IPsec encapsulation that is configured in the TEK policy. The possible values are ENCAPS_TUNNEL or ENCAPS_TRANSPORT.
Configured ACL	ACL that is configured on the KS for the group.
ACL Configured Locally	Details for any ACLs that are configured locally for the GM.
Group Member Information	List of details about the group to which the GM belongs.
Detail	List of details about the GMs registered to the KS.
Number of rekeys sent for group	Number of rekeys sent for the group.
Group Member ID	IP address of the GM.
KS IP Address	Address of the KS from which the GM received the RSA public key during registration.
Group ID	ID of the group to which the GM belongs.
Group Name	Name of the group to which the GM belongs.
Key Server ID	IP address of the KS for the group.
Rekeys sent	Number of unique rekeys sent to the group.
Rekeys retries	Number of rekeys resent after not being acknowledged by the group.
Rekey Acks Rcvd	Total number of rekeys acknowledged by the group.
Rekey Acks missed	Number of rekeys sent to the group but not acknowledged.
Sent seq num	Sequence number sent to protect against replay attacks.
Rcvd seq num	Sequence number received.
conn-id	Connection ID.
my-cookie	Identifier on the local device (the KS or a GM) that, when paired with the his-cookie identifier on another device (the KS or a GM), identifies a unique SA between the KS and GM. You can use this pair of identifiers to check that an RSA rekey has been properly received on a specific GM.

Field	Description
his-cookie	Identifier on the remote device (the KS or a GM) that, when paired with the my-cookie identifier on the local device (the KS or a GM), identifies a unique SA between the KS and GM.
Key Data	Contents of the key itself.
Version	Version of the GET VPN software that is running on the KS or GM.
Feature Supported	Indicates whether the specified feature (GM removal, policy replacement, GDOI MIB, and so on) is supported by the software version running on the KS or GM.
Data Path	IPv6 shows that group policies are defined in IPv6.
Control Path	IPv4 shows that the control path for this group is in IPv4.
Transform Mode	Indicates whether the configured transform mode for the KS or GM is counter (Suite B) or non-counter (non-Suite-B). If it is non-counter, GCM-AES or GMAC-AES is not configured (and no identifier information is displayed).
Re-initializing	Indicates whether the KS is reinitializing.
SID Length (Group Size)	SID length (group size) in bits for the KS or GM. The possible values are 8 bits (SMALL-8), 12 bits (SMALL-12), 16 bits (SMALL-16), 24 bits (MEDIUM), 32 bits (LARGE), or 4 bits (UNKNOWN).
Current KSSID In-Use	KSSID that is currently being used to assign SIDs to GMs during registration. If no KSSIDs are configured or assigned to a KS, the field displays a value of none.
Last GMSID Used	Group member SID (GMSID) that was last assigned to a registered GM as part of a SID. If no GMs have registered or no GMs have been assigned any SID yet, the field displays a value of none.
KSSID(s) Assigned	KSSIDs that have been configured and synchronized to the cooperative KS SID clients.
KSSID(s) Used	KSSIDs that have been previously used (including the current KSSID) with the current TEK or TEKs.
Old KSSID(s) Used	KSSIDs that were used with the previous set of TEKs after a reinitialization (and the lowered or adjusted lifetimes of the previous set of TEKs that have not yet expired).
Available KSSID(s)	KSSIDs that are assigned but are unused (or are old).
Local KS Role	Indicates whether the cooperative KS is the primary KS or a secondary KS.
Local KS Status	Indicates whether the local cooperative KS is alive.
Local Address	IP address of the local cooperative KS.

Field	Description
Next SID Client Operation	Next SID client operation. The possible values are QUERY, NOTIFY, OR UPDATE. For the local KS: • QUERY: Has not received the previous SID information for the local KS from *any* peer KS • NOTIFY: Has received the previous SID information for the local KS and is up to date • UPDATE: Needs to send an update to all peers (because something changed locally) For the peer KS: • QUERY: Has not received any SID information for the peer KS from *the* peer KS • NOTIFY: Has received the latest SID information for the peer KS and is up to date • UPDATE: The peer needs to merge (old) used KSSID sets and use the next KSSID
KSSID Overlap	Indicates whether two or more KSs are using the same KSSID.
SID Length (Group Size) Cfg	Configured SID length (group size) in bits for the cooperative KS.
SID Length (Group Size) Used	Actual SID length (group size) in bits for the cooperative KS.
Current KSSID In-Use	KSSID that is in use.
Old KSSID(s) Used	KSSIDs that were used with the previous set of TEKs after a reinitialization (and the lowered or adjusted lifetimes of the previous set of TEKs have not yet expired).
Peer Address	IP address of the peer cooperative KS.
COOP-KS Sender ID (SID) Information for Group *groupname*	SID details for cooperative KSs for the group. If no redundancy is configured for the group, the following message is displayed: `*NO* redundancy configured for this group.`
Cooperative key server infra Version	Version of the cooperative KS Protocol Infrastructure for the current GET VPN software version.
Client : KS_POLICY_CLIENT	Version of the cooperative KS Policy Client for the current GET VPN software version.
Client : GROUP_MEMBER_CLIENT	Version of the cooperative KS Group Member Database Client for the current GET VPN software version.
Client : SID_CLIENT	Version of the cooperative KS Sender Identifier (SID) Client for the current GET VPN software version.

Field	Description
# of SIDs Last Requested	Number of SIDs that were last requested.
CURRENT SIDs	List of details for the current SIDs used by the GM. If a GM has not yet received any SIDs or has no SIDs associated with the old TEK or TEKs, the display will show None.
OLD SIDs	SIDs that exist after a GM receives a rekey or reregisters and receives the new TEK or TEKs. The current SIDs become old SIDs (associated with the old TEKs).
# of SIDs Downloaded	Number of SIDS downloaded by the GM. The number of downloaded SIDs should always match the number of SIDs in the range of SIDs downloaded between the first downloaded SID and the last downloaded SID (inclusively). Also, the range of SIDs between the first and last SIDs should be continuous (no skipped values).
First SID Downloaded	First SID downloaded by the GM.
Last SID Downloaded	Last SID downloaded by the GM.
CM Interface	Statistics for the CM interfaces for the group (Bandwidth in Kbps, MTUs in bytes, and number of SIDs).
NEXT SID REQUEST	Statistics for the next SID request.
TEK Lifetime	TEK lifetime. The TEK lifetime might not match the configured TEK lifetime on the KS for two reasons: • The GM receives the *remaining* TEK lifetime in the TEK SA payload. If a GM registers in the middle of a TEK lifetime, it will not calculate SIDs based on the full TEK lifetime, but rather based only on the TEK lifetime remaining. On a rekey, the GM will store the full TEK lifetime, because the KS will send the full TEK lifetime (or as close to the full TEK lifetime as possible) and use that lifetime on the next registration (if necessary). • Using G-IKEv2 or GKM, there is no way to know the TEK lifetime before requesting SIDs. Therefore, the first registration assumes a default lifetime of 7200 seconds (to be displayed) and stores the actual TEK lifetime to use for the next registration. Also, the SID length (group size) on the first registration will always be 24 bits (MEDIUM) and will update after the first registration.

Related Commands

Command	Description
crypto key pubkey-chain rsa	Enters public key configuration mode (so you can manually specify other devices' RSA public keys).
rsa-pubkey	Defines the RSA manual key to be used for encryption or signature during IKE authentication.

Command	Description
crypto isakmp policy	Defines an IKE policy.
lifetime (IKE policy)	Specifies the lifetime of an IKE SA.

show crypto ha

To display all virtual IP (VIP) addresses that are currently in use by IP Security (IPSec) and Internet Key Exchange (IKE), use the **show crypto ha**command in privileged EXEC mode.

show crypto ha

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(11)T	This command was introduced.

Examples

The following output from the **show crypto ha** command shows all VIP addresses that are being used by IPSec and IKE:

```
Router# show crypto ha
IKE VIP: 209.165.201.3
  stamp: 74 BA 70 27 9C 4F 7F 81 3A 70 13 C9 65 22 E7 76
IKE VIP: 255.255.255.253
  stamp: Not set
IKE VIP: 255.255.255.254
  stamp: Not set
IPSec VIP: 209.165.201.3
IPSec VIP: 255.255.255.253
IPSec VIP: 255.255.255.254
```

show crypto identity

To display the crypto identity list, use the show crypto identity command in privileged EXEC mode.

show crypto identity [*identity-tag*]

Syntax Description

identity-tag	(Optional) The crypto identity tag value for which to display specific crypto identity list information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRB	This command was introduced in a release earlier than Cisco IOS Release 12.2(33)SRB.
12.2SX	This command was integrated into Cisco IOS Release 12.2SX.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
Cisco IOS XE 2.3	This command was integrated into Cisco IOS XE Release 2.3.

Usage Guidelines

Use the **show crypto identity**command to display the configured crypto identity of a router.

Examples

The following are sample outputs from the **show crypto identity** command:

```
Router# show crypto identity id12
crypto identity id12:
   Description: line 22
Router# show crypto identity id11
crypto identity id11:
   fqdn line22
Router# show crypto identity
crypto identity tag12:
   Description: Linedescription
   fqdn fullyauthorisedone
```

The table below describes the significant fields shown in the display.

Table 32: show crypto identity Field Descriptions

Field	Description
Description	Line description.
fqdn	Fully qualified distinguished name identifier

show crypto ikev2 cluster

To display the configuration of Internet Key Exchange Version 2 (IKEv2) cluster policy, use the **show crypto ikev2 cluster** command in privileged EXEC mode.

show crypto ikev2 cluster

Syntax Description

This command has no keywords or arguments.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.2(4)M	This command was introduced.

Examples

The following is sample output from the **show crypto ikev2 cluster** command for an HSRP primary gateway:

```
Device# show crypto ikev2 cluster

  Role: CLB Server
  Status: Up/Down
  CLB Clients: 5
  Cluster IP: 192.168.1.100
  Holdtime: 3000 ms

  Load statistics:
  Gateway         Role    Last seen     Prio   Load     IKE    IPsec
  ------------------------------------------------------------------
* 192.168.1.2     Master        -         80    20%     100      200
  192.168.1.4      Slave    00:00.200    100    75%      30       60
  192.168.1.8      Slave    00:00.150    100    50%      34       80
  192.168.1.23     Slave    00:00.300     95    60%     102      300
  192.168.1.34      Dead    00:15.100     95  (100%)  (3000)   (4000)
```

The following is sample output from the **show crypto ikev2 cluster** command for an HSRP subordinate gateway:

```
Device# show crypto ikev2 cluster

  Role: CLB Slave
  Status: Up/Down
  Cluster IP: 192.168.1.100
  Hello-interval: 1000 ms
  Update-interval: 3000 ms
  Holdtime: 3000 ms

  Load statistics:
  Gateway         Role     Last ACK     Prio   Load     IKE    IPsec
  ------------------------------------------------------------------
  192.168.1.4    Slave      00:00.200    100    75%      30       60
```

The following table describes the significant fields shown in the display.

Table 33: show crypto ikev2 cluster Field Descriptions

Field	Description
Role	Role played by a peer in the cluster. Cluster Load Balancing (CLB) Server refers to a primary gateway and CLB Slave refers to a subordinate gateway.
Status	Status of the peer in the cluster.
Cluster IP	IP address of the cluster. This is the virtual IP address (VIP) that is sent to the FlexVPN client.
Hello-interval	Hello interval specified in the configuration. If not specified, it is the default hello interval.
Update-interval	Update interval specified in the configuration. If not specified, it is the default update interval.
Holdtime	Hold time specified in the configuration. If not specified, it is the default hold time.
Gateway	IP address of peers.
Role	Role played by the peer in the cluster. An asterisk (*) indicates the best candidate when this command is issued.
Last seen/Last ACK	Time when the gateway was last seen or acknowledged.
Prio	Priority of the peer.
Load	Load, in percent, of the peer.
IKE	IKE load of the peer.
IPsec	IPsec load of the peer.

Related Commands

Command	Description
crypto ikev2 cluster	Defines an IKEv2 cluster policy in an HSRP cluster.

show crypto ikev2 diagnose error

To display the current Internet Key Exchange Version 2 (IKEv2) exit path database, use the **show crypto ikev2 diagnose error**command in privileged EXEC mode.

show crypto ikev2 diagnose error [**count**]

Syntax Description

count	(Optional) Display the error counters from the exit path database.

Command Default

The IKEv2 exit path database is displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(1)T	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

Use this command to display the IKEv2 exit path database. Enable or disable IKEv2 exit path logging using the **crypto ikev2 diagnose error**command. Use the **clear crypto ikev2 diagnose error** command to clear the IKEv2 exit path database.

Examples

The following example is a sample output from the **show crypto ikev2 diagnose error** command. The output is self-explanatory.

```
Router# show crypto ikev2 diagnose error
Exit Path Table - status: enable, current entry 2, deleted 0, max allow 50
Error(1): No pskey found
 -Traceback= 0x37ABEB8z 0x37AC29Cz 0x2C0CA74z 0x2C0CA70z
Error(1): No pskey found
 -Traceback= 0x37B609Cz 0x37ABEB8z 0x37AC29Cz 0x2C0CA74z 0x2C0CA70z
```

Related Commands

Command	Description
clear crypto ikev2 diagnose error	Clears the IKEv2 exit path database.
crypto ikev2 diagnose error	Enables IKEv2 error diagnosis.

show crypto ikev2 policy

To display the default or a user-defined Internet Key Exchange Version 2 (IKEv2) policy, use the **show crypto ikev2 policy** command in privileged EXEC mode.

show crypto ikev2 policy [*policy-name*]

Syntax Description

policy-name	(Optional) Displays the specified policy.

Command Default

If no option is specified, then this command displays all the policies.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(1)T	This command was introduced.
15.1(4)M	This command was modified. The command output was updated to support IPv6 addresses.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.

Usage Guidelines

Use this command to display the default or user-defined IKEv2 policy. User-defined policies display the default values of the commands that are not explicitly configured under the policy.

Examples

The following examples show the output for a default and user-defined policy.

Default IKEv2 Policy

The default IKEv2 policy matches all local addresses in global VRF and uses the default IKEv2 proposal.

```
Router# show crypto ikev2 policy default
 IKEv2 policy : default
      Match fvrf  : global
      Match address local : any
      Proposal    : default
Router# show crypto ikev2 policy default
```

This sample output shows the default IKEv2 policy that matches the local IPv6 address in global VRF: IKEv2 policy : default

```
      Match fvrf  : global
      Match address local : 2001:DB8:1::1
      Proposal    : default
```

User-defined IKEv2 policy

```
Router# show crypto ikev2 policy policy-1
    IKEv2 policy : policy-1
        Match fvrf : green
        Match local : 10.0.0.1
        Proposal    : proposal-A
        Proposal    : proposal-B
```

The table below describes the significant fields shown in the display.

Table 34: show crypto ikev2 policy Field Descriptions

Field	Description
IKEv2 policy	Name of the IKEv2 policy.
Match fvrf	The front door virtual routing and forwarding (FVRF) specified for matching the IKEv2 policy.
Match local	The local IP address (IPv4 or IPv6) assigned for matching the IKEv2 policy.
Proposal	The name of the proposal that is attached to the IKEv2 policy.

Related Commands

Command	Description
crypto ikev2 policy	Defines an IKEv2 policy.
crypto ikev2 proposal	Defines an IKE proposal.
match (ikev2 policy)	Matches an IKEv2 policy based on the parameters.
proposal	Specifies the proposals that must be used in the IKEv2 policy.

show crypto ikev2 profile

To display a user-defined Internet Key Exchange Version 2 (IKEv2) profile, use the **show crypto ikev2 profile** command in privileged EXEC mode.

show crypto ikev2 profile [*profile-name*]

Syntax Description

profile-name	(Optional) Name of the IKEv2 profile.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(1)T	This command was introduced.
15.1(4)M	This command was modified. The command output was updated to support IPv6 addresses.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

Use this command to display information about an IKEv2 profile. This command also displays the default values of the commands that are not explicitly configured in the IKEv2 profile. If a profile name is not specified, the command displays all the user-defined IKEv2 profiles.

Examples

The following example is sample output from the **show crypto ikev2 profile** command:

```
Router# show crypto ikev2 profile
IKEv2 profile: prof
 Ref Count: 3
 Match criteria:
  Fvrf: any
  Local address/interface: none
  Identities:
   fqdn smap-initiator
  Certificate maps: none
 Local identity: fqdn dmap-responder
 Remote identity: none
 Local authentication method: pre-share
 Remote authentication method(s): pre-share
 Keyring: v2-kr1
 Trustpoint(s): none
 Lifetime: 86400 seconds
 DPD: disabled
 NAT-keepalive: disabled
 Ivrf: global
 Virtual-template: none
 Accounting mlist: none
```

The table below describes the significant fields shown in the display.

Table 35: show crypto ikev2 profile Field Descriptions

Field	Description
IKEv2 profile	Name of the IKEv2 profile.
Match	The match parameter in the profile.
Local Identity	The local identity type.
Local authentication method	The local authentication methods.
Remote authentication method	The remote authentication methods.
Keyring	The keyring specified in the profile.
Trustpoint	The trustpoints used in the Rivest, Shamir and Adleman (RSA) signature authentication method.
Lifetime	The lifetime of the IKEv2 profile.
DPD	The status of Dead Peer Detection (DPD).
Ivrf	The Inside VRF (IVRF) in the profile.
Virtual-template	The virtual template in the profile.

show crypto ikev2 proposal

To display the Internet Key Exchange Version 2 (IKEv2) proposal, use the **show crypto ikev2 proposal** command in privileged EXEC mode.

show crypto ikev2 proposal [{*namedefault*}]

Syntax Description

name	(Optional) The user-defined proposal.
default	(Optional) The default proposal.

Command Default

If no option is specified, the default and user-defined proposals are displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(1)T	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.

Usage Guidelines

Use this command to display the user-defined and default proposals.

Examples

The following example is a sample output from the **show crypto ikev2 proposal**command:

```
Router# show crypto ikev2 proposal
 IKEv2 proposal: pr1
     Encryption : 3DES AES-CBC-192
     Integrity  : MD596
     PRF        : MD5
     DH Group   : DH_GROUP_768_MODP/Group 1 DH_GROUP_1536_MODP/Group 5
 IKEv2 proposal: default
     Encryption : AES-CBC-128 3DES
     Integrity  : SHA96 MD596
     PRF        : SHA1 MD5
     DH Group   : DH_GROUP_1536_MODP/Group 5 DH_GROUP_1024_MODP/Group 2
```

The table below describes the significant fields shown in the display.

Table 36: show crypto ikev2 proposal Field Descriptions

Field	Description
IKEv2 proposal	Name of the proposal.
Encryption	The encryption algorithm configured in the proposal.
Integrity	The integrity algorithm configured in the proposal.

Field	Description
PRF	The Pseudo-Random Function in the proposal. This is the same as the integrity algorithm.
DH Group	The Diffie-Hellman groups configured in the proposal.

Related Commands

Command	Description
crypto ikev2 proposal	Defines an IKEv2 proposal.
encryption (ikev2 proposal)	Specifies the encryption algorithm in an IKEv2 proposal.
group (ikev2 proposal)	Specifies the DH groups in an IKEv2 proposal.
integrity (ikev2 proposal)	Specifies the integrity algorithm in an IKEv2 proposal.

show crypto ikev2 sa

To display an Internet Key Exchange Version 2 (IKEv2) security associations (SA), use the **show crypto ikev2 sa** command in privileged EXEC mode.

show crypto ikev2 sa {**local** [{*ipv4-addressipv6-address*}] | **remote** [{*ipv4-addressipv6-address*}] | **fvrf** *vrf-name*} [**detailed**]

Syntax Description

local [*ipv4-address* | *ipv6-address*]	Displays current IKEv2 SAs that match the local IP address.
remote [*ipv4-address* | *ipv6-address*]	Displays current IKEv2 SAs that match the remote IP address.
fvrf *vrf-name*	Displays current IKEv2 SAs that match the specified forward virtual routing and forwarding (FVRF).
detailed	(Optional) Displays detailed information about current SAs.

Command Default

All current IKEv2 security associations are displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(1)T	This command was introduced.
15.1(4)M	This command was modified. The command output was updated to support IPv6 addresses.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.
15.2(4)M	This command was modified. The output for the **detailed** keyword was enhanced to include information about the IKEv2 redirect mechanism.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.

Usage Guidelines

Use this command to display information about the current IKEv2 security associations.

Examples

The following is sample output from the **show crypto ikev2 sa** command:

```
Device# show crypto ikev2 sa
Tunnel-id   Local          Remote           fvrf/ivrf          Status
2           10.0.0.1/500    10.0.0.2/500  (none)/(none)      READY
      Encr: 3DES, Hash: SHA96, DH Grp:2, Auth: PSK
      Life/Active Time: 86400/361 sec
Device# show crypto ikev2 sa
Tunnel-id   Local           Remote             fvrf/ivrf           Status
```

```
1   2001:DB8:0::1/500    2001:DB8:0::2/500      (none)/(none)      READY
      Encr: 3DES, Hash: SHA96, DH Grp:2, Auth: PSK
      Life/Active Time: 86400/361 sec
```

The following is sample output from the **show crypto ikev2 sa detailed** command:

```
Device# show crypto ikev2 sa detailed
Tunnel-id   Local          Remote           fvrf/ivrf          Status
2           10.0.0.1/500    10.0.0.2/500      (none)/(none)      READY
      Encr: 3DES, Hash: SHA96, DH Grp:2, Auth: PSK
      Life/Active Time: 86400/479 sec
      CE id: 0, Session-id: 2, MIB-id: 2
      Status Description: Negotiation done
      Local spi: BCF1453548BE731C       Remote spi: 85CB158F05817B3A
      Local id:          10.0.0.1           Remote id:          10.0.0.2
      Local req mess id:    3           Remote req mess id: 0
      Local next mess id:    3          Remote next mess id: 1
      Local req queued:    3            Remote req queued: 0
      Local window:    5                Remote window: 5
      DPD configured for 0 seconds
      NAT-T is not detected
      Redirected From: 10.1.1.100
```

The table below describes the significant fields shown in the display.

Table 37: show crypto ikev2 sa detailed Field Descriptions

Field	Description
Tunnel-id	Unique identifier of the IKEv2 tunnel.
Local	IP address (IPv4 or IPv6) and UDP port of the local IKEv2 endpoint.
Remote	IP address (IPv4 or IPv6) and UDP port of the remote IKEv2 endpoint.
fvrf/ivrf	Forward VRF (FVRF)/Inside VRF (IVRF) of the local IKEv2 endpoint.
Status	Status of the IKEv2 tunnel.
Encr	Encryption algorithm used by the IKEv2 tunnel.
Hash	Integrity algorithm used by the IKEv2 tunnel.
DH Grp	Diffie-Hellman (DH) group used by the IKEv2 tunnel.
Auth Sign	Authentication method used by the local IKEv2 endpoint.
Auth Verify	Authentication method used by the remote IKEv2 endpoint.
Life/Active Time	Total and active times of the IKEv2 tunnel.
CE id	Crypto engine (CE) ID used by the local IKEv2 endpoint.
Session-id	Session ID for the IKEv2 tunnel.
MIB-id	MIB identifier for the IKEv2 tunnel.
Status Description	Description of the IKEv2 tunnel status.

Field	Description
Local spi	IKEv2 security parameter index (SPI) of the local IKEv2 endpoint.
Remote spi	IKEv2 SPI of the remote IKEv2 endpoint.
Local id	IKEv2 identity of the local IKEv2 endpoint.
Remote id	IKEv2 identity of the remote IKEv2 endpoint.
Local req mess id	Message ID of the last IKEv2 request sent.
Remote req mess id	Message ID of the last IKEv2 request received.
Local next mess id	Message ID of the next IKEv2 request to be sent.
Remote next mess id	Message ID of the next IKEv2 request to be received.
Local req queued	Number of requests that are queued to be sent.
Remote req queued	Number of requests that are queued to be processed.
Local window	IKEv2 window size of the local IKEv2 endpoint.
Remote window	IKEv2 window size of the remote IKEv2 endpoint.
DPD	Dead Peer Detection (DPD) interval.
NAT_T	Network Address Translation (NAT) detection status.
Redirected From	IP address from which the request was redirected.

show crypto ikev2 session

To display the status of active Internet Key Exchange Version 2 (IKEv2) sessions, use the **show crypto ikev2 session**command in privileged EXEC mode.

show crypto ikev2 session [**detailed**]

Syntax Description

detailed	(Optional) Displays detailed information about the session.

Command Default

The session information is displayed in a brief format.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(1)T	This command was introduced.
15.1(4)M	This command was modified. The command output was updated to support IPv6 addresses.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

Use this command to display information about the active IKEv2 sessions. Use the **detailed** keyword to display information about IKEv2 parent and child security associations.

Examples

The following is a sample output from the **show crypto ikev2 session** and **show crypto ikev2 session detailed** command.

```
Router# show crypto ikev2 session
Session-id:4, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                 Remote                fvrf/ivrf            Status
1          10.10.10.1/500        20.20.20.1/500        none/none             READY
      Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:19, Auth sign: PSK,
Auth verify: PSK
      Life/Active Time: 86400/93 sec
      CE id: 1004, Session-id: 4
      Local spi: 392B7A3F58F8E75D       Remote spi: C700105C311A80FE
Child sa: local selector  0.0.0.0/0 - 255.255.255.255/65535
          remote selector 0.0.0.0/0 - 255.255.255.255/65535
          ESP spi in/out: 0xED36856/0xD0EDF99E

Router# show crypto ikev2 session detailed
Session-id:4, Status:UP-ACTIVE, IKE count:1, CHILD count:1

Tunnel-id Local                 Remote                fvrf/ivrf            Status
1         10.10.10.1/500        20.20.20.1/500        none/none            READY
      Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:19, Auth sign: PSK,
Auth verify: PSK
      Life/Active Time: 86400/96 sec
      CE id: 1004, Session-id: 4
      Local spi: 392B7A3F58F8E75D       Remote spi: C700105C311A80FE
```

```
      Status Description: Negotiation done
      Local id: 10.10.10.1
      Remote id: 20.20.20.1
      Local req msg id:  0              Remote req msg id:  4
      Local next msg id: 0              Remote next msg id: 4
      Local req queued:  0              Remote req queued:  4
      Local window:      5              Remote window:      5
      DPD configured for 0 seconds, retry 0
      Fragmentation not  configured.
      Dynamic Route Update: enabled
      Extended Authentication not configured.
      NAT-T is not detected
      Cisco Trust Security SGT is disabled
      Initiator of SA : No
Child sa: local selector  0.0.0.0/0 - 255.255.255.255/65535
          remote selector 0.0.0.0/0 - 255.255.255.255/65535
          ESP spi in/out: 0xED36856/0xD0EDF99E
          AH spi in/out: 0x0/0x0
          CPI in/out: 0x0/0x0
          Encr: AES-CBC, keysize: 128, esp_hmac: SHA96
          ah_hmac: None, comp: IPCOMP_NONE, mode tunnel
```

The table below describes the significant fields shown in the display.

Table 38: show crypto ikev2 session detailed Field Descriptions

Field	Description
Tunnel id	Unique identifier of IKEv2 tunnel.
Local	IP address (IPv4 or IPv6) and UDP port of the local IKEv2 endpoint.
Remote	IPv4 or IPv6 address and UDP port of the remote IKEv2 endpoint.
fvrf/ivrf	FVRF/IVRF of the local IKEv2 endpoint.
Status	Status of the IKEv2 tunnel.
Encr	Encryption algorithm used by the IKEv2 tunnel.
Hash	Integrity algorithm used by the IKEv2 tunnel.
DH Grp	DH group used by the IKEv2 tunnel.
Auth Sign	Authentication method used by the local IKEv2 endpoint.
Auth Verify	Authentication method used by the remote IKEv2 endpoint.
Life/Active Time	The total and active lifetime of the IKEv2 tunnel.
CE id	The crypto engine ID used by the local IKEv2 endpoint.
Session-id	The session ID for the IKEv2 tunnel.
MIB-id	The MIB identifier for the IKEv2 tunnel.
Status Description	Description of the IKEv2 tunnel status.
Local spi	IKEv2 security parameter index (SPI) of the local IKEv2 endpoint.

Field	Description
Remote spi	IKEv2 SPI of the remote IKEv2 endpoint.
Local id	IKEv2 identity of the local IKEv2 endpoint
Remote id	IKEv2 identity of the remote IKEv2 endpoint.
Local req mess id	Message ID of the last IKEv2 request sent.
Remote req mess id	Message ID of the last IKEv2 request received.
Local next mess id	Message ID of the next IKEv2 request to be sent.
Remote next mess id	Message ID of the next IKEv2 request to be received.
Local req queued	Number of requests queued to be sent.
Remote req queued	Number of requests queued to be processed.
Local window	IKEv2 window size of the local IKEv2 endpoint.
Remote window	IKEv2 window size of the remote IKEv2 endpoint.
DPD	DPD interval.
NAT	NAT detection status.
Child sa: local selector	Local network protected by the child security association (SA).
remote selector	Remote network protected by the child SA.
ESP spi in/out	Inbound and outbound SPI of the Encapsulating Security Payload (ESP) child SA.
CPI in/out	Inbound and outbound Cisco Product Identification (CPI) of the IP compression (IPComp) child SA.
AH spi in/out	Inbound and outbound SPI of the Authentication Header (AH) child SA.
Encr	Encryption algorithm used by the ESP child SA.
keysize	Size of the key in bits used by the encryption algorithm.
esp_hmac	Integrity algorithm used by the ESP child SA.
ah_hmac	Integrity algorithm used in the AH child SA, if available.
comp	Compression algorithm used by IPComp child SA.
mode	Tunnel or transport mode used by ESP/AH child SA.

show crypto ikev2 stats

To display Internet Key Exchange Version 2 (IKEv2) security association (SA) statistics, use the **show crypto ikev2 stats** command in privileged EXEC mode.

show crypto ikev2 stats [{**exchange** [{**detailed**}] | **ext-service** | **priority-queue** | **timeout** | **reconnect**}]

Syntax Description

exchange	(Optional) Displays information about IKEv2 exchange and notification statistics.
detailed	(Optional) Displays detailed information about IKEv2 exchange and notification statistics.
ext-service	(Optional) Displays information about pass and fail counters for IKEv2 external services.
priority-queue	(Optional) Displays information about the current size and the historical peak of the IKEv2 priority queue.
timeout	(Optional) Displays information about the number of timeouts in IKEv2 internal timers.
reconnect	(Optional) Displays information about the IKEv2 reconnect security associations.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(1)T	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.
15.2(4)S	This command was modified. The output of this command was enhanced to include the default IKEv2 maximum in-negotiation Call Admission Control (CAC) counter.
15.3(2)T	This command was modified. The **exchange**, **detailed**, **ext-service**, **priority-queue**, and **timeout** keywords were added.
15.4(1)T	This command was modified. The **reconnect** keyword was added.
Cisco IOS XE Release 3.11S	This command was integrated into Cisco IOS XE Release 3.11S.

Usage Guidelines

When you execute this command, the statistics are generated from the time of system start up or the last execution of the **clear** command whichever happened last.

If you use the **detailed** keyword in the **show crypto ikev2 stats exchange** command, the output displays information about all exchanges and notifications (including fields that have a value of zero).

External services are service requests that IKEv2 makes to other components, such as, IPsec, public key infrastructure (PKI), authentication, authorization, and accounting (AAA), and crypto engine.

IKEv2 priority queue is an internal data structure for storing incoming requests made to IKEv2 process. Historical peak value is the highest value of the priority queue over a period of time.

IKEv2 timers are internal programs that help IKEv2 to perform tasks on time or result in a timeout when the task exceeds the specified time limit.

Note In the output of "show crypto ikev2 stats" command, the active SAs show the sum total of IKEv2 SAs in READY state plus the IKEv2 SAs in DELETE state (marked for deletion SAs). Starting from release 16.8.1 a new counter called "Marked For Deletion SAs" was introduced, to show SAs that are about to be deleted. Hence "Active SAs" counter will show actual active IKEv2 SAs count.

Examples

The following is a sample output from the **show crypto ikev2 sa** command:

```
ISR-Bundle2# show crypto ikev2 sa | count READY
Number of lines which match regexp = 224

ISR-Bundle2# show crypto ikev2 sa | count DELETE
Number of lines which match regexp = 276
```

The following is a sample output from the **show crypto ikev2 stats** command:

```
Device(#) show crypto ikev2 stats

------------------------------------------------------------------------
              Crypto IKEV2 SA Statistics
------------------------------------------------------------------------------
System Resource Limit:   0        Max IKEv2 SAs: 0        Max in nego: 40
Total IKEv2 SA Count:    0        active:        0        negotiating: 0
Incoming IKEv2 Requests: 0        accepted:      0        rejected:    0
Outgoing IKEv2 Requests: 0        accepted:      0        rejected:    0
Rejected IKEv2 Requests: 0        rsrc low:      0        SA limit:    0
IKEv2 packets dropped at dispatch: 0
Incoming IKEV2 Cookie Challenged Requests: 0
    accepted: 0        rejected: 0        rejected no cookie: 0
```

The following table describes the significant fields shown in the display:

Table 39: show crypto ikev2 stats Field Descriptions

Field	Description
System Resource Limit	Percentage of system resources that a router is using before IKEv2 starts dropping all SA requests.
Max IKEv2 SAs	Number of active IKEv2 SA requests allowed on the router.
Max in nego	Default IKEv2 maximum in-negotiation CAC counter.
Total IKEv2 SA Count	Number of IKEv2 SAs.
active	Number of active SAs.
negotiating	Number of SA requests being negotiated.
Incoming IKEv2 Requests	Number of incoming IKEv2 SA requests.
accepted	Number of accepted IKEv2 SA requests.

Field	Description
rejected	Number of rejected incoming IKEv2 SA requests.
Outgoing IKEv2 Requests	Number of outgoing IKEv2 SA requests.
accepted	Number of accepted outgoing IKEv2 SA requests.
rejected	Number of rejected outgoing IKEv2 SA requests.
Rejected IKEv2 Requests	Number of IKEv2 requests that were rejected.
rsrc low	Number of IKEv2 requests that were rejected because system resources were low or the preconfigured system resource limit was exceeded.
SA limit	Number of IKEv2 SA requests that were rejected because the SA limit was reached.
IKEv2 packets dropped at dispatch	Number of IKEv2 packets dropped in transit.
Incoming IKEv2 Cookie Challenged Requests	Number of incoming IKEv2 cookie requests.
accepted	Number of accepted incoming IKEv2 cookie requests.
rejected	Number of rejected incoming IKEv2 cookie requests.
rejected no cookie	Number of incoming IKEv2 cookie requests rejected because the request did not contain cookies.

The following is a sample output from the **show crypto ikev2 stats exchange** command:

```
Device(#) show crypto ikev2 stats exchange
--------------------------------------------------------------------------------
EXCHANGE/NOTIFY                    TX(REQ)     TX(RES)     RX(REQ)     RX(RES)

EXCHANGES

IKE_SA_INIT                           1           0           0           1
IKE_AUTH                              1           0           0           1
CREATE_CHILD_SA                       3           0           0           3
CREATE_CHILD_SA_IPSEC_REKEY           1           0           0           1
CREATE_CHILD_SA_IKE_REKEY             2           0           0           2
INFORMATIONAL                         3           0           0           3

ERROR NOTIFY


OTHER NOTIFY

INITIAL_CONTACT                       1           0           0           0
SET_WINDOW_SIZE                       3           0           0           3
NAT_DETECTION_SOURCE_IP               1           0           0           1
NAT_DETECTION_DESTINATION_IP          1           0           0           1
HTTP_CERT_LOOKUP_SUPPORTED            1           0           0           1
REKEY_SA                              1           0           0           0
```

```
CONFIG PAYLOAD TYPE                 TX          RX
CFG_REQUEST                          1           0


OTHER COUNTERS
NO_NAT 1
------------------------------------------------------------------------------
```

The following table describes the significant fields shown in the display:

Note **REKEY_SA** only shows the number of rekey requests sent on the transmitter side (Tx) and the number of rekey requests received on the receiver side (Rx).

CREATE_CHILD_SA_IPSEC_REKEY enables the Tx request to be sent or Rx request to be received, and the Tx response to be received or Rx response to be received.

Table 40: show crypto ikev2 stats exchange Field Descriptions

Field	Description
EXCHANGE/NOTIFY	Type of information—exchange or notification.
TX (REQ)	Transmitted request.
TX (RES)	Transmitted response.
RX (REQ)	Received request.
RX (RES)	Received response.
EXCHANGES	IKEv2 exchanges.
IKE_SA_INIT	Number of IKE SA initiation requests.
ERROR NOTIFY	Number of error notifications.
OTHER NOTIFY	Number of other notifications.
NAT_DETECTION_SOURCE_IP	Number of IP addresses containing source Network Address Translation (NAT).
NAT_DETECTION_DESTINATION_IP	Number of IP addresses containing destination NAT.
CONFIG PAYLOAD TYPE	Configuration payload type.
OTHER COUNTERS	Exchanges or notifications that cannot be classified in the above fields.

The following is a sample output from the **show crypto ikev2 stats ext-service** command:

```
Device(#) show crypto ikev2 stats ext-service
------------------------------------------------------------
AAA OPERATION                              PASSED     FAILED
------------------------------------------------------------
RECEIVING PSKEY                               0          0
```

```
AUTHENTICATION USING EAP                          0          0
START ACCOUNTING                                  0          0
STOP ACCOUNTING                                   0          0
AUTHORIZATION                                     0          0
-----------------------------------------------------------------
IPSEC OPERATION                                PASSED     FAILED
-----------------------------------------------------------------
IPSEC POLICY VERIFICATION                         0          0
SA CREATION                                       0          0
SA DELETION                                       0          0
-----------------------------------------------------------------
CRYPTO ENGINE OPERATION                        PASSED     FAILED
-----------------------------------------------------------------
DH PUBKEY GENERATED                             7723          0
DH SHARED SECKEY GENERATED                        0          0
SIGNATURE SIGN                                    0          0
SIGNATURE VERIFY                                  0          0
-----------------------------------------------------------------
PKI OPERATION                                  PASSED     FAILED
-----------------------------------------------------------------
VERIFY CERTIFICATE                                0          0
FETCHING CERTIFICATE USING HTTP                   0          0
FETCHING PEER CERTIFICATE USING HTTP              0          0
GET ISSUERS                                       0          0
GET CERTIFICATES FROM ISSUERS                     0          0
GET DN FROM CERT                                  0          0
```

The following table describes the significant fields shown in the display:

Table 41: show crypto ikev2 stats ext-service Field Descriptions

Field	Description
AAA OPERATION	Indicates service requests sent for AAA.
PASSED	Indicates the number of requests that passed.
FAILED	Indicates the number of requests that failed.
RECEIVING PSKEY	Denotes the number of requests that passed or failed when a preshared key was requested from AAA.
AUTHENTICATION USING EAP	Denotes the number of requests that passed or failed when authenticating using Extensible Authentication Protocol (EAP).
START ACCOUNTING	Denotes the number of requests that passed or failed when AAA was requested to stop accounting.
STOP ACCOUNTING	Denotes the number of requests that passed or failed when AAA was requested to start accounting.
IPSEC OPERATION	Indicates service requests sent to IPsec.
IPSEC POLICY VERIFICATION	Denotes the number of requests that passed or failed during IPsec policy verification.
SA CREATION	Denotes the number of requests that passed or failed during IPsec SA creation.

Field	Description
SA DELETION	Denotes the number of requests that passed or failed during IPsec SA deletion.
CRYPTO ENGINE OPERATION	Indicates service requests sent to crypto engine.
DH PUBKEY GENERATED	Denotes the number of requests made (passed or failed) to the crypto engine to generate Diffie-Hellman (DH) public keys.
DH SHARED SECKEY GENERATED	Denotes the number of requests made (passed or failed) to the crypto engine to generate DH shared secret keys.
SIGNATURE SIGN	Denotes the number of requests made (passed or failed) to the crypto engine to sign the signature.
SIGNATURE VERIFY	Denotes the number of requests made (passed or failed) to the crypto engine to verify the signature.
PKI OPERATION	Indicates the service request sent to PKI.
VERIFY CERTIFICATE	Denotes the number of requests that passed or failed when requesting PKI to verify certificates.
FETCHING CERTIFICATE USING HTTP	Denotes the number of requests that passed or failed when requesting PKI to fetch certificates using HTTP.
FETCHING PEER CERTIFICATE USING HTTP	Denotes the number of requests that passed or failed when requesting PKI to fetch peer certificates using HTTP.
GET ISSUERS	Denotes the number of requests that passed or failed when requesting PKI to get issuers.
GET CERTIFICATES FROM ISSUERS	Denotes the number of requests that passed or failed when requesting PKI to get certificates from issuers.
GET DN FROM CERT	Denotes the number of requests that passed or failed when requesting PKI to fetch the distinguished name (DN) through the certificate authentication method.

The following is a sample output from the **show crypto ikev2 stats priority-queue** command:

```
Device(#) show crypto ikev2 stats priority-queue
------------------------------------------------
IKEV2 PRIORITY QUEUE                SIZE       PEAK
------------------------------------------------
HIGHEST                                0          2
HIGHER                                 0          0
HIGH                                   0          0
NORMAL                                 0          1
LOW                                    0          0
LOWER                                  0          0
LOWEST                                 0          1
```

The following table shows significant fields shown in the display.

Table 42: show crypto ikev2 stats priority-queue Field Descriptions

Field	Description
IKEV2 PRIORITY QUEUE	IKEv2 priority queue, which ranges from highest to lowest.
SIZE	Size of the priority queue.
PEAK	Historical peak of the priority queue.

The following is a sample output from the **show crypto ikev2 stats timeout** command:

```
Device(#) show crypto ikev2 stats timeout
----------------------------------------
IKEV2 TIMER                     TIMED OUT
----------------------------------------
EXT SERVICE TIMER                       0
AUTH TIMER                              0
PACKET MAXIMUM RETRANS TIMER         7736
DPD MAX RETRANS TIMER                   0
```

The following table shows significant fields shown in the display.

Table 43: show crypto ikev2 stats timeout Field Descriptions

Field	Description
IKEV2 TIMER	IKEv2 timer.
EXT SERVICE TIMER	Timer to ensure external services completes the service within the specified time.
AUTH TIMER	Timer to ensure that IKEv2 authorization is completed within the specified time.
PACKET MAXIMUM RETRANS TIMER	Timeouts that occurred when retransmitting the packets.
DPD MAX RETRANS TIMER	Timeouts that occurred when retransmitting the dead peer detection.

Related Commands

Command	Description
clear crypto ikev2 stats	Clears IKEv2 SA statistics.

show crypto ipsec client ezvpn

To display the Cisco Easy VPN Remote configuration, use the **show crypto ipsec client ezvpn** command in privileged EXEC mode.

show crypto ipsec client ezvpn

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(4)YA	This command was introduced on Cisco 806, Cisco 826, Cisco 827, and Cisco 828 routers; Cisco 1700 series routers; and Cisco uBR905 and Cisco uBR925 cable access routers.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS 12.2SX family of releases. Support in a specific 12.2SX release is dependent on your feature set, platform, and platform hardware.

Examples

The following example shows a typical display from the **show crypto ipsec client ezvpn**command for an active Virtual Private Network (VPN) connection when the router is in client mode. The last two lines indicate that a configuration URL and configuration version number have been pushed through the Mode-Configuration Exchange by the server to the Easy VPN remote device.

```
Router# show crypto ipsec client ezvpn

Tunnel name: hw1
Inside interface list: FastEthernet0/0, Serial1/0,
Outside interface: Serial0/0
Current State: IPSEC_ACTIVE
Last Event: SOCKET_UP
Address: 192.168.201.0
Mask: 255.255.255.224
DNS Primary: 192.168.201.1
DNS Secondary: 192.168.201.2
NBMS/WINS Primary: 192.168.201.3
NBMS/WINS Secondary: 192.168.201.4
Default Domain: cisco.com
Configuration URL: http://10.8.8.88/easy.cfg
Configuration Version: 10
```

The following example shows a typical display from the **show crypto ipsec client ezvpn**command for an active VPN connection when the router is in network-extension mode:

```
Router# show crypto ipsec client ezvpn

Tunnel name: hw1
Inside interface list: FastEthernet0/0, Serial1/0,
```

```
Outside interface: Serial0/0
Current State: IPSEC_ACTIVE
Last Event: SOCKET_UP
Address: 192.168.202.128
Mask: 255.255.255.224
Default Domain: cisco.com
Split Tunnel List: 1
       Address    : 192.168.200.225
       Mask       : 255.255.255.224
       Protocol   : 0x0
       Source Port: 0
       Dest Port  : 0
```

The following example shows a typical display from the **show crypto ipsec client ezvpn**command for an inactive VPN connection:

```
Router# show crypto ipsec client ezvpn

Current State: IDLE
Last Event: REMOVE INTERFACE CFG
Router#
```

The following example displays information about the outside interface "Virtual-Access1", which is bound to the real interface (Ethernet0/0) on which the user has configured Easy VPN as an outside interface:

```
Router# show crypto ipsec client ezvpn
Easy VPN Remote Phase: 5
Tunnel name : ez
Inside interface list: Ethernet1/0,
Outside interface: Virtual-Access1 (bound to Ethernet0/0)
Easy VPN connect ACL checking active
Connect : ACL based with access-list 101
Current State: CONNECT_REQUIRED
Last Event: TRACKED OBJECT UP
Save Password: Disallowed
Current EzVPN Peer: 10.0.0.2
```

The table below describes significant fields shown by the **show crypto ipsec client ezvpn** command:

Table 44: show crypto ipsec client ezvpn Field Descriptions

Field	Description
Current State	Displays whether the VPN tunnel connection is active or idle. Typically, when the tunnel is up, the current state is IPSEC ACTIVE.
Last Event	Displays the last event performed on the VPN tunnel. Typically, the last event before a tunnel is created is SOCKET UP.
Address	Displays the IP address used on the outside interface.
Mask	Displays the subnet mask used for the outside interface.
DNS Primary	Displays the primary domain name system (DNS) server provided by the Dynamic Host Configuration Protocol (DHCP) server.
DNS Secondary	Displays the secondary DNS server provided by the DHCP server.

Field	Description
Domain Name	Displays the domain name provided by the DHCP server.
NBMS/WINS Primary	Displays the primary NetBIOS Microsoft Windows Name Server provided by the DHCP server.
NBMS/WINS Secondary	Displays the secondary NetBIOS Microsoft Windows Name Server provided by the DHCP server.

Related Commands

Command	Description
show crypto ipsec transform	Displays the specific configuration for one or all transformation sets.

show crypto ipsec transform-set default

To display the default IP Security (IPsec) transform sets currently in use by Internet Key Exchange (IKE), use the **show crypto ipsec transform-set default** command in privileged EXEC mode.

show crypto ipsec transform-setdefault

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 series routers.

Usage Guidelines

If the default transform sets are in use, the **show crypto ipsec default transform-set** command displays the two default transform sets each of which defines an Encapsulation Security Protocol (ESP) encryption transform type and an ESP authentication transform type.

Examples

The following example displays the two default transform sets. No user defined transform sets have been configured, the default transform sets have not been disabled, and the crypto engine supports the encryption algorithm.

```
Router# show crypto ipsec default transform-set

Transform set #$!default_transform_set_1: { esp-aes esp-sha-hmac  }
   will negotiate = { Transport,  },

Transform set #$!default_transform_set_0: { esp-3des esp-sha-hmac  }
   will negotiate = { Transport,  },
```

Table 45: show crypto ipsec default transform-set Field Descriptions

Default Transform Name	ESP Encryption Transform and Description	ESP Authentication Transform and Description
#$!default_transform_set_1	esp-aes (ESP with the 128-bit Advanced Encryption Standard [AES] encryption algorithm)	esp-sha-hmac (ESP with the Secure Hash Algorithm [SHA-1, HMAC variant] authentication algorithm)
#$!default_transform_set_0	esp-3des (ESP with the 168-bit Triple Data Encryption Standard [3DES or Triple DES] encryption algorithm)	esp-sha-hmac

The following example shows that when the default transform sets are disabled with the **no crypto ipsec default transform-set**, the **show crypto ipsec default transform-set**has no output.

```
Router(config)# no crypto ipsec default transform-set
Router(config)# exit
Router#
Router# show crypto ipsec default transform-set

Router#
```

Related Commands

Command	Description
crypto ipsec transform-set	Defines a transform set.
show crypto ipsec transform-set	Displays the configured transform sets.
show crypto map (IPsec)	Displays the crypto map configuration.

show crypto ipsec sa

To display the settings used by IPsec security associations (SAs), use the **show crypto ipsec sa** command in privileged EXEC mode.

show crypto ipsec sa [{**active** | **address** | **detail** | **identity** [**detail**] | **interface** *type number* [{**detail** | **ipv6** [**detailed**] | **interface** *type number* [**detailed**]}] | **ipv6** [**interface** *typenumber*] [**detailed**] | **map** *map-name* [**detail**] | **peer** [{**detail** | [**vrf** *vrf*] [{*ipv4-address* [**detail**] | *ipv6-address* [{**detail** | **platform**}]}]}] | **standby** | **vrf** *vrf* [**detail**]}]

Syntax Description

active	(Optional) Displays high availability (HA)-enabled IPsec SAs that are in the active state.
address	(Optional) Displays all existing SAs. The SAs are sorted by the destination address (either the local address or the address of the IPsec remote peer) and then by protocol (Authentication Header [AH] or Encapsulation Security Protocol [ESP]).
detail	(Optional) Displays detailed information.
identity [**detail**]	(Optional) Displays only the flow information. SA information is not displayed.
interface *type number*	(Optional) Displays all SAs created for an interface.
ipv6	(Optional) Displays IPv6 IPsec SA information.
detailed	(Optional) Displays detailed error counters.
platform	(Optional) Displays platform-specific information about the IPsec flow.
ipv4-address	(Optional) Displays IPsec SAs for an IPv4 peer.
ipv6-address	(Optional) Displays IPsec SAs for an IPv6 peer.
map *map-name* [**detail**]	(Optional) Displays any existing SAs that were created for the crypto map set using a value for the *map-name* argument.
peer [**detail** | [**vrf** *vrf*] [*ipv4-address* [**detail**] | *ipv6-address* [**detail** | **platform**]]]	(Optional) Displays all existing SAs with the peer address.
standby	(Optional) Displays HA-enabled IPsec SAs that are in the standby state.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.3T	This command was introduced.

Release	Modification
12.2(13)T	This command was modified. The remote crypto endpt and in use settings fields were modified to support Network Address Translation (NAT) traversal.
12.2(15)T	This command was modified. The **interface** keyword and the *type* and *number* arguments were added. The **peer** keyword, the **vrf** keyword, and the *fvrf-name* argument were added. The **address** keyword was added to the **peer** keyword string. The **vrf** keyword and *ivrf-name* argument were added.
12.3(11)T	This command was modified. The **active** and **standby** keywords were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was implemented on the Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 3.7S	This command was modified. The **platform** keyword was added. The output was enhanced to display platform-specific information about the IPsec interface and peer.
15.3(2)T	This command was modified. The output was enhanced on group members (GMs) to display the name of the GDOI group to which each IPsec SA applies and the number of packets that are tagged with Cisco TrustSec security group tags (SGTs) in the outbound and inbound directions.
Cisco IOS XE Release 3.9S	This command was modified. The output was enhanced on GMs to display the name of the GDOI group to which each IPsec SA applies and the number of packets that are tagged with SGTs in the outbound and inbound directions.
15.4(1)T	This command was modified. The output was enhanced on GMs to display the name of the GDOI group to which each IPsec SA applies and the number of packets that are tagged with SGTs in the outbound and inbound directions.

Usage Guidelines

If no keyword is specified, all SAs are displayed. The SAs are sorted first by interface and then by traffic flow (for example, source or destination address, mask, protocol, or port). Within a flow, SAs are listed by protocol (ESP or AH) and direction (inbound or outbound).

Note The IPsec SA maximum transmission unit (MTU) is based on IPsec SA path MTU, not the interface MTU.

The **show crypto ipsec sa interface platform** command for a specific interface type displays the output from the following **show** commands, as listed in the order below:

- **show crypto ipsec sa**
- **show platform hardware qfp active feature ipsec interface**

Examples

The following is sample output from the **show crypto ipsec sa** command:

```
Device# show crypto ipsec sa

interface: Ethernet0/1.1
    Crypto map tag: GetvpnAdvanced, local addr 10.10.1.3
   protected vrf: (none)
   local  ident (addr/mask/prot/port): (10.10.1.4/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port): (10.10.0.1/255.255.255.255/0/0)
   Group: GetvpnAdvanced2
   current_peer 0.0.0.0 port 848
     PERMIT, flags={}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 10.10.1.3, remote crypto endpt.: 0.0.0.0
     plaintext mtu 1446, path mtu 1500, ip mtu 1500, ip mtu idb Ethernet0/1.1
     current outbound spi: 0x4A22A261(1243783777)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0x4A22A261(1243783777)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 5, flow_id: SW:5, sibling_flags 80000040, crypto map: GetvpnAdvanced
        sa timing: remaining key lifetime (sec): 379
        Kilobyte Volume Rekey has been disabled
        IV size: 8 bytes
        replay detection support: Y
        ecn bit support: Y status: off
        Status: ACTIVE(ACTIVE)

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x4A22A261(1243783777)
        transform: esp-3des esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 6, flow_id: SW:6, sibling_flags 80000040, crypto map: GetvpnAdvanced
        sa timing: remaining key lifetime (sec): 379
        Kilobyte Volume Rekey has been disabled
        IV size: 8 bytes
        replay detection support: Y
        ecn bit support: Y status: off
        Status: ACTIVE(ACTIVE)

     outbound ah sas:

     outbound pcp sas:
```

The following is sample output from the **show crypto ipsec sa detail** command, which displays the number of packets that are tagged with Cisco TrustSec SGTs:

```
Device# show crypto ipsec sa detail

interface: Ethernet0/0
```

```
   Crypto map tag: GET, local addr 5.0.0.2
   protected vrf: (none)
   local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   Group: GET-SGT
.
.
.
#pkts tagged (send): 0, #pkts untagged (rcv): 5
```

The following is sample output from the **show crypto ipsec sa identity detail** command:

```
Device# show crypto ipsec sa identity detail

interface: Tunnel1
   Crypto map tag: Tunnel1-head-0, local addr 10.5.5.2
   protected vrf: (none)
   local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
   Group: GET-SGT
   current_peer (none) port 500
     DENY, flags={ident_is_root,}
     #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
     #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
     #pkts compressed: 0, #pkts decompressed: 0
     #pkts not compressed: 0, #pkts compr. failed: 0
     #pkts not decompressed: 0, #pkts decompress failed: 0
     #pkts no sa (send) 0, #pkts invalid sa (rcv) 0
     #pkts encaps failed (send) 0, #pkts decaps failed (rcv) 0
     #pkts invalid prot (recv) 0, #pkts verify failed: 0
     #pkts invalid identity (recv) 0, #pkts invalid len (rcv) 0
     #pkts replay rollover (send): 0, #pkts replay rollover (rcv) 0
     ##pkts replay failed (rcv): 0
     #pkts internal err (send): 0, #pkts internal err (recv) 0
   protected vrf: (none)
   local  ident (addr/mask/prot/port): (10.5.5.2/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (10.5.5.1/255.255.255.255/47/0)
   Group: GET-SGT
   current_peer 10.5.5.1 port 500
     PERMIT, flags={origin_is_acl,}
     #pkts encaps: 492923510, #pkts encrypt: 492923510, #pkts digest: 492923510
     #pkts decaps: 492923408, #pkts decrypt: 492923408, #pkts verify: 492923408
     #pkts compressed: 0, #pkts decompressed: 0
     #pkts not compressed: 0, #pkts compr. failed: 0
     #pkts not decompressed: 0, #pkts decompress failed: 0
     #pkts no sa (send) 55, #pkts invalid sa (rcv) 0
     #pkts encaps failed (send) 0, #pkts decaps failed (rcv) 0
     #pkts invalid prot (recv) 0, #pkts verify failed: 0
     #pkts invalid identity (recv) 0, #pkts invalid len (rcv) 0
     #pkts replay rollover (send): 0, #pkts replay rollover (rcv) 0
     ##pkts replay failed (rcv): 0
     #pkts internal err (send): 0, #pkts internal err (recv) 0
```

The following is sample output from the **show crypto ipsec sa vrf** command:

```
Device# show crypto ipsec sa vrf vpn2

interface: Ethernet1/2
   Crypto map tag: ra, local addr. 172.16.1.1
   protected vrf: vpn2
   local  ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
```

```
   remote ident (addr/mask/prot/port): (10.4.1.4/255.255.255.255/0/0)
   Group: GET-SGT
   current_peer: 10.1.1.1:500
   PERMIT, flags={}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0
     local crypto endpt.: 172.16.1.1, remote crypto endpt.: 10.1.1.1
     path mtu 1500, media mtu 1500
     current outbound spi: 50110CF8
     inbound esp sas:
      spi: 0xA3E24AFD(2749516541)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 5127, flow_id: 7, crypto map: ra
        sa timing: remaining key lifetime (k/sec): (4603517/3503)
        IV size: 8 bytes
        replay detection support: Y
     inbound ah sas:
     inbound pcp sas:
     outbound esp sas:
      spi: 0x50110CF8(1343294712)
        transform: esp-3des esp-md5-hmac ,
        in use settings ={Tunnel, }
        slot: 0, conn id: 5128, flow_id: 8, crypto map: ra
        sa timing: remaining key lifetime (k/sec): (4603517/3502)
        IV size: 8 bytes
        replay detection support: Y
     outbound ah sas:
     outbound pcp sas:
```

The following configuration was in effect when the preceding **show crypto ipsec sa vrf** command was issued. The IPsec remote access tunnel was “up” when this command was issued.

```
crypto dynamic-map vpn1 1
 set transform-set vpn1
 set isakmp-profile vpn1-ra
 reverse-route
!
crypto dynamic-map vpn2 1
 set transform-set vpn2
 set isakmp-profile vpn2-ra
 reverse-route
!
!
crypto map ra 1 ipsec-isakmp dynamic vpn1
crypto map ra 2 ipsec-isakmp dynamic vpn2
```

The following is sample output from the **show crypto ipsec sa peer platform** command for the IPv4 address 10.1.1.1.

```
Device# show crypto ipsec sa peer 10.1.1.1 platform

 --------------- FLOW ID's:--------------

In crypto ipsec sa peer platform

Freeing the elements in context
```

The following sample output shows the status of HA-enabled IPsec SAs that are in the active state:

```
Device# show crypto ipsec sa active

interface: Ethernet0/0
   Crypto map tag: to-peer-outside, local addr 10.165.201.3
   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.0.1/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port): (172.16.0.1/255.255.255.255/0/0)
   Group: GET-SGT
   current_peer 192.168.200.225 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 3, #pkts encrypt: 3, #pkts digest: 3
    #pkts decaps: 4, #pkts decrypt: 4, #pkts verify: 4
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0
     local crypto endpt.: 192.168.201.3, remote crypto endpt.: 192.168.200.225
     path mtu 1500, media mtu 1500
     current outbound spi: 0xD42904F0(3559458032)
     inbound esp sas:
      spi: 0xD3E9ABD0(3555306448)
        transform: esp-3des ,
        in use settings ={Tunnel, }
        conn id: 2006, flow_id: 6, crypto map: to-peer-outside
        sa timing: remaining key lifetime (k/sec): (4586265/3542)
             HA last key lifetime sent(k): (4586267)
        ike_cookies: 9263635C CA4B4E99 C14E908E 8EE2D79C
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE
```

The following sample output shows the IPsec SA status of only the standby device. The fields in the display are either self-explanatory or can be found in the preceding tables.

```
Device# show crypto ipsec sa standby

interface: Ethernet0/0
   Crypto map tag: to-peer-outside, local addr 10.165.201.3
   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.0.1/255.255.255.255/0/0)
   remote ident (addr/mask/prot/port): (172.16.0.1/255.255.255.255/0/0)
   Group: GET-SGT
   current_peer 192.168.200.225 port 500
   PERMIT, flags={origin_is_acl,}
    #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
    #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0
     local crypto endpt.: 192.168.201.3, remote crypto endpt.: 192.168.200.225
     path mtu 1500, media mtu 1500
     current outbound spi: 0xD42904F0(3559458032)
     inbound esp sas:
        spi: 0xD3E9ABD0(3555306448)
        transform: esp-3des ,
        in use settings ={Tunnel, }
        conn id: 2012, flow_id: 12, crypto map: to-peer-outside
        sa timing: remaining key lifetime (k/sec): (4441561/3486)
```

```
        HA last key lifetime sent(k): (4441561)
   ike_cookies: 00000000 00000000 00000000 00000000
   IV size: 8 bytes
   replay detection support: Y
   Status: STANDBY
inbound ah sas:
   spi: 0xF3EE3620(4092474912)
   transform: ah-md5-hmac ,
   in use settings ={Tunnel, }
   conn id: 2012, flow_id: 12, crypto map: to-peer-outside
   sa timing: remaining key lifetime (k/sec): (4441561/3486)
        HA last key lifetime sent(k): (4441561)
   ike_cookies: 00000000 00000000 00000000 00000000
   replay detection support: Y
   Status: STANDBY
inbound pcp sas:
outbound esp sas:
   spi: 0xD42904F0(3559458032)
   transform: esp-3des ,
   in use settings ={Tunnel, }
   conn id: 2011, flow_id: 11, crypto map: to-peer-outside
   sa timing: remaining key lifetime (k/sec): (4441561/3485)
        HA last key lifetime sent(k): (4441561)
   ike_cookies: 00000000 00000000 00000000 00000000
   IV size: 8 bytes
   replay detection support: Y
   Status: STANDBY
outbound ah sas:
   spi: 0x75251086(1965363334)
   transform: ah-md5-hmac ,
   in use settings ={Tunnel, }
   conn id: 2011, flow_id: 11, crypto map: to-peer-outside
   sa timing: remaining key lifetime (k/sec): (4441561/3485)
        HA last key lifetime sent(k): (4441561)
   ike_cookies: 00000000 00000000 00000000 00000000
   replay detection support: Y
   Status: STANDBY
outbound pcp sas:
```

The following table describes the significant fields shown in the displays.

Table 46: show crypto ipsec sa Field Descriptions

Field	Description
interface	Interface on which the SA is created.
Crypto map tag	Policy tag for IPsec.
protected vrf	IVRF name that applies to the IPsec interface.
local ident (addr/mask/prot/port)	Local selector that is used for encryption and decryption.
remote ident (addr/mask/prot/port)	Remote selector that is used for encryption and decryption.
Group	Name of the GDOI group corresponding to the IPsec SA.
current peer	Peer that communicates with the IPsec tunnel.

Field	Description
PERMIT, flags	Indicates that the IPsec SA is triggered by the access control list (ACL) permit action.
pkts encaps	Number of packets that were successfully encapsulated by IPsec.
pkts encrypt	Number of packets that were successfully encrypted by IPsec.
pkts digest	Number of packets that were successfully hash digested by IPsec.
pkts decaps	Number of packets that were successfully decapsulated by IPsec.
pkts decrypt	Number of packets that were successfully decrypted by IPsec.
pkts verify	Number of received packets that passed the hash digest check.
pkts compressed	Number of packets that were successfully compressed by IPsec.
pkts decompressed	Number of packets that were successfully decompressed by IPsec.
pkts not compressed	Number of outbound packets that were not compressed.
pkts compr. failed	Number of packets that failed compression by IPsec.
pkts not decompressed	Number of inbound packets that were not compressed.
pkts decompress failed	Number of packets that failed decompression by IPsec.
send errors	Number of outbound packets with errors.
recv errors	Number of inbound packets with errors.
local crypto endpt.	Local endpoint terminated by IPsec.
remote crypto endpt.	Remote endpoint terminated by IPsec.
path mtu	MTU size that is calculated based on the Internet Control Message Protocol (ICMP) unreachable packet, including the IPsec overhead, if any.
media mtu	MTU value for media, such as an Ethernet interface or a serial interface.
ip mtu	Interface MTU size that is dependent on the IPsec overhead.
ip mtu idb	Interface description block (IDB) that is used to determine the crypto IP MTU.
current outbound spi	Current outbound Security Parameters Index (SPI).
current outbound spi	Current outbound Security Parameter Index (SPI).
inbound esp sas	Encapsulating Security Payload (ESP) for the SA for the inbound traffic.

Field	Description
spi	SPI for classifying the inbound packet.
transform	Security algorithm that is used to provide authentication, integrity, and confidentiality.
in use settings	Transform that the SA uses (such as tunnel mode, transport mode, UDP-encapsulated tunnel mode, or UDP-encapsulated transport mode).
conn id	ID that is stored in the crypto engine to identify the IPsec/Internet Key Exchange (IKE) SA.
flow_id	SA identity.
crypto map	Policy for IPsec.
sa timing: remaining key lifetime (k/sec)	Seconds or kilobytes remaining before a rekey occurs.
HA last key lifetime sent (k)	Last stored kilobytes lifetime value for HA.
ike_cookies	ID that identifies the IKE SAs.
IV size	Size of the initialization vector (IV) that is used for the cryptographic synchronization data used to encrypt the payload.
replay detection support	Replay detection feature enabled by a specific SA.
Status	Indicates whether the SA is active.
inbound ah sas	Authentication algorithm for the SA for inbound traffic.
inbound pcp sas	Compression algorithm for the SA for inbound traffic.
outbound esp sas	Encapsulating security payload for the SA for outbound traffic.
outbound ah sas	Authentication algorithm for the SA for outbound traffic.
outbound pcp sas	Compression algorithm for the SA for outbound traffic.
DENY, flags	Indicates that the IPsec SA is triggered by the ACL deny action.
pkts decompress failed	Packets decompressed by IPsec that failed.
pkts no sa (send)	Outbound packets that could not find the associated IPsec SA.
pkts invalid sa (rcv)	Received packets that failed the IPsec format check.
pkts invalid prot (recv)	Received packets that have the wrong protocol field.
pkts verify failed	Received packets that failed the hash digest check.
pkts invalid identity (recv)	Packets that could not find the associated selector after decryption.

Field	Description
pkts invalid len (rcv)	Inbound packets that have an incorrect pad length for the software crypto engine.
pkts replay rollover (send)	Sent packets that failed the replay test check.
pkts replay rollover (rcv)	Received packets that failed the replay test check.
pkts internal err (send)	Sent packets that failed because of a software or hardware error.
pkts internal err (rcv)	Received packets that failed because of a software or hardware error.
protected vrf	IVRF name that applies to the IPsec interface.
pkts tagged (send)	Packets tagged with a Cisco TrustSec SGT in the outbound direction.
pkts untagged (rcv)	Packets not tagged with a Cisco TrustSec SGT in the inbound direction.

Related Commands

Command	Description
crypto ipsec security-association	Configures IPsec security associations.

show crypto ipsec security-association idle-time

To display the security association (SA) idle-time value configured for crypto map entry, use the **show crypto ipsec security-association idle-time** command in privileged EXEC mode.

show crypto ipsec security-association idle-time

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRB	This command was introduced in a release earlier than Cisco IOS Release 12.2(33)SRB.
12.2SX	This command was integrated into Cisco IOS Release 12.2SX.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
Cisco IOS XE 2.3	This command was integrated into Cisco IOS XE Release 2.3.

Usage Guidelines

Use the **show crypto ipsec security-association idle-time**command to display the idle time.

When a router running the Cisco IOS software creates an IPsec SA for a peer, resources must be allocated to maintain the SA. The SA requires both memory and several managed timers. For idle peers, these resources are wasted. If enough resources are wasted by idle peers, the router could be prevented from creating new SAs with other peers. The IPsec Security Association Idle Timers feature introduces a configurable idle timer to monitor SAs for activity, allowing SAs for idle peers to be deleted. This increases the availability of the resources and improve scalability of Cisco IOS IPsec deployments.

Examples

The following is a sample output from the **show crypto ipsec security-association idle-time** command. The output is self-explanatory.

```
Router# show crypto ipsec security-association idle-time
Security association idletime: 567 seconds
```

Related Commands

Command	Description
show crypto ipsec security-association lifetime	Displays the SA lifetime value configured for a particular crypto map entry.

show crypto ipsec security-association lifetime

To display the security association (SA) lifetime value configured for a particular crypto map entry, use the **show crypto ipsec security-association lifetime** command in EXEC mode.

show crypto ipsec security-association lifetime

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.3 T	This command was introduced.\
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output for the **show crypto ipsec security-association lifetime**command:

```
Router# show crypto ipsec security-association lifetime
Security-association lifetime: 4608000 kilobytes/120 seconds
```

The following configuration was in effect when the previous **show crypto ipsec security-association lifetime**command was issued:

```
crypto ipsec security-association lifetime seconds 120
```

show crypto ipsec transform-set

To display the configured transform sets or active default transform sets, use the **show crypto ipsec transform-set**command in privileged EXEC mode.

show crypto ipsec transform-set [**tag** *transform-set-name*]

Syntax Description

tag *transform-set-name*	(Optional) Only the specified transform sets are displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.3 T	This command was introduced.
12.2(13)T	The command output was expanded to include a warning message for users who try to configure an IP Security (IPsec) transform that the hardware does not support.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	The command output was expanded to include information about active default transform sets.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 series routers.

Usage Guidelines

There are two default transform sets supported in Cisco IOS k9 images only:

- Esp-aes esp-sha-hmac
- Esp-3des esp-sha-hmac

The **show crypto ipsec transform-set**command will display the default transform sets if there are no other transform set configured, you have not disabled the default transform sets by issuing the **no crypto ipsec default transform-set** command, and the crypto engine supports the encryption algorithm.

Examples

The following is sample output for the **show crypto ipsec transform-set** command when the default transform sets have been disabled with the **no crypto ipsec default transform-set** command:

```
Router# show crypto ipsec transform-set
Transform set combined-des-sha: {esp-des esp-sha-hmac}
   will negotiate = { Tunnel,  },

Transform set combined-des-md5: {esp-des esp-md5-hmac}
   will negotiate = { Tunnel,  },
```

```
Transform set t1: {esp-des esp-md5-hmac}
   will negotiate = {Tunnel,},

Transform set t100: {ah-sha-hmac}
   will negotiate = {Transport,},

Transform set t2: {ah-sha-hmac}
   will negotiate = {Tunnel,},
   { esp-des  }
   will negotiate = {Tunnel,},
```

The following configuration was in effect when the previous **show crypto ipsec transform-set** command was issued:

```
crypto ipsec transform-set combined-des-sha esp-des esp-sha-hmac
crypto ipsec transform-set combined-des-md5 esp-des esp-md5-hmac
crypto ipsec transform-set t1 esp-des esp-md5-hmac
crypto ipsec transform-set t100 ah-sha-hmac
 mode transport
crypto ipsec transform-set t2 ah-sha-hmac esp-des
no crypto ipsec default transform-set
```

The following sample output from the s**how crypto ipsec transform-set** command displays a warning message after a user tries to configure an IPsec transform that the hardware does not support:

```
Router# show crypto ipsec transform-set
Transform set transform-1:{ esp-256-aes esp-md5-hmac  }
   will negotiate = { Tunnel,  },
WARNING: encryption hardware does not support transform esp-aes 256 within IPSec transform
 transform-1
```

The following is sample output for the **show crypto ipsec transform-set** command when the default transform sets are active and the crypto engine supports the encryption algorithm:

```
Router# show crypto ipsec transform-set
Transform set asset: { esp-256-aes esp-sha-hmac  }
   will negotiate = { Transport,  },

Transform set aesset: { esp-256-aes esp-sha-hmac  }
   will negotiate = { Transport,  },

Transform set #$!default_transform_set_1: { esp-aes esp-sha-hmac  }
   will negotiate = { Transport,  },

Transform set #$!default_transform_set_0: { esp-3des esp-sha-hmac  }
   will negotiate = { Transport,  },
```

Related Commands

Command	Description
show crypto ipsec default transform-set	Displays the default IPsec transform sets.
show crypto ipsec transform-set	Displays the configured transform sets.
show crypto map (IPsec)	Displays the crypto map configuration.

show crypto isakmp default policy

To display the default Internet Key Exchange (IKE) policies currently in use, use the **show crypto isakmp default policy** command in privileged EXEC mode.

show crypto isakmp default policy

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 series routers.

Usage Guidelines

If you have neither manually configured IKE policies with the **crypto isakmp policy** command nor issued the **no crypto isakmp default policy** command, IPsec will use the default IKE policies to negotiate IKE proposals. There are eight default IKE default policies supported (see the table below). The default IKE policies define the following policy set parameters:

- The priority, 65507-65514, where 65507 is the highest priority and 65514 is the lowest priority.
- The authentication method, Rivest, Shamir, and Adelman (RSA) or preshared keys (PSK).
- The encryption method, Advanced Encryption Standard (AES) or Triple Data Encryption Standard (3DES).
- The hash function, Secure Hash Algorithm (SHA-1) or Message-Digest algorithm 5 (MD5).
- The Diffie-Hellman (DH) group specification DH2 or DH5.
  - DH2 specifies the 768-bit Diffie-Hellman group.
  - DH5 specifies the 1536-bit Diffie-Hellman group.

Table 47: Default IKE Policies

Priority	Authentication	Encryption	Hash	Diffie-Hellman
65507	RSA	AES	SHA	DH5
65508	PSK	AES	SHA	DH5
65509	RSA	AES	MD5	DH5
65510	PSK	AES	MD5	DH5
65511	RSA	3DES	SHA	DH2
65512	PSK	3DES	SHA	DH2

Priority	Authentication	Encryption	Hash	Diffie-Hellman
65513	RSA	3DES	MD5	DH2
65514	PSK	3DES	MD5	DH2

If you have manually configured IKE policies and you issue the **show crypto isakmp default policy**command there is no output, since the default IKE policies are not in use.

Examples

The following example displays the eight default policies with protection suites of priorities 65507-65014. The default policies are displayed since there are no user configured policies, the default policies have not been disabled, and EzVPN is not configured.

```
Router# show crypto isakmp default policy
Default protection suite of priority 65507
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit keys).
        hash algorithm:         Secure Hash Standard
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite of priority 65508
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit keys).
        hash algorithm:         Secure Hash Standard
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite of priority 65509
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit keys).
        hash algorithm:         Message Digest 5
        authentication method:  Rivest-Shamir-Adleman signature
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite of priority 65510
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit keys).
        hash algorithm:         Message Digest 5
        authentication method:  pre-shared key
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite of priority 65511
        encryption algorithm:   Three key triple DES
        hash algorithm:         Secure Hash Standard
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite of priority 65512
        encryption algorithm:   Three key triple DES
        hash algorithm:         Secure Hash Standard
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite of priority 65513
        encryption algorithm:   Three key triple DES
        hash algorithm:         Message Digest 5
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
Default protection suite of priority 65514
        encryption algorithm:   Three key triple DES
        hash algorithm:         Message Digest 5
        authentication method:  Pre-Shared Key
```

```
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
```

The following example shows that there is no output from the **show crypto isakmp default policy** command when the default policies have been disabled.

```
Router(config)# no crypto isakmp default policy
! The default IKE policies have been disabled.
Router(config)# exit
Router# configure terminal
Router# show crypto isakmp default policy
Router#
! There is no output from the show crypto isakmp default policy command.
```

Related Commands

Command	Description
crypto isakmp policy	Defines an IKE policy.
no crypto isakmp default policy	Disables IKE default policies.
show crypto isakmp policy	Displays the parameters for each IKE policy.

show crypto isakmp diagnose error

To display Internet Key Exchange (IKE) error diagnostics, use the **show crypto isakmp diagnose error** command in global configuration mode.

show crypto isakmp diagnose error[{**count**}]

Syntax Description

count	(Optional) Displays error counters.

Command Default

IKE error diagnostics is enabled by default.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.3(2)T	This command was introduced.

Usage Guidelines

IKE is a key management protocol standard that is used in conjunction with the IPsec to configure basic IPsec VPNs. IPsec can be configured without IKE, but IKE enhances IPsec by providing additional features, flexibility, and ease of configuration for the IPsec standard. IKE is a hybrid protocol that implements the Oakley key exchange and Skeme key exchange inside the Internet Security Association and Key Management Protocol (ISAKMP) framework.

Use this command to display IKE error-path tracing and to specify the number of entries in the exit path database. When the entries exceed the specified number, new entries replace the old entries.

Examples

The following is sample output from the **show crypto isakmp diagnose error count** command. The fields in this output are self-explanatory.

```
Device# show crypto isakmp diagnose error count
Exit Trace counters
32 - Failed to access account record.
32 - Failed to send delete, peer isn't authenticated.
31 - SA is still negotiating.  Attached new ipsec request to it.
8 - Failed to delete policy.
```

show crypto isakmp key

To list the keyrings and their preshared keys, use the **show crypto isakmp key** command in privileged EXEC mode.

show crypto isakmp key

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.4(4)T	IPv6 address information was added to command output.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Examples

The following is sample output for the **show crypto isakmp key** command:

```
Router# show crypto isakmp key
Hostname/Address       Preshared Key
vpn1                   : 172.61.1.1          vpn1
vpn2                   : 10.1.1.1            vpn2
```

The following configuration was in effect when the above **show crypto isakmp key**command was issued:

```
crypto keyring vpn1
  pre-shared-key address 172.16.1.1 key vpn1
crypto keyring vpn2
  pre-shared-key address 10.1.1.1 key vpn2
```

The table below describes significant fields in the **show crypto isakmp key**profile.

Table 48: show crypto isakmp key Field Descriptions

Field	Description
Hostname/Address	The preshared key host name or address.
Preshared Key	The preshared key.
keyring	Name of the crypto keyring. The global keys are listed in the default keyring.
VRF string	The Virtual Private Network routing and forwarding (VRF) of the keyring. If the keyring does not have a VRF, an empty string is printed.

show crypto isakmp peers

To display the Internet Security Association and Key Management Protocol (ISAKMP) peer descriptions, use the **show crypto isakmp peers**command in privileged EXEC mode.

show crypto isakmp peers [{*ipaddressipv6address* | **config** [*peername*]}]

Syntax Description

ipaddress	(Optional) The IP address of the specific peer. **Note** If the optional *ipaddress* argument is not included with the command, a summarization of all peers is displayed.
ipv6address	(Optional) The IPv6 address of the specific peer.
config	(Optional) Displays detailed information about all peers or a specific peer.
peername	(Optional) The peer name.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.4(4)T	The **config** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.(33)SRA.
12.4(11)T	The **show crypto isakmp peer**command name was changed to **show crypto isakmp peers**.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1 on the Cisco ASR 1000 Series Routers.

Usage Guidelines

Before you can use the **config** keyword, the following commands must be enabled for the accounting update to work correctly: **aaa accounting update**with **new info** keyword and **radius-server vsa send** with **accounting** keyword.

Examples

The following output example shows information about the peer named "This-is-another-peer-at-10-1-1-3":

```
Router# show crypto isakmp peers
Peer: 10.1.1.3 Port: 500
 Description: This-is-another-peer-at-10-1-1-3
 Phase1 id: 10.1.1.3
```

In the following example, the **config** keyword is used to display all manageability information for an Easy VPN remote device. Cisco Easy VPN is an IP Security (IPsec) virtual private network (VPN) solution supported by Cisco routers and security appliances. It greatly simplifies VPN deployment for remote offices and mobile workers. The fields are self-explanatory.

```
Router# show crypto isakmp peers config
Client-Public-Addr=192.168.10.2:500; Client-Assigned-Addr=172.16.1.209; Client-Group=branch;
 Client-User=branch; Client-Hostname=branch.; Client-Platform=Cisco 1711;
Client-Serial=FOC080210E2 (412454448); Client-Config-Version=11; Client-Flash=33292284;
Client-Available-Flash=10202680; Client-Memory=95969280; Client-Free-Memory=14992140;
Client-Image=flash:c1700-advipservicesk9-mz.ef90241;
Client-Public-Addr=192.168.10.3:500; Client-Assigned-Addr=172.16.1.121; Client-Group=store;
 Client-User=store; Client-Hostname=831-storerouter.; Client-Platform=Cisco C831;
Client-Serial=FOC08472UXR (1908379618); Client-Config-Version=2; Client-Flash=24903676;
Client-Available-Flash=5875028; Client-Memory=45298688; Client-Free-Memory=6295596;
Client-Image=flash:c831-k9o3y6-mz.ef90241
```

Related Commands

Command	Description
aaa accounting update	Enables the periodic interim accounting records to be sent to the accounting server.
radius-server vsa send	Configures the network access server (NAS) to recognize and use vendor-specific attributes (VSAs).
clear crypto session	Deletes crypto sessions (IPSec and IKE) SAs.
show crypto session	Displays status information for active crypto sessions in a router.

show crypto isakmp policy

To display the parameters for each Internet Key Exchange (IKE) policy, use the **show crypto isakmp policy** command in privileged EXEC mode.

show crypto isakmp policy

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.3T	This command was introduced.
12.2(13)T	The command output was expanded to include a warning message for users who try to configure an IKE encryption method that the hardware does not support.
12.4(4)T	Support for IPv6 was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	The command output was expanded to include default IKE policies.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 series routers.

Usage Guidelines

There are eight default IKE default policies supported with protection suites of priorities 65507-65514, where 65507 is the highest priority and 65514 is the lowest priority. If you have neither manually configured IKE policies with the **crypto isakmp policy** command nor disabled the default IKE policies by issuing the **no crypto isakmp default policy** command, the default IKE policies will be displayed when the **show crypto isakmp policy** command is issued.

Examples

The following is sample output from the **show crypto isakmp policy** command, after two IKE policies have been configured (with priorities 15 and 20, respectively):

```
Router# show crypto isakmp policy
Protection suite priority 15
        encryption algorithm:    DES - Data Encryption Standard (56 bit keys)
        hash algorithm:  Message Digest 5
        authentication method:   Rivest-Shamir-Adleman Signature
        Diffie-Hellman Group:    #2 (1024 bit)
        lifetime:      5000 seconds, no volume limit
Protection suite priority 20
        encryption algorithm:    DES - Data Encryption Standard (56 bit keys)
        hash algorithm: Secure Hash Standard
        authentication method:   preshared Key
        Diffie-Hellman Group:    #1 (768 bit)
```

```
        lifetime:      10000 seconds, no volume limit
Default protection suite
        encryption algorithm:    DES - Data Encryption Standard (56 bit keys)
        hash algorithm: Secure Hash Standard
        authentication method:   Rivest-Shamir-Adleman Signature
        Diffie-Hellman Group:    #1 (768 bit)
        lifetime:      86400 seconds, no volume limit
```

Note Although the output shows "no volume limit" for the lifetimes, you can currently configure only a time lifetime (such as 86,400 seconds); volume limit lifetimes are not used.

The following sample output from the **show crypto isakmp policy** command displays a warning message after a user tries to configure an IKE encryption method that the hardware does not support:

```
Router# show crypto isakmp policy
Protection suite of priority 1
        encryption algorithm:  AES - Advanced Encryption Standard (256 bit keys).
WARNING:encryption hardware does not support the configured
encryption method for ISAKMP policy 1
        hash algorithm:        Secure Hash Standard
        authentication method: Pre-Shared Key
        Diffie-Hellman group:  #1 (768 bit)
        lifetime:              3600 seconds, no volume limit
```

The following sample output from the **show crypto isakmp policy** command displays the default IKE policies. The manually configured IKE policies with priorities 10 and 20 have been removed.

```
Router(config)# no crypto isakmp policy 10
Router(config)# no crypto isakmp policy 20
Router(config)# exit
R1# show crypto isakmp policy
Default IKE policy
Protection suite of priority 65507
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit key.
        hash algorithm:         Secure Hash Standard
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               86400 seconds, no volume limit
Protection suite of priority 65508
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit key.
        hash algorithm:         Secure Hash Standard
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               86400 seconds, no volume limit
Protection suite of priority 65509
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit key.
        hash algorithm:         Message Digest 5
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               86400 seconds, no volume limit
Protection suite of priority 65510
        encryption algorithm:   AES - Advanced Encryption Standard (128 bit key.
        hash algorithm:         Message Digest 5
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #5 (1536 bit)
        lifetime:               86400 seconds, no volume limit
Protection suite of priority 65511
        encryption algorithm:   Three key triple DES
        hash algorithm:         Secure Hash Standard
```

```
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
Protection suite of priority 65512
        encryption algorithm:   Three key triple DES
        hash algorithm:         Secure Hash Standard
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
Protection suite of priority 65513
        encryption algorithm:   Three key triple DES
        hash algorithm:         Message Digest 5
        authentication method:  Rivest-Shamir-Adleman Signature
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
Protection suite of priority 65514
        encryption algorithm:   Three key triple DES
        hash algorithm:         Message Digest 5
        authentication method:  Pre-Shared Key
        Diffie-Hellman group:   #2 (1024 bit)
        lifetime:               86400 seconds, no volume limit
```

The field descriptions in the display are self-explanatory.

Related Commands

Command	Description
authentication (IKE policy)	Specifies the authentication method within an IKE policy.
crypto isakmp policy	Defines an IKE policy.
encryption (IKE policy)	Specifies the encryption algorithm within an IKE policy.
group (IKE policy)	Specifies the DH group identifier within an IKE policy.
hash (IKE policy)	Specifies the hash algorithm within an IKE policy.
lifetime (IKE policy)	Specifies the lifetime of an IKE SA.
show crypto isakmp default policy	Displays the default IKE policies.

show crypto isakmp profile

To list all the Internet Security Association and Key Management Protocol (ISAKMP) profiles that are defined on a router, use the **show crypto isakmp profile**command in privileged EXEC mode.

show crypto isakmp profile [{**tag** *profilename* | **vrf** *vrfname*}]

Syntax Description

tag *profilename*	(Optional) Displays ISAKMP profile details specified by the profile name.
vrf *vrfname*	(Optional) Displays ISAKMP profile details specified by the VPN routing/forwarding instance (VRF) name.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.4(4)T	IPv6 support was added.
12.4(11)T	The tag *profilename*and vrf *vrfname*keywords and arguments were added.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Examples

The following is sample output from the **show crypto isakmp profile** command:

```
Router# show crypto isakmp profile
ISAKMP PROFILE vpn1-ra
   Identities matched are:
group vpn1-ra
   Identity presented is: ip-address
```

The following sample output shows information for an IPv6 router:

```
Router# show crypto isakmp profile
ISAKMP PROFILE tom
Identities matched are:
ipv6-address 2001:0DB8:0:1::1/32
Certificate maps matched are:
Identity presented is: ipv6-address fqdn
keyring(s): <none>
trustpoint(s): <all>
```

The table below describes the significant fields shown in the display.

Table 49: show crypto isakmp profile Field Descriptions

Field	Description
ISAKMP PROFILE	Name of the ISAKMP profile.

Field	Description
Identities matched are:	Lists all identities that the ISAKMP profile will match.
Identity presented is:	The identity that the ISAKMP profile will present to the remote endpoint.

The following configuration was in effect when the preceding s**how crypto isakmp profile**command was issued:

```
crypto isakmp profile vpn1-ra
 vrf vpn1
 self-identity address
 match identity group vpn1-ra
 client authentication list aaa-list
 isakmp authorization list aaa
 client configuration address initiate
 client configuration address respond
```

Related Commands

Command	Description
show crypto isakmp key	Lists the keyrings and their preshared keys.

show crypto isakmp sa

To display current Internet Key Exchange (IKE) security associations (SAs), use the **show crypto isakmp sa** command in privileged EXEC mode.

show crypto isakmp sa [{**active** | **standby** | **detail** | **nat**}] [**vrf** *vrfname*]

Syntax Description

active	(Optional) Displays high availability- (HA-) enabled Internet Security Association and Key Management Protocol (ISAKMP) SAs that are in the active state.
standby	(Optional) Displays HA-enabled ISAKMP SAs that are in the standby state.
detail	(Optional) Displays all existing IKE SAs, whether in an active or standby state.
nat	(Optional) Displays IKE SAs that have undergone network address translation (NAT).
vrf *vrfname*	(Optional) Displays IKE SA details about the specified VRF. • The *vrfname*value is the name of the VRF.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.3 T	This command was introduced.
12.3(11)T	The **active** and **standby** keywords were added.
12.4(4)T	IPv6 information was added to the command output. The **detail and nat**keywords were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.(33)SRA.
12.4(11)T	The vrf *vrfname* keyword and argument were added.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.4(2)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

Usage Guidelines

If neither the **active** keyword nor the **standby** keyword is specified, current SAs for all configured routers will be shown. Use the **nat** keyword to display the IP address and port address of a remote peer when NAT is used.

Examples

The following sample output shows the SAs of both the active and standby devices:

```
Router# show crypto isakmp sa
dst             src             state          conn-id slot status
10.165.201.3   10.165.200.225 QM_IDLE              2    0 STDBY
10.0.0.1        10.0.0.2        QM_IDLE             1    0 ACTIVE
```

The following sample output shows the SAs of only the active device:

```
Router# show crypto isakmp sa active
dst             src             state          conn-id slot status
10.165.201.3   10.165.200.225 QM_IDLE              5    0 ACTIVE
```

The following sample output shows the SAs of only the standby device:

```
Router# show crypto isakmp sa standby
dst             src             state          conn-id slot status
10.165.201.3   10.165.200.225 QM_IDLE              5    0 STDBY
10.165.201.3   10.165.200.225 QM_IDLE              1    0 STDBY
```

The following sample output shows the SAs of an active IPv6 device. The IPv4 device is inactive.

```
Router# show crypto isakmp sa detail
Codes: C - IKE configuration mode, D - Dead Peer Detection
       K - Keepalives, N - NAT-traversal
       X - IKE Extended Authentication
       psk - Preshared key, rsig - RSA signature
       renc - RSA encryption
IPv4 Crypto ISAKMP SA
C-id  Local           Remote          I-VRF    Status Encr Hash Auth DH
Lifetime Cap.
IPv6 Crypto ISAKMP SA
  dst: 3FFE:2002::A8BB:CCFF:FE01:2C02
  src: 3FFE:2002::A8BB:CCFF:FE01:9002
  conn-id: 1001  I-VRF:          Status: ACTIVE Encr: des  Hash: sha  Auth:
psk
  DH: 1  Lifetime: 23:45:00 Cap: D    Engine-id:Conn-id = SW:1
  dst: 3FFE:2002::A8BB:CCFF:FE01:2C02
  src: 3FFE:2002::A8BB:CCFF:FE01:9002
  conn-id: 1002  I-VRF:          Status: ACTIVE Encr: des  Hash: sha  Auth:
psk
  DH: 1  Lifetime: 23:45:01 Cap: D    Engine-id:Conn-id = SW:2
```

The first three tables below show the various states that may be displayed in the output of the **show crypto isakmp sa** command. When an Internet Security Association and Key Management Protocol (ISAKMP) SA exists, it will most likely be in its quiescent state (QM_IDLE). For long exchanges, some of the main mode (MM_xxx) states may be observed.

Table 50: States in Main Mode Exchange

State	Explanation
MM_NO_STATE	The ISAKMP SA has been created, but nothing else has happened yet. It is "larval" at this stage--there is no state.
MM_SA_SETUP	The peers have agreed on parameters for the ISAKMP SA.
MM_KEY_EXCH	The peers have exchanged Diffie-Hellman public keys and have generated a shared secret. The ISAKMP SA remains unauthenticated.
MM_KEY_AUTH	The ISAKMP SA has been authenticated. If the router initiated this exchange, this state transitions immediately to QM_IDLE, and a Quick Mode exchange begins.

Table 51: States in Aggressive Mode Exchange

State	Explanation
AG_NO_STATE	The ISAKMP SA has been created, but nothing else has happened yet. It is "larval" at this stage--there is no state.
AG_INIT_EXCH	The peers have done the first exchange in aggressive mode, but the SA is not authenticated.
AG_AUTH	The ISAKMP SA has been authenticated. If the router initiated this exchange, this state transitions immediately to QM_IDLE, and a quick mode exchange begins.

Table 52: States in Quick Mode Exchange

State	Explanation
QM_IDLE	The ISAKMP SA is idle. It remains authenticated with its peer and may be used for subsequent quick mode exchanges. It is in a quiescent state.

Table 53: show crypto isakmp sa Field Descriptions

Field	Description
f_vrf/i_vrf (not shown)	The front door virtual routing and forwarding (FVRF) and the inside VRF (IVRF) of the IKE SA. If the FVRF is global, the output shows f_vrf as an empty field.

Related Commands

Command	Description
crypto isakmp policy	Defines an IKE policy.
lifetime (IKE policy)	Specifies the lifetime of an IKE SA.

show crypto key mypubkey rsa

To display the RSA public keys of your router, use the **show crypto key mypubkey rsa**command in privileged EXEC mode.

show crypto key mypubkey rsa [*keyname*] [*key size*]

Syntax Description

keyname	The name of a generated key pair.
key size	The key size of the key pair.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3T	This command was introduced.
12.3(7)T	The show output was modified to display whether an RSA key is protected (encrypted) and locked or unlocked.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.(33)SRA.
12.4T	The key size variable was introduced.
15.0(1)M	This command was modified to display whether redundancy is specified in the **crypto key generate rsa**command.
15.2(2)SA2	This command was implemented on the Cisco ME 2600X Series Ethernet Access Switches.

Usage Guidelines

This command displays the RSA public keys of your router.

Note Secure Shell (SSH) may generate an additional RSA keypair if you generate a key pair on a router having no RSA keys. The additional key pair is used only by SSH and will have a name such as {*router.FQDN* }.server. For example, if the name of your router is "router1.cisco.com," the key name would be "router1.cisco.com.server."

Examples

The following is a sample output of the **show crypto key mypubkey rsa** command. Special usage RSA keys were previously generated for this router using the **crypto key generate rsa** command.

```
% Key pair was generated at: 06:07:49 UTC Jan 13 1996
Key name: myrouter.example.com
Key type: RSA KEYS 2048 bits
 Usage: Signature Key
 Key Data:
  005C300D 06092A86 4886F70D 01010105 00034B00 30480241 00C5E23B 55D6AB22
  04AEF1BA A54028A6 9ACC01C5 129D99E4 64CAB820 847EDAD9 DF0B4E4C 73A05DD2
  BD62A8A9 FA603DD2 E2A8A6F8 98F76E28 D58AD221 B583D7A4 71020301 0001
```

```
% Key pair was generated at: 06:07:50 UTC Jan 13 1996
Key name: myrouter.example.com
 Usage: Encryption Key
 Key Data:
  00302017 4A7D385B 1234EF29 335FC973 2DD50A37 C4F4B0FD 9DADE748 429618D5
  18242BA3 2EDFBDD3 4296142A DDF7D3D8 08407685 2F2190A0 0B43F1BD 9A8A26DB
  07953829 791FCDE9 A98420F0 6A82045B 90288A26 DBC64468 7789F76E EE21
```

The following example shows how to encrypt the RSA key "pki1-72a.cisco.com." Thereafter, the **show crypto key mypubkey rsa** command is issued to verify that the RSA key is encrypted (protected) and unlocked.

```
Router(config)# crypto key encrypt rsa name pki1-72a.cisco.com passphrase cisco1234
Router(config)# exit
Router# show crypto key mypubkey rsa
```

% Key pair was generated at:00:15:32 GMT Jun 25 2003

Key name:pki1-72a.cisco.com

Usage:General Purpose Key

*** The key is protected and UNLOCKED. ***

Key is not exportable.

Key Data:

305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00E0CC9A 1D23B52C

CD00910C ABD392AE BA6D0E3F FC47A0EF 8AFEE340 0EC1E62B D40E7DCC

23C4D09E

03018B98 E0C07B42 3CFD1A32 2A3A13C0 1FF919C5 8DE9565F 1F020301 0001

% Key pair was generated at:00:15:33 GMT Jun 25 2003

Key name:pki1-72a.cisco.com.server

Usage:Encryption Key

Key is exportable.

Key Data:

307C300D 06092A86 4886F70D 01010105 00036B00 30680261 00D3491E 2A21D383

854D7DA8 58AFBDAC 4E11A7DD E6C40AC6 66473A9F 0C845120 7C0C6EC8 1FFF5757

3A41CE04 FDCB40A4 B9C68B4F BC7D624B 470339A3 DE739D3E F7DDB549 91CD4DA4

DF190D26 7033958C 8A61787B D40D28B8 29BCD0ED 4E6275C0 6D020301 0001

The following example shows how to lock the key "TP-self-signed-2521856816." Thereafter, the **show crypto key mypubkey rsa** command is issued to verify that the key is protected (encrypted) and locked.

```
Router# crypto key lock rsa name TP-self-signed-2521856816
!
Router# show crypto key mypubkey rsa
% Key pair was generated at: 23:32:48 UTC Feb 16 2021
Key name: TP-self-signed-2521856816
Key type: RSA KEYS 2048 bits
```

```
*** The key is protected and LOCKED. ***
Key is exportable.
Key Data:
305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00D7808D C5FF14AC
0D2B55AC 5D199F2F 7CB4B355 C555E07B 6D0DECBE 4519B1F0 75B12D6F 902D6E9F
B6FDAD8D 654EF851 5701D5D7 EDA047ED 9A2A619D 5639DF18 EB020301 0001
The string "Redundancy enabled" in the following example indicates that the redundancy
keyword was specified when the key pair "MYKEYS" was generated by the crypto key generate
rsa
command.
Router# show crypto key mypubkey rsa MYKEYS
% Key pair was generated at: 23:32:48 UTC Feb 16 2021
Key name: MYKEYS
 Storage Device: not specified
 Usage: General Purpose Key
 Key is not exportable. Redundancy enabled.
 Key Data:
  305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00A63726 28C9EE7D
  A89AF6E1 5B42A854 A76EDF9F 35681024 A7868113 B93E2384 EF15CD78 8467A797
  F946268F 067FF15E A1734BE6 3E3444C2 BAE00618 BCAED5A3 BB020301 0001
```

Related Commands

Command	Description
crypto key encrypt rsa	Encrypts the RSA private key.
crypto key generate rsa	Generates RSA key pairs.
crypto key lock rsa	Locks the RSA private key in a router.

show crypto key pubkey-chain rsa

To display the RSA public keys of the peer that are stored on the router, use the **show crypto key pubkey-chain rsa** command in user EXEC mode or p rivileged EXEC mode.

show crypto key pubkey-chain rsa [{**address** *key-address* | **name** *key-name* | **vrf** *vrf-name* [**address** *ip-address*]}]

Syntax Description

address *key-address*	(Optional) Address of a specific key to view.
name *key-name*	(Optional) Name of a specific key to view.
vrf *vrf-name*	(Optional) Name of a specific Virtual Private Network (VPN) Routing and Forwarding (VRF) instance for which to display keys.
address *ip-address*	(Optional) IP address belonging to a VRF instance.

Command Default

Information is displayed for all RSA public keys stored on the router.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
11.3T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

The keys that are displayed include peers' RSA public keys that are manually configured at the router and keys that are received by the router via other means (such as by a certificate, if certification authority support is configured).

If a router reboots, any keys derived by certificates are lost. This is because the router requests certificates again (then the keys are derived again).

Examples

The following example shows how to display information for all RSA public keys stored on the router:

```
Router# show crypto key pubkey-chain rsa
Codes: M - Manually Configured, C - Extracted from certificate
Code Usage         IP-address            Keyring          Name
M    Signature     209.165.200.225       default          myrouter.example.com
M    Encryption    209.165.202.129       default          myrouter.example.com
```

```
C     Signature    209.165.200.225        default          routerA.example.com
C     Encryption   209.165.202.129        default          routerA.example.com
C     General      209.165.200.225        default          routerB.domain1.com
```

The example above shows manually configured special usage RSA public keys for the peer myrouter.example.com. This sample also indicates certificate support and therefore shows three keys obtained from peers' certificates: special usage keys for peer routerA.example.com and a general purpose key for peer routerB.domain1.com.

The following example shows how to display keys for a specific VRF instance.

Router# **show crypto key pubkey-chain rsa vrf**

```
Code Usage         IP-Address/VRF         Keyring          Name
M    General       209.165.200.225        default          Key_1
M    General       209.165.202.129        default          Key_2
```

The following example shows how to display details for a key named somerouter.example.com:

```
Router# show crypto key
pubkey-chain
 rsa
 name

somerouter.example.com

Key name: somerouter.example.com
Key address: 209.165.200.225
 Usage: Signature Key
 Source: Manual
 Data:
  305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00C5E23B 55D6AB22
  04AEF1BA A54028A6 9ACC01C5 129D99E4 64CAB820 847EDAD9 DF0B4E4C 73A05DD2
  BD62A8A9 FA603DD2 E2A8A6F8 98F76E28 D58AD221 B583D7A4 71020301 0001
Key name: somerouter.example.com
Key address: 209.165.200.225
 Usage: Encryption Key
 Source: Manual
 Data:
  00302017 4A7D385B 1234EF29 335FC973 2DD50A37 C4F4B0FD 9DADE748 429618D5
  18242BA3 2EDFBDD3 4296142A DDF7D3D8 08407685 2F2190A0 0B43F1BD 9A8A26DB
  07953829 791FCDE9 A98420F0 6A82045B 90288A26 DBC64468 7789F76E EE21
```

Note The Source field in the above example displays "Manual," which means that the keys were manually configured on the router (and not received in the peer's certificate).

The following example shows how to display details for a key with address 209.165.202.129:

```
Router# show crypto key pubkey-chain rsa
address 209.165.202.129
Key name: routerB.example.com
Key address: 209.165.202.129
 Usage: General Purpose Key
 Source: Certificate
 Data:
  0738BC7A 2BC3E9F0 679B00FE 53987BCC 01030201 42DD06AF E228D24C 458AD228
  58BB5DDD F4836401 2A2D7163 219F882E 64CE69D4 B583748A 241BED0F 6E7F2F16
  0DE0986E DF02031F 4B0B0912 F68200C4 C625C389 0BFF3321 A2598935 C1B1
```

Note The Source field in the above example displays "Certificate," which means that the keys were received by the router from the certificate authority.

The table below describes the significant fields shown in the displays.

Table 54: show crypto key pubkey-chain rsa Field Descriptions

Field	Description
Code	Source of the key: M (manually configured at the router) or C (received by the router via a certificate).
Usage	Purpose of the key: general purpose, signature, or encryption).
IP-Address/VRF	IP address or VRF of the key.
Keyring	Name of the keyring that stores the key. The possible values are either the name of a user-defined keyring or default (the default keyring).
Name	Name of the key. For manually inserted keys (code M), this name is manually configured. For keys that are extracted from the certificate (code C) the name is the subject name in the certificate itself.
Data	The contents of the key itself.

Related Commands

Command	Description
crypto key pubkey-chain rsa	Enters public key configuration mode (so you can manually specify other devices' RSA public keys).
rsa-pubkey	Defines the RSA manual key to be used for encryption or signature during IKE authentication.

show crypto map (IPsec)

To display the crypto map configuration, use the **show crypto map** command in user EXEC or privileged EXEC mode.

show crypto map [{**gdoi fail-close** *map-name* | **interface** *interface* | **tag** *map-name*}]

Syntax Description

gdoi	(Optional) Displays information about the status of the Group Domain of Interpretation (GDOI) fail-close mode.
fail-close	Specifies the list of crypto maps configured with the fail-close mode.
map-name	Name of the specified crypto map.
interface *interface*	(Optional) Displays only the crypto map set that is applied to the specified interface.
tag	(Optional) Displays only the crypto map set that is specified.

Command Default

No crypto maps are displayed.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
11.2	This command was introduced.
12.3(8)T	This command was integrated into Cisco IOS Release 12.3(8)T. The output was modified to display the crypto input and output Access Control Lists (ACLs) that have been configured.
12.4(4)T	This command was integrated into Cisco IOS Release 12.4(4)T. IPv6 address information was added to command output.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.(33)SRA.
12.2SX	This command was integrated into Cisco IOS Release 12.2SX. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T. The default transform set information was added to command output.
12.4(22)T	This command was integrated into Cisco IOS Release 12.4(22)T. The **gdoi fail-close** keywords and the *map-tag*arguments were added.
Cisco IOS XE Release 2.3	This command was modified. It was integrated into Cisco IOS XE Release 2.3.

Usage Guidelines

The **show crypto map** command allows you to specify a particular crypto map. The crypto maps shown in the command output are dynamically generated; you need not configure crypto maps in order for them to appear in this command output.

Two default transform sets are supported in Cisco IOS K9 images only:

- Esp-aes esp-sha-hmac
- Esp-3des esp-sha-hmac

The **show crypto map** command displays the default transform sets if no other transform sets are configured for the crypto map, if you have not disabled the default transform sets by issuing the **no crypto ipsec default transform-set** command, and if the crypto engine supports the encryption algorithm.

Examples

The following example shows that crypto input and output ACLs have been configured:

```
Router# show crypto map
Crypto Map "test" 10 ipsec-isakmp
 Peer
 Extended IP access list ipsec_acl
  access-list ipsec_acl permit ip 192.168.2.0 0.0.0.255 192.168.102.0 0.0.0.255
 Extended IP access check IN list 110
  access-list 110 permit ip host 192.168.102.47 192.168.2.0 10.0.0.15
  access-list 110 permit ip host 192.168.102.47 192.168.2.32 10.0.0.15
  access-list 110 permit ip host 192.168.102.47 192.168.2.64 10.0.0.15
  access-list 110 permit ip host 192.168.102.57 192.168.2.0 10.0.0.15
  access-list 110 permit ip host 192.168.102.57 192.168.2.32 10.0.0.15
  access-list 110 permit ip host 192.168.102.57 192.168.2.64 10.0.0.15
 Extended IP access check OUT list 120
  access-list 120 permit ip 192.168.2.0 10.0.0.15 host 192.168.102.47
  access-list 120 permit ip 192.168.2.32 10.0.0.15 host 192.168.102.47
  access-list 120 permit ip 192.168.2.64 10.0.0.15 host 192.168.102.47
  access-list 120 permit ip 192.168.2.0 10.0.0.15 host 192.168.102.57
  access-list 120 permit ip 192.168.2.32 10.0.0.15 host 192.168.102.57
  access-list 120 permit ip 192.168.2.64 10.0.0.15 host 192.168.102.57
 Current peer: 10.0.0.2
 Security association lifetime: 4608000 kilobytes/3600 seconds
 PFS (Y/N): N
 Transform sets=test
 Interfaces using crypto map test:
  Serial0/1
```

The table below describes the significant fields shown in the display.

Table 55: show crypto map Field Descriptions

Field	Description
Peer	Possible peers that are configured for this crypto map entry.
Extended IP access list	Access list that is used to define the data packets that need to be encrypted. Packets that are denied by this access list are forwarded but not encrypted. The "reverse" of this access list is used to check the inbound return packets, which are also encrypted. Packets that are denied by the "reverse" access list are dropped because they should have been encrypted but were not.

Field	Description
Extended IP access check	Access lists that are used to more finely control which data packets are allowed into or out of the IPsec tunnel. Packets that are allowed by the "Extended IP access list" ACL but denied by the "Extended IP access list check" ACL are dropped.
Current peer	Current peer that is being used for this crypto map entry.
Security association lifetime	Number of bytes that are allowed to be encrypted or decrypted or the age of the security association before new encryption keys must be negotiated.
PFS	(Perfect Forward Secrecy) If the field is marked as 'Yes', the Internet Security Association and Key Management Protocol (ISAKMP) SKEYID-d key is renegotiated each time security association (SA) encryption keys are renegotiated (requires another Diffie-Hillman calculation). If the field is marked as 'No', the same ISAKMP SKEYID-d key is used when renegotiating SA encryption keys. ISAKMP keys are renegotiated on a separate schedule, with a default time of 24 hours.
Transform sets	List of transform sets (encryption, authentication, and compression algorithms) that can be used with this crypto map.
Interfaces using crypto map test	Interfaces to which this crypto map is applied. Packets that are leaving from this interface are subject to the rules of this crypto map for encryption. Encrypted packets may enter the router on any interface, and they are decrypted. Nonencrypted packets that are entering the router through this interface are subject to the "reverse" crypto access list check.

The following example displays output from the **show crypto map** command. No transform sets are configured for the crypto map "mymap," the default transform sets are enabled, and the crypto engine supports the encryption algorithm.

```
Router# show crypto map

Crypto Map "mymap" 1 ipsec-isakmp
        Peer = 209.165.201.1
        Extended IP access list 102
            access-list 102 permit ip 192.168.1.0 0.0.0.255 10.0.0.0 0.0.255.255
        Security association lifetime: 4608000 kilobytes/3600 seconds
        PFS (Y/N): N
        Transform sets={
                #$!default_transform_set_1:  { esp-aes esp-sha-hmac  } ,
                #$!default_transform_set_0:  { esp-3des esp-sha-hmac  } ,
        }
        Reverse Route Injection Enabled
        Interfaces using crypto map mymap:
```

The following example displays output of the **show crypto map** command. No transform sets configured for the crypto map "mymap" and the default transform sets have been disabled.

```
Router(config)# no crypto ipsec default transform-set
Router(config)# exit
Router# configure terminal
Router# show crypto map

Crypto Map "mymap" 1 ipsec-isakmp
```

```
        Peer = 209.165.201.1
        Extended IP access list 102
            access-list 102 permit ip 192.168.1.0 0.0.0.255 10.0.0.0 0.0.255.255
        Security association lifetime: 4608000 kilobytes/3600 seconds
        PFS (Y/N): N
        Transform sets={
        }
! There are no transform sets for the crypto map "mymap."
        Reverse Route Injection Enabled
        Interfaces using crypto map mymap:
```

The following example displays output for the **show crypto map** command and **gdoi fail-close** keywords (**show crypto map gdoi fail-close**). Fail-close has been activated. In addition, an implicit "permit ip any any" entry is configured, causing any traffic other than Telnet and Open Shortest Path First (OSPF) to be dropped:

```
Router# show crypto map gdoi fail-close 23

Crypto Map: "svn"
        Activate: yes
        Fail-Close Access-List: (Deny = Forward In Clear, Permit = Drop)
            access-list 105 deny tcp any port = 23 any
            access-list 105 deny ospf any any
```

Related Commands

Command	Description
show crypto ipsec default transform-set	Displays the default IPsec transform sets.
show crypto ipsec transform-set	Displays the configured transform sets.

show crypto mib ipsec flowmib endpoint

To display the IP Security (IPsec) phase-2 tunnel endpoint table, use the **show crypto mib ipsec flowmib endpoint** command in privileged EXEC mode.

show crypto mib ipsec flowmib endpoint [**vrf** *vrf-name*]

Syntax Description

vrf *vrf-name*	(Optional) Displays the parameters for the specified Virtual Private Network (VPN) routing and forwarding (VRF) instance.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 series routers.

Usage Guidelines

The IPsec phase-2 tunnel endpoint table contains an entry for each active endpoint associated with an IPsec phase-2 tunnel.

Examples

The following example displays the IPsec phase 2 tunnel endpoint table for all VRFs:

```
Router# show crypto mib ipsec flowmib endpoint
vrf Global
  Index:               1
  Local type:          Single IP address
  Local address:       192.1.2.1
  Protocol:            0
  Local port:          0
  Remote type:         Single IP address
  Remote address:      192.1.2.2
  Remote port:         0
  Index:               2
  Local type:          Subnet
  Local address:       192.1.3.0 255.255.255.0
  Protocol:            0
  Local port:          0
  Remote type:         Subnet
  Remote address:      192.1.3.0 255.255.255.0
  Remote port:         0
```

The table below describes the significant fields shown in the display.

Table 56: show crypto mib ipsec flowmib endpoint Field Descriptions

Field	Description
Index	The number of the endpoint associated with the IPsec phase-2 tunnel table. The value of this index is a number which begins at one and is incremented with each endpoint associated with an IPsec phase-2 tunnel. The index value will wrap at 2,147,483,647.

Field	Description
Local type	The local endpoint identity type. The three possible values are a single IP address, an IP address range, or an IP subnet.
Local address	The first IP address of the local endpoint. If the local endpoint type is a single IP address, then the local address is the value of the IP address. If the local endpoint type is an IP address range, then the local address is the value of beginning IP address of the range. If the local endpoint type is an IP subnet, then the local address is the value of the subnet.
Protocol	The local endpoint traffic protocol number.
Local port	The local endpoint traffic port number.
Remote type	The remote endpoint identity type. The three possible values are a single IP address, an IP address range, or an IP subnet.
Remote address	The first IP address of the remote endpoint. If the remote endpoint type is a single IP address, then the remote address is the value of the IP address. If the remote endpoint type is an IP address range, then the remote address is the value of beginning IP address of the range. If the remote endpoint type is an IP subnet, then the remote address is the value of the subnet.
Remote port	The remote endpoint traffic port number.

Related Commands

Command	Description
show crypto mib ipsec flowmib failure	Displays statistics associated with IPsec phase-2 failure.
show crypto mib ipsec flowmib global	Displays IPsec phase-2 global statistics.
show crypto mib ipsec flowmib history	Displays statistics associated with previously active IPsec phase-2 tunnels.
show crypto mib ipsec flowmib spi	Displays the IPsec phase-2 security protection index (SPI) table.
show crypto mib ipsec flowmib tunnel	Displays statistics for all active IPsec phase-2 tunnels.

show crypto mib ipsec flowmib failure

To display statistics associated with IP Security (IPsec) phase-2 failure, use the **show crypto mib ipsec flowmib failure**command in privileged EXEC mode.

show crypto mib ipsec flowmib failure [**vrf** *vrf-name*]

Syntax Description

vrf *vrf-name*	(Optional) Displays the parameters for the specified Virtual Private Network (VPN) routing and forwarding (VRF) instance.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 series routers.

Examples

The following example displays the IPsec phase 2 MIB failure table for all indexes and VRFs:

```
Router# show crypto mib ipsec flowmib failure
vrf Global
  Index:                        1
  Reason:                       Operation request
  Failure time since reset:     00:25:18
  Src address:                  192.1.2.1
  Destination address:          192.1.2.2
  SPI:                          0
```

The table below describes the significant fields shown in the display.

Table 57: show crypto mib ipsec flowmib failure Field Descriptions

Field	Description
Index	The IPsec phase-2 failure table index. The value of the index is a number that begins at one and is incremented with each IPsec phase-1 failure. The index value will wrap at 2,147,483,647.

Field	Description
Reason	The reason for the failure, which are: • 1--All other reasons. • 2--An internal error occurred. • 3--A peer encoding error occurred. • 4--A proposal failure occurred. • 5--A protocol use failure occurred. • 6--The SA did not exist. • 7--A decryption failure occurred. • 8--An encryption failure occurred. • 9--An inbound authentication failure occurred. • 10--An outbound authentication failure occurred. • 11--A compression failure occurred. • 12--A system capacity failure occurred. • 13--A peer delete request was received. • 14--The contact with the peer was lost. • 15--The sequence rolled over. • 16--The operator requested tunnel termination.
Failure time since reset	The value of sysUpTime in hundredths of seconds at the time of the failure

Related Commands

Command	Description
show crypto mib ipsec flowmib endpoint	Displays IPsec phase-2 tunnel endpoint table.
show crypto mib ipsec flowmib global	Displays IPsec phase-2 global statistics.
show crypto mib ipsec flowmib history	Displays statistics associated with previously active IPsec phase-2 tunnels.
show crypto mib ipsec flowmib spi	Displays the IPsec phase-2 SPI table.
show crypto mib ipsec flowmib tunnel	Displays statistics for all active IPsec phase-2 tunnels.

show crypto mib ipsec flowmib global

To display IP Security (IPsec) phase-2 global statistics, use the **show crypto mib ipsec flowmib global**command in privileged EXEC mode.

show crypto mib ipsec flowmib global [**vrf** *vrf-name*]

Syntax Description

vrf *vrf-name*	(Optional) Displays the parameters for the specified Virtual Private Network (VPN) routing and forwarding (VRF) instance.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 series routers.

Examples

The following example displays IPsec phase 2 global statistics for all VRFs:

```
Router# show crypto mib ipsec flowmib global
 vrf Global
  Active Tunnels:                     2
  Previous Tunnels:                   0
  In octets:                          800
  Out octets:                         1408
  In packets:                         8
  Out packets:                        8
  Uncompressed encrypted bytes:       1408
  In packets drops:                   0
  Out packets drops:                  2
  In replay drops:                    0
  In authentications:                 8
  Out authentications:                8
  In decrypts:                        8
  Out encrypts:                       8
  Compressed bytes:                   0
  Uncompressed bytes:                 0
  In uncompressed bytes:              0
  Out uncompressed bytes:             0
  In decrypt failures:                0
  Out encrypt failures:               0
  No SA failures:                     0
  Protocol use failures:              0
  System capacity failures:           0
  In authentication failures:            0
  Out authentication failures:           0
```

The table below describes the significant fields shown in the display.

Table 58: show crypto mib ipsec flowmib global Field Descriptions

Field	Description
Active Tunnels	The total number of currently active IPsec phase-2 tunnels.
Previous Tunnels	The total number of previously active IPsec phase-2 tunnels.
In octets	The total number of octets received by all current and previous IPsec phase-2 tunnels. The total number is accumulated before determining whether or not the packet should be decompressed.
Out octets	The total number of octets sent by all current and previous IPsec phase-2 Tunnels. The total number is accumulated after determining whether or not the packet should be compressed.
In packets drops	The total number of packets dropped during receive processing by all current and previous IPsec phase-2 tunnels. The total number does not include packets dropped due to anti-replay processing.
Out packets drops	The total number of packets dropped during send processing by all current and previous IPsec phase-2 tunnels.
In replay drops	The total number of packets dropped during receive processing due to anti-replay processing by all current and previous IPsec phase-2 tunnels.
No SA failures	The total number of non-existent SA inbound failures that occurred during processing of all current and previous IPsec phase-2 tunnels.

Related Commands

Command	Description
show crypto mib ipsec flowmib endpoint	Displays IPsec phase-2 tunnel endpoint table.
show crypto mib ipsec flowmib failure	Displays statistics associated with IPsec phase-2 failure.
show crypto mib ipsec flowmib history	Displays statistics associated with previously active IPsec phase-2 tunnels.
show crypto mib ipsec flowmib spi	Displays the IPsec phase-2 SPI table.
show crypto mib ipsec flowmib tunnel	Displays statistics for all active IPsec phase-2 tunnels.

show crypto mib ipsec flowmib history

To display statistics associated with previously active IP Security (IPsec) phase-2 tunnels, use the **show crypto mib ipsec flowmib history**command in privileged EXEC mode.

show crypto mib ipsec flowmib history [**vrf** *vrf-name*]

Syntax Description

vrf *vrf-name*	(Optional) Displays the parameters for the specified Virtual Private Network (VPN) routing and forwarding (VRF) instance.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.
Cisco IOS XE Reelease 2.4	This command was implemented on the Cisco ASR 1000 series routers.

Examples

The following example displays the IPsec phase 2 history statistics for all VRFs:

```
Router# show crypto mib ipsec flowmib history
vrf Global
  Reason:                      Operation request
  Index:                       1
  Local address:               192.1.2.1
  Remote address:              192.1.2.2
  IPSEC keying:                IKE
  Encapsulation mode:          1
  Lifetime (KB):               4608000
  Lifetime (Sec):              3600
  Active time:                 00:24:32
  Lifetime threshold (KB):     423559168
  Lifetime threshold (Sec):    3590000
  Total number of refreshes:   0
  Expired SA instances:        4
  Current SA instances:        4
  In SA DH group:              1
  In sa encrypt algorithm      des
  In SA auth algorithm:        rsig
  In SA ESP auth algo:         ESP_HMAC_SHA
  In SA uncompress algorithm:  None
  Out SA DH group:             1
  Out SA encryption algorithm: des
  Out SA auth algorithm:       ESP_HMAC_SHA
  Out SA ESP auth algorithm:   ESP_HMAC_SHA
  Out SA uncompress algorithm: None
  In octets:                   400
  Decompressed octets:         400
  In packets:                  4
  In drops:                        0
  In replay drops:                 0
  In authentications:              4
  In authentication failures:      0
```

```
In decrypts:                    4
In decrypt failures:            0
Out octets:                     704
Out uncompressed octets:        704
Out packets:                    4
Out drops:                      1
Out authentications:            4
Out authentication failures:    0
Out encryptions:                4
Out encryption failures:        0
Compressed octets:              0
Decompressed octets:            0
Out uncompressed octets:        704
```

The table below describes the significant fields shown in the display.

Table 59: show crypto mib ipsec flowmib history Field Descriptions

Field	Description
Reason	The reason the IPsec phase-2 tunnel was terminated, which are: • 1--All other reasons. • 2--The tunnel terminated normally. • 3--The operator requested the tunnel termination. • 4--A peer delete request was received. • 5--The contact with peer was lost. • 6--A local failure occurred. • 7--The operator initiated a check point request.
Index	The index of the IPsec phase-2 tunnel history table. The value of the index is an integer that begins at one and is incremented with each tunnel that ends. The index value will wrap at 2,147,483,647.
IPSEC keying	The type of key used by the IPsec phase-2 tunnel.
Total number of refreshes	The total number of SA refreshes performed.
In octets	The total number of octets received by the IPsec phase-2 tunnel. The value is accumulated before determining whether or not the packet should be decompressed.
In drops	The total number of packets dropped during receive processing by this IPsec phase-2 tunnel. The number of drops does not include packets dropped due to anti-replay processing.
In replay drops	The total number of packets dropped during receive processing due to anti-replay processing by the IPsec phase-2 tunnel.

Related Commands

Command	Description
show crypto mib ipsec flowmib endpoint	Displays IPsec phase-2 tunnel endpoint table.
show crypto mib ipsec flowmib failure	Displays statistics associated with IPsec phase-2 failure.
show crypto mib ipsec flowmib global	Displays IPsec phase-2 global statistics.
show crypto mib ipsec flowmib spi	Displays the IPsec phase-2 SPI table.
show crypto mib ipsec flowmib tunnel	Displays statistics for all active IPsec phase-2 tunnels.

show crypto mib ipsec flowmib history failure size

To display the size of the IP Security (IPSec) failure history table, use the **show crypto mib ipsec flowmib history failure size** command in privileged EXEC mode.

show crypto mib ipsec flowmib history failure size

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(4)E	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **show crypto mib ipsec flowmib history failure size**command to display the size of the failure history table.

Examples

The following is sample output from the **show crypto mib ipsec flowmib history failure size**command:

```
Router# show crypto mib ipsec flowmib history failure size
IPSec Failure Window size: 140
```

Related Commands

Command	Description
crypto mib ipsec flowmib history failure size	Changes the size of the IPSec failure history table.
show crypto mib ipsec flowmib version	Displays the IPSec Flow MIB version used by the router.

show crypto mib ipsec flowmib history tunnel size

To display the size of the IP Security (IPSec) tunnel history table, use the **show crypto mib ipsec flowmib history tunnel size** command in privileged EXEC mode.

show crypto mib ipsec flowmib history tunnel *size*

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(4)E	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **show crypto mib ipsec flowmib history tunnel size**command to display the size of the tunnel history table.

Examples

The following is sample output from the **show crypto mib ipsec flowmib history tunnel size**command:

```
Router# show crypto mib ipsec flowmib history tunnel size
IPSec History Window Size: 130
```

Related Commands

Command	Description
crypto mib ipsec flowmib history tunnel size	Changes the size of the IPSec tunnel history table.
show crypto mib ipsec flowmib version	Displays the IPSec Flow MIB version used by the router.

show crypto mib ipsec flowmib spi

To display the IP Security (IPsec) phase-2 security protection index (SPI) table, use the **show crypto mib ipsec flowmib spi**command in privileged EXEC mode.

show crypto mib ipsec flowmib spi [**vrf** *vrf-name*]

Syntax Description

vrf *vrf-name*	(Optional) Displays the parameters for the specified Virtual Private Network (VPN) routing and forwarding (VRF) instance.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 series routers.

Usage Guidelines

The IPsec phase-2 SPI table contains an entry for each active and expiring security association (SA).

Examples

The following example displays the IPsec phase-2 SPI table for all VRFs:

```
Router# show crypto mib ipsec flowmib spi
vrf Global
 Tunnel Index:          1
  SPI Index:            1
  SPI Value:            0xCC57D053
  SPI Direction:        In
  SPI Protocol:         AH
  SPI Status:           Active
  SPI Index:            2
  SPI Value:            0x68612DF
  SPI Direction:        Out
  SPI Protocol:         AH
  SPI Status:           Active
  SPI Index:            3
  SPI Value:            0x56947526
  SPI Direction:        In
  SPI Protocol:         ESP
  SPI Status:           Active
  SPI Index:            4
  SPI Value:            0x8D7C2204
  SPI Direction:        Out
  SPI Protocol:         ESP
  SPI Status:           Active
```

The field descriptions in the display are self-explanatory.

Related Commands

Command	Description
show crypto mib ipsec flowmib endpoint	Displays IPsec phase-2 tunnel endpoint table.

Command	Description
show crypto mib ipsec flowmib failure	Displays statistics associated with IPsec phase-2 failure.
show crypto mib ipsec flowmib global	Displays IPsec phase-2 global statistics.
show crypto mib ipsec flowmib history	Displays statistics associated with previously active IPsec phase-2 tunnels.
show crypto mib ipsec flowmib tunnel	Displays statistics for all active IPsec phase-2 tunnels.

show crypto mib ipsec flowmib tunnel

To display statistics for all active IP Security (IPsec) phase-2 tunnels, use the **show crypto mib ipsec flowmib tunnel**command in privileged EXEC mode.

show crypto mib ipsec flowmib tunnel [**index** *tunnel-mib-index*] [**vrf** *vrf-name*]

Syntax Description

vrf *vrf-name*	(Optional) Displays the parameters for the specified Virtual Private Network (VPN) routing and forwarding (VRF) instance.
index *tunnel-mib-index*	(Optional) Displays tunnel MIB information for the specified active tunnel. The tunnel MIB index is an integer, 0-65535.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 series routers.

Examples

The following example displays statistics for all active IPsec phase-2 tunnels for all tunnel indexes and VRFs:

```
Router# show crypto mib ipsec flowmib tunnel
vrf Global
  Index:                              1
  Local address:                      192.0.2.1
  Remote address:                     192.0.2.2
  IPSEC keying:                       IKE
  Encapsulation mode:                 1
  Lifetime (KB):                      4608000
  Lifetime (Sec):                     3600
  Active time:                        00:05:46
  Lifetime threshold (KB):            64
  Lifetime threshold (Sec):           10
  Total number of refreshes:          0
  Expired SA instances:               0
  Current SA instances:               4
  In SA DH group:                     1
  In sa encrypt algorithm:            des
  In SA auth algorithm:               rsig
  In SA ESP auth algo:                ESP_HMAC_SHA
  In SA uncompress algorithm:         None
  Out SA DH group:                    1
  Out SA encryption algorithm:        des
  Out SA auth algorithm:              ESP_HMAC_SHA
  Out SA ESP auth algorithm:          ESP_HMAC_SHA
  Out SA uncompress algorithm:        None
  In octets:                             400
  Decompressed octets:                   400
  In packets:                            4
```

```
In drops:                          0
In replay drops:                   0
In authentications:                4
In authentication failures:        0
In decrypts:                       4
In decrypt failures:               0
Out octets:                        704
Out uncompressed octets:           704
Out packets:                       4
Out drops:                         1
Out authentications:               4
Out authentication failures:       0
Out encryptions:                   4
Out encryption failures:           0
Compressed octets:                 0
Decompressed octets:               0
Out uncompressed octets:           704
```

The table below describes the significant fields shown in the display.

Table 60: show crypto mib ipsec flowmib tunnel Field Descriptions

Field	Description
Index	The index of the IPsec phase-2 tunnel table. The index value is an integer that begins at one and is incremented with each tunnel that is created. The index value will wrap at 2,147,483,647.
Total number of refreshes	The total number of SA refreshes performed.
Current SA instances	The number of SA instances that are currently active or expiring.
In octets	The total number of octets received by the IPsec phase-2 tunnel. This total number is accumulated before determining whether or not the packet should be decompressed.
Decompressed octets	The total number of decompressed octets received by the IPsec phase-2 tunnel. The total number is accumulated after the packet is decompressed. If compression is not being used, the total number will match the value of cipSecTunInOctets.
In drops	The total number of packets dropped during receive processing by the IPsec phase-2 tunnel. This count does not include packets dropped due to anti-replay processing.
In replay drops	The total number of packets dropped during receive processing due to anti-replay processing by the IPsec phase-2 tunnel.
Out octets	The total number of octets sent by the IPsec phase-2 tunnel. This value is accumulated after determining whether or not the packet should be compressed.

Related Commands

Command	Description
show crypto mib ipsec flowmib endpoint	Displays IPsec phase-2 tunnel endpoint table.
show crypto mib ipsec flowmib failure	Displays statistics associated with IPsec phase-2 failure.

Command	Description
show crypto mib ipsec flowmib global	Displays IPsec phase-2 global statistics.
show crypto mib ipsec flowmib history	Displays statistics associated with previously active IPsec phase-2 tunnels.
show crypto mib ipsec flowmib spi	Displays the IPsec phase-2 SPI table.

show crypto mib ipsec flowmib version

To display the IP Security (IPSec) MIB version used by the router, use the **show crypto mib ipsec flowmib version**command in privileged EXEC mode.

show crypto mib ipsec flowmib version

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(4)E	This command was introduced.
12.2(4)T	This command was integrated into Cisco IOS Release 12.2(4)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **show crypto mib ipsec flowmib version**command to display the MIB version used by the management applications to identify the feature set.

Note The MIB version can also be obtained by querying the MIB element cipSecMibLevel using Simple Network Management Protocol (SNMP).

Examples

The following is sample output from the **show crypto mib ipsec flowmib version**command:

```
Router# show crypto mib ipsec flowmib version
IPSec Flow MIB version: 1
```

Related Commands

Command	Description
show crypto mib ipsec flowmib history failure size	Displays the size of the IPSec failure history table.
show crypto mib ipsec flowmib history tunnel size	Displays the size of the IPSec tunnel history table.

show crypto mib isakmp flowmib failure

To display the statistics associated with an Internet Security Association and Key Management Protocol (ISAKMP) phase-1 failure, use the **show crypto mib isakmp flowmib failure** command in privileged EXEC mode.

show crypto mib isakmp flowmib failure [**vrf** *vrf-name*]

Syntax Description

vrf *vrf-name*	(Optional) Displays the parameters for a specific Virtual Private Network (VPN) routing and forwarding (VRF) instance.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 series routers.

Examples

The following is sample output from the **show crypto mib isakmp flowmib failure** command:

```
vrf Global
 Index:                       1
 Reason:                      peer lost
 Failure time since reset:    00:07:27
 Local type:                  ID_IPV4_ADDR
 Local value:                192.0.2.1
 Remote type:                 ID_IPV4_ADDR
 Remote Value:                192.0.2.2
 Local Address:               192.0.2.1
 Remote Address:              192.0.2.2
 Index:                       2
 Reason:                      peer lost
 Failure time since reset:    00:07:27
 Local type:                  ID_IPV4_ADDR
 Local value:                192.0.3.1
 Remote type:                 ID_IPV4_ADDR
 Remote Value:                192.0.3.2
 Local Address:               192.0.3.1
 Remote Address:              192.0.3.2
 Index:                       3
 Reason:                      peer lost
 Failure time since reset:    00:07:32
 Local type:                  ID_IPV4_ADDR
 Remote type:                 ID_IPV4_ADDR
 Remote Value:                192.0.2.2
 Local Address:               192.0.2.1
 Remote Address:              192.0.2.2
```

The table below describes the significant fields shown in the display.

Table 61: show crypto mib isakmp flowmib failure Field Descriptions

Field	Description
Index	The IPsec phase-1 failure table index. The value of the index is a number that begins at one and is incremented with each IPsec phase-1 failure. The index value will wrap at 2,147,483,647.
Reason	The reason for the failure, which include: • 1--All other reasons. • 2--A peer delete request was received. • 3--The contact with peer was lost. • 4--A local failure occurred. • 5--An authentication failure occurred. • 6--A hash validation failure occurred. • 7--An encryption failure occurred. • 8--An internal error occurred. • 9--A system capacity failure occurred. • 10--A proposal failure occurred. • 11--The peer certificate was unavailable. • 12--The peer certificate was invalid. • 13--The local certificate expired. • 14--A certificate revoke list (CRL) failure occurred. • 15--A peer encoding error occurred. • 16--The SA did not exist. • 17--The operator requested tunnel termination.
Failure time since reset	The value of sysUpTime in hundredths of seconds at the time of the failure.
Local type	The type of local peer identity. • 1--Indicates an IP address identity type. • 2--Indicates a hostname identity type.
Local value	The value of the local peer identity. If the local peer type is an IP address, then the value is the IP address used to identify the local peer. If the local peer type is a hostname, then the value is the hostname used to identify the local peer.

Field	Description
Remote type	The type of remote peer identity. • 1--Indicates an IP address identity type. • 2--Indicates a hostname identity type.
Remote Value	The value of the remote peer identity. If the remote peer type is an IP address, then the value is the IP address used to identify the remote peer. If the remote peer type is a hostname, then the value is the hostname used to identify the remote peer.
Local Address	The IP address of the local peer.
Remote Address	The IP address of the remote peer.

Related Commands

Command	Description
show crypto ipsec transform-set	Displays configured IPsec transform sets.
show crypto map	Displays IPsec crypto map configurations.
show crypto mib isakmp flowmib global	Displays global ISAKMP statistics.
show crypto mib isakmp flowmib history	Displays statistics associated with previously active ISAKMP tunnels.
show crypto mib isakmp flowmib peer	Displays attributes for an ISKMP peer association.
show crypto mib isakmp flowmib tunnel	Displays statistics associated with active ISAKMP tunnels.

show crypto mib isakmp flowmib global

To display the global Internet Security Association and Key Management Protocol (ISAKMP) phase-1 statistics, use the **show crypto mib isakmp flowmib global** command in privileged EXEC mode.

show crypto mib isakmp flowmib global [**vrf** *vrf-name*]

Syntax Description

vrf *vrf-name*	(Optional) Displays the parameters for a specific Virtual Private Network (VPN) routing and forwarding (VRF) instance.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 series routers.

Examples

The following example displays global ISAKMP statistics:

```
Router# show crypto mib isakmp flowmib global
vrf Global
  Active Tunnels:                         3
  Previous Tunnels:                       0
  In octets:                              2856
  Out octets:                             3396
  In packets:                             16
  Out packets:                            19
  In packets drop:                        0
  Out packets drop:                       0
  In notifys:                             4
  Out notifys:                            7
  In P2 exchg:                            3
  Out P2 exchg:                           6
  In P2 exchg invalids:                   0
  Out P2 exchg invalids:                  0
  In P2 exchg rejects:                    0
  Out P2 exchg rejects:                   0
  In IPSEC delete:                        0
  Out IPSEC delete:                       0
  SAs locally initiated:                  3
  SAs locally initiated failed:           0
  SAs remotely initiated failed:          0
  System capacity failures:               0
  Authentication failures:                0
  Decrypt failures:                       0
  Hash failures:                          0
  Invalid SPI:                            0
```

The table below describes the fields shown in the display.

Table 62: show crypto mib isakmp flowmib global Field Descriptions

Field	Description
Active Tunnels	The number of currently active IPsec phase-1 IKE tunnels.
Previous Tunnels	The total number of previously active IPsec phase-1 IKE tunnels.
In octets	The total number of octets received by all currently and previously active IPsec phase-1 IKE tunnels.
Out octets	The total number of octets sent by all currently and previously active and IPsec phase-1 IKE tunnels.
In packets	The total number of packets received by all currently and previously active IPsec phase-1 IKE tunnels.
Out packets	The total number of packets sent by all currently and previously active and IPsec phase-1 tunnels.
In packets drop	The total number of packets that were dropped during receive processing by all currently and previously active IPsec phase-1 IKE tunnels.
Out packets drop	The total number of packets that were dropped during send processing by all currently and previously active IPsec phase-1 IKE tunnels.
In notifys	The total number of notifications received by all currently and previously active IPsec phase-1 IKE tunnels.
Out notifys	The total number of notifications sent by all currently and previously active IPsec phase-1 IKE tunnels.
In P2 exchg	The total number of IPsec phase-2 exchanges received by all currently and previously active IPsec phase-1 IKE tunnels.
Out P2 exchg	The total number of IPsec phase-2 exchanges that were sent by all currently and previously active IPsec phase-1 IKE tunnels.
In P2 exchg invalids	The total number of IPsec phase-2 exchanges that were received and found to be invalid by all currently and previously active IPsec phase-1 IKE tunnels.
Out P2 exchg invalids	The total number of IPsec phase-2 exchanges that were sent and found to be invalid by all currently and previously active IPsec phase-1 tunnels.
In P2 exchg rejects	The total number of IPsec phase-2 exchanges that were received and rejected by all currently and previously active IPsec phase-1 IKE tunnels.
Out P2 exchg rejects	The total number of IPsec phase-2 exchanges that were sent and rejected by all currently and previously active IPsec phase-1 IKE tunnels.
In IPSEC delete	The total number of IPsec phase-2 SA delete requests received by all currently and previously active and IPsec phase-1 IKE tunnels.
Out IPSEC delete	The total number of IPsec phase-2 SA delete requests sent by all currently and previously active IPsec phase-1 IKE tunnels.

Field	Description
SAs locally initiated	The total number of IPsec phase-1 IKE tunnels that were locally initiated.
SAs locally initiated failed	The total number of IPsec phase-1 IKE tunnels that were locally initiated and failed to activate.
SAs remotely initiated failed	The total number of IPsec phase-1 IKE tunnels that were remotely initiated and failed to activate.
System capacity failures	The total number of system capacity failures that occurred during processing of all current and previously active IPsec phase-1 IKE tunnels.
Authentication failures	The total number of authentications that ended in failure by all current and previous IPsec phase-1 IKE tunnels.
Decrypt failures	The total number of decryptions that ended in failure by all current and previous IPsec phase-1 IKE tunnels.
Hash failures	The total number of hash validations that ended in failure by all current and previous IPsec phase-1 IKE tunnels.
Invalid SPI	The total number of non-existent SAs in failures which occurred during processing of all current and previous IPsec phase-1 IKE tunnels.

Related Commands

Command	Description
show crypto mib isakmp flowmib failure	Displays statistics associated with an ISAKMP failure.
show crypto mib isakmp flowmib history	Displays statistics associated with previously active ISAKMP tunnels.
show crypto mib isakmp flowmib peer	Displays attributes for an ISKMP peer association.
show crypto mib isakmp flowmib tunnel	Displays statistics associated with active ISAKMP tunnels.

show crypto mib isakmp flowmib history

To display the statistics associated with previously active Internet Security Association and Key Management Protocol (ISAKMP) phase-1 tunnels, use the **show crypto mib isakmp flowmib history** command in privileged EXEC mode.

show crypto mib isakmp flowmib history [**vrf** *vrf-name*]

Syntax Description

vrf *vrf-name*	(Optional) Displays the parameters for a specific Virtual Private Network (VPN) routing and forwarding (VRF) instance.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 series routers.

Examples

The following example displays previous ISAKMP phase-1 tunnel information for all VRFs:

```
Router# show crypto mib isakmp flowmib history
vrf Global
  Reason:                              peer lost
  Index:                               2
  Local type:                          ID_IPV4_ADDR
  Local address:                       192.0.2.1
  Remote type:                         ID_IPV4_ADDR
  Remote address:                      192.0.2.2
  Negotiation mode:                    Main Mode
  Diffie Hellman Grp:                  2
  Encryption algo:                     des
  Hash algo:                           sha
  Auth method:                         psk
  Lifetime:                            86400
  Active time:                         00:06:30
  Policy priority:                     1
  Keepalive enabled:                   Yes
  In octets:                           3024
  In packets:                          22
  In drops:                            0
  In notifys:                          18
  In P2 exchanges:                     1
  In P2 exchg invalids:                0
  In P2 exchg rejected:                  0
  In P2 SA delete reqs:                  0
  Out octets:                            4188
  Out packets:                           33
  Out drops:                             0
  Out notifys:                           28
  Out P2 exchgs:                         2
  Out P2 exchg invalids:                 0
  Out P2 exchg rejects:                  0
```

```
Out P2 Sa delete requests:          0
Reason:                             peer lost
Index:                              3
Local type:                         ID_IPV4_ADDR
Local address:                      192.0.3.1
Remote type:                        ID_IPV4_ADDR
Remote address:                     192.0.3.2
Negotiation mode:                   Main Mode
Diffie Hellman Grp:                 2
Encryption algo:                    des
Hash algo:                          sha
Auth method:                        psk
Lifetime:                           86400
Active time:                        00:06:25
Policy priority:                    1
Keepalive enabled:                  Yes
In octets:                          3140
In packets:                         23
In drops:                           0
In notifys:                         19
In P2 exchanges:                    1
In P2 exchg invalids:               0
In P2 exchg rejected:               0
In P2 SA delete reqs:               0
Out octets:                         4304
Out packets:                        34
Out drops:                          0
Out notifys:                        29
Out P2 exchgs:                      2
Out P2 exchg invalids:              0
Out P2 exchg rejects:               0
Out P2 Sa delete requests:          0
```

The table below describes the significant fields shown in the display.

Table 63: show crypto mib isakmp flowmib history Field Descriptions

Field	Description
Reason	The reason the IPsec phase-1 IKE tunnel was terminated, which include: • 1--All other reasons. • 2--The tunnel terminated normally. • 3--The operator requested tunnel termination. • 4--A peer delete request was received. • 5--The contact with peer was lost. • 6--A local failure occurred. • 7--The operator initiated a check point request.
Index	The index of the IPsec phase-1 IKE tunnel history table. The value of the index is a number that begins at one and is incremented with each tunnel that ends. The value of this object will wrap at 2,147,483,647.

Field	Description
Local type	The type of local peer identity. • 1--Indicates an IP address identity type. • 2--Indicates a hostname identity type.
Local address	The value of the local peer identity. If the local peer type is an IP address, then the value is the IP address used to identify the local peer. If the local peer type is a hostname, then the value is the hostname used to identify the local peer.
Remote type	The type of remote peer identity. • 1--Indicates an IP address identity type. • 2--Indicates a hostname identity type.
Remote address	The value of the remote peer identity. If the remote peer type is an IP address, then the value is the IP address used to identify the remote peer. If the remote peer type is a hostname, then the value is the hostname used to identify the remote peer.
Lifetime	The negotiated lifetime of the IPsec phase-1 IKE tunnel in seconds.
Active time	The length of time the IPsec phase-1 IKE tunnel has been active in hundredths of seconds.
In octets	The total number of octets received by all currently and previously active IPsec phase-1 IKE tunnels.
In packets	The total number of packets received by all currently and previously active IPsec phase-1 IKE tunnels.
In drops	The total number of packets that were dropped during receive processing by all currently and previously active IPsec phase-1 IKE tunnels.
In notifys	The total number of notifications received by all currently and previously active IPsec phase-1 IKE tunnels.
In P2 exchanges	The total number of IPsec phase-2 exchanges received by all currently and previously active IPsec phase-1 IKE tunnels.
In P2 exchg invalids	The total number of IPsec phase-2 exchanges that were received and found to be invalid by all currently and previously active IPsec phase-1 IKE tunnels.
In P2 exchg rejected	The total number of IPsec phase-2 exchanges that were received and rejected by all currently and previously active IPsec phase-1 IKE tunnels.
In P2 SA delete reqs	The total number of IPsec phase-2 SA delete requests received by all currently and previously active and IPsec phase-1 IKE tunnels.
Out octets	The total number of octets sent by all currently and previously active and IPsec phase-1 IKE tunnels.

Field	Description
Out packets	The total number of packets sent by all currently and previously active and IPsec phase-1 tunnels.
Out drops	The total number of packets that were dropped during send processing by all currently and previously active IPsec phase-1 IKE tunnels.
Out notifys	The total number of notifications sent by all currently and previously active IPsec phase-1 IKE tunnels.
Out P2 exchgs	The total number of IPsec phase-2 exchanges that were sent by all currently and previously active IPsec phase-1 IKE tunnels.
Out P2 exchg invalids	The total number of IPsec phase-2 exchanges that were sent and found to be invalid by all currently and previously active IPsec phase-1 tunnels.
Out P2 exchg rejects	The total number of IPsec phase-2 exchanges that were sent and rejected by all currently and previously active IPsec phase-1 IKE tunnels.
Out P2 Sa delete requests	The total number of IPsec phase-2 SA delete requests sent by all currently and previously active IPsec phase-1 IKE tunnels.

Related Commands

Command	Description
show crypto mib isakmp flowmib failure	Displays statistics associated with an ISAKMP failure.
show crypto mib isakmp flowmib global	Displays global ISAKMP statistics.
show crypto mib isakmp flowmib peer	Displays attributes for an ISKMP peer association.
show crypto mib isakmp flowmib tunnel	Displays statistics associated with active ISAKMP tunnels.

show crypto mib isakmp flowmib peer

To display attributes for an active Internet Security Association and Key Management Protocol (ISAKMP) phase-1 peer association, use the **show crypto mib isakmp flowmib peer** command in privileged EXEC mode.

show crypto mib isakmp flowmib peer [**index** *peer-mib-index*] [**vrf** *vrf-name*]

Syntax Description

index *peer-mib-index*	(Optional) Displays MIB information for the specified peer. The peer MIB index is an integer, 0-65535.
vrf *vrf-name*	(Optional) Displays the parameters for the specified Virtual Private Network (VPN) routing and forwarding (VRF) instance.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 series routers.

Examples

The following example displays ISAKMP peer information for all indexes and VRFs:

```
Router# show crypto mib isakmp flowmib peer
 vrf Global
  Index:              1
  Local type:         ID_IPV4_ADDR
  Local address:      192.0.2.1
  Remote type:        ID_IPV4_ADDR
  Remote address:     192.0.2.2
  Index:              2
  Local type:         ID_IPV4_ADDR
  Local address:      192.0.3.1
  Remote type:        ID_IPV4_ADDR
  Remote address:     192.0.3.1
  Index:              3
  Local type:         ID_IPV4_ADDR
  Local address:      192.0.4.1
  Remote type:        ID_IPV4_ADDR
  Remote address:     192.0.4.1
```

The table below describes the significant fields shown in the display.

Table 64: show crypto mib isakmp flowmib peer Field Descriptions

Field	Description
Index	The index of the active IPsec phase-1 IKE tunnel for this peer association. If an IPsec phase-1 IKE tunnel is not currently active, then the value of this object will be zero.

Field	Description
Local type	The type of local peer identity. • 1--Indicates an IP address identity type. • 2--Indicates a hostname identity type.
Local address	The IP address of the local peer.
Remote type	The type of remote peer identity. • 1--Indicates an IP address identity type. • 2--Indicates a hostname identity type.
Remote address	The IP address of the remote peer.

Related Commands

Command	Description
show crypto mib isakmp flowmib failure	Displays statistics associated with an ISAKMP failure.
show crypto mib isakmp flowmib global	Displays global ISAKMP statistics.
show crypto mib isakmp flowmib history	Displays statistics associated with previously active ISAKMP tunnels.
show crypto mib isakmp flowmib tunnel	Displays statistics associated with active ISAKMP tunnels.

show crypto mib isakmp flowmib tunnel

To display statistics associated with active Internet Security Association and Key Management Protocol (ISAKMP) phase-1 tunnels, use the **show crypto mib isakmp flowmib tunnel** command in privileged EXEC mode.

show crypto mib isakmp flowmib tunnel [**index** *tunnel-mib-index*] [**vrf** *vrf-name*]

Syntax Description

index *tunnel-mib-index*	(Optional) Displays tunnel MIB information for the specified tunnel. The tunnel MIB index is an integer, 0-65535.
vrf *vrf-name*	(Optional) Displays the parameters for the specified Virtual Private Network (VPN) routing and forwarding (VRF) instance.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 series routers.

Examples

The following example displays ISAKMP tunnel information for all indexes and VRFs:

```
Router# show crypto mib isakmp flowmib tunnel
vrf Global
  Index:                    1
  Local type:               ID_IPV4_ADDR
  Local address:            192.0.2.1
  Remote type:              ID_IPV4_ADDR
  Remote address:           192.0.2.2
  Negotiation mode:         Main Mode
  Diffie Hellman Grp:       2
  Encryption algo:          des
  Hash algo:                sha
  Auth method:              psk
  Lifetime:                 86400
  Active time:              00:03:08
  Policy priority:          1
  Keepalive enabled:        Yes
  In octets:                2148
  In packets:               15
  In drops:                 0
  In notifys:               11
  In P2 exchanges:          1
  In P2 exchg invalids:     0
  In P2 exchg rejected:     0
  In P2 SA delete reqs:     0
  Out octets:               2328
  Out packets:              16
  Out drops:                    0
  Out notifys:                  12
```

```
Out P2 exchgs:                  2
Out P2 exchg invalids:          0
Out P2 exchg rejects:           0
Out P2 Sa delete requests:      0
```

The table below describes the significant fields shown in the display.

Table 65: show crypto mib isakmp flowmib tunnel Field Descriptions

Field	Description
Index	The index of the IPsec phase-1 IKE tunnel table. The value of the index is a number that begins at one and is incremented with each tunnel that is created. The value of this object will wrap at 2,147,483,647.
Local type	The type of local peer identity. • 1--Indicates an IP address identity type. • 2--Indicates a hostname identity type.
Local address	The value of the local peer identity. If the local peer type is an IP address, then the local address is the IP address used to identify the local peer. If the local peer type is a hostname, then the local address is the hostname used to identify the local peer.
Remote type	The type of remote peer identity. • 1--Indicates an IP address identity type. • 2--Indicates a hostname identity type.
Remote address	The value of the remote peer identity. If the remote peer type is an IP address, then the remote address is the IP address used to identify the remote peer. If the remote peer type is a hostname, then the remote address is the hostname used to identify the remote peer.
Negotiation mode	The negotiation mode of the IPsec phase-1 IKE tunnel.
Diffie Hellman Grp	The Diffie Hellman group used in IPsec phase-1 IKE negotiations.
Encryption algo	The encryption algorithm used in IPsec phase-1 IKE negotiations.
Hash algo	The hash algorithm used in IPsec phase-1 IKE negotiations.
Auth method	The authentication method used in IPsec phase-1 IKE negotiations.
Lifetime	The negotiated lifetime of the IPsec phase-1 IKE tunnel in seconds
Active time	The length of time the IPsec phase-1 IKE tunnel has been active in hundredths of seconds.
In octets	The total number of octets received by all currently and previously active IPsec phase-1 IKE tunnels.

Field	Description
In packets	The total number of packets received by all currently and previously active IPsec phase-1 IKE tunnels.
In drops	The total number of packets that were dropped during receive processing by all currently and previously active IPsec phase-1 IKE tunnels.
In notifys	The total number of notifications received by all currently and previously active IPsec phase-1 IKE tunnels.
In P2 exchanges	The total number of IPsec phase-2 exchanges received by all currently and previously active IPsec phase-1 IKE tunnels.
In P2 exchg invalids	The total number of IPsec phase-2 exchanges that were received and found to be invalid by all currently and previously active IPsec phase-1 IKE tunnels.
In P2 exchg rejected	The total number of IPsec phase-2 exchanges that were received and rejected by all currently and previously active IPsec phase-1 IKE tunnels.
In P2 SA delete reqs	The total number of IPsec phase-2 SA delete requests received by all currently and previously active and IPsec phase-1 IKE tunnels.
Out octets	The total number of octets sent by all currently and previously active and IPsec phase-1 IKE tunnels.
Out packets	The total number of packets sent by all currently and previously active and IPsec phase-1 tunnels.
Out drops	The total number of packets that were dropped during send processing by all currently and previously active IPsec phase-1 IKE tunnels.
Out notifys	The total number of notifications sent by all currently and previously active IPsec phase-1 IKE tunnels.
Out P2 exchgs	The total number of IPsec phase-2 exchanges that were sent by all currently and previously active IPsec phase-1 IKE tunnels.
Out P2 exchg invalids	The total number of IPsec phase-2 exchanges that were sent and found to be invalid by all currently and previously active IPsec phase-1 tunnels.
Out P2 exchg rejects	The total number of IPsec phase-2 exchanges that were sent and rejected by all currently and previously active IPsec phase-1 IKE tunnels.
Out P2 Sa delete requests	The total number of IPsec phase-2 SA delete requests sent by all currently and previously active IPsec phase-1 IKE tunnels.

Related Commands

Command	Description
show crypto mib isakmp flowmib failure	Displays statistics associated with an ISAKMP failure.
show crypto mib isakmp flowmib global	Displays global ISAKMP statistics.

Command	Description
show crypto mib isakmp flowmib history	Displays statistics associated with previously active ISAKMP tunnels.
show crypto mib isakmp flowmib peer	Displays attributes for an ISKMP peer association.

show crypto pki benchmarks

To display benchmarking data for Public Key Infrastructure (PKI) performance monitoring and optimization that was collected, use the **show crypto pki benchmarks**command in privileged EXEC mode.

show crypto pki benchmarks [**failures**]

Syntax Description

failures	(Optional) Includes validation failures only.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(3)T	This command was introduced.

Usage Guidelines

Use the **show crypto pki benchmarks** command to display benchmarking data for PKI performance monitoring and optimization that was collected.

The IOS PKI Performance Monitoring and Optimization feature enables you to collect the following types of PKI performance data:

- Time to validate entire certificate chain.
- Time to verify each certificate.
- Time to check revocation status for each certificate.
- Time to fetch certificate revocation list (CRL) database for each fetch location.
- Time to fetch Simple Certificate Enrollment Protocol (SCEP) method capabilities to retrieve the CRL.
- Time to process each CRL.
- Time to process the Online Certificate Status Protocol (OCSP) response. OCSP is a certificate revocation mechanism.
- Time to fetch Authentication, Authorization, and Accounting (AAA).
- CRL size.
- Validation result.
- Validation Bypass (pubkey cached).
- Method used to fetch a CRL.
- PKI session identifier.
- Crypto engine used (hardware, software, etoken).

Examples

The following example displays **show crypto pki benchmark** command output of all PKI benchmarking data:

```
Router# show crypto pki benchmark
Display Validation Benchmark Table
 4 Records collected
Validation Session 10006
  Start: 20:47:29.021 GMT Wed Oct 27 2010
  Duration: 756 ms
  Peer Certificate Serial Number (hex): 296ED1EB0000000052FA
  Pubkey Bypass: no
  Result: Success
  Size of Chain to Validate: 1
  Revocation Check for Certificate 1 of 1
    Start: 20:47:29.063 GMT Wed Oct 27 2010
    Duration: 714 ms
  CRL Fetch - http://msca-root/CertEnroll/msca-root.crl
      Start: 20:47:29.067 GMT Wed Oct 27 2010
      Duration: 661 ms
      Fetch Result: Success
  CRL Insert
      Start: 20:47:29.731 GMT Wed Oct 27 2010
      Duration: 24 ms
  CRL Size: 582
Validation Session 10007
  Start: 20:48:15.897 GMT Wed Oct 27 2010
  Duration: 26 ms
  Pubkey Bypass: no
  Result: Failed CRYPTO_CERT_EXPIRED
  Size of Chain to Validate: 1
Validation Session 10008
  Start: 20:49:08.916 GMT Wed Oct 27 2010
  Duration: 26 ms
  Pubkey Bypass: no
  Result: Failed CRYPTO_CERT_EXPIRED
  Size of Chain to Validate: 1
Validation Session 10009
  Start: 20:49:15.051 GMT Wed Oct 27 2010
  Duration: 32 ms
  Peer Certificate Serial Number (hex): 296ED1EB0000000052FA
  Pubkey Bypass: no
  Result: Success
  Size of Chain to Validate: 1
  Revocation Check for Certificate 1 of 1
    Start: 20:49:15.076 GMT Wed Oct 27 2010
    Duration: 6 ms
The following example displays show crypto pki benchmark
 command output of a section filter in PKI benchmarking data:
Router# show crypto pki benchmark | section Revocation
  Revocation Check for Certificate 1 of 1
    Start: 20:47:29.063 GMT Wed Oct 27 2010
    Duration: 714 ms
  Revocation Check for Certificate 1 of 1
    Start: 20:49:15.076 GMT Wed Oct 27 2010
    Duration: 6 ms
```

Related Commands

Command	Description
clear crypto pki benchmark	Clears PKI benchmarking performance monitoring and optimization data and releases all memory associated with this data.
crypto pki benchmark	Starts or stops benchmarking data for PKI performance monitoring and optimization.

show crypto pki certificates

To display information about your certificate, the certification authority certificate (CA), and any registration authority (RA) certificates, use the **show crypto pki certificates** command in privileged EXEC mode.

show crypto pki certificates [*trustpoint-name* [**verbose**]]

Syntax Description

trustpoint-name	(Optional) Name of the trustpoint. Using this argument indicates that only certificates that are related to the trustpoint are to be displayed.
verbose	(Optional) More detailed information is to be displayed. **Note** The **verbose** keyword can be used only if a trustpoint name is entered.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.3 T	The **show crypto ca certificates**command was introduced.
12.2(13)T	The *trustpoint-name* argument was added.
12.3(7)T	This command replaced the **show crypto ca certificates** command.
12.3(8)T	The **verbose** keyword was added.
12.3(14)T	The command output was modified to include persistent self-signed certificate parameters.
12.4(2)T	The command output was modified to include shadow public key infrastructure (PKI), or rollover, certificate details.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(22)T	The command output was modified to include X.509 certificate IP address extension information.

Usage Guidelines

This command shows information about the following certificates:

- Your certificate, if you have requested one from the CA (see the **crypto pki enroll** command)
- The certificate of the CA, if you have received the certificate of the CA (see the **crypto pki authenticate** command)
- RA certificates, if you have received RA certificates (see the **crypto pki authenticate** command)
- A self-signed certificate, if one has been requested
- Shadow PKI, or rollover, certificate details, if one or more shadow PKI certificates exist

Examples

The following is sample output from the **show crypto pki certificates** command after you authenticated the CA by requesting the certificate of the CA and public key with the **crypto pki authenticate** command:

```
CA Certificate
  Status: Available
  Certificate Serial Number: 3051DF7123BEE31B8341DFE4B3A338E5F
  Key Usage: Not Set
```

The CA certificate might show Key Usage as "Not Set."

The following is sample output from the **show crypto pki certificates** command, and it shows the certificate of the router and the certificate of the CA. In this example, a single, general-purpose Rivest, Shamir, and Adelman (RSA) key pair was previously generated, and a certificate was requested but not received for that key pair.

```
Certificate
  Subject Name
    Name: myrouter.example.com
    IP Address: 10.0.0.1
    Serial Number: 04806682
  Status: Pending
  Key Usage: General Purpose
    Fingerprint: 428125BD A3419600 3F6C7831 6CD8FA95 00000000
CA Certificate
  Status: Available
  Certificate Serial Number: 3051DF7123BEE31B8341DFE4B3A338E5F
  Key Usage: Not Set
```

Note that in the previous sample, the certificate status of the router shows "Pending." After the router receives its certificate from the CA, the Status field changes to "Available" in the **show** output.

The following is sample output from the **show crypto pki certificates** command, and it shows the certificates of two routers and the certificate of the CA. In this example, special-usage RSA key pairs were previously generated, and a certificate was requested and received for each key pair.

```
Certificate
  Subject Name
    Name: myrouter.example.com
    IP Address: 10.0.0.1
  Status: Available
  Certificate Serial Number: 428125BDA34196003F6C78316CD8FA95
  Key Usage: Signature

Certificate
  Subject Name
    Name: myrouter.example.com
    IP Address: 10.0.0.1
  Status: Available
  Certificate Serial Number: AB352356AFCD0395E333CCFD7CD33897
  Key Usage: Encryption

CA Certificate
  Status: Available
  Certificate Serial Number: 3051DF7123BEE31B8341DFE4B3A338E5F
  Key Usage: Not Set
```

The following is sample output from the **show crypto pki certificates** command when the CA supports an RA. In this example, the CA and RA certificates were previously requested with the **crypto pki authenticate** command.

```
CA Certificate
  Status: Available
  Certificate Serial Number: 3051DF7123BEE31B8341DFE4B3A338E5F
  Key Usage: Not Set
RA Signature Certificate
  Status: Available
  Certificate Serial Number: 34BCF8A0
  Key Usage: Signature

RA KeyEncipher Certificate
  Status: Available
  Certificate Serial Number: 34BCF89F
  Key Usage: Encryption
```

The following is sample output from the **show crypto pki certificates** command using the optional *trustpoint-name* argument and **verbose** keyword. The output shows the certificate of a router and the certificate of the CA. In this example, general-purpose RSA key pairs were previously generated, and a certificate was requested and received for the key pair.

```
Certificate
   Status: Available
   Version: 3
   Certificate Serial Number: 18C1EE03000000004CBD
   Certificate Usage: General Purpose
   Issuer:
     cn=msca-root
     ou=pki msca-root
     o=company
     l=stown
     st=state
     c=US
     ea=user@example.com
   Subject:
     Name: myrouter.example.com
     hostname=myrouter.example.com
   CRL Distribution Points:
     http://msca-root/CertEnroll/msca-root.crl
   Validity Date:
     start date: 19:50:40 GMT Oct 5 2004
     end   date: 20:00:40 GMT Oct 12 2004
   Subject Key Info:
     Public Key Algorithm: rsaEncryption
     RSA Public Key: (360 bit)
   Signature Algorithm: SHA1 with RSA Encryption
   Fingerprint MD5: 2B5F53E6 E3E892E6 3A9D3706 01261F10
   Fingerprint SHA1: 315D127C 3AD34010 40CE7F3A 988BBDA5 CD528824
   X509v3 extensions:
     X509v3 Key Usage: A0000000
       Digital Signature
       Key Encipherment
     X509v3 Subject Key ID: D156E92F 46739CBA DFE66D2D 3559483E B41ECCF4
     X509v3 Authority Key ID: 37F3CC61 AF5E7C0B 434AB364 CF9FA0C1 B17C50D9
     Authority Info Access:
   Associated Trustpoints: msca-root
   Key Label: myrouter.example.com
CA Certificate
   Status: Available
   Version: 3
   Certificate Serial Number: 1244325DE0369880465F977A18F61CA8
   Certificate Usage: Signature
   Issuer:
     cn=msca-root
```

```
    ou=pki msca-root
    o=company
    l=town
    st=state
    c=US
    ea=user@example.com
  Subject:
    cn=msca-root
    ou=pki msca-root
    o=company
    l=town
    st=state
    c=US
    ea=user@example.com
  CRL Distribution Points:
    http://msca-root.example.com/CertEnroll/msca-root.crl
  Validity Date:
    start date: 22:19:29 GMT Oct 31 2002
    end   date: 22:27:27 GMT Oct 31 2017
  Subject Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (512 bit)
  Signature Algorithm: SHA1 with RSA Encryption
  Fingerprint MD5: 84E470A2 38176CB1 AA0476B9 C0B4F478
  Fingerprint SHA1: 0F57170C 654A5D7D 10973553 EFB0F94F 2FAF9837
  X509v3 extensions:
    X509v3 Key Usage: C6000000
      Digital Signature
      Non Repudiation
      Key Cert Sign
      CRL Signature
    X509v3 Subject Key ID: 37F3CC61 AF5E7C0B 434AB364 CF9FA0C1 B17C50D9
    X509v3 Basic Constraints:
        CA: TRUE
    Authority Info Access:
  Associated Trustpoints: msca-root
```

The following is sample output from the **show crypto pki certificates** command using the optional *trustpoint-name*argument and **verbose** keyword. The output shows the SIGNED PKCS10 fingerprint irrespective of the enrollment through a CA server or a RA server. Additionally, it displays the SIGNED PKCS10 SHA2 fingerprint along with SHA1 SIGNED PKCS10 fingerprint, and MD5 SIGNED PKCS10 fingerprint.

```
CA Certificate
  Status: Available
  Version: 3
  Certificate Serial Number (hex): 01
  Certificate Usage: Signature
  Issuer:
    cn=ca
  Subject:
    cn=ca
  Validity Date:
    start date: 22:55:38 IST Aug 25 2022
    end   date: 22:55:38 IST Aug 24 2025
  Subject Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (2048 bit)
  Signature Algorithm: MD5 with RSA Encryption
  Fingerprint MD5: F6345AE9 3A554053 5F009F1A 4DD8F572
  Fingerprint SHA1: 2E46DB45 03B2968A FB0B79B0 56C8E106 DB12529A
  X509v3 extensions:
    X509v3 Key Usage: 86000000
```

```
      Digital Signature
      Key Cert Sign
      CRL Signature
    X509v3 Subject Key ID: 23B4C7F8 F3025142 18E60729 B4A98A3D 54277D5D
    X509v3 Basic Constraints:
        CA: TRUE
    X509v3 Authority Key ID: 23B4C7F8 F3025142 18E60729 B4A98A3D 54277D5D
    Authority Info Access:
  Cert install time: 22:55:38 IST Aug 25 2022
  Associated Trustpoints: test ca


Certificate
  Subject:
    Name: Router
   Status: Pending
   Key Usage: General Purpose
   Certificate Request Fingerprint MD5 :CD76F722 60617951 DE5AF18D 3FC74A2A
   Certificate Request Fingerprint SHA1 :10A04557 9B5613B2 D0DD8AA5 72B0601B 05940E3D
   Certificate Request Fingerprint SHA2 :3E96A4CE 9824A2D4 07344A63 3D5EF642 7C53ADD0
B0C7B521 61DA06D8 289FA221
   Certificate Request Fingerprint MD5  (unsigned):D68D4DF6 84A58B40 76EBD026 40CE42B3
   Associated Trustpoint: test
```

The following example shows that a self-signed certificate has been created using a user-defined trustpoint:

```
Router Self-Signed Certificate
  Status: Available
  Certificate Serial Number: 01
  Certificate Usage: General Purpose
  Issuer:
    serialNumber=C63EBBE9+ipaddress=10.3.0.18+hostname=test.company.com
  Subject:
    Name: router.company.com
    IP Address: 10.3.0.18
    Serial Number: C63EBBE9
    serialNumber=C63EBBE9+ipaddress=10.3.0.18+hostname=test.company.com
  Validity Date:
    start date: 20:51:40 GMT Nov 29 2004
    end   date: 00:00:00 GMT Jan 1 2020
  Associated Trustpoints: local
```

The following example shows that a shadow CA certificate, or rollover certificate, is available and shows its status:

```
Router# show crypto ca certificates
   Rollover Certificate
  Status: Waiting for rollover
  Certificate Serial Number: 3C
  Certificate Usage: General Purpose
  Issuer:
    cn=ezsdd
  Subject:
    Name: Router.company.com
    Serial Number: 3A9BEC55
    serialNumber=3A9BEC55+hostname=Router.company.com
  Validity Date:
    start date: 21:22:08 UTC Mar 17 2004
    end   date: 21:22:08 UTC Mar 17 2005
    renew date: 00:00:00 UTC Jan 1 1970
  Associated Trustpoints: tti
```

Related Commands

Command	Description
crypto pki authenticate	Authenticates the CA (by obtaining the certificate of the CA).
crypto pki enroll	Obtains the certificates of your router from the CA.
debug crypto pki messages	Displays debug messages for the details of the interaction (message dump) between the CA and the route.
debug crypto pki transactions	Displays debug messages for the trace of interaction (message type) between the CA and the router.

show crypto pki certificates pem

To display information about the PKI certificates associated with trustpoint in PEM (Privacy Enhanced Mail) format, use the **show crypto pki certificates pem** command in privileged EXEC mode.

show crypto pki certificates pem [*trustpoint-name*]

Syntax Description

trustpoint-name	(Optional) Name of the trustpoint. Using this argument indicates that only certificates that are related to the trustpoint are to be displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
IOS XE Fuji 16.9.1	This command was introduced.

Examples

The following is sample output from the **show crypto pki certificates pem** command :

```
Router# show crypto pki certificates pem
------Trustpoint: TP-self-signed-777972883------
% The specified trustpoint is not enrolled (TP-self-signed-777972883).
% Only export the CA certificate in PEM format.
% Error: failed to get CA cert.
------Trustpoint: rootca------
% The specified trustpoint is not enrolled (rootca).
% Only export the CA certificate in PEM format.
% CA certificate:
-----BEGIN CERTIFICATE-----
MIICAzCCAWygAwIBAgIBAjANBgkqhkiG9w0BAQ0FADAVMRMwEQYDVQQDEwpSQ0Ex
IEM9cGtpMB4XDTE4MDYwMzAxMzQ1NloXDTE5MDYwMjAxMzQ1NlowFTETMBEGA1UE
AxMKUkNBMSBDPXBraTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEArRK9Piyn
Oz8cGaGM1TvfYYJ3AFEjV6lcFB5N57FH70/J3MDri32oHSDjJaS1PIfRn2H2OuUq
gnJBgvPeM66lmrt7nG9NnflEsKt4n2NcdAzBAXPOMEN+ppL03PqxW5l4KwwBQ++k
ukJCzeIPd925aMDIte8qP9MxPG9J2T4S2Y0CAwEAAaNjMGEwDwYDVR0TAQH/BAUw
AwEB/zAOBgNVHQ8BAf8EBAMCAYYwHwYDVR0jBBgwFoAURuQoekWXHhkEq1fXjoJJ
VP+cH5AwHQYDVR0OBBYEFEbkKHpFlx4ZBKtX146CSVT/nB+QMA0GCSqGSIb3DQEB
DQUAA4GBAFrMgQAQYLsd1WhH886q6HHJbiFMYP1cVsEFoVxnmct0ZLUYiX4v6WyH
X/VGMRIkvOKu9ZnbYcsFdqcHV+YYOjI4hj5U+5WTM8hWIVDe9vpo2N4lJtaPQb5y
JsMCkgQtFtOtqBqYzB2Uze0GqeprK+lGgnYMf6cUYwbZXQem8a32
-----END CERTIFICATE-----

------Trustpoint: test------
% CA certificate:
-----BEGIN CERTIFICATE-----
MIICAzCCAWygAwIBAgIBAjANBgkqhkiG9w0BAQ0FADAVMRMwEQYDVQQDEwpSQ0Ex
IEM9cGtpMB4XDTE4MDYwMzAxMzQ1NloXDTE5MDYwMjAxMzQ1NlowFTETMBEGA1UE
AxMKUkNBMSBDPXBraTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEArRK9Piyn
Oz8cGaGM1TvfYYJ3AFEjV6lcFB5N57FH70/J3MDri32oHSDjJaS1PIfRn2H2OuUq
gnJBgvPeM66lmrt7nG9NnflEsKt4n2NcdAzBAXPOMEN+ppL03PqxW5l4KwwBQ++k
ukJCzeIPd925aMDIte8qP9MxPG9J2T4S2Y0CAwEAAaNjMGEwDwYDVR0TAQH/BAUw
AwEB/zAOBgNVHQ8BAf8EBAMCAYYwHwYDVR0jBBgwFoAURuQoekWXHhkEq1fXjoJJ
VP+cH5AwHQYDVR0OBBYEFEbkKHpFlx4ZBKtX146CSVT/nB+QMA0GCSqGSIb3DQEB
DQUAA4GBAFrMgQAQYLsd1WhH886q6HHJbiFMYP1cVsEFoVxnmct0ZLUYiX4v6WyH
```

```
X/VGMRIkvOKu9ZnbYcsFdqcHV+YYOjI4hj5U+5WTM8hWIVDe9vpo2N4lJtaPQb5y
JsMCkgQtFtOtqBqYzB2Uze0GqeprK+lGgnYMf6cUYwbZXQem8a32
-----END CERTIFICATE-----

% General Purpose Certificate:
-----BEGIN CERTIFICATE-----
MIICAzCCAWygAwIBAgIBBDANBgkqhkiG9w0BAQ0FADAVMRMwEQYDVQQDEwpSQ0Ex
IEM9cGtpMB4XDTE4MDYwMzAxMzYxOVoXDTE5MDYwMjAxMzQ1NlowKTERMA8GA1UE
AxMIUjEgQz1wa2kxFDASBgkqhkiG9w0BCQIWBXBraV9hMIGfMA0GCSqGSIb3DQEB
AQUAA4GNADCBiQKBgQDNt5ivJHXfSk3VJsYCzcJzWPLZCkvn+lj1qy5UlcfutVUT
o1cznDGTks39KPYHvb27dyEmH5SmI7aUqWb59gMnWCtqbKDuwOitjncV/7UBvL59
LeDs0tmFpSS/3qohR9fUWhmCBYWzFOqn6TmshSojha/53lhxPJpB32g7r9XS0wID
AQABo08wTTALBgNVHQ8EBAMCBaAwHwYDVR0jBBgwFoAURuQoekWXHhkEq1fXjoJJ
VP+cH5AwHQYDVR0OBBYEFO+7q9HuzMgOPK5ZsMasYzORBwrBMA0GCSqGSIb3DQEB
DQUAA4GBAIZZ+BhaW3aRKMN/HHsaMtAkQ4vIchrGrVDx6elvyNyUE5rN+oJIWPT6
gp97rAmgQK9aWlOrrG6l5urcK/y/szA2xClbGMXMFB2jvOeRbiUSP0q8V0blafBy
UawecQ6HKgmAEuVHgg4invc9jA6IGLtcj55J1iLum/MCikC70Org
-----END CERTIFICATE-----
```

show crypto pki certificates storage

To display the current public key infrastructure (PKI) certificate storage location, use the **show crypto pki certificates storage**command in privileged EXEC mode.

show crypto pki certificates storage

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

Use the **show crypto pki certificates storage**command to display the current PKI certificate storage location.

Examples

The following is sample output for the **show crypto pki certificates storage** command where the certificates are stored in the certs subdirectory of disk0:

```
Router# show crypto pki certificates storage
Certificates will be stored in disk0:/certs/
```

Related Commands

Command	Description
crypto pki certificate storage	Specifies local storage device for PKI certificates.

show crypto pki counters

To display the public key infrastructure (PKI) counters that are configured on the router, use the **show crypto pki counters** command in privileged EXEC mode.

show crypto pki counters

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(13)T	This command was introduced.

Examples

```
The following example shows the listing of all PKI counters that are configured in a router:
Router# show crypto pki counters
PKI Sessions Started: 5
PKI Sessions Ended: 5
PKI Sessions Active: 0
Successful Validations: 1
Failed Validations: 4
Bypassed Validations: 0
Pending Validations: 0
CRLs checked: 3
CRL - fetch attempts: 2
CRL - failed attempts: 0
AAA authorizations: 0
```

The table below describes the significant fields shown in the display.

Table 66: show crypto pki counters Field Descriptions

Field	Description
PKI Sessions Started	Number of PKI sessions that are started in a router.
PKI Sessions Ended	Number of PKI sessions that are ended in a router.
PKI Sessions Active	Number of PKI sessions that are actively running in a router.
Successful Validations	Number of successful PKI counter validations in a router.
Failed Validations	Number of failed PKI counter validations in a router.
Bypassed Validations	Number of validations that were bypassed during a PKI counter validation in a router.
Pending Validations	Number of pending PKI counter validations in a router.
CRLs checked	Number of certificate revocation lists (CRLs) that are checked in a PKI session.

Field	Description
CRL - fetch attempts	Number of times a CRL is queried and fetched.
CRL - failed attempts	Number of times failed in querying and fetching a CRL.
AAA authorizations	Number of authentication, authorization, and accounting (AAA) authorizations that were used to create named methods lists in a PKI session.

Related Commands

Command	Description
show crypto pki certificates	Displays information about the certification authority certificate and any RA certificates.
show crypto pki crls	Displays the current CRL on the router.
show crypto pki server	Displays the current state and configuration of the certificate server.
show crypto pki timers	Displays the status of the managed timers that are maintained by Cisco IOS for PKI.
show crypto pki token	Displays the Cisco IOS PKI tokens that are configured on the router.
show crypto pki trustpoints	Displays the Cisco IOS PKI trustpoints that are configured in the router.

show crypto pki crls

To display the current certificate revocation list (CRL) on the router, use the **show crypto pki crls** command in privileged EXEC mode.

show crypto pki crls

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.1	The **show crypto ca crls** command was introduced.
12.3(7)T	This command replaced the **show crypto ca crls** command.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.(33)SXH.
12.4(20)T	The output of this command was updated to include information on the CRL cache size if set by the crypto pki crl cache command.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 series routers.

Examples

The following is sample output of the **show crypto pki crls**command:

```
Router# show crypto pki crls

          CRL Issuer Name:
              OU = vpn, O = company, C = us
              LastUpdate: 16:17:34 PST Jan 10 2002
              NextUpdate: 17:17:34 PST Jan 11 2002
              Retrieved from CRL Distribution Point:
```

LDAP: CN = CRL1, OU = vpn, O = company, C = us

The following is sample output of the **show crypto pki crls**command with the maximum CRL cache size set to 2048 bytes:

```
Router# show crypto pki crls

     CRL Issuer Name:
           cn=ioscs,l=Anytown,c=US
           LastUpdate: 02:53:41 GMT Mar 6 2007
           NextUpdate: 02:53:41 GMT Mar 13 2007
           Retrieved from CRL Distribution Point:
                ** CDP Not Published - Retrieved via SCEP
     CRL DER is 475 bytes
     CRL is stored in parsed CRL cache
     Parsed CRL cache current size is 1705 bytes
     Parsed CRL cache maximum size is 2048 bytes
```

Related Commands

Command	Description
crypto pki crl cache	Sets the maximum amount of volatile memory used to cache CRLs.
crypto pki crl request	Requests that a new CRL be obtained immediately from the CA.

show crypto pki server

To display the current state and configuration of the certificate server, use the **show crypto pki server**command in privileged EXEC mode.

show crypto pki server [*cs-label*]

Syntax Description

cs-label	(Optional) Name of the certificate server. The name must match the name specified through the **crypto pki server** command.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.4(2)T	The command output was modified to include shadow, or rollover, public key infrastructure (PKI) certificate information.
15.0(1)M	The command output was modified. • To include whether the server is configured for redundancy and whether its state is active or standby or simplex (active, but standby is not up). • To show the high availability (HA) status while the Hot Standby Router Protocol (HSRP) is coming up.

Usage Guidelines

At startup, the certificate server must check the current configuration before issuing any certificates. As it starts up, the certificate server transitions through the states defined in the table below. Use the **show crypto pki server**command to display the state of the certificate server.

Table 67: Certificate Server Startup State Descriptions

Certificate Server State	Description
configured	The server is available and has generated the certificate server certificates.
storage configuration incomplete	The server is verifying that the configured storage location is available.
waiting for HTTP server	The server is verifying that the HTTP server is running.
waiting for time setting	The server is verifying that the time has been set.

Examples

The following is sample output from the **show crypto pki server**command:

```
Router# show crypto pki server
Certificate Server status: disabled, storage configuration incomplete
```

```
    Granting mode is: manual
    Last certificate issued serial number: 0
    CA certificate expiration timer: 21:29:38 GMT Jun 5 2006
    CRL NextUpdate timer: 21:31:39 GMT Jun 6 2003
    Current storage dir:
ftp://myftpserver
    Database Level: Minimum - no cert data written to storage
```

The table below describes the significant fields shown in the display.

Table 68: show crypto pki server Field Descriptions

Field	Description
Granting mode is	Specifies whether certificate enrollment requests should be granted manually (which is the default) or automatic (through the **grant automatic** command). **Note** The **grant automatic**command should be used *only* when testing and building simple networks. This command *must* be disabled before the network is accessible by the Internet.
Last certificate issued serial number	The serial number of the latest certificate. (To specify the distinguished name (DN) as the certification authority (CA) issuer name, use the **issuer-name** command.)
CA certificate expiration timer	The expiration date for the CA certificate. (To specify the expiration date, use the **lifetime** command.)
CRL NextUpdate timer	The next time the certificate revocation list (CRL) will be updated. (To specify the CRL lifetime, in hours, use the **lifetime crl**command.)
Current storage dir	The location where all database entries for the certificate server will be written out. (To specify a location, use the **database url** command.)
Database Level	The type of data that is stored in the certificate enrollment database--Minumum, names, or complete. (To specify the data type to be stored, use **database level** command.)

The following is sample output from the **show crypto pki server** command when redundancy is configured and its state is simplex:

```
Router# show crypto pki server cert1

Certificate Server cert1:
    Status: disabled
    State: disabled
    Server's configuration is unlocked  (enter "no shut" to lock it)
    Issuer name: CN=cert1
    CA cert fingerprint: -Not found-
    Granting mode is: manual
    Last certificate issued serial number (hex): 0
    CA certificate expiration timer: 00:00:00 UTC Jan 1 1970
    CRL not present.
    Current primary storage dir: nvram:
    Database Level: Minimum - no cert data written to storage
    Redundancy configured.  Simplex mode.
The following is sample output from the show crypto pki server
 command when redundancy is configured and its state is active:
```

```
Certificate Server HA:
    Status: enabled
    State: enabled
    Server's configuration is locked  (enter "shut" to unlock it)
    Issuer name: CN=ioscs,L=Santa Cruz,C=US
    CA cert fingerprint: 42308002 188180FC 9265946F FDC68A52
    Granting mode is: auto
    Last certificate issued serial number (hex): 2
    CA certificate expiration timer: 20:22:55 PST Apr 26 2013
    CRL NextUpdate timer: 20:27:46 PST May 11 2010
    Current primary storage dir: nvram:
    Database Level: Complete - all issued certs written as <serialnum>.cer
    Redundancy configured.  This is active.
The following is sample output from the show crypto pki server
 command when redundancy is configured and its state is standby:
Certificate Server HA:
    Status: enabled
    State: enabled
    Server's configuration is locked  (enter "shut" to unlock it)
    Issuer name: CN=ioscs,L=Santa Cruz,C=US
    CA cert fingerprint: 42308002 188180FC 9265946F FDC68A52
    Granting mode is: auto
    Last certificate issued serial number (hex): 2
    CA certificate expiration timer: 20:22:55 PST Apr 26 2013
    CRL NextUpdate timer: 20:27:46 PST May 11 2010
    Current primary storage dir: nvram:
    Database Level: Complete - all issued certs written as <serialnum>.cer
    Redundancy configured.  This is standby.
```

The following example shows that the certificate server MyCS has rollover configured. Rollover has not yet occurred. The rollover status "pending" and rollover CA certificate timer show when the rollover timer will be triggered. When this timer is triggered, the shadow certificate will become the active certificate and the previously active certificate will be deleted.

```
Router# show crypto pki server
Certificate Server routercs:
   Status: enabled, configured
   Issuer name: CN=walnutcs
   CA cert fingerprint: 800F5944 74337E5B C2DF6C52 9A7B1BDB
   Granting mode is: auto
   Last certificate issued serial number: 0x6
   CA certificate expiration timer: 22:10:29 GMT Jan 29 2007
   CRL NextUpdate timer: 21:50:56 GMT Mar 5 2004
   Current storage dir: nvram:
   Database Level: Minimum - no cert data written to storage
    Rollover status: pending
    Rollover CA certificate timer: 20:34:23 GMT Jan 8 2005
```

The following example shows that the certificate server MyCS has rollover configured. The rollover time has occurred and the rollover certificate is available. The status shows the rollover certificate fingerprint and rollover CA certificate expiration timer information.

```
Router# show crypto pki server

Certificate Server routercs:
   Status: enabled, configured
   Issuer name: CN=walnutcs
   CA cert fingerprint: 800F5944 74337E5B C2DF6C52 9A7B1BDB
   Granting mode is: auto
   Last certificate issued serial number: 0x7
   CA certificate expiration timer: 22:10:29 GMT Jan 29 2007
   CRL NextUpdate timer: 21:50:56 GMT Mar 5 2004
```

```
   Current storage dir: nvram:
   Database Level: Minimum - no cert data written to storage
    Rollover status: available for rollover
    Rollover CA cert fingerprint: 6AAF5944 74227A5B 23DF3E52 9A7F1FEF
    Rollover CA certificate expiration timer: 22:10:29 GMT Jan 29 2017
```

The following example shows a certificate server (CS) that has been prevented from entering rollover state because the Cisco IOS configuration cannot be saved.

```
Router# show crypto pki server
Certificate Server routercs:
   Status: enabled, configured
   Issuer name: CN=walnutcs
   CA cert fingerprint: 800F5944 74337E5B C2DF6C52 9A7B1BDB
   Granting mode is: auto
   Last certificate issued serial number: 0x7
   CA certificate expiration timer: 22:10:29 GMT Jan 29 2007
   CRL NextUpdate timer: 21:50:56 GMT Mar 5 2004
   Current storage dir: nvram:
   Database Level: Minimum - no cert data written to storage
    Rollover status: disabled, unable to save configuration
    Rollover CA cert fingerprint: 6AAF5944 74227A5B 23DF3E52 9A7F1FEF
    Rollover CA certificate expiration timer: 22:10:29 GMT Jan 29 2017
```

Related Commands

Command	Description
crypto pki server	Enables a Cisco IOS certificate server and enter certificate server configuration mode.

show crypto pki server certificates

To display certificate information for all certificates of the specified certificate server, use the **show crypto pki server certificates** command in privileged EXEC mode.

show crypto pki server *cs-label* **certificates** [*start-number* [*end-number*]] [**expired**]

Syntax Description

cs-label	Name of the certificate server. The name must match the name specified through the **crypto pki server** command.
start -number	(Optional) The beginning of the certificate serial number range to display. If only the starting certificate serial number is indicated, information for only the designated certificate is shown if available.
end-number	(Optional) The end of the certificate serial number range to display.
expired	(Optional) Displays the expired certificates.

Command Default

Certificate information is shown for all serial numbers for the specified certificate server, from the first serial number in the certificate database to the last serial number in the certificate database.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

This command displays available information on each certificate for the specified certificate server. If the certificate information is not available, the output displayed reads as "<cert not available>". If the certificate information is incomplete, or if it has been corrupted, the output displayed reads as "<certificate incomplete or corrupted>".

You may display information on all the certificates in the certificate database, one certificate in the certificate database, or a range of certificates in the certificate database by setting the *start-number* and *end-number* arguments.

Examples

```
The following example shows the listing of all certificates in the certificate database for
 the certificate server "mycs":
Router#
show crypto pki server mycs certificates
Serial   Issued date               Expire date               Subject Name
1        02:09:09 PST Jan 22 2007  02:09:09 PST Jan 21 2010  cn=company
2        02:57:59 PST Jan 22 2007  02:57:59 PST Jan 22 2008  hostname=client.example.com
3        03:00:12 PST Jan 22 2007  03:00:12 PST Jan 22 2008  hostname=client.example.com
4        19:53:07 PST Jan 18 2007  19:53:07 PST Jan 19 2007  hostname=client.example.com
5        <cert not available>
6        <cert not available>
7        <cert not available>
8        02:57:59 PST Jan 22 2007  02:57:59 PST Jan 22 2008  hostname=client.example.com
```

```
9        <Certificate incomplete or corrupted>
A        <cert not available>
```

B <cert not available>

```
The following example shows the information for certificate serial number 3 in the certificate
 database for the certificate server "mycs":
Router#
show crypto pki server mycs certificates start 3
Serial   Issued date               Expire date               Subject Name
3        03:00:12 PST Jan 22 2007  03:00:12 PST Jan 22 2008  hostname=client.example.com
```

```
The following example shows the information for certificate serial number 3 through
certificate serial number 7 in the certificate database for the certificate server "mycs":
Router#
show crypto pki server mycs certificates start 3 end 7
show crypto pki server mycs certificates
Serial   Issued date               Expire date               Subject Name
3        03:00:12 PST Jan 22 2007  03:00:12 PST Jan 22 2008  hostname=client.example.com
4        19:53:07 PST Jan 18 2007  19:53:07 PST Jan 19 2007  hostname=client.example.com
5        <cert not available>
6        <cert not available>
7        <cert not available>
```

Related Commands

Command	Description
crypto pki server	Enables a Cisco IOS certificate server and enters certificate server configuration mode.
show crypto pki server	Displays the current state and configuration of the certificate server.
show crypto pki server crl	Displays the current status of the CRL.

show crypto pki server crl

To display information regarding the status of the current certificate revocation list (CRL), use the **show crypto pki server crl** command in privileged EXEC mode.

show crypto pki server *cs-label* **crl**

Syntax Description

cs-label	Name of the certificate server. The name must match the name specified via the **crypto pki server** command.

Command Default

None.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

CRLs are issued once every specified time period via the **lifetime crl** command. It is the responsibility of the network administrator to ensure that the CRL is available from the location that is specified via the **cdp-url** command. To access information, such as the lifetime and location of the CRL, use the **show crypto pki server crl**command.

Examples

The following example shows how to access CRL information for the certificate server "mycs":

```
Router# show crypto pki server mycs crl
```

Related Commands

Command	Description
cdp-url	Specifies a CDP to be used in certificates that are issued by the certificate server.
crypto pki server	Enables a Cisco IOS certificate server and enter certificate server configuration mode.
lifetime crl	Defines the lifetime of the CRL that is used by the certificate server.

show crypto pki server requests

To display all outstanding certificate enrollment requests, use the **show crypto pki server requests**command in privileged EXEC mode.

show crypto pki server *cs-label* **requests**

Syntax Description

cs-label	Name of the certificate server. The name must match the name specified via the **crypto pki server** command.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

A certificate enrollment request functions as follows:

- The certificate server receives the enrollment request from an end user, and the following actions occur:
  - A request entry is created in the enrollment request database with the initial state. (See the **show pki server** command for a complete list of certificate enrollment request states.)
  - The certificate server refers to the command-line interface (CLI) configuration (or the default behavior any time a parameter is not specified) to determine the authorization of the request. Thereafter, the state of the enrollment request is updated in the enrollment request database.
- At each Simple Certificate Enrollment Protocol (SCEP) query for a response, the certificate server examines the current request and performs one of the following actions:
  - Responds to the end user with a "pending" or "denied" state.
  - Forwards to the request to the certification authority (CA) core, where it will generate and sign the appropriate certificate, store the certificate in the enrollment request database, and return the request to the built-in certificate server SCEP server, who will reply to the end user with the certificate on the next SCEP request.

If the connection of the client has closed, the certificate server will wait for the client user to request another certificate.

All enrollment requests transitions through the certificate enrollment states that are defined in the table below.

Table 69: Certificate Enrollment Request State Descriptions

Certificate Enrollment State	Description
authorized	The certificate server has authorized the request.

Certificate Enrollment State	Description
denied	The certificate server has denied the request for policy reasons.
granted	The CA core has generated the appropriate certificate for the certificate request.
initial	The request has been created by the SCEP server.
malformed	The certificate server has determined that the request is invalid for cryptographic reasons.
pending	The enrollment request must be manually accepted by the network administrator.

Examples

The following example shows output for the certificate server "certsrv1," which has a pending certificate enrollment request:

```
Router# show crypto pki server certsrv1 requests
   Enrollment Request Database:
   ReqID  State      Fingerprint                       SubjectName
   --------------------------------------------------------------
   1      pending    0A71820219260E526D250ECC59857C2D serialNumber=2326115A+hostname=831.
```

The following example shows the output for shadow public key infrastructure (PKI) certificate info requests:

```
Router# show crypto pki server mycs requests
Enrollment Request Database:

Subordinate CA certificate requests:
  ReqID  State      Fingerprint                       Fingerprint(unsigned)
SubjectName
--------------------------------------------------------------------------------------------------
RA certificate requests:
  ReqID  State      Fingerprint                       Fingerprint(unsigned)
SubjectName

--------------------------------------------------------------------------------------------------
Router certificates requests:
  ReqID  State      Fingerprint                       Fingerprint(unsigned)
SubjectName
--------------------------------------------------------------------------------------------------
1      pending    9A0A1392A438AF02E6DD720A9890C449  2991D157A1686BEF65B075D138FEE9F9
hostname=middlerouter1

  Router rollover certificates requests:
  ReqID  State      Fingerprint                       SubjectName
  --------------------------------------------------------------
  2      pending    B69062E0E47198E5BFA426AF07FE3A4B hostname=client
```

Related Commands

Command	Description
crypto pki server	Enables a Cisco IOS certificate server and enters PKI configuration mode.

show crypto pki timers

To display the status of the managed timers that are maintained by Cisco IOS for public key infrastructure (PKI), use the **show crypto pki timers**command in EXEC mode.

show crypto pki timers

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
12.2(8)T	The **show crypto ca timers**command was introduced.
12.3(7)T	This command replaced the **show crypto ca timers** command.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.

Usage Guidelines

For each timer, this command displays the time remaining before the timer expires. It also associates trustpoint certification authorities (CAs), except for certificate revocation list (CRL) timers, by displaying the CRL distribution point.

Examples

The following example is sample output for the **show crypto pki timers** command:

```
Router# show crypto pki timers
PKI Timers
| 4d15:13:33.144
 | 4d15:13:33.144  CRL http://msca-root.cisco.com/CertEnroll/msca-root.crl
 |328d11:56:48.372  RENEW msroot
 | 6:43.201  POLL verisign
```

Related Commands

Command	Description
auto-enroll	Enables autoenrollment.
crypto pki trustpoint	Declares the CA that your router should use.

show crypto pki timer detail

To display the absolute time stamp of the timers that are maintained by Cisco IOS for public key infrastructure (PKI) in ISO8601 format , use the **show crypto pki timer detail** command in EXEC mode.

show crypto pki timer detail

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.1	This command was introduced.

Examples

The following example is sample output for the **show crypto pki timer detail** command:

```
Router # show crypto pki timer detail
PKI Timers
|        1:44.647  (2018-06-03T07:09:19Z)
  |        1:44.647  (2018-06-03T07:09:19Z) SHADOW test
  |       11:11.420  (2018-06-03T07:18:46Z) SESSION CLEANUP
Expiry Alert Timers
|303d23:57:20.646  (2019-04-03T07:04:55Z)
  |303d23:57:20.646  (2019-04-03T07:04:55Z) ID(test)
  |303d23:57:21.325  (2019-04-03T07:04:56Z) CS(test)
Trustpool Timers
|3693d22:22:24.339  (2028-07-14T05:29:59Z)
  |3693d22:22:24.339  (2028-07-14T05:29:59Z) TRUSTPOOL
CS Timers
|     5:57:21.277  (2018-06-03T13:04:56Z)
  |     5:57:21.277  (2018-06-03T13:04:56Z) CS CRL UPDATE
  |363d23:57:20.995  (2019-06-02T07:04:55Z) CS CERT EXPIRE
```

show crypto pki token

To display the Cisco IOS public key infrastructure (PKI) tokens that are configured on the router, use the **show crypto pki token** command in privileged EXEC mode.

show crypto pki token [*name*]

Syntax Description

name	(Optional) Specifies the name of the token.

Command Default

If the *name* argument is not specified, command output is displayed for all PKI tokens.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(15)T	This command was introduced.

Examples

The following is sample output from the **show crypto pki token** command:

```
Router# show crypto pki token
Configuration for token usbtoken0:
Automatic login enabled.
Removal timeout 60 seconds
Configuration for token default:
Secondary Config file "BIFT.CFG"
```

The table below describes the significant fields shown in the display.

Table 70: show crypto pki token Field Descriptions

Field	Description
Automatic login enabled	Indicates that the crypto PKI token is configured to log in automatically.
Removal timeout 60 seconds	Indicates that the router waits for 60 seconds before removing the Rivest, Shamir, and Adelman (RSA) keys that are stored in the eToken.
Secondary Config file	Indicates that the specified file will be merged with the running configuration after the eToken is logged into the router.

Related Commands

Command	Description
crypto pki token removal timeout	Sets the time interval that the router waits before removing the RSA keys that are stored in the eToken.
crypto pki token secondary config	Merges a specified file with the running configuration after the eToken is logged into the router.

show crypto pki trustpoints

To display the trustpoints that are configured in the router, use the **show crypto pki trustpoints**command in privileged EXEC or user EXEC mode.

show crypto pki trustpoints [{**status** | *label* [**status**]}]

Syntax Description

status	(Optional) Trustpoint status.
label	(Optional) Trustpoint name.

Command Default

If the *label* argument (trustpoint name) is not specified, command output is displayed for all trustpoints.

Command Modes

Privileged EXEC (#)
User EXEC (>)

Command History

Release	Modification
12.2(8)T	The **show crypto ca trustpoints** command was introduced.
12.3(7)T	This command replaced the **show crypto ca trustpoints** command.
12.3(11)T	The **status** keyword and *label* argument were added.
12.3(14)T	The command output was modified to include persistent self-signed certificate parameters.
12.4(2)T	The command output was modified to include shadow, or rollover, public key infrastructure (PKI) certificate availability and Simple Certificate Enrollment Protocol (SCEP) capabilities.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(22)T	The command output was modified to include X.509 certificate IP address extension information.

Examples

The following is sample output from the **show crypto pki trustpoints** command:

```
Router# show crypto pki trustpoints
Trustpoint bo:
    Subject Name:
    CN = host Certificate Manager
     O = company.com
     C = US
          Serial Number:01
    Certificate configured.
    CEP URL:http://host
    CRL query url:ldap://host
```

The following is sample output from the **show crypto pki trustpoints** command when a persistent self-signed certificate has been configured:

```
Router# show crypto pki trustpoints
Trustpoint local:
    Subject Name:
    serialNumber=C63EBBE9+ipaddress=10.3.0.18+hostname=test.company.com
          Serial Number: 01
    Persistent self-signed certificate trust point
```

The following output shows that a shadow PKI certificate is available and shows the SCEP capabilities:

```
Router# show crypto pki trustpoints
Trustpoint vpn:
   Subject Name:
   cn=Company SSL CA
   o=Company
   Serial Number: 0FFEBBDC1B6F6D9D0EA7875875E4C695
   Certificate configured.
   Rollover certificate configured.
   Enrollment Protocol:
   SCEPv1, PKI Rollover
```

The following output using the **status** keyword shows that the trustpoint is configured in query mode and is currently trying to query the certificates (the certificate authority (CA) certificate and the router certificate are both pending):

```
Router# show crypto pki trustpoints status
Trustpoint yni:
  Issuing CA certificate pending:
    Subject Name:
     cn=r1 Cert Manager,ou=pki,o=company.com,c=country
    Fingerprint: C21514AC 12815946 09F635ED FBB6CF31
  Router certificate pending:
    Subject Name:
     hostname=host.company.com,o=company.com
  Next query attempt:
    52 seconds
```

The following output using the **status** keyword shows that the trustpoint has been authenticated:

```
Router# show crypto pki trustpoints status
Trustpoint yni:
  Issuing CA certificate configured:
    Subject Name:
     cn=r1 Cert Manager,ou=pki,o=company.com,c=country
    Fingerprint: C21514AC 12815946 09F635ED FBB6CF31
  State:
    Keys generated ..... No
    Issuing CA authenticated ..... Yes
    Certificate request(s) ..... None
```

The following output using the **status** keyword shows that the trustpoint is enrolling and that two of the certificate requests are pending (Signature and Encryption):

```
Router# show crypto pki trustpoints status
Trustpoint yni:
  Issuing CA certificate configured:
    Subject Name:
     cn=r1 Cert Manager,ou=pki,o=company.com,c=country
```

```
    Fingerprint: C21514AC 12815946 09F635ED FBB6CF31
  Router Signature certificate pending:
    Requested Subject Name:
     hostname=host.company.com
    Request Fingerprint: FAE0D74E BB844EA1 54B26698 56AB42EC
    Enrollment polling: 1 times (9 left)
    Next poll: 32 seconds
  Router Encryption certificate pending:
    Requested Subject Name:
     hostname=host.company.com
    Request Fingerprint: F4E815DB D9D9B60F 9B5B1724 3E155DBF
    Enrollment polling: 1 times (9 left)
    Next poll: 44 seconds
  Last enrollment status: Pending
  State:
    Keys generated ..... Yes (Signature, Encryption)
    Issuing CA authenticated ..... Yes
    Certificate request(s) ..... Pending
```

The following output using the **status** keyword shows that enrollment has succeeded and that two router certificates have been granted (Signature and Encryption):

```
Router# show crypto pki trustpoints status

Trustpoint yni:
  Issuing CA certificate configured:
    Subject Name:
     cn=r1 Cert Manager,ou=pki,o=company.com,c=country
    Fingerprint: C21514AC 12815946 09F635ED FBB6CF31
  Router Signature certificate configured:
    Subject Name:
     hostname=host.company.com,o=company.com
    Fingerprint: 8A370B8B 3B6A2464 F962178E 8385E9D6
  Router Encryption certificate configured:
    Subject Name:
     hostname=host.company.com,o=company.com
    Fingerprint: 43A03218 C0AFF844 AE0C162A 690B414A
  Last enrollment status: Granted
  State:
    Keys generated ..... Yes (Signature, Encryption)
    Issuing CA authenticated ..... Yes
    Certificate request(s) ..... Yes
```

The following output using the **status** keyword shows that trustpoint enrollment has been rejected:

```
Router# show crypto pki trustpoints status
Trustpoint yni:
  Issuing CA certificate configured:
    Subject Name:
     cn=r1 Cert Manager,ou=pki,o=company.com,c=country
    Fingerprint: C21514AC 12815946 09F635ED FBB6CF31
  Last enrollment status: Rejected
  State:
    Keys generated ..... Yes (General Purpose)
    Issuing CA authenticated ..... Yes
    Certificate request(s) ..... None
```

The following output using the **status** keyword shows that enrollment has succeeded and that the router is configured for autoenrollment using a regenerated key. In addition, the running configuration has been modified so that it will not be saved automatically after autoenrollment.

```
Router# show crypto pki trustpoints status
```

```
Trustpoint yni:
  Issuing CA certificate configured:
    Subject Name:
     cn=r1 Cert Manager,ou=pki,o=company.com,c=country
    Fingerprint: C21514AC 12815946 09F635ED FBB6CF31
  Router General Purpose certificate configured:
    Subject Name:
     hostname=host.company.com,o=company.com
    Fingerprint: FC365F95 E24D4B55 81347510 10FFE331
  Last enrollment status: Granted
  Next enrollment attempt:
    01:58:25 PST Feb 14 2004
    * A new key will be generated *
    * Configuration will not be saved after enrollment *
  State:
    Keys generated ..... Yes (General Purpose)
    Issuing CA authenticated ..... Yes
    Certificate request(s) ..... Yes
```

The following output displays SIGNED PKCS10 fingerprint irrespective of being enrolled through a CA server or a RA server. Additionally, it displays SIGNED PKCS10 SHA2 fingerprint along with SHA1 SIGNED PKCS10 fingerprint, and MD5 SIGNED PKCS10 fingerprint.

```
Router# show crypto pki trustpoints test status
Trustpoint test:
  Issuing CA certificate configured:
    Subject Name:
     cn=ca
     Fingerprint MD5: F6345AE9 3A554053 5F009F1A 4DD8F572
     Fingerprint SHA1: 2E46DB45 03B2968A FB0B79B0 56C8E106 DB12529A
    Router General Purpose certificate pending:
Requested Subject Name:
     hostname=Router,cn=test
    Request Fingerprint MD5: CD76F722 60617951 DE5AF18D 3FC74A2A
    Request Fingerprint SHA1: 10A04557 9B5613B2 D0DD8AA5 72B0601B 05940E3D
   Request Fingerprint SHA2: 3E96A4CE 9824A2D4 07344A63 3D5EF642 7C53ADD0 B0C7B521 61DA06D8
 289FA221
    Request Fingerprint MD5 (unsigned): D68D4DF6 84A58B40 76EBD026 40CE42B3
Enrollment polling: 0 times (999 left)
    Next poll: 38 seconds
  Last enrollment status: Pending
  State:
    Keys generated ..... Yes (General Purpose, non-exportable)
    Issuing CA authenticated ..... Yes
    Certificate request(s) ..... Pending
```

The table below describes the significant fields shown in the display.

Table 71: show crypto pki trustpoints Field Descriptions

Field	Description
Trustpoint	Name of the trustpoint.
Issuing CA certificate pending	The CA certificate is being retrieved (query mode).
Issuing CA certificate [not] configured	A CA certificate is [not] configured.
Subject Name	Subject name of the indicated certificate.
Next query attempt	Time until the next query attempt (query mode).

Field	Description
Router certificate pending/Router [key usage] certificate pending	The trustpoint is attempting to obtain the certificate from the CA server (through query mode or enrollment).
Router [key usage] certificate configured	Certificate of the specified key usage is configured.
Requested Subject Name	Subject name used in the enrollment request (Public Key Cryptography Standards 10 [PKCS10]).
Fingerprint MD5/SHA1	Fingerprint of the indicated certificate (Message Digest 5 [MD5] or Secure Hash Algorithm 1 [SHA]1).
Request Fingerprint MD5/SHA1	Fingerprint of the PKCS10 enrollment request (MD5/SHA1).
Enrollment polling: [polled] times ([remaining] left)/Next poll: in seconds	Number of SCEP polling attempts that have been made and that remain before the router gives up/Time until the next polling attempt.
Last enrollment status: Pending/Granted/Rejected/Failed	Last enrollment attempt status (pending, granted, rejected, or failed).
Next enrollment attempt: *time* (Optional) A new key will be generated. (Optional) Configuration will not be saved after enrollment.	The trustpoint is configured autoenrollment and the autoenrollment will happen at *time.* (Optional) The trustpoint is configured to generate a new key when autoenrollment occurs. (Optional) The running configuration is "dirty," so the configuration will not be saved automatically after autoenrollment.
State	Current state of the trustpoint.
Keys generated	"Yes or No" and the key usage (General Purpose or Signature, Encryption).
Issuing CA authenticated	"Yes or No" if crypto CA authentication has been done successfully.
Certificate request(s)	Progress of current enrollment: "Pending," "Yes," (complete), or "None" (not in progress).

Related Commands

Command	Description
crypto pki trustpoint	Declares the CA that your router should use.

show crypto pki trustpool

To display the public key infrastructure (PKI) trustpool certificates of the router, use the **show crypto pki trustpool** command in privileged EXEC or user EXEC mode.

show crypto pki trustpool [**policy**]

Syntax Description

policy	(Optional) Displays the PKI trustpool policy.

Command Modes

User EXEC (>) and Privileged EXEC (#)

Command History

Release	Modification
15.2(2)T	This command was introduced.
15.1(1)SY	This command was integrated into Cisco IOS 15.1(1)SY.

Usage Guidelines

If the **show crypto pki trustpool** is used without the **policy** keyword, then the PKI certificates of the router are displayed in a verbose format.

If the **show crypto pki trustpool** is used with the **policy** keyword, then the PKI trustpool of the router is displayed.

Examples

The following **show crypto pki trustpool policy** command output displays the default PKI trustpool policy:

```
Router# show crypto pki trustpool policy

Chain validation will stop at the first CA certificate in the pool
   Trustpool CA certificates will expire 12:58:31 PST Apr 5 2012
   Trustpool policy revocation order:      crl
   Certficate matching is disabled
   Policy Overrides:
```

The following **show crypto pki trustpool** command output displays the certificates in PKI trustpool:

Note The command output in this example is abridged because it is verbose.

```
Router# show crypto pki trustpool

CA Certificate
  Status: Available
  Version: 3
  Certificate Serial Number (hex): 00D01E474000000111C38A964400000002
  Certificate Usage: Signature
  Issuer:
    cn=DST Root CA X3
    o=Digital Signature Trust Co.
  Subject:
    cn=Cisco SSCA
```

```
    o=Cisco Systems
  CRL Distribution Points:
    http://crl.identrust.com/DSTROOTCAX3.crl
  Validity Date:
    start date: 12:58:31 PST Apr 5 2007
    end   date: 12:58:31 PST Apr 5 2012

CA Certificate
  Status: Available
  Version: 3
  Certificate Serial Number (hex): 6A6967B3000000000003
  Certificate Usage: Signature
  Issuer:
    cn=Cisco Root CA 2048
    o=Cisco Systems
  Subject:
    cn=Cisco Manufacturing CA
    o=Cisco Systems
  CRL Distribution Points:
    http://www.cisco.com/security/pki/crl/crca2048.crl
  Validity Date:
    start date: 14:16:01 PST Jun 10 2005
    end   date: 12:25:42 PST May 14 2029
```

Related Commands

Command	Description
cabundle url	Configures the URL from which the PKI trustpool CA bundle is downloaded.
chain-validation	Enables chain validation from the peer's certificate to the root CA certificate in the PKI trustpool.
crl	Specifes the CRL query and cache options for the PKI trustpool.
crypto pki trustpool import	Manually imports (downloads) the CA certificate bundle into the PKI trustpool to update or replace the existing CA bundle.
crypto pki trustpool policy	Configures PKI trustpool policy parameters.
default	Resets the value of a ca-trustpool configuration subcommand to its default.
match	Enables the use of certificate maps for the PKI trustpool.
ocsp	Specifies OCSP settings for the PKI trustpool.

Command	Description
revocation-check	Disables revocation checking when the PKI trustpool policy is being used.
show	Displays the PKI trustpool policy of the router in ca-trustpool configuration mode.
source interface	Specifies the source interface to be used for CRL retrieval, OCSP status, or the downloading of a CA certificate bundle for the PKI trustpool.
storage	Specifies a file system location where PKI trustpool certificates are stored on the router.
vrf	Specifies the VRF instance to be used for CRL retrieval.

show crypto route

To display routes that are created through IPsec via Reverse Route Injection (RRI) or Easy VPN virtual tunnel interfaces (VTIs) in one table, use the **show crypto route** command in privileged EXEC mode.

show crypto route

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(15)T	This command was introduced.
15.1(3)S	This command was integrated into Cisco IOS Release 15.1(3)S.

Examples

The following example displays routes that were created through IPSec using RRI and VTIs:

```
Router# show crypto route
VPN Routing Table: Shows RRI and VTI created routes
Codes: RRI - Reverse-Route, VTI- Virtual Tunnel Interface
        S - Static Map ACLs
Routes created in table GLOBAL DEFAULT
192.168.6.2/255.255.255.255 [0/0] via 10.0.0.133
                                  on Virtual-Access3 RRI
10.1.1.0/255.255.255.0 [10/0] via Virtual-Access2 VTI
192.168.6.1/255.255.255.255 [0/0] via Virtual-Access2 VTI
```

The fields in the above display are self-explanatory.

Related Commands

Command	Description
reverse-route	Creates source proxy information for a crypto map entry.
set reverse-route	Defines a distance metric for each static route or tags a RRI-created route.

show crypto ruleset

To display information about crypto rules on outgoing packets, use the **show crypto ruleset** command in privileged EXEC mode.

show crypto ruleset [{**detail** | **platform**}]

Syntax Description

detail	(Optional) Displays the directional mode of the IPsec security association (SA).
platform	(Optional) Displays information about IPsec crypto rules for hardware and software platforms.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(20)T	This command was introduced.
15.2(3)T	This command was modified. The output was enhanced to display crypto rules on outgoing IPv6 packets.
Cisco IOS XE Release 3.7S	This command was modified. The **platform** keyword was added. The output was enhanced to display information about the IPsec crypto rules for hardware and software platforms.

Usage Guidelines

The **show crypto ruleset platform** command displays the output from the following **show** commands, as listed in the order below:

- **show platform software ipsec f0 access-list all**
- **show platform hardware qfp active classification class-group-manager class-group client ipsec all**

Examples

Assuming that the key server (KS) has the following GET VPN IPv4 group access control list (ACL) policy, the example that follows the policy shows information about the crypto rules on outgoing packets:

```
ip access-list extended get-acl
 deny   ospf any any
 deny   ip any host 192.168.2.5
 deny   ip host 192.168.2.5 any
 permit ip any any

crypto gdoi group GETVPN
 identity number 1111
 server local
 rekey authentication mypubkey rsa mykeys
 rekey transport unicast
 sa ipsec 1
 profile GET_PROFILE
 match address ipv4 get-acl
 replay time window-size 10
 address ipv4 192.168.2.5
```

```
Device# show crypto ruleset

Mtree:
  11 192.168.2.1/500 ANY Forward, Forward
  11 192.168.2.1/4500 ANY Forward, Forward
  11 ANY/848 ANY Forward, Forward
  11 ANY ANY/848 Forward, Forward
  59 ANY ANY DENY
 IP ANY 192.168.2.5 DENY
 IP 192.168.2.5 ANY DENY
 IP ANY ANY Discard, Encrypt
```

The following example shows the directional mode of the IPsec SA for the above policy:

```
Device# show crypto ruleset detail

Mtree:
 199 VRF 0  11 192.168.2.1/500 ANY Forward, Forward
 299 VRF 0  11 192.168.2.1/4500 ANY Forward, Forward
 200000199 VRF 0  11 ANY/848 ANY Forward, Forward
 200000299 VRF 0  11 ANY ANY/848 Forward, Forward
 1000000000000201 VRF 0  59 ANY ANY DENY -> 1000000009999900
 1000000000000301 VRF 0 IP ANY 192.168.2.5 DENY -> 1000000009999900
 1000000000000401 VRF 0 IP 192.168.2.5 ANY DENY -> 1000000009999900
 1000000000000501 VRF 0 IP ANY ANY Discard, Encrypt
```

Assuming that KS has the following GET VPN IPv6 group ACL policy, the example that follows the policy shows information about the crypto rules on outgoing packets:

```
ipv6 access-list ACL_GETV6_ANY
 permit ipv6 any any

crypto gdoi group ipv6 GETV6
 identity number 1111
 server local
 rekey authentication mypubkey rsa GETKEY
 rekey transport unicast
 sa ipsec 1
 profile IPSEC_PROF_GETV6
 match address ipv6 ACL_GETV6_ANY
 replay time window-size 10
 address ipv4 192.168.2.2


Device# show crypto ruleset

Mtree:
IPv6:
0/0/1/1
 17 2001:DB8::A8BB:CCFF:FE01:2C02 500 ANY Forward, Forward
0/0/2/1
 17 2001:DB8::A8BB:CCFF:FE01:2C02 4500 ANY Forward, Forward
0/2/1/1
 17 ANY 848 ANY Forward, Forward
0/2/2/1
 17 ANY ANY 848 Forward, Forward
10/0/2/0
 IPV6 ANY ANY Discard, Encrypt
Mtree:
  11 192.168.2.3/500 ANY Forward, Forward
  11 192.168.2.3/4500 ANY Forward, Forward
```

```
  11 ANY/848 ANY Forward, Forward
  11 ANY ANY/848 Forward, Forward
  01 192.168.2.3 192.168.2.4 Discard, Encrypt
  01 192.168.2.4 192.168.2.3 Discard, Encrypt
```

The following example shows the directional mode of the IPsec SA for the above policy:

```
Device# show crypto ruleset detail

IPv6:
0/0/1/1
 17 2001:DB8::A8BB:CCFF:FE01:2C02 500 ANY Forward, Forward
0/0/2/1
 17 2001:DB8::A8BB:CCFF:FE01:2C02 4500 ANY Forward, Forward
0/2/1/1
 17 ANY 848 ANY Forward, Forward
0/2/2/1
 17 ANY ANY 848 Forward, Forward
10/0/2/0
 IPV6 ANY ANY Discard, Encrypt
Mtree:
 199 VRF 0  11 192.168.2.3/500 ANY Forward, Forward
 299 VRF 0  11 192.168.2.3/4500 ANY Forward, Forward
 200000199 VRF 0  11 ANY/848 ANY Forward, Forward
 200000299 VRF 0  11 ANY ANY/848 Forward, Forward
 1000000000000201 VRF 0  01 192.168.2.3 192.168.2.4 Discard, Encrypt
 1000000000000301 VRF 0  01 192.168.2.4 192.168.2.3 Discard, Encrypt
```

The following table describes the significant fields shown in the displays.

Table 72: show crypto ruleset Field Descriptions

Field	Description
59 ANY ANY DENY	• 59—Hexadecimal value of the Open Shortest Path First (OSPF) protocol. • First ANY—Any source IP address. • Second ANY—Any destination IP address. • DENY packets matching this rule will not be encrypted.
11 ANY/848 ANY/848 DENY	• 11—Hexadecimal value of the UDP. • First ANY/848—Any source IP address that has a source port 848. • Second ANY/848—Any destination IP address having a destination port 848. • DENY—Packets matching this rule will not be encrypted.
IP ANY ANY IPSec SA Passive	• Policy of "IP packets with any source or destination address or port" is in IPsec security association (SA) passive mode—Receives clear and encrypted packets; sends only encrypted packets.

Field	Description
IP ANY ANY IPSec Cryptomap	• Policy of "IP packets with any source or destination address or port" is created by an IPsec crypto map—Receives or sends only encrypted packets.
20000001000019 59 ANY ANY DENY -> 20000001999999	• The first number is the priority number of the policy or rule. • The second number is the deny priority number of the policy or rule. **Note** These numbers are internal data values and are generally used by developers.

show crypto session

To display status information for active crypto sessions, use the **show crypto session** command in privileged EXEC mode.

show crypto session [{**groups** | **interface** *type* [{**brief** | **detail**}] | **isakmp** [{**group** *group-name* | **profile** *profile-name*}] [{**brief** | **detail**}] | [{**local** | **remote**}] [{*ip-address ipv6-address*}] [**port** *port-number*] | [**fvrf** *fvrf-name*] [**ivrf** *ivrf-name*] [{**brief** | **detail** }] | **summary** *group-name* | **username** *username*}]

IPsec and IKE Stateful Failover Syntax
show crypto session [{**active** | **standby**}]

Syntax Description

groups	(Optional) Displays crypto session group usage for all groups.
interface *type*	(Optional) Displays crypto sessions on the connected interface. • The *type* value is the type of interface connection.
brief	(Optional) Provides brief information about the session, such as the peer IP address, interface, username, group name or phase1 ID, length of session uptime, and current session status (up/down).
detail	(Optional) Provides detailed information about the session, such as the capability of the Internet Key Exchange (IKE) security association (SA), connection ID, remaining lifetime of the IKE SA, inbound or outbound encrypted or decrypted packet number of the IP security (IPsec) flow, dropped packet number, and kilobyte-per-second lifetime of the IPsec SA.
isakmp group *group-name*	(Optional) Displays crypto sessions using the Internet Security Association and Key Management Protocol (ISAKMP) group. • The *group-name* value is the name of the group.
isakmp profile *profile-name*	(Optional) Displays crypto sessions using the ISAKMP profile. • The *profile-name* value is the name of the profile.
local	(Optional) Displays status information about crypto sessions of a local crypto endpoint.
remote	(Optional) Displays status information about crypto sessions of a remote session.
ip-address	IP address of the local or remote crypto endpoint.
ipv6-address	IPv6 address of the local or remote crypto endpoint.
port *port-number*	(Optional) Displays status information about the port of the local crypto endpoint. • The *port-number* value can be from 1 to 65535. The default value is 500.

fvrf *fvrf-name*	(Optional) Displays status information about the front door virtual routing and forwarding (fVRF) session. • The *fvrf-name* value is the name of the fVRF session.
ivrf *ivrf-name*	(Optional) Displays status information about the inside VRF (iVRF) session. • The *ivrf-name* value is the name of the iVRF session. **Note** The iVRF session can have an empty value when VRF-aware IPsec (fVRF and iVRF) uses IPsec protected tunnels sharing the same tunnel source and the same IPsec profile. This scenario is valid for the following conditions: • IPsec protected multipoint generic routing encapsulation (mGRE) • IPsec protected Point-to-Point GRE tunnels
summary *group-name*	(Optional) Displays a list of crypto session groups and associated group members.
username *username*	(Optional) Displays the crypto session for the specified extended authentication (XAUTH), public key infrastructure (PKI), or authentication, authorization, and accounting (AAA) username.
active	(Optional) Displays all crypto sessions in the active state.
standby	(Optional) Displays all crypto sessions that are in the standby state.

Command Default

When no optional keywords and arguments are specified, all existing sessions are displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.3(11)T	This command was modified. The **active** and **standby** keywords were added.
12.4(4)T	This command was modified. IPv6 address information was added to the command output.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.4(11)T	This command was modified. The **brief**, **groups**, **interface** *interface-type*, **isakmp group** *group-name*, **isakmp profile** *profile-name*, **summary**, and **username** *username* keywords and arguments were added. The **show crypto session** output was updated to include the username, ISAKMP profile, ISAKMP group, assigned address, and session uptime.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

This command lists all the active VPN sessions and the IKE and IPsec SAs for each VPN session. The listing includes the following information:

- Interface.
- IKE peer description, if available.
- IKE SAs that are associated with the peer by which the IPsec SAs are created.
- IPsec SAs serving the flows of a session.

Multiple IKE or IPsec SAs may be established for the same peer (for the same session). In such a case, IKE peer descriptions are repeated with different values for the IKE SAs associated with the peer and for the IPsec SAs serving the flows of the session.

IPv6 does not support the **fvrf** and **ivrf** keywords and the *vrf-name* argument.

Note The Session status field displays UP-NO-IKE and IP-IDLE value when different Inside VRFs (IVRFs) are configured for different shared protection tunnels in a DMVPN configuration. This is because the interface-VRF field is not known until the IPsec SAs are established and debugging filters based on IVRF will not work. Secondly, the **tunnel protection shared** command will not display the correct VRF since shared tunnel is not established with the interface-VRF.

Examples

The following example shows the status information for all active crypto sessions:

```
Device# show crypto session

Crypto session current status
Interface: Virtual-Access2
Username: cisco
Profile: prof
Group: easy
Assigned address: 10.3.3.4
Session status: UP-ACTIVE
Peer: 10.1.1.2 port 500
  IKE SA: local 10.1.1.1/500 remote 10.1.1.2/500 Active
  IKE SA: local 10.1.1.1/500 remote 10.1.1.2/500 Inactive
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 host 3.3.3.4
        Active SAs: 2, origin: crypto map
```

The following example shows the **show crypto session brief** command output:

```
Device# show crypto session brief

Status: A- Active, U - Up, D - Down, I - Idle, S - Standby, N - Negotiating
        K - No IKE
ivrf = (none)
           Peer         I/F     Username     Group/Phase1_id    Uptime      Status
           10.1.1.2     Vi2     cisco        easy               00:50:30    UA
```

The following example shows the **show crypto session detail** command output:

```
Device# show crypto session detail

Crypto session current status
Code: C - IKE Configuration mode, D - Dead Peer Detection
```

```
K - Keepalives, N - NAT-traversal, X - IKE Extended Authentication
Interface: Virtual-Access2
Username: cisco
Profile: prof
Group: easy
Assigned address: 10.3.3.4
Uptime: 00:49:33
Session status: UP-ACTIVE
Peer: 10.1.1.2 port 500 fvrf: (none) ivrf: (none)
Phase1_id: easy
Desc: (none)
IKE SA: local 10.1.1.1/500 remote 10.1.1.2/500 Active
Capabilities:CX connid:1002 lifetime:23:10:15
IPSEC FLOW: permit ip 10.0.0.0/0.0.0.0 host 10.3.3.4
Active SAs: 2, origin: crypto map
Inbound: #pkts dec'ed 0 drop 0 life (KB/Sec) 4425776/626
Outbound: #pkts enc'ed 0 drop 0 life (KB/Sec) 4425776/626
```

The following table describes the significant fields shown in the display.

Table 73: show crypto session Field Descriptions

Field	Description
Interface	Interface to which the crypto session is related.
Session status	Current status of the crypto (VPN) sessions. See the table below for explanations of the status of the IKE SA, IPsec SA, and tunnel as shown in the display.
IKE SA	Information is provided about the IKE SA, such as the local and remote address and port, SA status, SA capabilities, crypto engine connection ID, and remaining lifetime of the IKE SA.
IPSEC FLOW	A snapshot of information about the IPsec-protected traffic flow, such as the status of the flow (for example, permit IP host 10.1.1.5 host 10.1.2.5), the number of IPsec SAs, the origin of the SA, such as manually entered, dynamic, or static crypto map, number of encrypted or decrypted packets or dropped packets, and the IPsec SA remaining lifetime in kilobytes per second.

The following table provides an explanation of the current status of the VPN sessions shown in the display.

Table 74: Current Status of the VPN Sessions

IKE SA	IPsec SA	Tunnel Status	Description
Exist, active	Exist (flow exists)	UP-ACTIVE	Both IPsec and IKE Phase1 SAs exist and are active.
Exist, active	None (flow exists)	UP-IDLE	IKE Phase1 SAs exist, and IPsec SAs are not present.
Exist, active	None (no flow)	UP-IDLE	

IKE SA	IPsec SA	Tunnel Status	Description
Exist, inactive	Exist (flow exists)	UP-NO-IKE	IPsec SAs exist, and either IKE Phase1 SAs are not present in the IKE Phase1 database for this peer or IKE Phase1 SAs are inactive. **Note** IKE Phase1 SAs being inactive or not being ready can be because IKE Phase1 is still negotiating or because IKE Phase1 SA is marked to be deleted.
None	Exist (flow exists)	UP-NO-IKE	
Exist, inactive	None (flow exists)	DOWN-NEGOTIATING	IPsec SAs are not present, and IKE Phase1 SAs are either inactive or do not exist.
Exist, inactive	None (no flow)	DOWN-NEGOTIATING	
None	None (flow exists)	DOWN	Both IPsec and IKE Phase1 SAs are not present.
None	None (no flow)	DOWN	

Note IPsec flow may not exist if a dynamic crypto map is being used.

Note The UP-NO-IKE tunnel status in the **show crypto session** command output does not indicate a failure in the following scenario.

Scenario: VRF-aware IPsec (fVRF and iVRF) using IPsec protected tunnels sharing the same tunnel source and the same IPsec profile. This scenario is valid for the following conditions:

- IPsec protected mGRE.
- IPsec protected p2p GRE tunnels.

For more specific IKE-related status information, see either the **show crypto isakmp sa** or the **show crypto isakmp sa detail** command outputs.

The following example shows the status information for all crypto sessions in the standby state:

```
Router# show crypto session standby

Crypto session current status
Interface: Ethernet0/0
Session status: UP-STANDBY
Peer: 10.165.200.225 port 500
  IKE SA: local 10.165.201.3/500 remote 10.165.200.225/500 Active
  IKE SA: local 10.165.201.3/500 remote 10.165.200.225/500 Active
  IPSEC FLOW: permit ip host 192.168.0.1 host 172.16.0.1
        Active SAs: 4, origin: crypto map
```

Related Commands

Command	Description
clear crypto session	Deletes crypto sessions (IPsec and ISAKMP SAs).
description	Adds a description for an IKE peer.
show crypto isakmp peer	Displays peer descriptions.

show crypto session group

To display groups that are currently active on the Virtual Private Network (VPN) device, use the **show crypto session group** command in privileged EXEC mode.

show crypto session group

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS 12.2SX family of releases. Support in a specific 12.2SX release is dependent on your feature set, platform, and platform hardware.

Usage Guidelines

If the **crypto isakmp client configuration group** command and **max-users** keyword have not been enabled in any VPN group profile, this command will yield a blank result.

Examples

The following example shows that at least one session is active for the group Connections:

```
Router# show crypto session group
 Group: Connections
 cisco: 1
```

Related Commands

Command	Description
crypto isakmp client configuration group	Specifies to which group a policy profile will be defined.
show crypto session summary	Displays groups that are currently active on the VPN device and the users that are connected for each of those groups.

show crypto session summary

To display groups that are currently active on the Virtual Private Network (VPN) device and the users that are connected for each of those groups, use the **show crypto session summary** command in privileged EXEC mode.

show crypto session summary

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS 12.2SX family of releases. Support in a specific 12.2SX release is dependent on your feature set, platform, and platform hardware.

Usage Guidelines

If the **crypto isakmp client configuration group** command and **max-users** keyword are not enabled in any VPN group profile and the **crypto isakmp client configuration group**command and **max-logins** keyword are not enabled, this command will yield a blank result.

Examples

The following example shows that the group "cisco" is active and that it has one user connected, green, who is connected one time. The number in parentheses (1) is the number of simultaneous logins for that user.

```
Router# show crypto session summary
 Group cisco has 1 connections
  User (Logins)
  green (1)
```

Related Commands

Command	Description
crypto isakmp client configuration group	Specifies to which group a policy profile will be defined.
show crypto session group	Displays groups that are currently active on the VPN device.

show crypto socket

To list crypto sockets and their state, use the **show crypto socket** command in privileged EXEC mode.

show crypto socket

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(11)T	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.4(5)	This command was modified. The Flags field was added to command output.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.(33)SRA.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1 and implemented on the Cisco ASR 1000 Series Aggregation Services Routers.

Examples

The following is sample output from the **show crypto socket** command:

```
Device# show crypto socket

 Number of Crypto Socket connections 2
   Tu0 Peers (local/remote): 192.168.2.2/192.168.1.1
       Local Ident  (addr/mask/port/prot): (192.168.2.2/255.255.255.255/0/47)
       Remote Ident (addr/mask/port/prot): (192.168.1.1/255.255.255.255/0/47)
       IPsec Profile: "dmvpn-profile"
       Flags: shared
       Socket State: Open
       Client: "TUNNEL SEC" (Client State: Active)
   Tu1 Peers (local/remote): 192.168.2.2/192.168.1.3
       Local Ident  (addr/mask/port/prot): (192.168.2.2/255.255.255.255/0/47)
       Remote Ident (addr/mask/port/prot): (192.168.1.3/255.255.255.255/0/47)
       IPsec Profile: "default"
       Flags: shared
       Socket State: Open
       Client: "TUNNEL SEC" (Client State: Active)
Crypto Sockets in Listen state:
Client: "TUNNEL SEC" Profile: "dmvpn-profile" Map-name: "dmvpn-profile-head-2"
Client: "TUNNEL SEC" Profile: "default" Map-name: "Tunnel0-head-0"
```

The following table describes the significant fields shown in the display.

Table 75: show crypto socket Field Descriptions

Field	Description
Number of Crypto Socket connections	Number of crypto sockets in the system.

Field	Description
Flags	If this field displays “shared,” the socket is shared with more than one tunnel interface.
Socket State	This state can be Open, which means that active IPsec security associations (SAs) exist, or it can be Closed, which means that no active IPsec SAs exist.
Client	Application name and its state.
Crypto Sockets in Listen state	Names of the crypto IPsec profiles. For each tunnel interface, one listener socket is displayed.

show crypto tech-support

To display the crypto technical support information, use the show crypto tech-support command in privileged EXEC mode.

show crypto tech-support [{**peer** *ip-address* | **vrf** *vrf-name*}]

Syntax Description

peer	(Optional) Displays the crypto technical support information related to a peer.
ip-address	(Optional) The peer IPv4 address.
vrf	(Optional) Displays the crypto technical support information related to VPN routing or forwarding (VRF).
vrf-name	(Optional) The VRF name.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(22)T	This command was introduced.

Usage Guidelines

Use the optional keywords and arguments to display the specific crypto technical support information.

Examples

The following is sample output from the **show crypto tech-support** command. The fields are self-explanatory.

```
Router# show crypto tech-support
------------------ show crypto session remote 1.0.1.2 detail ------------------
------------------ show crypto ipsec sa peer 1.0.1.2 detail ------------------
------------------ show crypto isakmp sa peer 1.0.1.2 detail ------------------
IPv4 Crypto ISAKMP SA
dst             src             state          conn-id status
------------------ show crypto isakmp peers 1.0.1.2  ------------------
------------------ show crypto ruleset detail ------------------
------------------ show processes memory | include  Crypto IKMP ----------------
 240   0       7112        252      20064          0          0 Crypto IKMP
------------------ show processes cpu |  include Crypto IKMP ------------------
 240           0         3          0  0.00%  0.00%  0.00%   0 Crypto IKMP
------------------ show crypto eli ------------------
Hardware Encryption : ACTIVE
 Number of hardware crypto engines = 1
 CryptoEngine Onboard VPN details: state = Active
 Capability      : IPPCP, DES, 3DES, AES, IPv6, FAILCLOSE
 IPSec-Session :     0 active,  1400 max, 0 failed

------------------ show cry engine accelerator statistic ------------------
Device:   Onboard VPN
Location: Onboard: 0
        :Statistics for encryption device since the last clear
         of counters 1818819 seconds ago
                     0 packets in                          0 packets out
```

```
      0 bytes in                          0 bytes out
      0 paks/sec in                       0 paks/sec out
      0 Kbits/sec in                      0 Kbits/sec out
      0 packets decrypted                 0 packets encrypte
      0 bytes before decrypt              0 bytes encrypted
      0 bytes decrypted                   0 bytes after encr
      0 packets decompressed              0 packets compress
      0 bytes before decomp               0 bytes before com
      0 bytes after decomp                0 bytes after comp
      0 packets bypass decompr            0 packets bypass cs
      0 bytes bypass decompres            0 bytes bypass comi
      0 packets not decompress            0 packets not compd
      0 bytes not decompressed            0 bytes not compre
  1.0:1 compression ratio               1.0:1 overall
Last 5 minutes:
      0 packets in                        0 packets out
```

show crypto vlan

To display the VPN running state for an IPSec VPN SPA, use the **show crypto vlan**command in privileged EXEC mode.

show crypto vlan

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)SXE2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

When you **show** the configuration, the crypto engine subslot configuration state is expressed in the context of the associated interface VLAN. The interface VLAN is also shown as having been added to the appropriate inside trunk port. This is the case even if the configuration was loaded from a legacy (pre-crypto engine subslot) configuration file, or if VLANs were manually added instead of being added through the **crypto engine subslot** command.

Examples

In the following example, the interface VLAN belongs to the IPSec VPN SPA inside port:

```
Router# show crypto vlan
  Interface VLAN 2 on IPSec Service Module port 7/1/1 connected to Fa8/3
```

In the following example, VLAN 2 is the interface VLAN and VLAN 2022 is the hidden VLAN:

```
Router# show crypto vlan
Interface VLAN 2 on IPSec Service Module port 3/1/1 connected to VLAN 2022 with crypto map
 set coral2
```

In the following example, either the interface VLAN is missing on the IPSec VPN SPA inside port, the IPSec VPN SPA is removed from the chassis, or the IPSec VPN SPA was moved to a different subslot:

```
Router# show crypto vlan
  Interface VLAN 2 connected to VLAN 3 (no IPSec Service Module attached)
```

Related Commands

Command	Description
crypto connect vlan	Creates an interface VLAN for an IPSec VPN SPA and enters crypto-connect mode.
crypto engine subslot	Assigns an interface VLAN that requires encryption to the IPSec VPN SPA.

show cts credentials

To display the Cisco TrustSec (CTS) device ID, use the **show cts credentials** command in EXEC or privileged EXEC mode.

show cts credentials

Syntax Description

This command has no commands or keywords.

Command Modes

Privileged EXEC (#) User EXEC (>)

Command History

Release	Modification
12.2(33)SXI	This command was introduced on the Catalyst 6500 series switches.
15.2(2)T	This command was integrated into Cisco IOS Release 15.2(2)T.

Examples

```
Router# show cts credentials

CTS password is defined in keystore, device-id = r4
```

Related Commands

Command	Description
cts credentials	Specifies the TrustSec ID and password.

show cts interface

To display Cisco TrustSec (CTS) configuration statistics for an interface(s), use the **show cts interface** command in EXEC or privileged EXEC mode.

show cts interface [{**GigabitEthernet** *port* | **Vlan** *number* | **brief** | **summary**}]

Syntax Description

port	(Optional) Gigabit Ethernet interface number. A verbose status output for this interface is returned.
number	(Optional) VLAN interface number from 1 to 4095.
brief	(Optional) Displays abbreviated status for all CTS interfaces.
summary	(Optional) Displays a tabular summary of all CTS interfaces with 4 or 5 key status fields for each interface.

Command Default

None

Command Modes

EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SXI	This command was introduced on the Catalyst 6500 series switches.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.1(3)S	This command was integrated into Cisco IOS Release 15.1(3)S.

Usage Guidelines

Use the **show cts interface** command without keywords to display verbose status for all CTS interfaces.

Examples

The following example displays output without using a keyword (verbose status for all CTS interfaces):

```
Device# show cts interface

Global Dot1x feature is Disabled
 Interface GigabitEthernet0/1/0:
     CTS is enabled, mode:    MANUAL
     IFC state:               OPEN
     Interface Active for 00:00:18.232
     Authentication Status:   NOT APPLICABLE
         Peer identity:       "unknown"
         Peer's advertised capabilities: ""
     Authorization Status:    NOT APPLICABLE
     SAP Status:              NOT APPLICABLE
         Configured pairwise ciphers:
             gcm-encrypt
             null

         Replay protection:      enabled
```

```
        Replay protection mode: STRICT

        Selected cipher:

    Propagate SGT:          Enabled
    Cache Info:
        Cache applied to link : NONE

    Statistics:
        authc success:              0
        authc reject:               0
        authc failure:              0
        authc no response:          0
        authc logoff:               0
        sap success:                0
        sap fail:                   0
        authz success:              0
        authz fail:                 0
        port auth fail:             0
        Ingress:
            control frame bypassed: 0
            sap frame bypassed:     0
            esp packets:            0
            unknown sa:             0
            invalid sa:             0
            inverse binding failed: 0
            auth failed:            0
            replay error:           0
        Egress:
            control frame bypassed: 0
            esp packets:            0
            sgt filtered:           0
            sap frame bypassed:     0
            unknown sa dropped:     0
            unknown sa bypassed:    0
```

The following example displays output using the **brief** keyword:

```
Device# show cts interface brief

Global Dot1x feature is Disabled
 Interface GigabitEthernet0/1/0:
     CTS is enabled, mode:    MANUAL
     IFC state:               OPEN
     Interface Active for 00:00:40.386
     Authentication Status:   NOT APPLICABLE
         Peer identity:       "unknown"
         Peer's advertised capabilities: ""
     Authorization Status:    NOT APPLICABLE
     SAP Status:              NOT APPLICABLE
     Propagate SGT:           Enabled
     Cache Info:
         Cache applied to link : NONE
```

Related Commands

Command	Description
cts manual	Enables an interface for CTS.
cts sxp enable	Configures SXP on a network device.

Command	Description
propagate sgt	Enables Security Group Tag (SGT) propagation at Layer 2 on Cisco TrustSec Security (CTS) interfaces.

show cts platform

To display Cisco TrustSec configuration statistics for a platform, use the **show cts platform** command in user EXEC or privileged EXEC mode.

show cts platform [**interface** *interface-type*] **stats** [**detail**]

Syntax Description

interface *interface-type*	(Optional) Displays information about the interfaces available on the platform.
stats	Displays platform-specific Cisco TrustSec statistics.
detail	(Optional) Displays detailed information for platform-specific Cisco TrustSec statistics.

Command Modes

EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
15.3(2)T	This command was introduced.

Examples

The following is sample output from the **show cts platform interface** *interface-type* **stats detail** command, which displays detailed output for platform-specific Cisco TrustSec statistics:

```
Device# show cts platform interface gigabitethernet 0/0/0 stats detail

Interface gigabitethernet 0/0/0
 L2-SGT Statistics
 Pkts In : 31627
 Pkts (policy SGT assigned) : 24
 Pkts Out : 6866
 Pkts Drop (malformed packet): 0
 Pkts Drop (invalid SGT) : 0
```

Related Commands

Command	Description
cts manual	Enables an interface for Cisco TrustSec.
cts sxp enable	Configures SXP on a network device.
propagate sgt	Enables SGT propagation at Layer 2 on Cisco TrustSec interfaces.

show cts server-list

To display the list of RADIUS servers available to Cisco TrustSec (CTS) seed and nonseed devices, use the **show cts server-list** command in user EXEC or privileged EXEC mode.

show cts server-list

Syntax Description

This command has no commands or keywords.

Command Modes

Privileged EXEC (#) User EXEC (>)

Command History

Release	Modification
12.2(33)SXI	This command was introduced on the Catalyst 6500 series switches.
15.2(2)T	This command was integrated into Cisco IOS Release 15.2(2)T.

Usage Guidelines

This command is useful for gathering CTS RADIUS server address and status information.

Examples

The following example displays the CTS RADIUS server list:

```
Router> show cts server-list
CTS Server Radius Load Balance = DISABLED
Server Group Deadtime = 20 secs (default)
Global Server Liveness Automated Test Deadtime = 20 secs
Global Server Liveness Automated Test Idle Time = 60 mins
Global Server Liveness Automated Test = ENABLED (default)
Preferred list, 1 server(s):
 *Server: 10.0.1.6, port 1812, A-ID 1100E046659D4275B644BF946EFA49CD
          Status = ALIVE
          auto-test = TRUE, idle-time = 60 mins, deadtime = 20 secs
Installed list: ACSServerList1-0001, 1 server(s):
 *Server: 101.0.2.61, port 1812, A-ID 1100E046659D4275B644BF946EFA49CD
          Status = ALIVE
          auto-test = TRUE, idle-time = 60 mins, deadtime = 20 secs
```

Related Commands

Command	Description
address ipv4 (config-radius-server)	Configures the RADIUS server accounting and authentication parameters for PAC provisioning.
pac key	Specifies the PAC encryption key.

show cts sxp

To display Cisco TrustSec Security Group Tag (SGT) Exchange Protocol (CTS-SXP) connection or source IP-to-SGT mapping information, use the **show cts sxp** command in user EXEC or privileged EXEC mode.

show cts sxp {**connections** | **sgt-map**} [{**brief** | **vrf** *instance-name*}]

Syntax Description

connections	Displays Cisco TrustSec SXP connections information.
sgt-map	Displays the IP-to-SGT mappings received through SXP.
brief	(Optional) Displays an abbreviation of the SXP information.
vrf *instance-name*	(Optional) Displays the SXP information for the specified Virtual Routing and Forwarding (VRF) instance name.

Command Default

None

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SXI3	This command was introduced on the Catalyst 6500 series switches.
12.2(50)SG7	This command was integrated on the Catalyst 4000 series switches.
12.2(53)SE2	This command was integrated into Cisco IOS Release 12.2(53)SG7 on the Catalyst 3750(E) and 3560(E) series switches.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.
15.1(3)S	This command was integrated into Cisco IOS Release 15.1(3)S.
15.4(1)T	This command was integrated into Cisco IOS Release 15.4(1)T.

Examples

The following example displays the SXP connections using the **brief** keyword:

```
Device# show cts sxp connection brief

 SXP              : Enabled
 Default Password : Set
 Default Source IP: Not Set
Connection retry open period: 10 secs
Reconcile period: 120 secs
Retry open timer is not running
------------------------------------------------------------------------------
Peer_IP          Source_IP        Conn Status       Duration
------------------------------------------------------------------------------
10.10.10.1          10.10.10.2          On               0:00:02:14 (dd:hr:mm:sec)
10.10.2.1          10.10.2.2          On               0:00:02:14 (dd:hr:mm:sec)
```

```
Total num of SXP Connections = 2
```

The following example displays the CTS-SXP connections:

```
Device# show cts sxp connections

 SXP              : Enabled
 Default Password : Set
 Default Source IP: Not Set
Connection retry open period: 10 secs
Reconcile period: 120 secs
Retry open timer is not running
----------------------------------------------
Peer IP          : 10.10.10.1
Source IP        : 10.10.10.2
Set up           : Peer
Conn status      : On
Connection mode  : SXP Listener
Connection inst# : 1
TCP conn fd      : 1
TCP conn password: not set (using default SXP password)
Duration since last state change: 0:00:01:25 (dd:hr:mm:sec)
----------------------------------------------
Peer IP          : 10.10.2.1
Source IP        : 10.10.2.2
Set up           : Peer
Conn status      : On
Connection mode  : SXP Listener
TCP conn fd      : 2
TCP conn password: not set (using default SXP password)
Duration since last state change: 0:00:01:25 (dd:hr:mm:sec)
Total num of SXP Connections = 2
```

The following example displays the CTS-SXP connections for a bi-directional connection when the device is both the speaker and listener:

```
Device# show cts sxp connections

SXP : Enabled
Highest Version Supported: 4
Default Password : Set
Default Source IP: Not Set
Connection retry open period: 120 secs
Reconcile period: 120 secs
Retry open timer is running
----------------------------------------------
Peer IP : 2.0.0.2
Source IP : 1.0.0.2
Conn status : On (Speaker) :: On (Listener)
Conn version : 4
Local mode : Both
Connection inst# : 1
TCP conn fd : 1(Speaker) 3(Listener)
TCP conn password: default SXP password
Duration since last state change: 1:03:38:03 (dd:hr:mm:sec) :: 0:00:00:46 (dd:hr:mm:sec)
```

The following example displays output from a CTS-SXP listener with a torn down connection to the SXP speaker. Source IP-to-SGT mappings are held for 120 seconds, the default value of the Delete Hold Down timer.

```
Device# show cts sxp connections

 SXP              : Enabled
 Default Password : Set
 Default Source IP: Not Set
Connection retry open period: 10 secs
Reconcile period: 120 secs
Retry open timer is not running
------------------------------------------------
Peer IP          : 10.10.10.1
Source IP        : 10.10.10.2
Set up           : Peer
Conn status      : Delete_Hold_Down
Connection mode  : SXP Listener
Connection inst# : 1
TCP conn fd      : -1
TCP conn password: not set (using default SXP password)
Delete hold down timer is running
Duration since last state change: 0:00:00:16 (dd:hr:mm:sec)
------------------------------------------------
Peer IP          : 10.10.2.1
Source IP        : 10.10.2.2
Set up           : Peer
Conn status      : On
Connection inst# : 1
TCP conn fd      : 2
TCP conn password: not set (using default SXP password)
Duration since last state change: 0:00:05:49 (dd:hr:mm:sec)
Total num of SXP Connections = 2
```

Related Commands

Command	Description
cts sxp connection peer	Enters the Cisco TrustSec SXP peer IP address and specifies if a password is used for the peer connection
cts sxp default password	Configures the Cisco TrustSec SXP default password.
cts sxp default source-ip	Configures the Cisco TrustSec SXP source IPv4 address.
cts sxp enable	Enables Cisco TrustSec SXP on a device.
cts sxp log	Enables logging for IP-to-SGT binding changes.
cts sxp reconciliation	Changes the Cisco TrustSec SXP reconciliation period.
cts sxp retry	Changes the Cisco TrustSec SXP retry period timer.

show cts sxp filter-group

To display information about the configured filter groups, use the **show cts sxp filter-group** command in privileged EXEC mode.

show cts sxp filter-group [**speaker** | **listener** | {**speaker** | **listener**} **filter-group-name**] [**detailed**]
show cts sxp filter-group [**global**] [**detailed**]

Syntax Description

speaker	Displays information about the speaker filter group or groups.
listener	Displays information about the listener filter group or groups.
filter-group-name	Displays information about a specific filter group.
global	Displays information about the global groups.
detailed	Displays detailed information about a specific group or a set of groups.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
16.6.1	This command was introduced.

Example

The following example shows how to display the details of a specific speaker filter group:

```
Device# show cts sxp filter-group speaker group_1
    Filter-group: group_1
        Filter-name: filter_1
        peer 1.1.1.1
        peer 1.1.1.2
```

The following example shows how to display the complete details of all the listener filter groups:

```
Device# show cts sxp filter-group listener detailed
    Global Listener Filter Name: filter_1
    Filter-rules:
    10 deny ipv4 1.1.1.0/24 permit sgt 2 (0)
    Total Matches: 0
    Default Deny Count: 0

    Global Speaker Filter Name: filter_1
    Filter-rules:
    10 deny ipv4 1.1.1.0/24 permit sgt 2 (0)
    Total Matches: 0
    Default Deny Count: 0

    Listener Groups:
```

```
Filter-group: group_1
Filter-name: filter_1
Filter-rules:
10 deny ipv4 1.1.1.0/24 permit sgt 2 (0)
Total Matches: 0
Default Deny Count: 0
peer 1.1.1.1

Speaker Groups:

Filter-group: group_3
peer 1.1.1.1
```

Note The number within round barackets against each rule is the count of the number of times that rule has matched.

Related Commands

Command	Description
cts sxp filter-enable	Enables filtering.
cts sxp filter-group	Creates a filter group for grouping a set of peers and applying a filter list to them
cts sxp filter-list	Creates a SXP filter list to hold a set of filter rules for filtering IP-SGT bindings in a SXP connection.
show cts sxp filter-list	Displays information about the configured filter lists.
debug cts sxp filter events	Logs events related to the creation, deletion and update of filter-lists and filter-groups.

show cts sxp filter-list

To display information about the configured filter lists, use the **show cts sxp filter-list** command in privileged EXEC mode.

show cts sxp filter-list [*filter-list-name*]

Syntax Description

filter-list-name	Name of the filter list.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
16.6.1	This command was introduced.

Example

The following example shows how to display the rules in a specific filter list:

```
Device# show cts sxp filter-list filter_1
   Filter-name: filter_1
   10 deny ipv4 1.1.1.0/24 permit sgt 2 (0)
```

The following example shows how to display all the filter lists and their corresponding rules:

```
Device# show cts sxp filter-list
    Filter-name: filter_1 (0)
    10 deny ipv4 1.1.1.0/24 permit sgt 2 (0)
    Filter-name: default_sgt (0)
    10 permit sgt all (0)
    20 deny ipv4 5.5.5.0/24 (0)
    30 deny ipv6 ::/0 (0)
    40 permit ipv6 66:99::88/128 (0)
    50 permit sgt 100 200 300 (0)
    60 deny sgt 99 (0)
    90 permit ipv4 8.8.8.8/32 deny sgt 89 (0)
    100 deny ipv6 1::1/128 permit sgt 90 70 (0)
```

Note The number within round barackets against each rule is the count of the number of times that rule has matched.

Related Commands

Command	Description
cts sxp filter-enable	Enables filtering.

Command	Description
cts sxp filter-group	Creates a filter group for grouping a set of peers and applying a filter list to them.
cts sxp filter-list	Creates a SXP filter list to hold a set of filter rules for filtering IP-SGT bindings in a SXP connection.
show cts sxp filter-group	Displays information about the configured filter groups.
debug cts sxp filter events	Logs events related to the creation, deletion and update of filter-lists and filter-groups.

show cws

To display Cloud Web Security content-scan information, use the **show cws** command in user EXEC or privileged EXEC mode.

show cws {**session** {**active** [{**detail** | **egress-vrf** *vrf-number* | **ingress-vrf** *vrf-number* | **ip-addr** *ip-address* [{**all**}]}] | **history** *sessions*} | **statistics** [{**all** | **detailed** | **failures** | **memory-usage**}] | **summary**}

Syntax Description

session	Displays Cloud Web Security session information.
active	Displays active sessions.
detail	(Optional) Displays Cloud Web Security content-scan session details.
egress-vrf	(Optional) Displays information about the virtual routing and forwarding (VRF) instance at the egress interface.
vrf-number	(Optional) Egress or ingress VRF ID. Valid values are from 0 to 1024.
igress-vrf	(Optional) Displays information about the VRF instance at the ingress interface.
ip-addr *ip-address*	(Optional) Displays information about the specified IP address.
all	(Optional) Displays information about all sessions.
history	Displays information about terminated sessions.
sessions	Number of sessions. Valid values are from 1 to 512.
statistics	Displays statistics of the content scanned by Cloud Web Security.
detailed	(Optional) Displays detailed statistics of the content scanned.
failures	(Optional) Displays Cloud Web Security content-scan failure statistics.
memory-usage	(Optional) Displays Cloud Web Security content-scan memory usage statistics.
summary	Displays a summary of the Cloud Web Security content scan information.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
15.4(2)T	This command was introduced. This command replaces the **show content-scan** command.

Usage Guidelines

Cloud Web Security provides content scanning of HTTP and secure HTTP (HTTPS) traffic and malware protection services to web traffic. The content-scanning process redirects client web traffic to the Cloud Web

Security servers. These servers scan the web traffic content and allow or block traffic based on compliance with the configured policies and thus protect clients from malware. Content scanning is enabled on an Internet-facing WAN interface to protect the web traffic that goes out. Use the **show cws** command to view Cloud Web Security content-scan information.

The **show cws session history** command displays information about a maximum of 512 terminated sessions.

Examples

The following is sample output from the **show cws session history** command:

```
Device# show cws session history 6

 Protocol  Source              Destination           Bytes         URI                  Time

 HTTP      192.168.100.2:1347 209.165.201.104:80    (102:45)       www.google.com
00:01:13
 HTTP      192.168.100.2:1326 209.165.201.106:80    (206:11431)    www.google.com
00:12:55
 HTTP      192.168.100.2:1324 209.165.201.105:80    (206:11449)    www.google.com
00:15:20
 HTTP      192.168.100.2:1318 209.165.201.105:80    (206:11449)    www.google.com
00:17:43
 HTTP      192.168.100.2:1316 209.165.201.104:80    (206:11449)    www.google.com
00:20:04
 HTTP      192.168.100.2:1315 10.254.145.107:80     (575:1547)     alert.scansafe.net
00:21:32
```

The following table describes the significant fields shown in the display.

Table 76: show cws session history Field Descriptions

Field	Description
Protocol	Protocol used for content scanning.
Source	IP address of the source with the port number.
Destination	IP address of the destination with the port number.
URI	Uniform Resource Identifier (URI) that identifies a name or a resource on the Internet.
Time	Duration of time when a session was terminated.

The following is sample output from the **show cws statistics** command:

```
Device# show cws statistics

 Current HTTP sessions: 3
 Current HTTPS sessions: 0
 Total HTTP sessions: 11
 Total HTTPS sessions: 0
 White-listed sessions: 0
 Time of last reset: 00:01:58
```

The following table describes the fields shown in the display.

Table 77: show cws statistics Field Descriptions

Field	Description
Current HTTP sessions	Number of current HTTP sessions.
Current HTTPS sessions	Number of current secure HTTP (HTTPS) sessions.
Total HTTP sessions	Total number of HTTP sessions.
Total HTTPS sessions	Total number of HTTPS sessions.
White-listed sessions	Number of sessions that appear on the allowed lising. An allowed list is an approved list of entities that are provided a particular privilege, service, mobility, access, or recognition. Allowed listing means to grant access.
Time of last reset	Duration of time since sessions were last reset.

The following is sample output from the **show cws statistics failures** command:

```
Device# show cws statistics failures

Reset during proxy Mode:               0
HTTPS reconnect failures:              0
Buffer enqueue failures:               0
Buffer length exceeded:                0
Particle coalesce failures:            0
L4F failures:                          0
Lookup failures:                       0
Memory failures:                       0
Tower unreachable:                     0
Resets sent:                           0
```

The following table describes the significant fields shown in the display.

Table 78: show cws statistics failures Field Descriptions

Field	Description
Reset during proxy Mode	Reset messages that are received when content scan is in proxy mode.
HTTPS reconnect failures	Connection failures while reconnecting to HTTPS.
Buffer enqueue failures	Buffering queue failures. When a packet fails to reach its destination, the packet is buffered in a queue for a retry. This queue to which packets are buffered can fail, and this failure is added to the statistics.
Buffer length exceeded	Packets that exceed the buffer length.
Particle coalesce failures	Packet defragmentation failures. When content scan receives packet fragments, these fragments are joined together or coalesced, and any failures during the coalescing are added to the statistics.

Field	Description
L4F failures	Layer 4 Forwarding (L4F) failures. When content scan and L4F is out of sync with each other, the statistics are incremented. **Note** We recommend that you inform TAC, if this counter increments rapidly.
Lookup failures	Content-scan entry lookup failures. During normal packet flows, content scan entries are checked at certain points. When such a lookup fails (when it was not expected to fail), it is added to the statistics.
Memory failures	Memory failures in the content scan subsystem (can be malloc, chunk_malloc, list, and so on).
Tower unreachable	Cloud Web Security tower unreachable during packet flows.
Resets sent	Packet processing errors. During packet processing, if errors are encountered, reset messages are sent to end hosts.

The following sample output from the **show cws session active egress-vrf** command:

```
Device# show cws session active egress-vrf 1

Protocol      Source          Destination     Bytes             Time
HTTP [0]:     10.1.1.1:25176   10.2.2.1:80    (262:10495)       00:00:00
        URI: 10.2.2.1
        Username/usergroup(s): /
```

Related Commands

Command	Description
cws out	Enables Cloud Web Security content scanning on an egress interface.
debug cws	Enables Cloud Web Security debugging.

show cws tower-whitelist

To display allowed lists downloaded from the Cloud Web Security tower, use the **show cws tower-whitelist** command in privileged EXEC mode.

show cws tower-whitelist [{**stats**}]

Syntax Description

stats	(Optional) Displays Cloud Web Security tower allowed list statistics.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS Release 15.5(1)T	This command was introduced.

Usage Guidelines

Allowed list patterns from the Cloud Web Security tower are not stored in the configuration. However; allowed list patterns configured through the CLI are stored in the configuration. Both, patterns configured via the CLI and patterns downloaded from the tower can be used for allowed listing. To view allowed listing patterns, use the **show cws tower-whitelist** command.

Examples

The following is sample output from the **show cws tower-whitelist** command. The output fields are self-explanatory.

```
Device# show cws tower-whitelist

 Last modified time at tower : Wed, 06 Nov 2014 05:47:52 UTC
Domain names:
  .*redhat.*
  .*xerox.*
  .*yahoo.*.
Extended IP access list cws-internal-dnld-wl-acl
    10 permit ip 10.10.1.16 0.0.0.15 any
    20 permit ip any host 202.3.77.184
User-agent patterns:
  mozilla
  Safari
```

The following is sample output from the **show cws tower-whitelist stats** command:

```
Device# show cws tower-whitelist statistics

Total Connect Request:                                      13
Total Connect Response:                                     13
Total WL download request:                                  13
SSL failures:                                               0
WL download response:                                       13
     Total success response:                                1
     Total no config change:                                7
     Total no config:                                       0
     Total other responses(Other than 200/304/404):         5
     Total other failures(no encoding/HTTP version):        0
XML parse errors:                                           0
```

```
Memory failures:                                        0

XML parser stats:
  Src ACLs     Dst ACLs    Domain-name      User-agent
   1            1           1                2
```

The following table describes the significant fields shown in the display.

Table 79: show cws tower-whitelist stats Field Descriptions

Field	Description
Total Connect Request	Connect requests sent to the Cloud Web Security tower.
Total Connect Response	Responses to connect requests sent back by the Cloud Web Security tower.
Total WL download request	Requests sent to the Cloud Web Security tower for downloading allowed listing patterns.
SSL failures	Secure Sockets Layer (SSL) handshake failures due to missing or wrong certificates in the router.
WL download response	Responses from the tower for allowed listing download requests.
Total success response	200 OK responses received by using new allowed listing patterns from the tower.
Total no config change	304 responses received from the tower indicating that patterns were not changed since the last download.
Total no config	404 responses received from the tower indicating that there are no allowed listing patterns for download, and no allowed listing patterns are removed for that device/group.
Total other responses (Other than 200/304/404)	Responses to allowed listing download requests, excluding HTTP messages 200 (OK), 304 (File not modified), and 404 (File not found).
Total other failures(no encoding/HTTP version)	Responses with missed HTTP version, or XML files that do not include an encoding attribute.
XML parse errors	XML parser failures such as invalid tags.
Memory failures	Memory allocation failures during allowed listing download.

Related Commands

Command	Description
parameter-map type inspect cws global	Configures a global Cloud Web Security parameter map and enters parameter-map type inspect configuration mode.
whitelist download enable	Enables the download of allowed listing from the Cloud Web Security tower.

show diameter peer through show object-group

show device-sensor cache

To display device sensor cache entries, use the **show device-sensor cache** command in privileged EXEC mode.

show device-sensor cache {**mac** *mac-address* | **all**}

Syntax Description

mac *mac-address*	Specifies the MAC address of the device for which the sensor cache entries are to be displayed.
all	Displays sensor cache entries for all devices.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)SE1	This command was introduced.
15.1(1)SG	This command was integrated into Cisco IOS Release 15.1(1)SG.

Usage Guidelines

Use the **show device-sensor cache** command to display a list of Type-Length-Value (TLV) fields or options received from a particular device or from all devices.

Examples

The following is sample output from the **show device-sensor cache mac** *mac-address* command:

```
Device# show device-sensor cache mac 0024.14dc.df4d

Device: 0024.14dc.df4d on port GigabitEthernet1/0/24
-------------------------------------------------
Proto   Type:Name                       Len Value
cdp     26:power-available-type          16 00 1A 00 10 00 00 00 01 00 00 00 00 FF FF FF FF
cdp     22:mgmt-address-type             17 00 16 00 11 00 00 00 01 01 01 CC 00 04 09 1B 65
                                            0E
cdp     11:duplex-type                    5 00 0B 00 05 01
cdp      9:vtp-mgmt-domain-type           4 00 09 00 04
cdp      4:capabilities-type              8 00 04 00 08 00 00 00 28
cdp      1:device-name                   14 00 01 00 0E 73 75 70 70 6C 69 63 61 6E 74
lldp     0:end-of-lldpdu                  2 00 00
lldp     8:management-address            14 10 0C 05 01 09 1B 65 0E 03 00 00 00 01 00
lldp     7:system-capabilities            6 0E 04 00 14 00 04
lldp     4:port-description              23 08 15 47 69 67 61 62 69 74 45 74 68 65 72 6E 65
                                            74 31 2F 30 2F 32 34
lldp     5:system-name                   12 0A 0A 73 75 70 70 6C 69 63 61 6E 74
dhcp    82:relay-agent-info              20 52 12 01 06 00 04 00 18 01 18 02 08 00 06 00 24
                                            14 DC DF 80
dhcp    12:host-name                     12 0C 0A 73 75 70 70 6C 69 63 61 6E 74
dhcp    61:client-identifier             32 3D 1E 00 63 69 73 63 6F 2D 30 30 32 34 2E 31 34
                                            64 63 2E 64 66 34 64 2D 47 69 31 2F 30 2F 32 34
dhcp    57:max-message-size               4 39 02 04 80
```

The following is sample output from the **show device-sensor cache all** command:

```
Device# show device-sensor cache all

Device: 001c.0f74.8480 on port GigabitEthernet2/1
-------------------------------------------------
Proto   Type:Name                          Len  Value
dhcp    52:option-overload                  3  34 01 03
dhcp    60:class-identifier                11  3C 09 64 6F 63 73 69 73 31 2E 30
dhcp    55:parameter-request-list           8  37 06 01 42 06 03 43 96
dhcp    61:client-identifier               27  3D 19 00 63 69 73 63 6F 2D 30 30 31 63 2E 30 66
                                               37 34 2E 38 34 38 30 2D 56 6C 31
dhcp    57:max-message-size                 4  39 02 04 80

Device: 000f.f7a7.234f on port GigabitEthernet2/1
-------------------------------------------------
Proto   Type:Name                          Len  Value
cdp     22:mgmt-address-type                8  00 16 00 08 00 00 00 00
cdp     19:cos-type                         5  00 13 00 05 00
cdp     18:trust-type                       5  00 12 00 05 00
cdp     11:duplex-type                      5  00 0B 00 05 01
cdp     10:native-vlan-type                 6  00 0A 00 06 00 01
cdp      9:vtp-mgmt-domain-type             9  00 09 00 09 63 69 73 63 6F
```

The following table describes the significant fields shown in the display.

Table 80: show device-sensor global Field Descriptions

Field	Description
Device	MAC address of the device and the interface that it is connected to.
Proto	Protocol from which the endpoint device data is being gleaned.
Type	Type of TLV.
Name	Name of the TLV.
Len	Length of the TLV.
Value	Value of the TLV.

Related Commands

Command	Description
debug device-sensor	Enables debugging for device sensor.
device-sensor accounting	Adds the device sensor protocol data to accounting records and generates additional accounting events when new sensor data is detected.
device-sensor filter-list cdp	Creates a Cisco Discovery Protocol filter containing a list of options that can be included or excluded in the device sensor output.
device-sensor filter-list dhcp	Creates a DHCP filter containing a list of options that can be included or excluded in the device sensor output.
device-sensor filter-list lldp	Creates an LLDP filter containing a list of TLV fields that can be included or excluded in the device sensor output.

Command	Description
show device-sensor cache	Displays device sensor cache entries.

show diameter peer

To display the configuration and status of a specific Diameter peer, or all Diameter peers, use the **show diameter peer** command in privileged EXEC mode.

show diameter peer [*peer-name*]

Syntax Description

peer- name	Displays the configuration and status of the specified Diameter peer. **Note** If no peer name is specified, the command will display information for all configured Diameter peers.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

This command displays the peer status information, as well as counters, including:

- Total packets sent
- Total responses seen
- Packets with responses
- Packets without responses
- Average response delay (ms)
- Number of Diameter timeouts
- Buffer allocation failures

Examples

The following is a sample output from the **show diameter peer command**:

```
Router#
show diameter peer iwan-view5
Peer information for iwan-view5
------------------------------
Peer name: iwan-view 5
Peer type: Server
Peer transport protocol: TCP
Peer listening port: 3688
Peer security protocol: IPSEC
Peer connection timer value: 30 seconds
Peer watch dog timer value: 35 seconds
Peer vrf name: default
Peer connection status: UP
```

The fields shown above are self-explanatory.

Related Commands

Command	Description
debug diameter	Displays information about the Diameter protocol.

show dmvpn

To display Dynamic Multipoint VPN (DMVPN)-specific session information, use the **show dmvpn** command in privileged EXEC mode.

show dmvpn [{**ipv4** [**vrf** *vrf-name*] | **ipv6** [**vrf** *vrf-name*]}] [{**debug-condition** | **interface tunnel** *number* | **peer** {**nbma** {*ipv4-addressipv6-address*} | **network** *network-mask* | **tunnel** *ip-address*} | **static** | **detail**}]

Syntax Description

ipv4	(Optional) Displays information about IPv4 private networks.
vrf *vrf-name*	(Optional) Displays information based on the specified virtual routing and forwarding (VRF) instance.
ipv6	(Optional) Displays information about IPv6 private networks.
debug-condition	(Optional) Displays DMVPN conditional debugging.
interface	(Optional) Displays DMVPN information based on a specific interface.
tunnel	(Optional) Displays DMVPN information based on the peer Virtual Private Network (VPN) address.
number	(Optional) The tunnel address for a DMVPN peer.
peer	(Optional) Displays information for a specific DMVPN peer.
nbma	Displays DMVPN information based on nonbroadcast multiaccess (NBMA) addresses.
ipv4-address	The DMVPN peer IPv4 address.
ipv6-address	The DMVPN peer IPv6 address.
network *network-mask*	Displays DMVPN information based on a specific destination network and mask address.
static	(Optional) Displays only static DMVPN information.
detail	(Optional) Displays detail DMVPN information for each session, including Next Hop Server (NHS) and NHS status, crypto session information, and socket details.

Command Default

Information is displayed for all DMVPN-specific sessions.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(9)T	This command was introduced.

Release	Modification
12.4(20)T	This command was modified. The following were added: **ipv4**, **ipv6**, *ipv6-address*, **network,**and *ipv6-address*.
12.4(22)T	This command was modified. The output of this command was extended to display the NHRP group received from the spoke and the Quality of Service (QoS) policy applied to the spoke tunnel.
15.2(1)T	This command was modified. The*ipv6-address* argument was added.

Usage Guidelines

Use this command to obtain DMVPN-specific session information. By default, summary information will be displayed.

When the **detail** keyword is used, command output will include information from the **show crypto session detail** command, including inbound and outbound security parameter indexes (SPIs) and the **show crypto socket** command.

Examples

The following example shows sample summary output:

```
Device# show dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        # Ent --> Number of NHRP entries with same NBMA peer
! The line below indicates that the sessions are being displayed for Tunnel1.
! Tunnel1 is acting as a spoke and is a peer with three other NBMA peers.
Tunnel1, Type: Spoke, NBMA Peers: 3,
 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     2    192.0.2.21       192.0.2.116   IKE     3w0d D
     1    192.0.2.102      192.0.2.11   NHRP 02:40:51 S
     1    192.0.2.225      192.0.2.10     UP     3w0d S
Tunnel2, Type: Spoke, NBMA Peers: 1,
 # Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
     1      192.0.2.25     192.0.2.171   IKE    never S
```

The table below describes the significant fields shown in the display.

Table 81: show dmvpn Field Descriptions

Field	Description
# Ent	The number of Next Hop Routing Protocol (NHRP) entries in the current session.
Peer NBMA Addr	The remote NBMA address.
Peer Tunnel Add	The remote tunnel endpoint IP address.
State	The state of the DMVPN session. The DMVPN session is either up or down. If the DMVPN state is down, the reason for the down state error is displayed--Internet Key Exchange (IKE), IPsec, or NHRP.
UpDn Tm	Displays how long the session has been in the current state.

Field	Description
Attrib	Displays any associated attributes of the current session. One of the following attributes will be displayed--dynamic (D), static (S), incomplete (I), Network Address Translation (NAT) for the peer address, or NATed, (N), local (L), no socket (X).

The following example shows sample summary output of the **show dmvpn** command with IPv6 information:

```
Device# show dmvpn

Interface: Tunnel0, IPv4 NHRP Details
Type:Spoke, NHRP Peers:1,

  Ent  Peer NBMA Addr        Peer Tunnel Add   State   UpDn Tm     Attrb
 ----- ---------------       ---------------   -----    --------  -----
     1 2001:DB8:0:ABCD::1    10.255.255.254    IKE      05:55:30   S

Interface: Tunnel0, IPv6 NHRP Details
Type:Spoke, Total NBMA Peers (v4/v6): 1
    1.Peer NBMA Address: 2001:DB8:0:ABCD::1
        Tunnel IPv6 Address: 2001:DB8:0:FFFF::1
        IPv6 Target Network: 2001:DB8:A:B::1/64
         Ent: 1, Status: IKE, UpDn Time: 05:55:30, Cache Attrib: S
```

In this example output the first line displays only tunnel count and peer NBMA address entries irrespective of the IPv6 address length. Other entries are displayed in the immediate next line. When you use **show dmvpn detail** command and in case if there are two tunnel entries with same NBMA address in the command output, tunnel count “0” in the second entry is not displayed and the extra line is removed between the entries in the output.

The following example shows output of the **show dmvpn** command with the **detail** keyword:

```
Device# show dmvpn detail

Legend: Attrb --> S - Static, D - Dynamic, I - Incomplete
        N - NATed, L - Local, X - No Socket
        # Ent --> Number of NHRP entries with same NBMA peer
-------------- Interface Tunnel1 info: --------------
Intf. is up, Line Protocol is up, Addr. is 192.0.2.5
   Source addr: 192.0.2.229, Dest addr: MGRE
  Protocol/Transport: "multi-GRE/IP", Protect "gre_prof",
Tunnel VRF "" ip vrf forwarding ""
NHRP Details: NHS: 192.0.2.10 RE 192.0.2.11  E
Type: Spoke, NBMA Peers: 4
# Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb    Target Network
----- --------------- --------------- ----- -------- ----- -----------------
    2        192.0.2.21      192.0.2.116    UP 00:14:59 D      192.0.2.118/24
                                            UP 00:14:59 D      192.0.2.116/32
  IKE SA: local 192.0.2.229/500 remote 192.0.2.21/500 Active
          Capabilities:(none) connid:1031 lifetime:23:45:00
  Crypto Session Status: UP-ACTIVE
  fvrf: (none)
  IPSEC FLOW: permit 47 host 192.0.2.229 host 192.0.2.21
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 1 drop 0 life (KB/Sec) 4494994/2700
        Outbound: #pkts enc'ed 1 drop 0 life (KB/Sec) 4494994/2700
   Outbound SPI : 0xD1EA3C9B, transform : esp-3des esp-sha-hmac
    Socket State: Open
```

```
# Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb    Target Network
----- --------------- --------------- ----- -------- ----- -----------------
    1     192.0.2.229       192.0.2.5    UP 00:15:00 DLX        192.0.2.5/32
# Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb    Target Network
----- --------------- --------------- ----- -------- ----- -----------------
    1     192.0.2.102      192.0.2.11 NHRP 02:55:47  S         192.0.2.11/32
  IKE SA: local 192.0.2.229/4500 remote 192.0.2.102/4500 Active
          Capabilities:N connid:1028 lifetime:11:45:37
  Crypto Session Status: UP-ACTIVE
  fvrf: (none)
  IPSEC FLOW: permit 47 host 192.0.2.229 host 192.0.2.102
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 199056 drop 393401 life (KB/Sec) 4560270/1524
        Outbound: #pkts enc'ed 416631 drop 10531 life (KB/Sec) 4560322/1524
   Outbound SPI : 0x9451AF5C, transform : esp-3des esp-sha-hmac
    Socket State: Open
# Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb    Target Network
----- --------------- --------------- ----- -------- ----- -----------------
    1     192.0.2.225      192.0.2.10    UP     3w0d S         192.0.2.10/32
  IKE SA: local 192.0.2.229/500 remote 192.0.2.225/500 Active
          Capabilities:(none) connid:1030 lifetime:03:46:44
  Crypto Session Status: UP-ACTIVE
  fvrf: (none)
  IPSEC FLOW: permit 47 host 192.0.2.229 host 192.0.2.225
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 430261 drop 0 life (KB/Sec) 4415197/3466
        Outbound: #pkts enc'ed 406232 drop 4 life (KB/Sec) 4415197/3466
   Outbound SPI : 0xAF3E15F2, transform : esp-3des esp-sha-hmac
    Socket State: Open
 -------------- Interface Tunnel2 info: --------------
Intf. is up, Line Protocol is up, Addr. is 192.0.2.172
   Source addr: 192.0.2.20, Dest addr: MGRE
  Protocol/Transport: "multi-GRE/IP", Protect "gre_prof",
Tunnel VRF "" ip vrf forwarding ""
NHRP Details: NHS:         192.0.2.171  E
Type: Spoke, NBMA Peers: 1
# Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb    Target Network
----- --------------- --------------- ----- -------- ----- -----------------
    1      192.0.2.25     192.0.2.171  IKE     never S        192.0.2.171/32
  IKE SA: local 192.0.2.20/500 remote 192.0.2.25/500 Inactive
          Capabilities:(none) connid:0 lifetime:0
  IKE SA: local 192.0.2.20/500 remote 192.0.2.25/500 Inactive
          Capabilities:(none) connid:0 lifetime:0
  Crypto Session Status: DOWN-NEGOTIATING
  fvrf: (none)
  IPSEC FLOW: permit 47 host 192.0.2.20 host 192.0.2.25
        Active SAs: 0, origin: crypto map
        Inbound:  #pkts dec'ed 0 drop 0 life (KB/Sec) 0/0
        Outbound: #pkts enc'ed 0 drop 436431 life (KB/Sec) 0/0
   Outbound SPI : 0x       0, transform :
    Socket State: Closed
Pending DMVPN Sessions:
!There are no pending DMVPN sessions.
```

The following example shows output of the **show dmvpn** command with the **detail** keyword. This example displays the NHRP group received from the spoke and the QoS policy applied to the spoke tunnel:

```
Device# show dmvpn detail

Legend: Attrb --> S - Static, D - Dynamic, I - Incompletea
        N - NATed, L - Local, X - No Socket
        # Ent --> Number of NHRP entries with same NBMA peer
```

```
 -------------- Interface Tunnel0 info: --------------
Intf. is up, Line Protocol is up, Addr. is 10.0.0.1
   Source addr: 172.17.0.1, Dest addr: MGRE
  Protocol/Transport: "multi-GRE/IP", Protect "dmvpn-profile",
Tunnel VRF "", ip vrf forwarding ""
NHRP Details:
Type:Hub, NBMA Peers:2
# Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb    Target Network
----- --------------- --------------- ----- -------- ----- -----------------
    1      172.17.0.2        10.0.0.2    UP 00:19:57 D           10.0.0.2/32
NHRP group: test-group-0
 Output QoS service-policy applied: queueing
  IKE SA: local 172.17.0.1/500 remote 172.17.0.2/500 Active
  Crypto Session Status: UP-ACTIVE
  fvrf: (none), Phase1_id: 172.17.0.2
  IPSEC FLOW: permit 47 host 172.17.0.1 host 172.17.0.2
        Active SAs: 2, origin: crypto map
   Outbound SPI : 0x44E4E634, transform : esp-des esp-sha-hmac
    Socket State: Open
  IKE SA: local 172.17.0.1/500 remote 172.17.0.2/500 Active
  IPSEC FLOW: permit 47 host 172.17.0.1 host 172.17.0.2
        Active SAs: 2, origin: crypto map
   Outbound SPI : 0x44E4E634, transform : esp-des esp-sha-hmac
    Socket State: Open
# Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb    Target Network
----- --------------- --------------- ----- -------- ----- -----------------
    1      172.17.0.3        10.0.0.3    UP 00:02:21 D           10.0.0.3/32
NHRP group: test-group-0
 Output QoS service-policy applied: queueing
  IKE SA: local 172.17.0.1/500 remote 172.17.0.3/500 Active
  Crypto Session Status: UP-ACTIVE
  fvrf: (none), Phase1_id: 172.17.0.3
  IPSEC FLOW: permit 47 host 172.17.0.1 host 172.17.0.3
        Active SAs: 2, origin: crypto map
   Outbound SPI : 0xBF13C9CC, transform : esp-des esp-sha-hmac
    Socket State: Open
  IKE SA: local 172.17.0.1/500 remote 172.17.0.3/500 Active
  IPSEC FLOW: permit 47 host 172.17.0.1 host 172.17.0.3
        Active SAs: 2, origin: crypto map
   Outbound SPI : 0xBF13C9CC, transform : esp-des esp-sha-hmac
    Socket State: Open
 -------------- Interface Tunnel1 info: --------------
Intf. is up, Line Protocol is up, Addr. is 11.0.0.1
   Source addr: 172.17.0.1, Dest addr: MGRE
  Protocol/Transport: "multi-GRE/IP", Protect "dmvpn-profile",
Tunnel VRF "", ip vrf forwarding ""
NHRP Details:
Type:Hub, NBMA Peers:1
# Ent  Peer NBMA Addr Peer Tunnel Add State  UpDn Tm Attrb    Target Network
----- --------------- --------------- ----- -------- ----- -----------------
    1      172.17.0.2        11.0.0.2    UP 00:20:01 D           11.0.0.2/32
NHRP group: test-group-1
 Output QoS service-policy applied: queueing
Pending DMVPN Sessions:
```

The following example shows DMVPN debug-condition information:

```
Device#  show dmvpn debug-condition

NBMA addresses under debug are:
Interfaces under debug are:
Tunnel101,
Crypto DMVPN filters:
```

```
Interface = Tunnel101
DMVPN Conditional debug context unmatched flag: OFF
```

Related Commands

Command	Description
debug dmvpn	Debugs DMVPN sessions.
show crypto session detail	Displays detailed status information for active crypto sessions.
show crypto socket	Lists crypto sockets.
show policy-map mgre	Displays statistics about a specific QoS policy as it is applied to a tunnel endpoint.

show dnsix

To display state information and the current configuration of the DNSIX audit writing module, use the **show dnsix**command in privil eged EXEC mode.

show dnsix

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following is sample output from the **show dnsix** command:

```
Router# show dnsix

Audit Trail Enabled with Source 192.168.2.5
          State: PRIMARY
          Connected to 192.168.2.4
          Primary 192.168.2.4
          Transmit Count 1
          DMDP retries 4
          Authorization Redirection List:
               192.168.2.4
          Record count: 0
          Packet Count: 0
          Redirect Rcv: 0
```

show dot1x

To display details for an identity profile, use the **show dot1x** command in privileged EXEC mode.

Note Effective with Cisco IOS Release 12.2(33)SXI, the **show dot1x** command is supplemented by the **show authentication** command. The **show dot1x** command is reserved for displaying output specific to the use of the 802.1X authentication method. The **show authentication sessions**command has a wider remit of displaying information for all authentication methods and authorization features. See the **show authentication sessions**command for more information.

show dot1x [{**all** [**summary**] | **interface** *interface-name* | **details** | **statistics**}]

Syntax Description

all	(Optional) Displays 802.1X status for all interfaces.
summary	(Optional) Displays summary of 802.1X status for all interfaces.
interface *interface-name*	(Optional) Specifies the interface name and number.
details	(Optional) Displays the interface configuration as well as the authenticator instances on the interface.
statistics	(Optional) Displays 802.1X statistics for all the interfaces.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.1(11)AX	This command was introduced.
12.1(14)EA1	The **all** keyword was added.
12.3(2)XA	This command was integrated into Cisco IOS Release 12.3(2)XA.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(25)SED	The output display was expanded to include auth-fail-vlan information in the authorization state machine state and port status fields.
12.2(25)SEE	The **details** and **statistics** keywords were added.
12.3(11)T	The PAE, HeldPeriod, StartPeriod, and MaxStart fields were added to the **show dot1x** command output.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

If you do not specify a port, global parameters and a summary appear. If you specify a port, details for that port appear in the output.

Note In some IOS versions, the **show dot1x** command may not display the AUTHORIZED or UNAUTHORIZED value in the Port Status command output field if authentication methods other than the 802.1X authentication method are used. If the Port Status field does not contain a value, then use the **show authentication sessions** command to display the Authz Success or Authz Failed port status authentication value.

Examples

The following is sample output from the **show dot1x** command using both the **interface** and **details** keywords. The clients are successfully authenticated in this example.

```
Router# show dot1x interface ethernet1/0 details
Dot1x Info for Ethernet1/0
----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = AUTO
ControlDirection          = Both
HostMode                  = MULTI_HOST
QuietPeriod               = 60
ServerTimeout             = 0
SuppTimeout               = 30
ReAuthMax                 = 2
MaxReq                    = 1
TxPeriod                  = 30
Dot1x Authenticator Client List
-------------------------------
Supplicant                = aabb.cc00.c901
Session ID                = 0A3462800000000000009F8
    Auth SM State         = AUTHENTICATED
    Auth BEND SM State    = IDLE
```

The following is sample output from the **show dot1x** command using both the **interface** and **details** keywords. The clients are unsuccessful at authenticating in this example.

```
Router# show dot1x interface ethernet1/0 details
Dot1x Info for Ethernet1/0
----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = AUTO
ControlDirection          = Both
HostMode                  = MULTI_HOST
QuietPeriod               = 60
ServerTimeout             = 0
SuppTimeout               = 30
ReAuthMax                 = 2
MaxReq                    = 1
TxPeriod                  = 30
Dot1x Authenticator Client List Empty
```

The table below describes the significant fields shown in the displays.

Table 82: show dot1x Field Descriptions

Field	Description
PAE	Port Access Entity. Defines the role of an interface (as a supplicant, as an authenticator, or as an authenticator and supplicant).
PortControl	Port control value. • AUTO--The authentication status of the client PC is being determined by the authentication process. • Force-authorize--All the client PCs on the interface are being authorized. • Force-unauthorized--All the client PCs on the interface are being unauthorized.
ControlDirection	Indicates whether control for an IEEE 802.1X controlled port is applied to both directions (ingress and egress), or inbound direction only (ingress). See 'dot1x control-direction', or effective from Cisco IOS Release 12.2(33)SXI onwards, authentication control-direction for more detail.
HostMode	Indicates whether the host-mode is single-host or multi-host, and effective from Cisco IOS Release 12.2(33)SXI onwards, multi-auth or multi-domain as well. See 'dot1x host-mode', or effective from Cisco IOS Release 12.2(33)SXI onwards, 'authentication host-mode' for more detail.
QuietPeriod	If authentication fails for a client, the authentication gets restarted after the quiet period shown in seconds.
ServerTimeout	Timeout that has been set for RADIUS retries. If an 802.1X packet is sent to the server and the server does not send a response, the packet will be sent again after the number of seconds that are shown.
SuppTimeout	Time that has been set for supplicant (client PC) retries. If an 802.1X packet is sent to the supplicant and the supplicant does not send a response, the packet will be sent again after the number of seconds that are shown.
ReAuthMax	The maximum amount of time in seconds after which an automatic reauthentication of a client PC is initiated.
MaxReq	Maximum number of times that the router sends an Extensible Authentication Protocol (EAP) request/identity frame (assuming that no response is received) to the client PC before concluding that the client PC does not support 802.1X.
TxPeriod	Timeout for supplicant retries, that is the timeout for EAP Identity Requests. See 'dot1x timeout tx-period' for more detail.
Supplicant	MAC address of the client PC or any 802.1X client.
Session ID	The ID of the network session.
Auth SM State	Describes the state of the client PC as either AUTHENTICATED or UNAUTHENTICATED.
Auth BEND SM State	The state of the IEEE 802.1X authenticator backend state machine.

Related Commands

Command	Description
clear dot1x	Clears 802.1X interface information.
debug dot1x	Displays 802.1X debugging information.
dot1x default	Resets the global 802.1X parameters to their default values.
identity profile	Creates an identity profile.
show authentication sessions	Displays information about current Authentication Manager sessions.

show dot1x (EtherSwitch)

To display the 802.1X statistics, administrative status, and operational status for the Ethernet switch network module or for the specified interface, use the **show dot1x** command in privileged EXEC mode.

show dot1x [**statistics**] [**interface interface-type interface-number**]

Syntax Description

statistics	(Optional) Displays 802.1X statistics.
interface *interface-type interface-number*	(Optional) Specifies the slot and port number of the interface to reauthenticate.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(6)EA2	This command was introduced.
12.2(15)ZJ	This command was implemented on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T on the following platforms: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series routers.

Usage Guidelines

If you do not specify an interface, global parameters and a summary appear. If you specify an interface, details for that interface appear.

If you specify an interface with the **statistics** keyword, statistics appear for all physical ports.

Examples

The following is sample output from the **show dot1x** command:

```
Router# show dot1x
Global 802.1X Parameters
    reauth-enabled               no
    reauth-period              3600
    quiet-period                 60
    tx-period                    30
    supp-timeout                 30
    server-timeout               30
    reauth-max                    2
    max-req                       2
802.1X Port Summary
    Port Name               Status      Mode                Authorized
    Gi0/1                   disabled    n/a                 n/a
    Gi0/2                   enabled     Auto (negotiate)    no
    802.1X Port Details
    802.1X is disabled on GigabitEthernet0/1
802.1X is enabled on GigabitEthernet0/2
      Status                Unauthorized
      Port-control          Auto
      Supplicant            0060.b0f8.fbfb
      Multiple Hosts        Disallowed
```

```
Current Identifier    2
Authenticator State Machine
  State               AUTHENTICATING
  Reauth Count        1
Backend State Machine
  State               RESPONSE
  Request Count       0
  Identifier (Server) 2
Reauthentication State Machine
  State               INITIALIZE
```

The table below describes the significant fields shown in the display.

Table 83: show dot1x Field Descriptions

Field	Description
reauth-enabled	Periodic reauthentication of client PCs on the interface has been enabled or disabled.
reauth-period	Time, in seconds, after which an automatic reauthentication will be initiated.
quiet-period	After authentication fails for a client, the authentication gets restarted after this quiet period shown in seconds.
tx-period	Time, in seconds, that the device waits for a response from a client to an Extensible Authentication Protocol (EAP) request or identity frame before retransmitting the request.
supp-timeout	Time, in seconds, that has been set for supplicant (client PC) retries. If an 802.1X packet is sent to the supplicant and the supplicant does not send a response, the packet will be sent again after the number of seconds that are shown.
server-timeout	Timeout, in seconds, that has been set for RADIUS retries. If an 802.1X packet is sent to the server and the server does not send a response, the packet will be sent again after the number of seconds that are shown.
reauth-max	The maximum number of times that the device tries to authenticate the client without receiving any response before the switch resets the port and restarts the authentication process.
max-req	Maximum number of times that the router sends an EAP request/identity frame (assuming that no response is received) to the client PC before concluding that the client PC does not support 802.1X.
Port Name	Interface type and slot/port numbers.
Status	Displays the 802.1X status of the port as either enabled or disabled.
Mode	Operational status of the port: • Auto--The port control value has been configured to be Force-unauthorized but the port has not changed to that state. • n/a--802.1X is disabled.
Authorized	Authorization state of the port.

Field	Description
Status	Status of the port (authorized or unauthorized). The status of a port appears as authorized if the **dot1x port-control** interface configuration command is set to **auto**, and authentication was successful.
Port-control	Setting of the **dot1x port-control** interface configuration command. The port control value is one of the following: • Auto--The authentication status of the client PC is being determined by the authentication process. • Force-authorize--All the client PCs on the interface are being authorized. • Force-unauthorized--All the client PCs on the interface are being unauthorized.
Supplicant	Ethernet MAC address of the client, if one exists. If the device has not discovered the client, this field displays *Not set* .
Multiple Hosts	Setting of the **dot1x multiple-hosts** interface configuration command (allowed or disallowed).
Current Identifier	Each exchange between the device and the client includes an identifier, which matches requests with responses. This number is incremented with each exchange and can be reset by the authentication server. **Note** This field and the remaining fields in the output show internal state information. For a detailed description of these state machines and their settings, refer to the IEEE 802.1X standard.

The following is sample output from the **show dot1x interface gigabitethernet0/2** privileged EXEC command. The table below describes the fields in the output.

```
Router# show dot1x interface gigabitethernet0/2
802.1X is enabled on GigabitEthernet0/2
  Status               Authorized
  Port-control         Auto
  Supplicant           0060.b0f8.fbfb
  Multiple Hosts       Disallowed
  Current Identifier   3
  Authenticator State Machine
    State              AUTHENTICATED
    Reauth Count       0
  Backend State Machine
    State              IDLE
    Request Count      0
    Identifier (Server) 2
Reauthentication State Machine
    State              INITIALIZE
```

The following is sample output from the **show dot1x statistics interface gigiabitethernet0/1** command. The table below describes the fields in the example.

```
Router# show dot1x statistics interface gigabitethernet0/1
GigabitEthernet0/1
    Rx: EAPOL     EAPOL     EAPOL     EAPOL     EAP       EAP       EAP
        Start     Logoff    Invalid   Total     Resp/Id   Resp/Oth  LenError
```

```
    0         0         0         21        0         0         0
    Last      Last
    EAPOLVer  EAPOLSrc
    1         0002.4b29.2a03
Tx: EAPOL     EAP       EAP
    Total     Req/Id    Req/Oth
    622       445       0
```

Table 84: show dot1x statistics Field Descriptions

Field	Description
Rx EAPOL Start	Number of valid EAPOL-start frames that have been received. **Note** EAPOL = Extensible Authentication Protocol over LAN
Rx EAPOL Logoff	Number of EAPOL-logoff frames that have been received.
Rx EAPOL Invalid	Number of EAPOL frames that have been received and have an unrecognized frame type.
Rx EAPOL Total	Number of valid EAPOL frames of any type that have been received.
Rx EAP Resp/ID	Number of EAP-response/identity frames that have been received.
Rx EAP Resp/Oth	Number of valid EAP-response frames (other than response/identity frames) that have been received.
Rx EAP LenError	Number of EAPOL frames that have been received in which the packet body length field is invalid.
Last EAPOLVer	Protocol version number carried in the most recently received EAPOL frame.
LAST EAPOLSrc	Source MAC address carried in the most recently received EAPOL frame.
Tx EAPOL Total	Number of EAPOL frames of any type that have been sent.
Tx EAP Req/Id	Number of EAP-request/identity frames that have been sent.
Tx EAP Req/Oth	Number of EAP-request frames (other than request/identity frames) that have been sent.

Related Commands

Command	Description
dot1x default	Resets the global 802.1X parameters to their default values.

show dss log

To display the invalidation routes for the DSS range on the NetFlow table in the EXEC command mode, use the **show dss log** command.

show dss log {**ip** | **ipv6**}

Syntax Description

ip	Displays the range-invalidation profile for the DSS IP.
ipv6	Displays the range-invalidation profile for the DSS IPv6.

Command Default

This command has no default settings.

Command Modes

EXEC

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17b)SXA	This command was changed to support the **ipv6** keyword.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.

Usage Guidelines

This command is not supported in Cisco 7600 series routers that are configured with a Supervisor Engine 2.

Whenever an IPv6 entry is deleted from the routing table, a message is sent to the switch processor to remove the entries that are associated to that network. Several IPv6 prefixes are collapsed to the less specific one if too many invalidations occur in a short period of time.

Examples

This example shows how to display the range-invalidation profile for the DSS IP:

```
Router# show dss log ip
22:50:18.551  prefix 172.20.52.18 mask 172.20.52.18
22:50:20.059  prefix 127.0.0.0 mask 255.0.0.0
22:51:48.767  prefix 172.20.52.18 mask 172.20.52.18
22:51:52.651  prefix 0.0.0.0 mask 0.0.0.0
22:53:02.651  prefix 0.0.0.0 mask 0.0.0.0
22:53:19.651  prefix 0.0.0.0 mask 0.0.0.0
Router#
```

show eap registrations

To display Extensible Authentication Protocol (EAP) registration information, use the **show eap registrations** command in privileged EXEC mode.

show eap registrations [{**method** | **transport**}]

Syntax Description

method	(Optional) Displays information about EAP method registrations only.
transport	(Optional) Displays information about EAP transport registrations only.

Command Default

If a keyword is not used, information is displayed for all lower layers used by EAP and for the methods that are registered with the EAP framework.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(25)SEE	This command was introduced.
12.4(6)T	This command was integrated into Cisco IOS Release 12.4(6)T.

Usage Guidelines

This command is used to check which EAP methods are enabled on a router.

Examples

The following is an example of output from the show eap registrations command:

```
Router# show eap registrations
Registered EAP Methods:
Method Type Name
4 Peer MD5
Registered EAP Lower Layers:
Handle Type Name
2 Authenticator Dot1x-Authenticator
1 Authenticator MAB
```

The following is an example of output from the show eap registrations command using the transport keyword:

```
Router# show eap registrations transport
Registered EAP Lower Layers:
Handle Type Name
2 Authenticator Dot1x-Authenticator
```

The output fields are self-explanatory.

Related Commands

Command	Description
clear eap	Clears EAP session information for the switch or specified port.

show eap sessions

To display active Extensible Authentication Protocol (EAP) session information, use the **show eap sessions** command in privileged EXEC mode.

show eap sessions [{**credentials** *credentials-name* | **interface** *interface-name* | **method** *method-name* | **transport** *transport-name*}]

Syntax Description

credentials *credentials-name*	(Optional) Displays information about the specified credentials profile.
interface *interface-name*	(Optional) Displays information, such as type, module, and port number, about sessions that are associated with the specified interface.
method *method-name*	(Optional) Displays information about sessions that are associated with the specified EAP method.
transport *transport-name*	(Optional) Displays information about sessions that are associated with the specified lower layer.

Command Default

All active EAP sessions are displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(25)SEE	This command was introduced.
12.4(6)T	This command was integrated into Cisco IOS Release 12.4(6)T.

Usage Guidelines

The command output can be filtered using any of the optional keywords, singly or in combination.

Examples

The following is an example of output from the show eap sessions command:

```
Router# show eap sessions
Role: Authenticator Decision: Fail
Lower layer: Dot1x-AuthenticaInterface: Gi1/0/1
Current method: None Method state: Uninitialised
Retransmission count: 0 (max: 2) Timer: Authenticator
ReqId Retransmit (timeout: 30s, remaining: 2s)
EAP handle: 0x5200000A Credentials profile: None
Lower layer context ID: 0x93000004 Eap profile name: None
Method context ID: 0x00000000 Peer Identity: None
Start timeout (s): 1 Retransmit timeout (s): 30 (30)
Current ID: 2 Available local methods: None
Role: Authenticator Decision: Fail
Lower layer: Dot1x-AuthenticaInterface: Gi1/0/2
Current method: None Method state: Uninitialised
Retransmission count: 0 (max: 2) Timer: Authenticator
ReqId Retransmit (timeout: 30s, remaining: 2s)
EAP handle: 0xA800000B Credentials profile: None
Lower layer context ID: 0x0D000005 Eap profile name: None
```

```
Method context ID: 0x00000000 Peer Identity: None
Start timeout (s): 1 Retransmit timeout (s): 30 (30)
Current ID: 2 Available local methods: None
.
.
.
```

The following is an example of output from the show eap sessions interface command:

```
Router# show eap sessions interface gigabitethernet1/0/1
Role: Authenticator Decision: Fail
Lower layer: Dot1x-AuthenticaInterface: Gi1/0/1
Current method: None Method state: Uninitialised
Retransmission count: 1 (max: 2) Timer: Authenticator
ReqId Retransmit (timeout: 30s, remaining: 13s)
EAP handle: 0x5200000A Credentials profile: None
Lower layer context ID: 0x93000004 Eap profile name: None
Method context ID: 0x00000000 Peer Identity: None
Start timeout (s): 1 Retransmit timeout (s): 30 (30)
```

The fields in the above output are self-explanatory.

Related Commands

Command	Description
clear eap sessions	Clears EAP session information for the switch or for the specified port.

show eou

To display information about Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP) global values or EAPoUDP session cache entries, use the **show eou** command in privileged EXEC mode.

show eou {**all** | **authentication** {**clientless** | **eap** | **static**} | **interface** *interface-type* | **ip** *ip-address* | **mac** *mac-address* | **posturetoken** *name*} [{**begin** | **exclude** | **include**} *expression*]

Syntax Description

all	Displays EAPoUDP information about all clients.
authentication	Authentication type.
clientless	Authentication type is clientless, that is, the endpoint system is not running Cisco Trust Agent (CTA) software.
eap	Authentication type is EAP.
static	Authentication type is statically configured.
interface	Provides information about the interface.
interface-type	Type of interface (see the table below for the interface types that may be shown).
ip	Specifies an IP address.
ip-address	IP address of the client device.
mac	Specifies a MAC address.
mac-address	The 48-bit address of the client device.
posturetoken	Displays information about a posture token name.
name	Name of the posture token.
begin	(Optional) Display begins with the line that matches the *expression* argument.
exclude	(Optional) Display excludes lines that match the *expression*argument.
include	(Optional) Display includes lines that match the specified *expression* argument.
expression	(Optional) Expression in the output to use as a reference point.

Command Default

All global EAPoUDP global values are displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(8)T	This command was introduced.

Release	Modification
12.2(18)SXF	This command was integrated into Cisco IOS Release 12.2(18)SXF.
12.2(25)SED	This command was integrated into Cisco IOS Release 12.2(25)SED.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(11)T	The output of this command was enhanced to display information about whether the session is using the AAA timeout policy.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

If you do not specify a port, global parameters and a summary appear. If you specify a port, details for that port appear.

Expressions are case sensitive. For example, if you enter "**exclude output**," the lines that contain "output" are not displayed, but the lines that contain "Output" appear.

The table below lists the interface types that may be used for the *interface-type* argument.

Table 85: Description of Interface Types

Interface Type	Description
Async	Asynchronous interface
BVI	Bridge-Group Virtual Interface
CDMA-Ix	Code division multiple access Internet exchange (CDMA Ix) interface
CTunnel	Connectionless Network Protocol (CLNS) tunnel (Ctunnel) interface
Dialer	Dialer interface
Ethernet	IEEE 802.3 standard interface
Lex	Lex interface
Loopback	Loopback interface
MFR	Multilink Frame Relay bundle interface
Multilink	Multilink-group interface
Null	Null interface
Serial	Serial interface
Tunnel	Tunnel interface
Vif	Pragmatic General Multicast (PGM) Multicase Host interface
Virtual-PPP	Virtual PPP interface

Interface Type	Description
Virtual-Template	Virtual template interface
Virtual-TokenRing	Virtual TokenRing interface

Examples

The following output displays information about a global EAPoUDP configuration. The default values can be changed or customized using the **eou default**, **eou max-retry**, **eou revalidate**, or **eou timeout** commands, depending on whether you configure them globally or on a specific interface.

```
Router# show eou
Global EAPoUDP Configuration
----------------------------
EAPoUDP Version     = 1
EAPoUDP Port        = 0x5566
Clientless Hosts    = Disabled
IP Station ID       = Disabled
Revalidation        = Enabled
Revalidation Period = 36000 Seconds
ReTransmit Period   = 3 Seconds
StatusQuery Period  = 300 Seconds
Hold Period         = 180 Seconds
AAA Timeout         = 60 Seconds
Max Retries         = 3
EAPoUDP Logging     = Disabled
Clientless Host Username = clientless
Clientless Host Password = clientless
Interface Specific EAPoUDP Configurations
----------------------------------------
Interface Ethernet2/1
```

No interface specific configuration

```
The following output displays information about a global EAPoUDP configuration that includes
 a NAC Auth Fail Open policy for use when the AAA server is unavailable:
Router# show eou ip 10.0.0.1
Address : 10.0.0.1
MAC Address : 0001.027c.f364
Interface : Vlan333
AuthType : AAA DOWN
AAA Down policy : rule_policy
Audit Session ID : 00000000011C11830000000311000001
PostureToken : -------
Age(min) : 0
URL Redirect : NO URL REDIRECT
URL Redirect ACL : NO URL REDIRECT ACL
ACL Name : rule_acl
Tag Name : NO TAG NAME
User Name : UNKNOWN USER
Revalidation Period : 500 Seconds
Status Query Period : 300 Seconds
Current State : AAA DOWN
```

The table below describes the significant fields shown in the display

Table 86: show eou Field Descriptions

Field	Description
EAPoUDP Version	EAPoUDP protocol version.
EAPoUDP Port	EAPoUDP port number.
Clientless Hosts	Clientless hosts are enabled or disabled.
IP Station ID	Specifies whether the IP address is allowed in the AAA station-id field. By default, it is disabled.
Revalidation	Revalidation is enabled or disabled.
Revalidation Period	Specifies whether revalidation of hosts is enabled. By default, it is disabled.
ReTransmit Period	Specifies the EAPoUDP packet retransmission interval. The default is 3 seconds.
StatusQuery Period	Specifies the EAPoUDP status query interval for validated hosts. The default is 300 seconds.
Hold Period	Hold period following a failed authentication.
AAA Timeout	AAA timeout period.
Max Retries	Maximum number of allowable retransmissions.
EAPoUDP Logging	Logging is enabled or disabled.
AAA Down policy	Name of policy to be applied when the AAA server is unreachable. (This is the NAC Auth Fail Open policy.)

Related Commands

Command	Description
eou default	Sets global EAPoUDP parameters to the default values.
eou max-retry	Sets the number of maximum retry attempts for EAPoUDP.
eou rate-limit	Sets the number of simultaneous posture validations for EAPoUDP.
eou timeout	Sets the EAPoUDP timeout values.

show epm session

To display information about Enforcement Policy Module (EPM) sessions, use the **show epm session**command in privileged EXEC mode.

show epm session {**interface** *type number* | **ip** {*ip-address* [**client** *client-type*] | **all**} | **mac** {*mac-address* [**client** *client-type*] | **all**} | **summary**}

Syntax Description

interface	Displays interface based session information.
type	Interface type.
number	Interface number.
ip	Displays information specifically for an IP address.
ip-address	IP address for the session.
client	(Optional) Specifies information about the type of client.
client-type	(Optional) Type of client. Values are **cts**, **dot1x**, **eapoudp**, **mab**, and **proxy**.
mac	Displays MAC address based session information.
mac-address	MAC address of the client.
all	Displays information for all sessions.
summary	Displays summary of session information such as IP address, MAC address, and so on for all the active sessions.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.2(33)SXI2	This command was integrated into Cisco IOS Release 12.2(33)SXI2. The **all** keyword was added, and, **cts**, **dot1x**, and **mab** values for the *client-type* argument were added.

Examples

The following output shows information specifically for MAC address 0001.027c.f380:

```
Router#
show epm session mac 0001.027c.f380 client dot1x
Admission feature       : DOT1X
AAA Policies            :
ACS ACL                 : xACSACLx-IP-VERY_SIMPLE_ACL-459b9870
SGT                     : 1357-BAD123456789
```

The following output shows information specifically for IP address 10.9.0.1:

```
Router# show epm session ip 10.9.0.1
Admission feature       : AUTHPROXY
AAA Policies            :
Input Service Policy    : epm-pol-map
Proxy ACL               : permit udp any any
Proxy ACL               : deny icmp any any
ACS ACL                 : xACSACLx-IP-VERY_SIMPLE_ACL-472594af
Admission feature       : EAPOUDP
AAA Policies            :
ACS ACL                 : xACSACLx-IP-VERY_SIMPLE_ACL-459b9870
Proxy ACL               : permit udp any any
Proxy ACL               : permit icmp any any
Proxy ACL               : permit tcp an
Admission feature       : DOT1X
AAA Policies            :
ACS ACL                 : xACSACLx-IP-VERY_SIMPLE_ACL-459b9870
SGT                     : 1357-BAD123456789
```

The following example shows summary information for all sessions:

```
Router# show epm session summary
EPM Session Information
-------------------------
Total sessions seen so far : 5
Total active sessions      : 5
Interface              IP Address          MAC Address       Audit Session Id:
-------------------------------------------------------------------------------
GigabitEthernet7/2     209.165.200.225     0001.027c.f380    160000020000000000003A4EC
GigabitEthernet7/2     209.165.200.227     0001.027c.f380    160000020000000010003AD68
GigabitEthernet7/2     209.165.200.230     0001.027c.f380    160000020000000020003C110
GigabitEthernet7/2     209.165.200.235     0001.027c.f380    160000020000000030003D6BC
GigabitEthernet7/15    0.0.0.0             0030.6eb6.c69a    0904010C000000000002F6A4
```

The table below describes significant fields shown in the displays.

Table 87: show epm session ip Field Descriptions

Field	Description
Admission feature	Admission feature authentication proxy or Extensible Authentication Protocol over UDP (EOU) acting on the host.
AAA Policies	AAA policy information.
ACS ACL	Access control server (ACS) access control list (ACL).
SGT	Security group tag (SGT) value assigned to the host of that initiated the session.
Input Service Policy	Input service policy for the session.
Proxy ACL	Proxy access control list.
Total sessions seen so far	Total number of hosts connected to the Network Access Device (NAD) until now.
Total active sessions	Total number of active sessions.
Interface	Interface type and number.
IP Address	IP address of the host.

Field	Description
MAC Address	MAC address of the host.
Audit Session Id	Audit session ID.

show firewall vlan-group

To display secure virtual LANs (VLANs) attached to a secure group, use the **show firewall vlan-group** command in user EXEC or privileged EXEC mode.

show firewall vlan-group [*number*]

Syntax Description

number	(Optional) VLAN group number. The range is from 1 to 65535.

Command Default

This command has no default settings.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SXI1	This command was introduced.
12.2(33)SXJ	This command was modified. The command output was modified to display the VLAN groups created by both the Application Control Engine (ACE) and firewall.

Examples

The following is sample output from the **show firewall vlan-group** command:

```
Router# show firewall vlan-group

Display vlan-groups created by both ACE module and Firewall
Group    Created by      vlans
-----    ----------      -----
  142      Firewall      142
  200      Firewall      200-201
  360      Firewall      360-369
  380      Firewall      380-389
  500      Firewall      390-399
  660      Firewall      660-669
```

The table below describes the fields shown in the display.

Table 88: show firewall vlan-group Field Descriptions

Field	Description
Group	Group number to which the VLANs belong.
Created by	Indicates whether the VLAN groups are created by the ACE or the firewall.
vlans	VLAN ranges.

Related Commands

Command	Description
firewall	Specifies secure VLAN groups and attaches them to firewall modules.

show flow internal field

To display Flexible NetFlow flow export fields, use the **show flow internal field** in privileged EXEC mode.

show flow internal field [{**apps** | **builtin**}]

Syntax Description

apps	(Optional) Displays the application fields.
builtin	(Optional) Displays the built-in fields.

Command Modes

Privileged EXEC(#)

Command History

Release	Modification
15.4(2)T	This command was introduced.

Usage Guidelines

Use this command to view the flow fields supported by Flexible NetFlow and Cisco Performance Monitor.

Examples

The following is sample output from the **show flow internal field** command. The output fields are self-explanatory.

```
Device# show flow internal field

Builtin field                                    Available in records
=============                                    ====================
reserved                                         None
unrecognised                                     None
unsupported                                      None
l2 src vlan id                                   None
l2 dst vlan id                                   None
datalink encap size                              None
datalink ethertype                               None
datalink frametype                               None
datalink bridgegroup                             None
datalink header len                              None
datalink payload len                             None
datalink header paksect                          None
datalink payload paksect                         None
datalink vlan input                              None
datalink dot1q vlan input                        FNF, MMON
datalink dot1q vlan output                       FNF, MMON
datalink dot1q ce vlan                           None
datalink dot1q priority                          None
datalink dot1q ce priority                       None
datalink metro vcid                              None
datalink metro vctype                            None
datalink metro control word                      None
datalink metro peer id                           None
mac src addr                                     None
mac dst addr                                     None
datalink mac src addr input                      FNF, MMON
datalink mac src addr output                     FNF, MMON
datalink mac dst addr input                      FNF, MMON
```

```
datalink mac dst addr output                  FNF, MMON
ip version                                    FNF, MMON
ip tos                                        FNF, MMON
ip dscp                                       FNF, MMON
ip prec                                       FNF, MMON
ip prot                                       FNF, MMON
ip ttl                                        FNF, MMON
ip ttl min                                    FNF, MMON
ip ttl max                                    FNF, MMON
ip length header                              FNF, MMON
ip length payload                             FNF, MMON
ip length total                               FNF, MMON
ip length total min                           FNF, MMON
ip length total max                           FNF, MMON
ip frag flags                                 FNF, MMON
ip frag offset                                FNF, MMON
ip frag id                                    None
ip header paksect                             FNF, MMON
ip payload paksect                            FNF, MMON
ip src as                                     FNF, MMON
ip dst as                                     FNF, MMON
ip src peer as                                FNF, MMON
ip dst peer as                                FNF, MMON
ip src as 4-octet                             FNF, MMON
ip dst as 4-octet                             FNF, MMON
ip src peer as 4-octet                        FNF, MMON
ip dst peer as 4-octet                        FNF, MMON
ip src traffic index                          FNF, MMON
ip dst traffic index                          FNF, MMON
ip fwd status                                 FNF, MMON
ip is multicast                               FNF, MMON
ip replication                                FNF, MMON
ip vrf id input                               FNF, MMON
ip vrf name                                   None
ipv4 next hop addr                            FNF, MMON
ipv4 next hop addr bgp                        FNF, MMON
ipv6 next hop addr                            FNF, MMON
ipv6 next hop addr bgp                        FNF, MMON
ipv4 version                                  None
ipv4 header len                               FNF, MMON
ipv4 length header                            None
ipv4 length payload                           None
ipv4 length total                             None
ipv4 length total min                         None
ipv4 length total max                         None
!
!
!
```

Related Commands

Command	Description
flow exporter	Creates or modifies a Flexible NetFlow flow exporter and enters flow exporter configuration mode.

show fm private-hosts

To display information about the Private Hosts feature manager, use the **show fm private-hosts** command in privileged EXEC mode.

show fm private-hosts {**all** | **interface** *type* / *num*}

Syntax Description

all	Displays the feature manager information for all of the interfaces that are configured for Private Hosts.
interface *type* / *num*	Displays the feature manager information for a specific interface. The slash (/) is required.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Examples

The following example displays information about the Private Hosts feature manager:

```
Router# show fm private-hosts interface GigabitEthernet1/2
------------------------------------------------------------------------------
FM_FEATURE_PVT_HOST_INGRESS      i/f: Gi1/2      map name:
PVT_HOST_ISOLATED
==============================================================================
------------------------------------------------------------
MAC Seq. No: 10          Seq. Result : PVT_HOSTS_ACTION_DENY
------------------------------------------------------------
Indx - VMR index      T     - V(Value)M(Mask)R(Result)
EtTy - Ethernet Type  EtCo  - Ethernet Code
+----+-+--------------+--------------+----+----+
|Indx|T|   Dest Node  |  Source Node |EtTy|EtCo|
+----+-+--------------+--------------+----+----+
 1    V 0000.0000.0000 0000.1111.4001    0 0
      M 0000.0000.0000 ffff.ffff.ffff    0 0
      TM_PERMIT_RESULT
 2    V 0000.0000.0000 0000.0000.0000    0 0
      M 0000.0000.0000 0000.0000.0000    0 0
      TM_L3_DENY_RESULT
------------------------------------------------------------
MAC Seq. No: 20          Seq. Result : PVT_HOSTS_ACTION_PERMIT
------------------------------------------------------------
+----+-+--------------+--------------+----+----+
|Indx|T|   Dest Node  |  Source Node |EtTy|EtCo|
+----+-+--------------+--------------+----+----+
 1    V 0000.1111.4001 0000.0000.0000    0 0
      M ffff.ffff.ffff 0000.0000.0000    0 0
      TM_PERMIT_RESULT
 2    V 0000.0000.0000 0000.0000.0000    0 0
      M 0000.0000.0000 0000.0000.0000    0 0
```

```
      TM_L3_DENY_RESULT
-------------------------------------------------------------
MAC Seq. No: 30          Seq. Result : PVT_HOSTS_ACTION_REDIRECT
-------------------------------------------------------------
+----+-+--------------+--------------+----+----+
|Indx|T|   Dest Node  |  Source Node |EtTy|EtCo|
+----+-+--------------+--------------+----+----+
 1    V ffff.ffff.ffff 0000.0000.0000    0 0
      M ffff.ffff.ffff 0000.0000.0000    0 0
      TM_PERMIT_RESULT
 2    V 0000.0000.0000 0000.0000.0000    0 0
      M 0000.0000.0000 0000.0000.0000    0 0
      TM_L3_DENY_RESULT
-------------------------------------------------------------
MAC Seq. No: 40          Seq. Result : PVT_HOSTS_ACTION_PERMIT
-------------------------------------------------------------
+----+-+--------------+--------------+----+----+
|Indx|T|   Dest Node  |  Source Node |EtTy|EtCo|
+----+-+--------------+--------------+----+----+
 1    V 0100.5e00.0000 0000.0000.0000    0 0
      M ffff.ff80.0000 0000.0000.0000    0 0
      TM_PERMIT_RESULT
 2    V 3333.0000.0000 0000.0000.0000    0 0
      M ffff.0000.0000 0000.0000.0000    0 0
      TM_PERMIT_RESULT
 3    V 0000.0000.0000 0000.0000.0000    0 0
      M 0000.0000.0000 0000.0000.0000    0 0
      TM_L3_DENY_RESULT
-------------------------------------------------------------
MAC Seq. No: 50          Seq. Result : PVT_HOSTS_ACTION_DENY
-------------------------------------------------------------
+----+-+--------------+--------------+----+----+
|Indx|T|   Dest Node  |  Source Node |EtTy|EtCo|
+----+-+--------------+--------------+----+----+
 1    V 0000.0000.0000 0000.0000.0000    0 0
      M 0000.0000.0000 0000.0000.0000    0 0
      TM_PERMIT_RESULT
 2    V 0000.0000.0000 0000.0000.0000    0 0
      M 0000.0000.0000 0000.0000.0000    0 0
      TM_L3_DENY_RESULT
Interfaces using this pvt host feature in ingress dir.:
-----------------------------------------------
  Interfaces (I/E = Ingress/Egress)
```

Related Commands

Command	Description
private-hosts	Enables or configures the private host feature.
private-hosts mode	Sets the switchport mode.
show fm private-hosts	Displays the FM-related private hosts information.
show private-hosts configuration	Displays Private Hosts configuration information for the router.
show **private-hosts interface configuration**	Displays Private Hosts configuration information for individual interfaces.

show fpm package-group

Note Effective with Cisco IOS Release 15.2(4)M, the **show fpm package-group** command is not available in Cisco IOS software.

To display configuration information about flexible packet matching (FPM) package support, use the **show fpm package-group** command in user EXEC or privileged EXEC mode.

show fpm package-group [{**control-plane** | **fpm-package-group** | **interface interface-name**}]

Syntax Description

control-plane	(Optional) Displays FPM package group control plane information.
fpm-group-name	(Optional) Displays FPM group name information.
interface	(Optional) Displays FPM package group interface information.
interface-name	Name of the Interface for which you want to show the FPM package group information. See the table below for a list of valid interfaces.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced.
15.2(4)M	This command was removed from the Cisco IOS software.

Usage Guidelines

The table below displays valid interfaces that may be shown as the *interface-name* argument with the **interface** keyword.

Table 89: Interfaces That Can Be Shown

Interface	Description
ATM	ATM interface
Async	Asynchronous interface
Auto-template	Auto-Template interface
BVI	Bridge-Group Virtual Interface
CDMA-Ix	CDMA Ix interface
CTunnel	CTunnel interface

Interface	Description
Dialer	Dialer interface
FastEthernet	FastEthernet IEEE 802.3
Lex	Lex interface
LongReachEthernet	Long-Reach Ethernet interface
Loopback	Loopback interface
MFR	Multilink Frame Relay bundle interface
Multilink	Multilink-group interface
Null	Null interface
Pos	Packet over SONET interface
Port-channel	Ethernet channel of interfaces
SSLVPN-VIF	Secure Socket Layer Virtual Private Network (SSLVPN) Virtual Interface
Serial	Serial
Tunnel	Tunnel interface
vif	Pragmatic General Multicast (PGM) multicast host interface
virtual-PPP	Virtual PPP interface
virtual-Template	Virtual template interface
virtual-TokenRing	Virtual TokenRing
vmi	Virtual Multipoint Interface

Examples

The following is sample output from the **show fpm package-group** command.

```
Router# show fpm package-group

 group name: cisco-fpm-packages
  auto-load
  fpm package: fpm-package-11
  fpm package: fpm-package-43
   package action: log
```

The table below describes the significant fields shown in the display.

Table 90: show fpm package-group Field Descriptions

Field	Description
Auto-load	Displays if automatic loading of FPM package support is configured.

Field	Description
FPM package	Displays the name of the FPM package loaded from the FPM-server.
Group name	Displays the protocol to connect to the FPM-server.
Package action	Displays the action taken when the FPM package is loaded.

Related Commands

Command	Description
show fpm package-info	Displays FPM package transfer configuration details.

show fpm package-info

Note Effective with Cisco IOS Release 15.2(4)M, the **show fpm package-info** command is not available in Cisco IOS software.

FPM server

To display information about fpm package transfer between an FPM server and a local server, use the **show fpm package-info** command in user EXEC or privileged EXEC mode.

show fpm package-info

Syntax Description

This command has no keywords or arguments.

Command Default

The command displays information about the transfer of fpm package groups from the FPM server to a local server.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced.
15.2(4)M	This command was removed from the Cisco IOS software.

Examples

The following is sample output from the **show fpm package-info** command.

```
Router# show fpm package-info
Router# show fpm package-info
 fpm package-info
  host 10.0.0.1
  remote-path bluebell/
  local-path flash:
  user cisco
  password 7 0101130A5D04141D245F5A1B0C0B57
  protocol tftp
  time-range weekly
```

The table below describes the significant fields shown in the display.

Table 91: show fpm package-info Field Descriptions

Field	Description
Host	Displays the download server address.
Local-path	Displays the location where packages are stored on the local router.

Field	Description
Password	Displays and encrypted password for the server.
Protocol	Displays the protocol to connect to the server.
Remote-path	Displays the file server name.
Time-range	Displays the interval between searches for fpm updates.
User	Displays the username on the server.

Related Commands

Command	Description
show fpm package-group	Displays fpm package matching support configuration details.

show fm raguard

To display the interfaces configured with router advertisement (RA) guard, use the **show fm raguard**command in privileged EXEC mode.

show fm raguard

Syntax Description

This command has no arguments or keywords.

Command Default

RA guard interface information is not displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(33)SXI4	This command was introduced.
12.2(54)SG	This command was modified. Support for Cisco IOS Release 12.2(54)SG was added.

Usage Guidelines

Use the **show fm raguard** command to verify information about interfaces that are configured with RA guard.

Examples

The following example enables the display of interfaces configured with IPv6 RA guard:

```
Router# show fm raguard
------------------------------------------------------------------------------
 IPV6 RA GUARD in Ingress direction is configured on following interfaces
==============================================================================
Interface: Port-channel23
Interface: GigabitEthernet4/6
```

The table below describes the significant fields shown in the display.

Table 92: show fm raguard Field Descriptions

Field	Description
IPV6 RA GUARD in Ingress direction is configured on following interfaces	Displays the interfaces configured with IPv6 RA guard.

show idmgr

To display information related to the Intelligent Services Gateway (ISG) session identity, use the **show idmgr** command in privileged EXEC mode.

show idmgr {[**memory detailed component** *substring*] | **service key session-handle** *session-handle* **service-key** *key-value* | **session key** | **aaa-unique-id** *aaa-unique-id-string* | **domainip-vrf ip-address** *ip-address* **vrf-id** *vrf-id* | **nativeip-vrf ip-address** *ip-address* **vrf-id** *vrf-id* | **portbundle ip** *ip-address* **bundle** *bundle-number* | **session-guid** *session-guid* | **session-handle** *session-handle-string* | **session-id** *session-id-string* | **circuit-id** *circuit-id* | **pppoe-unique-id** *pppoe-id* | **statistics**}

Syntax Description

memory	Displays memory-usage information related to ID management.
detailed	(Optional) Displays detailed memory-usage information related to ID management.
component	(Optional) Displays information for the specified ID management component.
substring	(Optional) Substring to match the component name.
service key	Displays ID information for a specific service.
session-handle *session-handle-string*	Displays the unique identifier for a session.
service-key *key-value*	Displays ID information for a specific service.
session key	Displays ID information for a specific session and its related services.
aaa-unique-id *aaa-unique-id-string*	Displays the authentication, authorization, and accounting (AAA) unique ID for a specific session.
domainip-vrf ip-address *ip-address*	Displays the service-facing IP address for a specific session.
vrf-id *vrf-id*	Displays the VPN routing and forwarding (VRF) ID for the specific session.
nativeip-vrf ip-address *ip-address*	Displays the subscriber-facing IP address for a specific session.
portbundle ip *ip-address*	Displays the port bundle IP address for a specific session.
bundle *bundle-number*	Displays the bundle number for a specific session.
session-guid *session-guid*	Displays the global unique identifier for a session.
session-handle *session-handle-string*	Displays the session identifier for a specific session.
session-id *session-id-string*	Displays the session identifier used to construct the value for RADIUS attribute 44 (Acct-Session-ID).
circuit-id *circuit-id*	Displays the user session information in the ID Manager (IDMGR) database when you specify the unique circuit ID tag.

pppoe-**unique-id** *pppoe-id*	Displays the PPPoE unique key information in the ID Manager (IDMGR) database when you specify the unique PPPoE unique ID tag
statistics	Displays statistics related to storing and retrieving ID information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(28)SB	This command was introduced.
Cisco IOS XE Release 2.6	The circuit-id keyword and *circuit-id*argument was added.

Examples

The following sample output for the **show idmgr** command displays information about the service called “service”:

```
Router# show idmgr service key session-handle 48000002 service-key service
session-handle = 48000002
service-name = service
idmgr-svc-key = 4800000273657276696365
authen-status = authen
```

The following sample output for the **show idmgr** command displays information about a session and the service that is related to the session:

```
Router# show idmgr session key session-handle 48000002

session-handle = 48000002
aaa-unique-id = 00000002
authen-status = authen
username = user1
Service 1 information:
session-handle = 48000002
service-name = service
idmgr-svc-key = 4800000273657276696365
```

The following sample output for the **show idmgr** command displays information about the global unique identifier of a session:

```
Router# show idmgr session key session-guid 020202010000000C
session-handle = 18000003
aaa-unique-id = 0000000C
authen-status = authen
interface = nas-port:0.0.0.0:2/0/0/42
authen-status = authen
username = FortyTwo
addr = 100.42.1.1
session-guid = 020202010000000C
The following sample output for the show idmgr
 command displays information about the user session information in the ID Manager (IDMGR)
 database by specifying the unique circuit ID tag:
Router# show idmgr session key circuit-id Ethernet4/0.100:PPPoE-Tag-1
session-handle = AA000007
aaa-unique-id = 0000000E
circuit-id-tag = Ethernet4/0.100:PPPoE-Tag-1
```

```
interface = nas-port:0.0.0.0:0/1/1/100
authen-status = authen
username = user1@cisco.com
addr = 106.1.1.3
session-guid = 650101020000000E
The session hdl AA000007 in the record is valid
The session hdl AA000007 in the record is valid
No service record found
```

The table below describes the significant fields shown in the display.

Table 93: show idmgr Field Descriptions

Field	Description
session-handle	Unique identifier of the session.
service-name	Service name for this session.
idmgr-svc-key	The ID manager service key of this session.
authen-status	Indicates whether the session has been authenticated or unauthenticated.
aaa-unique-id	AAA unique ID of the session.
username	The username associated with this session.
interface	The interface details of this session.
addr	The IP address of this session.
session-guid	Global unique identifier of this session.

Related Commands

Command	Description
subscriber access pppoe unique-key circuit-id	Specifies a unique circuit ID tag for a PPPoE user session to be tapped on the router.

show interface virtual-access

To display virtual access interface information, use the **show interface virtual-access** command in user EXEC or privileged EXEC mode.

show interface virtual-access *interface-number* [{**accounting** | **configuration** | **counters protocol status** | **crb** | **dampening** | **description** | **fair-queue** | **irb** | **mpls-exp** | **precedence** | **random-detect** | **rate-limit** | **stats** | **summary** | **switching**}]

Syntax Description

interface-number	Virtual access interface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.
accounting	(Optional) Displays virtual access interface accounting information.
configuration	(Optional) Displays virtual access interface configuration information.
counters protocol status	(Optional) Displays information about the current status of protocol counters that are enabled.
crb	(Optional) Displays virtual access interface concurrent routing and bridging (CRB) information.
dampening	(Optional) Displays virtual access interface dampening information.
description	(Optional) Displays virtual access interface description.
fair-queue	(Optional) Displays virtual access interface weighted fair queueing (WFQ) information.
irb	(Optional) Displays virtual access interface integrated routing and bridging (IRB) information.
mpls-exp	(Optional) Displays virtual interface Multiprotocol Label Switching (MPLS) experimental accounting information.
precedence	(Optional) Displays virtual interface precedence accounting information.
random-detect	(Optional) Displays virtual interface Weighted Random Early Detection (WRED) information.
rate-limit	(Optional) Displays virtual interface rate-limit information.
stats	(Optional) Displays virtual interface packets and octets, in and out, by switching path.
summary	(Optional) Displays the virtual interface summary.
switching	(Optional) Displays virtual interface switching information.

Command Default

If no keyword is specified, general information about virtual access interfaces is displayed.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
15.1(1)T	This command was introduced in a release earlier than Cisco IOS Release 15.1(1)T.

Examples

The following is sample output from the **show interface virtual-access**command:

```
Router# show interface virtual-access 1
Virtual-Access1 is up, line protocol is up
Hardware is Virtual Access interface
Description: ***Internally created by SSLVPN context c3***
Interface is unnumbered. Using address of Virtual-Access1 (0.0.0.0)
MTU 1406 bytes, BW 100000 Kbit/sec, DLY 100000 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation SSL
SSL vaccess, cloned from Virtual-Template1
Vaccess status 0x4, loopback not set
ARP type: ARPA, ARP Timeout 04:00:00
Last input never, output never, output hang never
Last clearing of "show interface" counters 2d16h
Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
Queueing strategy: fifo
Output queue: 0/40 (size/max)
5 minute input rate 24 bits/sec, 10 packets/sec
5 minute output rate 16 bits/sec, 10 packets/sec
100 packets input, 2000 bytes, 23 no buffer
Received 79 broadcasts, 30 runts, 20 giants, 29 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
12 packets output, 1100 bytes, 10 underruns
6 output errors, 5 collisions, 1 interface resets
9 unknown protocol drops
10 unknown protocol drops
29 output buffer failures, 10 output buffers swapped out
25 carrier transitions
```

The table below describes the significant fields shown in the display.

Table 94: show interface virtual-access Field Descriptions

Field	Description
Using address of Virtual-Access1	IP address of the virtual interface.
MTU	MTU, in bytes. Default: 1500.
BW	Bandwidth, in Kb/s.
DLY	Delay, in microseconds.
reliability	Reliability of the interface as a fraction of 255. Default: Calculated as an exponential average over five minutes. • 255/255 provides 100 percent reliability.

Field	Description
txload	Transmission load on an interface as a fraction of 255.
rxload	Receiver load on an interface as a fraction of 255.
Encapsulation	Data-link encapsulation.
SSL vaccess	Specifies Secure Socket Layer Virtual Private Network (SSL VPN) virtual access.
Vaccess status	Status of the virtual access.
ARP type	Type of Address Resolution Protocol (ARP).
ARP Timeout	Amount of time an entry remains in the ARP cache.
Input queue	Number of packets in the input queue.
Total output drops	Total number of packets dropped.
Queueing strategy	Theory followed to treat the packets in a queue.
Output queue	Number of packets in the output queue.
broadcasts	Total number of broadcast or multicast packets received.
runts	Total number of packets discarded due to the packet size being less than the minimum packet size (64 bytes).
giants	Total number of packets discarded due to the packet size exceeding the maximum packet size.
throttles	Total number of throttles.
input errors	Total number of errors that prevented the receipt of datagrams.
CRC	Mismatch generated by the cyclic redundancy checksum (CRC).
frame	Total number of packets received with a CRC error.
overrun	Total number of times data has not reached the serial receiver buffer because of the input rate is more than the receiver can handle.
ignored	Total number of packets ignored by the interface because of the scarcity of internal buffers.
abort	Total number of packets terminated.
output errors	Total number of errors that prevented the final transmission.
collisions	Total number of collisions encountered.
interface resets	Total number of times an interface has been completely reset.
output buffer failures	Total number of buffer failures.

Field	Description
carrier transitions	Interface transitions.

Related Commands

Command	Description
clear interface virtual-access	Clears the virtual access interface and frees the memory for other dial-in uses.

show ip access-lists

To display the contents of all current IP access lists, use the **show ip access-lists** command in user EXEC or privileged EXEC modes.

show ip access-lists [{*access-list-numberaccess-list-number-expanded-rangeaccess-list-name* | **dynamic** [*dynamic-access-list-name*] | **interface** *name number* [{**in** | **out**}]}]

Syntax Description

access-list-number	(Optional) Number of the IP access list to display.
access-list-number-expanded-range	(Optional) Expanded range of the IP access list to display.
access-list-name	(Optional) Name of the IP access list to display.
dynamic *dynamic-access-list-name*	(Optional) Displays the specified dynamic IP access lists.
interface *name number*	(Optional) Displays the access list for the specified interface.
in	(Optional) Displays input interface statistics.
out	(Optional) Displays output interface statistics.

Note Statistics for OGACL is not supported

Command Default

All standard and expanded IP access lists are displayed.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
10.3	This command was introduced.
12.3(7)T	The **dynamic** keyword was added.
12.4(6)T	The **interface** *name*and *number* keyword and argument pair was added. The **in** and **out** keywords were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(11)T	This command was modified. Example output from the **dynamic** keyword was added.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Release	Modification
12.4(20)T	This command was modified. The output of this command was extended to display access lists that contain object groups.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.

Usage Guidelines

The **show ip access-lists** command provides output identical to the **show access-lists** command, except that it is IP-specific and allows you to specify a particular access list.

Examples

The following is sample output from the **show ip access-lists** command when all access lists are requested:

```
Router# show ip access-lists
Extended IP access list 101
   deny udp any any eq nntp
   permit tcp any any
   permit udp any any eq tftp
   permit icmp any any
   permit udp any any eq domain
```

The table below describes the significant fields shown in the display.

Table 95: show ip access-lists Field Descriptions

Field	Description
Extended IP access list	Extended IP access-list number.
deny	Packets to reject.
udp	User Datagram Protocol.
any	Source host or destination host.
eq	Packets on a given port number.
nntp	Network News Transport Protocol.
permit	Packets to forward.
tcp	Transmission Control Protocol.
tftp	Trivial File Transfer Protocol.
icmp	Internet Control Message Protocol.
domain	Domain name service.

The following is sample output from the **show ip access-lists** command when the name of a specific access list is requested:

```
Router# show ip access-lists Internetfilter
Extended IP access list Internetfilter
   permit tcp any 192.0.2.0 255.255.255.255 eq telnet
```

```
   deny tcp any any
   deny udp any 192.0.2.0 255.255.255.255 lt 1024
   deny ip any any log
```

The following is sample output from the **show ip access-lists** command when the name of a specific access list that contains an object group is requested:

```
Router# show ip access-lists my-ogacl-policy
Extended IP access list my-ogacl-policy
   10 permit object-group eng-service any any
```

The following sample output from the **show ip access-lists** command shows input statistics for Fast Ethernet interface 0/0:

```
Router#
 show ip access-lists interface FastEthernet0/0 in

Extended IP access list 150 in
   10 permit ip host 10.1.1.1 any
   30 permit ip host 10.2.2.2 any (15 matches)
```

The following is sample output from the **show ip access-lists** command using the **dynamic** keyword:

```
Router#
show ip access-lists dynamic CM_SF#1
Extended IP access list CM_SF#1
    10 permit udp any any eq 5060 (650 matches)
    20 permit tcp any any eq 5060
    30 permit udp any any dscp ef (806184 matches)
```

To check your configuration, use the **show run interfaces cable** command:

```
Router#
show run interfaces cable 0/1/0
Building configuration...
Current configuration : 144 bytes
!
interface cable-modem0/1/0
 ip address dhcp
 load-interval 30
 no keepalive
  service-flow primary upstream
   service-policy output llq
end
```

Related Commands

Command	Description
deny	Sets conditions in a named IP access list or OGACL that will deny packets.
ip access-group	Applies an ACL or OGACL to an interface or a service policy map.
ip access-list	Defines an IP access list or OGACL by name or number.
object-group network	Defines network object groups for use in OGACLs.
object-group service	Defines service object groups for use in OGACLs.
permit	Sets conditions in a named IP access list or OGACL that will permit packets.

Command	Description
show object-group	Displays information about object groups that are configured.
show run interfaces cable	Displays statistics on the cable modem.

show ip admission

To display the network admission cache entries and information about web authentication sessions, use the **show ip admission** command in user EXEC or privileged EXEC mode.

Cisco IOS XE Release 3SE and Later Releases
show ip admission {**cache** | **statistics** [{**brief** | **details** | **httpd** | **input-feature**}] | **status** [{**banners** | **custom-pages** | **httpd** | **parameter-map** [*parameter-map-name*]}] | **watch-list**}

All Other Releases
show ip admission {**cache** [{**consent** | **eapoudp** | **ip-addr** *ip-address* | **username** *username*}] | **configuration** | **httpd** | **statistics** | [{**brief** | **details** | **httpd**}] | **status** [**httpd**] | **watch-list**}

Syntax Description

cache	Displays the current list of network admission entries.
statistics	Displays statistics for web authentication.
brief	(Optional) Displays a statistics summary for web authentication.
details	(Optional) Displays detailed statistics for web authentication.
httpd	(Optional) Displays information about web authentication HTTP processes
input-feature	Displays statistics about web authentication packets.
status	Displays status information about configured web authentication features including banners, custom pages, HTTP processes, and parameter maps.
banners	Displays information about configured banners for web authentication.
custom-pages	Displays information about custom pages configured for web authentication. Custom files are read into a local cache and served from the cache. A background process periodically checks if the files need to be re-cached.
parameter-map *parameter-map-name*	Displays information about configured banners and custom pages for all parameter maps or only for the specified parameter map.
watch-list	Displays the list of IP addresses in the watch list.
consent	(Optional) Displays the consent web page cache entries.
eapoudp	(Optional) Displays the Extensible Authentication Protocol over UDP (EAPoUDP) network admission cache entries. Includes the host IP addresses, session timeout, and posture state.
ip-addr *ip-address*	(Optional) Displays information for a client IP address.
username *username*	(Optional) Display information for a client username.

configuration	(Optional) Displays the NAC configuration. **Note** This keyword is not supported in Cisco IOS XE Release 3.2SE and later releases. Use the **show running-config all** command to see the running web authentication configuration and the commands configured with default parameters.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.4(11)T	This command was modified. The output of this command was enhanced to display whether the AAA timeout policy is configured.
12.4(15)T	This command was modified. The **consent** keyword was added.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
15.3(1)T	This command was modified. The **statistics**, **brief**, **details**, **httpd**, and **status** keywords were added.
Cisco IOS XE Release 3.2SE	This command was modified. The **input-feature**, **banners**, **custom-pages**, and **parameter-map** keywords were added. The **configuration** keyword was removed.

Usage Guidelines

Use the **show ip admission** command to display information about network admission entries and information about web authentication sessions.

Examples

The following is sample output from the **show ip admission cache** command:

```
Device# show ip admission cache

Authentication Proxy Cache
Total Sessions: 1 Init Sessions: 1
 Client MAC 5cf3.fc25.7e3d Client IP 1.150.128.2 IPv6 :: Port 0, State INIT, Method Webauth
```

The following is sample output from the **show ip admission statistics** command:

```
Device# show ip admission statistics

Webauth input-feature statistics:
                                                        IPv4          IPv6
  Total packets received                                46            0
    Delivered to TCP                                    46            0
    Forwarded                                           0             0
    Dropped                                             0             0
    TCP new connection limit reached                    0             0

Webauth HTTPd statistics:

  HTTPd process 1
    Intercepted HTTP requests:                          8
```

```
  IO Read events:                                 9
  Received HTTP messages:                         7
  IO write events:                                11
  Sent HTTP replies:                              7
  IO AAA messages:                                4
  SSL OK:                                         0
  SSL Read would block:                           0
  SSL Write would block:                          0
  HTTPd process scheduled count:                  23
```

The following is sample output from the **show ip admission status** command:

```
Device# show ip admission status

IP admission status:
  Enabled interfaces            1
  Total sessions                1
  Init sessions                 1     Max init sessions allowed     100
    Limit reached               0     Hi watermark                  1
  TCP half-open connections     0     Hi watermark                  0
  TCP new connections           0     Hi watermark                  0
  TCP half-open + new           0     Hi watermark                  0
  HTTPD1 Contexts               0     Hi watermark                  1

  Parameter Map: Global
    Custom Pages
      Custom pages not configured
    Banner
      Banner not configured

  Parameter Map: PMAP_WEBAUTH
    Custom Pages
      Custom pages not configured
    Banner
      Type: text
        Banner                  " <H2>Login Page Banner</H2> "
        Html                    " <H2>Login Page Banner</H2> "
        Length                  48

  Parameter Map: PMAP_CONSENT
    Custom Pages
      Custom pages not configured
    Banner
      Banner not configured

  Parameter Map: PMAP_WEBCONSENT
    Custom Pages
      Custom pages not configured
    Banner
      Banner not configured

  Parameter Map: PMAP_WEBAUTH_CUSTOM_FLASH
    Custom Pages
      Type: "login"
        File                    flash:webauth_login.html
        File status             Ok - File cached
        File mod time           2012-07-20T02:29:36.000Z
        File needs re-cached    No
        Cache                   0x3AEE1E1C
        Cache len               246582
        Cache time              2012-09-18T13:56:57.000Z
        Cache access            0 reads, 1 write
      Type: "success"
        File                    flash:webauth_success.html
        File status             Ok - File cached
```

```
        File mod time           2012-02-21T06:57:28.000Z
        File needs re-cached    No
        Cache                   0x3A529B3C
        Cache len               70
        Cache time              2012-09-18T13:56:57.000Z
        Cache access            0 reads, 1 write
      Type: "failure"
        File                    flash:webauth_fail.html
        File status             Ok - File cached
        File mod time           2012-02-21T06:55:49.000Z
        File needs re-cached    No
        Cache                   0x3A5BEBC4
        Cache len               67
        Cache time              2012-09-18T13:56:57.000Z
        Cache access            0 reads, 1 write
      Type: "login expired"
        File                    flash:webauth_expire.html
        File status             Ok - File cached
        File mod time           2012-02-21T06:55:25.000Z
        File needs re-cached    No
        Cache                   0x3AA20090
        Cache len               69
        Cache time              2012-09-18T13:56:57.000Z
        Cache access            0 reads, 1 write
    Banner
      Banner not configured

  Parameter Map: PMAP_WEBAUTH_CUSTOM_EXTERNAL
    Custom Pages
      Custom pages not configured
    Banner
      Banner not configured
```

The following is sample output from the **show ip admission status banners** command for a banner configured with the **banner text** command:

```
Device# show ip admission status banners

IP admission status:
  Parameter Map: Global
    Banner not configured

  Parameter Map: PMAP_WEBAUTH
    Type: text
      Banner                    " <H2>Login Page Banner</H2> "
      Html                      " <H2>Login Page Banner</H2> "
      Length                    48
```

The following is sample output from the **show ip admission status banners** command for a banner configured with the **banner file** command:

```
Device# show ip admission status banners

IP admission status:
  Parameter Map: Global
    Banner not configured

  Parameter Map: PMAP_WEBAUTH
    Type: file
      Banner                    <h2>Cisco Systems</h2>
<h3>Webauth Banner from file</h3>

      Length                    60
      File                      flash:webauth_banner1.html
      File status               Ok - File cached
```

```
      File mod time             2012-07-24T07:07:09.000Z
      File needs re-cached      No
      Cache                     0x3AF6CEE4
      Cache len                 60
      Cache time                2012-09-19T10:13:59.000Z
      Cache access              0 reads, 1 write
```

The following is sample output from the **show ip admission status custom pages** command:

```
Device# show ip admission status custom pages

IP admission status:
  Parameter Map:  Global
    Custom pages not configured
  Parameter Map:  PMAP_WEBAUTH
    Type: "login"
      File                      flash:webauth_login.html
      File status               Ok - File cached
      File mod time             2012-07-20T02:29:36.000Z
      File needs re-cached      No
      Cache                     0x3B0DCEB4
      Cache len                 246582
      Cache time                2012-09-18T16:26:13.000Z
      Cache access              0 reads, 1 write
    Type: "success"
      File                      flash:webauth_success.html
      File status               Ok - File cached
      File mod time             2012-02-21T06:57:28.000Z
      File needs re-cached      No
      Cache                     0x3A2E9090
      Cache len                 70
      Cache time                2012-09-18T16:26:13.000Z
      Cache access              0 reads, 1 write
    Type: "failure"
      File                      flash:webauth_fail.html
      File status               Ok - File cached
      File mod time             2012-02-21T06:55:49.000Z
      File needs re-cached      No
      Cache                     0x3AF6D1A4
      Cache len                 67
      Cache time                2012-09-18T16:26:13.000Z
      Cache access              0 reads, 1 write
    Type: "login expired"
      File                      flash:webauth_expire.html
      File status               Ok - File cached
      File mod time             2012-02-21T06:55:25.000Z
      File needs re-cached      No
      Cache                     0x3A2E8284
      Cache len                 69
      Cache time                2012-09-18T16:26:13.000Z
      Cache access              0 reads, 1 write
  Parameter Map:  PMAP_CONSENT
    Custom pages not configured
```

The following table describes the significant fields shown in the above display.

Table 96: show ip admission Field Descriptions

File mod time	Time stamp when the file was changed on the file system.
Cache time	Time stamp when the file was last read into cache.

The following output displays all the IP admission control rules that are configured on a router:

```
Device# show ip admission configuration

Authentication Proxy Banner not configured
Consent Banner is not configured
Authentication Proxy webpage
        Login page              : flash:test1.htm
        Success page            : flash:test1.htm
        Fail page               : flash:test1.htm
        Login Expire page       : flash:test1.htm
Authentication global cache time is 60 minutes
Authentication global absolute time is 0 minutes
Authentication global init state time is 5 minutes
Authentication Proxy Watch-list is disabled

Authentication Proxy Max HTTP process is 7
Authentication Proxy Auditing is disabled
Max Login attempts per user is 5
```

The following output displays the host IP addresses, the session timeout, and the posture states. If the posture statue is POSTURE ESTAB, the host validation was successful.

```
Device# show ip admission cache eapoudp

Posture Validation Proxy Cache
Total Sessions: 3 Init Sessions: 1
 Client IP 10.0.0.112, timeout 60, posture state POSTURE ESTAB
 Client IP 10.0.0.142, timeout 60, posture state POSTURE INIT
 Client IP 10.0.0.205, timeout 60, posture state POSTURE ESTAB
```

The fields in the displays are self-explanatory.

Related Commands

Command	Description
banner (parameter-map webauth)	Displays a banner on the web-authentication login web page.
clear ip admission cache	Clears IP admission cache entries from the router.
custom-page	Displays custom web pages during web authentication login.
ip admission name	Creates a Layer 3 network admission control rule.

show ip audit configuration

To display additional configuration information, including default values that may not be displayed using the **show running-config**command, use the **show ip audit configuration** command in EXEC mode.

show ip audit configuration

Syntax Description

This command has no argument or keywords.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **show ip audit configuration** EXEC command to display additional configuration information, including default values that may not be displayed using the **show running-config** command.

Examples

The following example displays the output of the **show ip audit configuration** command:

```
Event notification through syslog is enabled
Event notification through Net Director is enabled
Default action(s) for info signatures is alarm
Default action(s) for attack signatures is alarm
Default threshold of recipients for spam signature is 25
PostOffice:HostID:5 OrgID:100 Addr:10.2.7.3 Msg dropped:0
HID:1000 OID:100 S:218 A:3 H:14092 HA:7118 DA:0 R:0
    CID:1 IP:172.21.160.20 P:45000 S:ESTAB (Curr Conn)

Audit Rule Configuration
 Audit name AUDIT.1
    info actions alarm
```

Related Commands

Command	Description
clear ip audit statistics	Resets statistics on packets analyzed and alarms sent.

show ip audit interface

To display the interface configuration, use the **show ip audit interface** command in EXEC mode.

show ip audit interface

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **show ip audit interface** EXEC command to display the interface configuration.

Examples

The following example displays the output of the **show ip audit interface** command:

```
Interface Configuration
 Interface Ethernet0
  Inbound IDS audit rule is AUDIT.1
    info actions alarm
  Outgoing IDS audit rule is not set
 Interface Ethernet1
  Inbound IDS audit rule is AUDIT.1
    info actions alarm
  Outgoing IDS audit rule is AUDIT.1
    info actions alarm
```

show ip audit statistics

To display the number of packets audited and the number of alarms sent, among other information, use the **show ip audit statistics** command in EXEC mode.

show ip audit statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **show ip audit statistics** EXEC command to display the number of packets audited and the number of alarms sent, among other information.

Examples

The following displays the output of the **show ip audit statistics** command:

```
Signature audit statistics [process switch:fast switch]
  signature 2000 packets audited: [0:2]
  signature 2001 packets audited: [9:9]
  signature 2004 packets audited: [0:2]
  signature 3151 packets audited: [0:12]
Interfaces configured for audit 2
Session creations since subsystem startup or last reset 11
Current session counts (estab/half-open/terminating) [0:0:0]
Maxever session counts (estab/half-open/terminating) [2:1:0]
Last session created 19:18:27
Last statistic reset never

HID:1000 OID:100 S:218 A:3 H:14085 HA:7114 DA:0 R:0
```

Related Commands

Command	Description
clear ip audit statistics	Resets statistics on packets analyzed and alarms sent.

show ip auth-proxy

To display the authentication proxy entries or the authentication proxy configuration, use the **show ip auth-proxy** command in privileged EXEC mode.

show ip auth-proxy {**cache** | **configuration** | **httpd** | **statistics** | [{**brief** | **details** | **httpd**}] | **watch-list**}

Syntax Description

cache	Displays the current list of the authentication proxy entries.
configuration	Displays the authentication proxy configuration. **Note** This keyword is not available in Cisco IOS XE Release 3.2SE and later releases. Use the **show running-config all** command to see the running web authentication configuration and the commands configured with default parameters.
httpd	Displays information about web authentication HTTP processes
statistics	Displays statistics for web authentication.
brief	(Optional) Displays a statistics summary for web authentication.
details	(Optional) Displays detailed statistics for web authentication.
watch-list	Displays the list of users on the watch list.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.3(1)T	This command was modified. The **httpd**, **statistics**, **brief**, and **details** keywords were added.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE. The **configuration** keyword was removed.

Usage Guidelines

Use the **show ip auth-proxy** to display either the authentication proxy entries or the running authentication proxy configuration. Use the **cache** keyword to list the host IP address, the source port number, the timeout value for the authentication proxy, and the state for connections using authentication proxy. If authentication proxy state is HTTP_ESTAB, the user authentication was successful.

Use the **configuration** keyword to display all authentication proxy rules configured on the device.

Examples

The following example shows sample output from the **show ip auth-proxy cache** command after one user authentication using the authentication proxy:

```
Device# show ip auth-proxy cache
Authentication Proxy Cache
Client IP 192.168.25.215 Port 57882, timeout 1, state HTTP_ESTAB
```

The following example shows how the **show ip auth-proxy configuration** command displays the information about the authentication proxy rule named pxy. The global idle timeout value is 60 minutes. The idle timeouts value for this named rule is 30 minutes. No host list is specified in the rule, meaning that all connection initiating HTTP traffic at the interface is subject to the authentication proxy rule.

```
Device# show ip auth-proxy configuration
Authentication cache time is 60 minutes
Authentication Proxy Rule Configuration
Auth-proxy name pxy
http list not specified auth-cache-time 30 minutes
```

Related Commands

Command	Description
clear ip auth-proxy cache	Clears authentication proxy entries from the device.
ip auth-proxy	Sets the authentication proxy idle timeout value (the length of time an authentication cache entry, along with its associated dynamic user ACL, is managed after a period of inactivity).
ip auth-proxy (interface configuration)	Applies an authentication proxy rule at a firewall interface.
ip auth-proxy name	Creates an authentication proxy rule.

show ip auth-proxy watch-list

To display the information about the authentication proxy watch list in the EXEC command mode, use the **show ip auth-proxy watch-list** command.

show ip auth-proxy watch-list

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default settings.

Command Modes

EXEC

Command History

Release	Modification
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 720.

Examples

This example shows how to display the information about the authentication proxy watch list:

```
Router# show ip auth-proxy watch-list
Authentication Proxy Watch-list is enabled
Watch-list expiry timeout is 2 minutes
Total number of watch-list entries: 3
 Source IP       Type         Violation-count
 10.0.0.2        MAX_RETRY    MAX_LIMIT
 10.0.0.3        TCP_NO_DATA  MAX_LIMIT
 10.255.255.255 CFGED        N/A
Total number of watch-listed users: 3
Router#
```

Related Commands

Command	Description
clear ip auth-proxy watch-list	Deletes a single watch-list entry or all watch-list entries.
ip auth-proxy max-login-attempts	Limits the number of login attempts at a firewall interface.
ip auth-proxy watch-list	Enables and configures an authentication proxy watch list.

show ip bgp labels

To display information about Multiprotocol Label Switching (MPLS) labels from the external Border Gateway Protocol (eBGP) route table, use the **show ip bgp labels** command in privileged EXEC mode.

show ip bgp labels

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(21)ST	This command was introduced.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and implemented on the Cisco 10000 series router.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
15.2(2)SNG	This command was integrated into Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

Use this command to display eBGP labels associated with an Autonomous System Boundary Router (ASBR).

This command displays labels for BGP routes in the default table only. To display labels in the Virtual Private Network (VPN) routing and forwarding (VRF) tables, use the **show ip bgp vpnv4** {**all** | **vrf** *vrf-name*} command with the optional **labels** keyword.

Examples

The following example shows output for an ASBR using BGP as a label distribution protocol:

```
Router# show ip bgp labels
Network          Next Hop         In Label/Out Label
10.3.0.0/16       0.0.0.0          imp-null/exp-null
10.15.15.15/32   10.15.15.15      18/exp-null
10.16.16.16/32   0.0.0.0          imp-null/exp-null
10.17.17.17/32   10.0.0.1         20/exp-null
10.18.18.18/32   10.0.0.1         24/31
10.18.18.18/32   10.0.0.1         24/33
```

The table below describes the significant fields shown in the display.

Table 97: show ip bgp labels Field Descriptions

Field	Description
Network	Displays the network address from the eBGP table.
Next Hop	Specifies the eBGP next hop address.
In Label	Displays the label (if any) assigned by this router.
Out Label	Displays the label assigned by the BGP next hop router.

Related Commands

Command	Description
show ip bgp vpnv4	Displays VPN address information from the BGP table.

show ip device tracking

To display information about entries in the IP device tracking table, use the **show ip device tracking** command in privileged EXEC mode.

show ip device tracking {**all count** | **interface** *type-of-interface* | **ip** *ip-address* | **mac** *mac-address*}

Syntax Description

all count	Displays a count of all IP tracking host entries.
interface *type-of-interface*	Displays interface information. See the table below for a list of valid interfaces.
ip *ip-address*	Displays the IP address of the client.
mac *mac-address*	Displays the 48-bit hardware MAC address.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2SX	This command was introduced.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T.

Usage Guidelines

The table below displays valid interfaces that may be shown as the *type-of-interface*argument with the **interface**keyword.

Table 98: Interfaces That Can Be Tracked

Interface	Description
Async	Asynchronous interface
BVI	Bridge-Group Virtual Interface
CDMA-Ix	CDMA Ix interface
CTunnel	CTunnel interface
Dialer	Dialer interface
FastEthernet	FastEthernet IEEE 802.3
Lex	Lex interface
Loopback	Loopback interface
MFR	Multilink Frame Relay bundle intrface
Multilink	Multilink-group interface

Interface	Description
Null	Null interface
Port-channel	Ethernet channel of interfaces
Serial	Serial
Tunnel	Tunnel interface
vif	Pragmatic General Multicast (PGM) multicast host interface
virtual	Virtual interface
virtual-PPP	Virtual PPP interface
virtual-Template	Virtual template interface
virtual-TokenRing	Virtual TokenRing
XTagATM	Extended Tag ATM interface

Examples

The following example shows that all host entries are to be tracked:

```
Router# show ip device tracking all count
IP Device Tracking = Enabled
Probe Count: 2
Probe Interval: 10
```

The fields in the above display are self-explanatory.

show ip inspect

To display Context-Based Access Control (CBAC) configuration and session information, use the **show ip inspect**command in privileged EXEC mode.

ACL Bypass Statistics Syntax
show ip inspect {**name** *inspection-name* | **config** | **interfaces** | **sessions** [**detail**] | **statistics** [**reset**] | **all** | **sis** [**detail**] | **tech-support** [**reset**]} [**vrf** *vrf-name*]

Firewall MIB Statistics Syntax
show ip inspect mib connection-statistics {**global** | **l4-protocol** {**all** | **icmp** | **tcp** | **udp**} | **l7-protocol** [*protocol-type*] | **policy** *policy-name* **interface** [*interface-type interface-number*] **l4-protocol** {**all** | **icmp** | **tcp** | **udp**} | **l7-protocol** [*protocol-type*]}

Syntax Description

name *inspection-name*	Displays the configured inspection rule with the name *inspection-name*.
config	Displays the complete CBAC or High Availability (HA) inspection configuration.
interfaces	Displays the interface configuration with respect to applied inspection rules and access lists.
sessions [**detail**]	Displays existing sessions that are currently being tracked and inspected by CBAC or HA. The optional **detail** keyword allows additional details about these sessions to be shown.
statistics [**reset**]	Displays CBAC session statistics, such as the number of TCP and HTTP packets that are processed through the inspection, the number of sessions that have been created since the subsystem startup, the current session count, the maximum session count, and the session creation rate. The optional **reset** keyword resets the counters to reflect the latest statistics.
all	Displays all CBAC configuration and all existing sessions that are currently being tracked and inspected by CBAC.
sis [**detail**]	Displays CBAC session information such as window-size information of initiator and responder windows in a session. The optional **detail** keyword allows additional details about these sessions to be shown.
tech-support [**reset**]	Displays additional information regarding drops that are not shown in the **show ip inspect statistics**command. This information is useful for troubleshooting IP inspect issues. The optional **reset** keyword resets the counters to reflect the latest statistics.
vrf *vrf-name*	(Optional) Displays information only for the specified Virtual Routing and Forwarding (VRF) interface.
mib connection-statistics	Displays firewall performance summary statistics that are monitored via firewall MIBs.

global	Displays global connection summary statistics, which are kept for the entire device.
l4-protocol	Displays Layer 4 protocol-based connection summary statistics. Valid values include **all**, **icmp**, **tcp**, **udp**.
l7-protocol [*protocol-type*]	Displays Layer 7 protocol-based connection summary statistics. Refer to the table below for the protocols that can be entered for the *protocol-type* argument.
policy *policy-name*	Displays the name of the firewall policy that is being monitored.
interface	Displays the type of the interface on which the specified firewall policy is applied.
interface-type	Interface type. For more information, use the question mark (?) online help function.
interface-number	Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.2 P	This command was introduced.
12.3(4)T	This command was modified. The output for the **show ip inspect session detail** command was enhanced to support dynamic access control list (ACL) bypass.
12.3(11)T	This command was modified. The **statistics** keyword was added.
12.3(14)T	This command was modified. The output shows the IMAP and POP3 configuration. The **vrf** *vrf-name*keyword/argument pair was added.
12.4(6)T	This command was modified. • The firewall MIB statistics syntax was added to support firewall performance via SNMP. • High Availability (HA) configuration and session information was added to support Stateful Failover.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.4(11)T	This command was modified. The **tech-support**and **sis** keywords were unhidden and are now supported.
12.2SX	This command was integrated into Cisco IOS Release 12.2SX. Support in a specific 12.2SX release depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to view the CBAC and HA configuration and session information.

ACL Bypass Functionality

ACL bypass allows a packet to avoid redundant ACL checks by allowing the firewall to permit the packet on the basis of existing inspection sessions instead of dynamic ACLs. Because input and output dynamic ACLs have been eliminated from the firewall configuration, the **show ip inspect session detail** command output no longer shows dynamic ACLs. Instead, the output displays the matching inspection session for each packet that is permitted through the firewall.

Firewall MIB Functionality

The Cisco Unified Firewall MIB monitors the following firewall performance statistics:

- Connection statistics, which are a record of the firewall traffic streams that have attempted to flow through the firewall system. Connection statistics can be displayed on a global basis, a protocol-specific basis, or a firewall policy basis.
- URL filtering statistics, which include the status of distinct URL filtering servers that are configured on the firewall and the impact of the performance of the URL filtering servers on the latency and throughput of the firewall.

The table below shows the types of protocols that can be configured for the *protocol-type* argument with the **l7-protocol** keyword:

Table 99: Protocol Types for the l7-protocol Keyword

Protocol-Type	Description
802-11-iapp	IEEE 802.11 WLANs WG IAPP
ace-svr	ACE Server/Propagation
all	All protocols
aol	America Online Instant Messenger
appleqtc	Apple QuickTime
bgp	Border Gateway Protocol
biff	Bliff Mail Notification
bootpc	Bootstrap Protocol Client
bootps	Bootstrap Protocol Server
cddbp	CD Database Protocol
cifs	CIFS
cisco-fna	Cisco FNATIVE
cisco-net-mgmt	Cisco Network Management
cisco-svcs	Cisco license/perf/GDP/X.25/ident svcs
cisco-sys	Cisco SYSMAINT

Protocol-Type	Description
cisco-tdp	Cisco Tag Distribution Protocol
cisco-tna	Cisco TNATIVE
citrix	Citrix IMA/ADMIN/RTMP
citirixmaclient	Citrix IMA Client
clp	Cisco Line Protocol
creativepartnr	Creative Partner
creativeserver	Creative Server
cuseeme	CUSeeMe Protocol
daytime	Daytime Protocol (RFC 867)
dbase	dBASE Unix
dbcontrol_agent	Oracle Database Control Agent
ddns-v3	Dynamic Domain Name Server Version 3
dhcp-failover	Dynamic Host Control Protocol failover
discard	Discard Protocol
dns	Domain Name Server
dnsix	DNSIX Security Attribute Token Map
echo	Echo Protocol
entrust-svc-hdlr	Entrust KM/Admin Service Handler
entrust-svcs	Entrust sps/aaas/aams
exec	Remote Process Execution
fcip-port	Fibre Channel over IP
finger	Finger Protocol
ftp	File Transfer Protocol
ftps	File Transfer Protocol over Transport Layer Security/ Secure Sockets Layer
gdoi	Group Domain of Interpretation
giop	Oracle GIOP/SSL
gopher	Gopher Protocol
gtpv0	GPRS Tunneling Protocol Version 0

Protocol-Type	Description
gtpv1	GPRS Tunneling Protocol Version 1
h323	H.323 Protocol for audio-visual communication
h323-annexe	H.323 Protocol AnnexE
h323-nxg	H.323 Protocol AnnexG
hp-alarm-mgr	HP Performance Data Alarm Manager
hp-collector	HP Performance Data Collector
hp-managed-node	HP Performance Data Managed Node
hsrp	Hot Standby Router Protocol
http	Hyper Text Transfer Protocol
https	Secure Hyper Text Transfer Protocol
ica	ICA from Citrix
icabrowser	ICA browser from Citrix
ident	Ident Protocol
igmpv3lite	Internet Group Management Protocol over User Datagram Protocol for SSM
imap	Internet Message Access Protocol
imap3	Interactive Mail Access Protocol 3
imaps	IMAP over TLS/SSL
ipass	IPASS
ipsec-msft	Microsoft IPsec NAT-T
ipx	IPX
irc	Internet Relay Chat Protocol
ircs	IRC over TLS/SSL
irc-serv	IRC Serv
ircu	IRCU
isakmp	Internet Security Association and Key Management Protocol
iscsi	Internet Small Computer System Interface
iscsi-target	iSCSI Port
kerberos	Kerberos Protocol

Protocol-Type	Description
kermit	Kermit Protocol
l2tp	Layer 2 Tunneling Protocol
ldap	Lightweight Directory Access Protocol
ldap-admin	LDAP admin server port
ldaps	LDAP over TLS/SSL
login	Remote Login
lotusmtap	Lotus Mail Tracking Agent Protocol
lotusnotes	Lotus Note
mgcp	Media Gateway Control Protocol
microsoft-ds	Microsoft DS
ms-cluster-net	Microsoft Cluster Net
ms-dotnetster	Microsoft .NETster Port
ms-sna	Microsoft SNA Server/Base
ms-sql	Microsoft SQL
ms-sql-m	Microsoft SQL Monitor
msexch-routing	Microsoft Exchange Routing
msnmsgr	MSN Instant Messenger
msrpc	Microsoft Remote Procedure Call
mysql	MySQL
n2h2server	N2H2 Filter Service Port
ncp	NetWare Core Protocol
net8-cman	Oracle Net8 Cman/Admin
netbios-dgm	NETBIOS Datagram Service
netbios-ns	NETBIOS Name Service
netbios-ssn	NETBIOS Session Service
netshow	Microsoft NetShow
netstat	Network Statistics
nfs	Network File System

Protocol-Type	Description
nntp	Network News Transport Protocol
ntp	Network Time Protocol
oem-agent	Oracle Enterprise Manager Agent
oracle	Oracle
oracle-em-vp	Oracle Enterprise Manager/VP
oraclenames	Oracle Names
orasrv	Oracle SQL *NET Version 1/2
other	Non-listed Protocols
pcanywheredata	pcAnywhere data
pcanywherestat	pcAnywhere stat
pop3	Post Office Protocol Version 3
pop3s	POP3 over TLS/SSL
pptp	Point-to-Point Tunneling Protocol
pwdgen	Password Generator Protocol
qmtp	Quick Mail Transfer Protocol
radius	RADIUS and Accounting
rdb-dbs-disp	Oracle Relational Database
realmedia	Real Network's Realmedia Protocol
realsecure	ISS Real Secure Console Service Port
router	Local Routing Process
rsvd	RSVD
rsvp-encap	RSVP Encapsulation-1/2
rsvp_tunnel	RSVP Tunnel
rtc-pm-port	Oracle RTC-PM Port
rtelnet	Remote Telnet Service
rtsp	Real Time Streaming Protocol
r-winsock	Remote Winsock
send	SEND

Protocol-Type	Description
shell	Remote Command
sip	Session Initiation Protocol
sip-tls	SIP-TLS
skinny	Skinny Client Control Protocol
sms	SMS
smtp	Simple Mail Transfer Protocol
snmp	Simple Network Management Protocol
snmptrap	SNMP Trap
socks	Socks
sql-net	SQL-NET
sqlserv	SQL Services
sqlsrv	SQL Service
ssh	SSH Remote Login Protocol
sshell	SSLshell
ssp	State Sync Protocol
streamworks	StreamWorks Protocol
stun	Cisco STUN
sunrpc	SUN Remote Procedure Call
syslog	Syslog Service
syslog-conn	Reliable Syslog Service
tacacs	Terminal Access Controller Access-Control System
tacacs-ds	TACACS Database Service
tarantella	Tarantella
telnet	Telecommunication Network Protocol.
telnets	Telnet over TLS or SSL
tftp	Trivial File Transfer Protocol
time	Time
timed	Time Server

Protocol-Type	Description
tr-rsrb	Cisco RSBR
ttc	Oracle TTC or SSL
uucp	Unix-to-Unix Copy Program
vdolive	VDOLive Protocol
vqp	VLAN Query Protocol
webster	Webster Network dictionary
who	Who's Service
wins	Windows Internet Name Service
x11	X Window System
xdmcp	XDM Control Protocol
ymsgr	Yahoo Instant Messenger

Examples

The following is sample output for the **show ip inspect name myinspectionrule**command, where the inspection rule "myinspectionrule" is configured. In this example, the output shows the protocols that should be inspected by CBAC and the corresponding idle timeouts for each protocol.

```
Router# show ip inspect name myinspectionrule
Inspection Rule Configuration
 Inspection name myinspectionrule
    tcp timeout 3600
    udp timeout 30
    ftp timeout 3600
```

The following is sample output from the **show ip inspect config**command. In this example, the output shows CBAC configuration, including global timeouts, thresholds, and inspection rules.

```
Router# show ip inspect config
Session audit trail is disabled
one-minute (sampling period) thresholds are [400:500] connections
max-incomplete sessions thresholds are [400:500]
max-incomplete tcp connections per host is 50. Block-time 0 minute.
tcp synwait-time is 30 sec -- tcp finwait-time is 5 sec
tcp idle-time is 3600 sec -- udp idle-time is 30 sec
dns-timeout is 5 sec
Inspection Rule Configuration
 Inspection name myinspectionrule
    tcp timeout 3600
    udp timeout 30
    ftp timeout 3600
```

The following is sample output from the **show ip inspect interfaces**command:

```
Router# show ip inspect interfaces
Interface Configuration
 Interface Ethernet0
```

```
  Inbound inspection rule is myinspectionrule
    tcp timeout 3600
    udp timeout 30
    ftp timeout 3600
  Outgoing inspection rule is not set
  Inbound access list is not set
  Outgoing access list is not set
```

The following is sample output from the **show ip inspect sessions**command. In this example, the output shows the source and destination addresses and port numbers (separated by colons), and it indicates that the session is an FTP session.

```
Router# show ip inspect sessions
Established Sessions
 Session 25A3318 (10.0.0.1:20)=>(10.1.0.1:46068) ftp-data SIS_OPEN
 Session 25A6E1C (10.1.0.1:46065)=>(10.0.0.1:21) ftp SIS_OPEN
```

The following is sample output from the **show ip inspect all**command:

```
Router# show ip inspect all
Session audit trail is disabled
one-minute (sampling period) thresholds are [400:500] connections
max-incomplete sessions thresholds are [400:500]
max-incomplete tcp connections per host is 50. Block-time 0 minute.
tcp synwait-time is 30 sec -- tcp finwait-time is 5 sec
tcp idle-time is 3600 sec -- udp idle-time is 30 sec
dns-timeout is 5 sec
Inspection Rule Configuration
 Inspection name all
    tcp timeout 3600
    udp timeout 30
    ftp timeout 3600
Interface Configuration
 Interface Ethernet0
  Inbound inspection rule is all
    tcp timeout 3600
    udp timeout 30
    ftp timeout 3600
  Outgoing inspection rule is not set
  Inbound access list is not set
  Outgoing access list is not set
 Established Sessions
 Session 25A6E1C (10.3.0.1:46065)=>(10.4.0.1:21) ftp SIS_OPEN
 Session 25A34A0 (10.4.0.1:20)=>(10.3.0.1:46072) ftp-data SIS_OPEN
```

The following is sample output from the **show ip inspect session detail**command, which shows that an outgoing ACL and an inbound ACL (dynamic ACLs) have been created to allow return traffic:

```
Router# show ip inspect session detail

Established Sessions
 Session 80E87274 (192.168.1.116:32956)=>(192.168.101.115:23) tcp SIS_OPEN
   Created 00:00:08, Last heard 00:00:04
   Bytes sent (initiator:responder) [140:298] acl created 2
   Outgoing access-list 102 applied to interface FastEthernet0/0
   Inbound access-list 101 applied to interface FastEthernet0/1
```

The following is sample output from the **show ip inspect session detail**command, which shows related ACL information (such as session identifiers [SIDs]), but does not show dynamic ACLs, which are no longer created:

```
Router# show ip inspect session detail
Established Sessions
 Session 814063CC (192.168.1.116:32955)=>(192.168.101.115:23) tcp SIS_OPEN
  Created 00:00:10, Last heard 00:00:06
  Bytes sent (initiator:responder) [140:298]
  HA state: HA_STANDBY
  In  SID 192.168.101.115[23:23]=>192.168.1.117[32955:32955] on ACL 101 (15 matches)
  Out SID 192.168.101.115[23:23]=>192.168.1.116[32955:32955] on ACL 102
```

The following is sample output from the **show ip inspect statistics** command:

```
Router# show ip inspect statistics
Packet inspection statistics [process switch:fast switch]
  tcp packets: [616668:0]
  http packets: [178912:0]
Interfaces configured for inspection 1
Session creations since subsystem startup or last reset 42940
Current session counts (estab/half-open/terminating) [0:0:0]
Maxever session counts (estab/half-open/terminating) [98:68:50]
Last session created 5d21h
Last statistic reset never
Last session creation rate 0
Last half-open session total 0
```

The following is sample output from the **show ip inspect tech-support** command:

```
Router# show ip inspect tech-support
Packet inspection statistics [process switch:fast switch]
  tcp packets: [21:879]
Interfaces configured for inspection 1 Pre-gen sessions 0
Session creations since subsystem startup or last reset 19
Current session counts (estab/half-open/terminating) [0:0:0]
Maxever session counts (estab/half-open/terminating) [1:1:1]
Last session created 02:25:37
Last statistic reset never
Last session creation rate 0
Last half-open session total 0
Packet disposition statistics [process switch:fastswitch]
  tcp packets dropped: [1:3]
  tcp packets skipped: [0:35]
TCP session reset: 0
```

The following is sample output from the **show ip inspect sis detail** command:

```
Router# show ip inspect sis detail
 Half-open Sessions
 Session 459B498 (75.75.75.3:25471)=>(10.10.10.3:5060) tcp SIS_OPENING
 Created 00:00:01, Last heard 00:00:01
 Bytes sent (initiator:responder) [0:0]
 Initiator->Responder Window size 8000 Scale factor 0
 Responder->Initiator Window size 0 Scale factor 0
Router#
```

The following is sample output from the **show ip inspect mib**command with global or protocol-specific keywords.

Global MIB Statistics

```
Router# show ip inspect mib connection-statistics global
```

```
Connections Attempted 7
Connections Setup Aborted 0
Connections Policy Declined 0
Connections Resource Declined 0
Connections Half Open 2
Connections Active 3
Connections Expired 2
Connections Aborted 0
Connections Embryonic 0
Connections 1-min Setup Rate 5
Connections 5-min Setup Rate 7
```

Protocol-Based MIB Statistics

```
Router# show ip inspect mib connection-statistics l4-protocol tcp
Protocol tcp
Connections Attempted 3
Connections Setup Aborted 0
Connections Policy Declined 0
Connections Resource Declined 0
Connections Half Open 1
Connections Active 2
Connections Aborted 0
Connections 1-min Setup Count 3
Connections 5-min Setup Count 3
Router# show ip inspect mib connection-statistics l7-protocol http
Protocol http
Connections Attempted 3
Connections Setup Aborted 0
Connections Policy Declined 2
Connections Resource Declined 0
Connections Half Open 0
Connections Active 1
Connections Aborted 0
Connections 1-min Setup Rate 1
Connections 5-min Setup Rate 2
```

Policy-target-Based MIB Statistics

```
Router# show ip inspect mib connection-statistics policy ftp interface GigabitEthernet0/0
l4-protocol tcp
! Policy Target Protocol Based Connection Summary Stats
Policy ftp-inspection
Target GigabitEthernet0/0
Protocol tcp
Connections Attempted 3
Connections Setup Aborted 0
Connections Policy Declined 0
Connections Resource Declined 0
Connections Half Open 1
Connections Active 2
Connections Aborted 0
Router# show ip inspect mib connection-statistics policy ftp interface GigabitEthernet0/0
l7-protocol ftp
! Policy Target Protocol Based Connection Summary Stats
Policy ftp-inspection
Target GigabitEthernet0/0
Protocol ftp
```

```
Connections Attempted 3
Connections Setup Aborted 0
Connections Policy Declined 0
Connections Resource Declined 0
Connections Half Open 1
Connections Active 2
Connections Aborted 0
```

show ip inspect ha

To display stateful failover high availability (HA) session information, use the **show ip inspect ha**command in privileged EXEC mode.

show ip inspect ha [{**sessions** [**detail**] [**vrf** *vrf-name*] | **statistics**}]

Syntax Description

sessions	(Optional) Displays information about the sessions.
detail	(Optional) Displays additional information on pinholes created for the return traffic, number of bytes that have passed through this session, and session time information.
vrf *vrf-name*	(Optional) Displays information for the specified virtual routing and forwarding (VRF) instance.
statistics	(Optional) Displays HA sessions statistics for both the active and standby devices.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(6)T	This command was introduced.

Examples

The following is sample output from the **show ip inspect ha sessions**command.

```
Router# show ip inspect ha sessions

Sess_ID  (src_addr:port)=>(dst_addr:port)  proto  sess_state ha_state  Established Session
2CA8958 (10.0.0.5:37690)=>(10.0.0.4:00023) tcp    SIS_OPEN   HA_ACTIVE
```

The table below describes the significant fields shown in the display.

Table 100: show ip inspect ha sessions Field Descriptions

Field	Description
Sess_ID	Displays the session ID.
src_addr:port	Displays source address and port.
dst_addr:port	Displays the destination address and port.
proto	Displays the name of the protocol.
sess_state	Displays the session state.
ha_state	Displays the HA state.
Established Session	Displays the name of the established session.

The following sample output from the **show ip inspect ha sessions detail** command displays additional information for each session.

```
Router# show ip inspect ha sessions detail
Sess_ID  (src_addr:port)=>(dst_addr:port)  proto  sess_state ha_state  Established Session
2CA8958 (10.0.0.5:37690)=>(10.0.0.4:00023) tcp    SIS_OPEN   HA_ACTIVE
 Created 00:01:52, Last heard 00:01:39
 Bytes sent (initiator:responder) [50:91]
 In  SID   10.11.0.4[23:23]=>10.0.0.5[37690:37690] on ACL test  (25 matches)
```

The table below describes the significant fields shown in the display.

Table 101: show ip inspect ha sessions detail Field Descriptions

Field	Description
Created	Displays the date the session was created.
Last heard	Displays the date the packets were received last on the session.
Bytes sent (initiator:responder)	Displays the ratio of bytes sent from the initiator to the responder.
In SID	Session identifier.
on ACL test	Session identifier entry open on an Access Control List (ACL) named test.

The following sample output from the **show ip inspect ha statistics** command displays the following information for the session on the active and standby routers.

On the active router:

```
Router # show ip inspect ha statistics

************************************************
FW HA ACTIVE STATS
************************************************
FW HA active num add session sent             1
FW HA active num delete session sent             0
FW HA active num update session requests             0
FW HA active num update session sent             17
FW HA active bulk sync session             0
FW HA active num error             0
FW HA active RF error             0
FW HA active CF error             0
FW HA active manager error             0
************************************************
```

On the standby router:

```
Router # show ip inspect ha statistics

************************************************
FW HA STANDBY STATS
************************************************
FW HA standby num add session received             1
FW HA standby num delete session received             0
FW HA standby num update session received             17
FW HA standby num bulk sync request sent             0
FW HA standby num error             0
```

```
FW HA standby config error              0
**************************************************
```

The table below describes the significant fields shown in the display.

Table 102: show ip inspect ha Field Descriptions

Field	Description
num add session sent	Displays the number of add session messages sent.
num delete session sent	Displays the number of delete session messages sent.
num update session requests	Displays the number of update session message requests.
num update session sent	Displays the number of update session messages sent.
bulk sync session	Displays the number of bulk synchronization requests received.
num error	Displays the number of errors.
RF error	Displays the number of Redundancy Framework (RF) errors.
CF error	Displays the number of Checkpointing Facility (CF) errors.
manager error	Displays the number of manager errors.
bulk sync request sent	Displays the number of bulk synchronization requests sent.
config error	Displays the number of configuration errors.

Related Commands

Command	Description
show ip inspect	Displays CBAC configuration and session information.

show ip interface

To display the usability status of interfaces configured for IP, use the **show ip interface** command in privileged EXEC mode.

show ip interface [*type number*] [**brief**]

Syntax Description

type	(Optional) Interface type.
number	(Optional) Interface number.
brief	(Optional) Displays a summary of the usability status information for each interface.

Command Default

The full usability status is displayed for all interfaces configured for IP.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
10.0	This command was introduced.
12.0(3)T	The command output was modified to show the status of the **ip wccp redirect out** and **ip wccp redirect exclude add in** commands.
12.2(14)S	The command output was modified to display the status of NetFlow on a subinterface.
12.2(15)T	The command output was modified to display the status of NetFlow on a subinterface.
12.3(6)	The command output was modified to identify the downstream VPN routing and forwarding (VRF) instance in the output.
12.3(14)YM2	The command output was modified to show the usability status of interfaces configured for Multiprocessor Forwarding (MPF) and implemented on the Cisco 7301 and Cisco 7206VXR routers.
12.2(14)SX	This command was implemented on the Supervisor Engine 720.
12.2(17d)SXB	This command was integrated into Cisco IOS 12.2(17d)SXB on the Supervisor Engine 2, and the command output was changed to include NDE for hardware flow status.
12.4(4)T	This command was integrated into Cisco IOS Release 12.4(4)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	The command output was modified to display information about the Unicast Reverse Path Forwarding (RPF) notification feature.

Release	Modification
12.4(20)T	The command output was modified to display information about the Unicast RPF notification feature.
12.2(33)SXI2	This command was modified. The command output was modified to display information about the Unicast RPF notification feature.
Cisco IOS XE Release 2.5	This command was modified. This command was implemented on the Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS XE Release 3.9S	This command was implemented on Cisco 4400 Series ISRs.

Usage Guidelines

The Cisco IOS software automatically enters a directly connected route in the routing table if the interface is usable (which means that it can send and receive packets). If an interface is not usable, the directly connected routing entry is removed from the routing table. Removing the entry lets the software use dynamic routing protocols to determine backup routes to the network, if any.

If the interface can provide two-way communication, the line protocol is marked "up." If the interface hardware is usable, the interface is marked "up."

If you specify an optional interface type, information for that specific interface is displayed. If you specify no optional arguments, information on all the interfaces is displayed.

When an asynchronous interface is encapsulated with PPP or Serial Line Internet Protocol (SLIP), IP fast switching is enabled. A **show ip interface** command on an asynchronous interface encapsulated with PPP or SLIP displays a message indicating that IP fast switching is enabled.

You can use the **show ip interface brief** command to display a summary of the router interfaces. This command displays the IP address, the interface status, and other information.

The **show ip interface brief** command does not display any information related to Unicast RPF.

Examples

The following example shows configuration information for interface Gigabit Ethernet 0/3. In this example, the IP flow egress feature is configured on the output side (where packets go out of the interface), and the policy route map named PBRNAME is configured on the input side (where packets come into the interface).

```
Router# show running-config interface gigabitethernet 0/3
interface GigabitEthernet0/3
 ip address 10.1.1.1 255.255.0.0
 ip flow egress
 ip policy route-map PBRNAME
 duplex auto
 speed auto
 media-type gbic
 negotiation auto
end
```

The following example shows interface information on Gigabit Ethernet interface 0/3. In this example, MPF is enabled, and both Policy Based Routing (PBR) and NetFlow features are not supported by MPF and are ignored.

```
Router# show ip interface gigabitethernet 0/3
```

```
GigabitEthernet0/3 is up, line protocol is up
  Internet address is 10.1.1.1/16
  Broadcast address is 255.255.255.255
  Address determined by setup command
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP CEF switching is enabled
  IP Feature Fast switching turbo vector
  IP VPN Flow CEF switching turbo vector
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast, CEF
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Policy routing is enabled, using route map PBR
  Network address translation is disabled
  BGP Policy Mapping is disabled
  IP Multi-Processor Forwarding is enabled
     IP Input features, "PBR",
         are not supported by MPF and are IGNORED
     IP Output features, "NetFlow",
         are not supported by MPF and are IGNORED
```

The following example identifies a downstream VRF instance. In the example, "Downstream VPN Routing/Forwarding "D"" identifies the downstream VRF instance.

```
Router# show ip interface virtual-access 3
Virtual-Access3 is up, line protocol is up
  Interface is unnumbered. Using address of Loopback2 (10.0.0.8)
  Broadcast address is 255.255.255.255
  Peer address is 10.8.1.1
  MTU is 1492 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is enabled
  IP Flow switching is disabled
  IP CEF switching is enabled
```

```
  IP Feature Fast switching turbo vector
  IP VPN CEF switching turbo vector
  VPN Routing/Forwarding "U"
  Downstream VPN Routing/Forwarding "D"
  IP multicast fast switching is disabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast, CEF
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Policy routing is disabled
  Network address translation is disabled
  WCCP Redirect outbound is disabled
  WCCP Redirect inbound is disabled
  WCCP Redirect exclude is disabled
  BGP Policy Mapping is disabled
```

The following example shows the information displayed when Unicast RPF drop-rate notification is configured:

```
Router# show ip interface ethernet 2/3
Ethernet2/3 is up, line protocol is up
  Internet address is 10.0.0.4/16
  Broadcast address is 255.255.255.255
  Address determined by non-volatile memory
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is disabled
  IP Flow switching is disabled
  IP CEF switching is disabled
  IP Null turbo vector
  IP Null turbo vector
  IP multicast fast switching is disabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are No CEF
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Probe proxy name replies are disabled
  Policy routing is disabled
  Network address translation is disabled
  WCCP Redirect outbound is disabled
  WCCP Redirect inbound is disabled
  WCCP Redirect exclude is disabled
  BGP Policy Mapping is disabled
```

Unicast RPF Information

```
  Input features: uRPF
  IP verify source reachable-via RX, allow default
   0 verification drops
   0 suppressed verification drops
   0 verification drop-rate
Router#
```

The following example shows how to display the usability status for a specific VLAN:

```
Router# show ip interface vlan 1
Vlan1 is up, line protocol is up
  Internet address is 10.0.0.4/24
  Broadcast address is 255.255.255.255
Address determined by non-volatile memory
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Outgoing access list is not set
  Inbound  access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachables are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP CEF switching is enabled
  IP Fast switching turbo vector
  IP Normal CEF switching turbo vector
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast, CEF
  Router Discovery is disabled
  IP output packet accounting is disabled
  IP access violation accounting is disabled
  TCP/IP header compression is disabled
  RTP/IP header compression is disabled
  Probe proxy name replies are disabled
  Policy routing is disabled
  Network address translation is disabled
  WCCP Redirect outbound is disabled
  WCCP Redirect inbound is disabled
  WCCP Redirect exclude is disabled
  BGP Policy Mapping is disabled
  Sampled Netflow is disabled
  IP multicast multilayer switching is disabled
  Netflow Data Export (hardware) is enabled
```

The table below describes the significant fields shown in the display.

Table 103: show ip interface Field Descriptions

Field	Description
Virtual-Access3 is up	Shows whether the interface hardware is usable (up). For an interface to be usable, both the interface hardware and line protocol must be up.
Broadcast address is	Broadcast address.
Peer address is	Peer address.
MTU is	MTU value set on the interface, in bytes.
Helper address	Helper address, if one is set.
Directed broadcast forwarding	Shows whether directed broadcast forwarding is enabled.
Outgoing access list	Shows whether the interface has an outgoing access list set.
Inbound access list	Shows whether the interface has an incoming access list set.
Proxy ARP	Shows whether Proxy Address Resolution Protocol (ARP) is enabled for the interface.
Security level	IP Security Option (IPSO) security level set for this interface.
Split horizon	Shows whether split horizon is enabled.
ICMP redirects	Shows whether redirect messages will be sent on this interface.
ICMP unreachables	Shows whether unreachable messages will be sent on this interface.
ICMP mask replies	Shows whether mask replies will be sent on this interface.
IP fast switching	Shows whether fast switching is enabled for this interface. It is generally enabled on serial interfaces, such as this one.
IP Flow switching	Shows whether Flow switching is enabled for this interface.
IP CEF switching	Shows whether Cisco Express Forwarding switching is enabled for the interface.
Downstream VPN Routing/Forwarding "D"	Shows the VRF instance where the PPP peer routes and AAA per-user routes are being installed.
IP multicast fast switching	Shows whether multicast fast switching is enabled for the interface.
IP route-cache flags are Fast	Shows whether NetFlow is enabled on an interface. Displays "Flow init" to specify that NetFlow is enabled on the interface. Displays "Ingress Flow" to specify that NetFlow is enabled on a subinterface using the **ip flow ingress**command. Shows "Flow" to specify that NetFlow is enabled on a main interface using the **ip route-cache flow** command.

Field	Description
Router Discovery	Shows whether the discovery process is enabled for this interface. It is generally disabled on serial interfaces.
IP output packet accounting	Shows whether IP accounting is enabled for this interface and what the threshold (maximum number of entries) is.
TCP/IP header compression	Shows whether compression is enabled.
WCCP Redirect outbound is disabled	Shows the status of whether packets received on an interface are redirected to a cache engine. Displays "enabled" or "disabled."
WCCP Redirect exclude is disabled	Shows the status of whether packets targeted for an interface will be excluded from being redirected to a cache engine. Displays "enabled" or "disabled."
Netflow Data Export (hardware) is enabled	NetFlow Data Expert (NDE) hardware flow status on the interface.

The table below describes the significant fields shown in the display.

Display a Summary of Interfaces on Cisco 4400 Series ISR: Example

The following is a sample out of the **show ip interface brief** command displaying a summary of the interfaces and their status on the device.

```
Router#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0/0   unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/1   unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/2   unassigned      YES NVRAM  down                  down
GigabitEthernet0/0/3   unassigned      YES NVRAM  down                  down
Serial1/0/0            unassigned      YES unset  down                  down
GigabitEthernet0       unassigned      YES NVRAM  up                    up
```

Display a Summary of the Usability Status: Example

The following example shows how to display a summary of the usability status information for each interface:

```
Router# show ip interface brief
Interface     IP-Address     OK?  Method  Status                  Protocol
Ethernet0     10.108.00.5    YES  NVRAM   up                      up
Ethernet1     unassigned     YES  unset   administratively down   down
Loopback0     10.108.200.5   YES  NVRAM   up                      up
Serial0       10.108.100.5   YES  NVRAM   up                      up
Serial1       10.108.40.5    YES  NVRAM   up                      up
Serial2       10.108.100.5   YES  manual  up                      up
Serial3       unassigned     YES  unset   administratively down   down
```

Table 104: show ip interface brief Field Descriptions

Field	Description
Interface	Type of interface.
IP-Address	IP address assigned to the interface.
OK?	"Yes" means that the IP Address is valid. "No" means that the IP Address is not valid.
Method	The Method field has the following possible values: • RARP or SLARP--Reverse Address Resolution Protocol (RARP) or Serial Line Address Resolution Protocol (SLARP) request. • BOOTP--Bootstrap protocol. • TFTP--Configuration file obtained from the TFTP server. • manual--Manually changed by the command-line interface. • NVRAM--Configuration file in NVRAM. • IPCP--**ip address negotiated** command. • DHCP--**ip address dhcp** command. • unset--Unset. • other--Unknown.
Status	Shows the status of the interface. Valid values and their meanings are: • up--Interface is up. • down--Interface is down. • administratively down--Interface is administratively down.
Protocol	Shows the operational status of the routing protocol on this interface.

Related Commands

Command	Description
ip address	Sets a primary or secondary IP address for an interface.
ip vrf autoclassify	Enables VRF autoclassify on a source interface.
match ip source	Specifies a source IP address to match to required route maps that have been set up based on VRF connected routes.
route-map	Defines the conditions for redistributing routes from one routing protocol into another or to enable policy routing.
set vrf	Enables VPN VRF selection within a route map for policy-based routing VRF selection.

Command	Description
show ip arp	Displays the ARP cache, in which SLIP addresses appear as permanent ARP table entries.
show route-map	Displays static and dynamic route maps.

show ip ips

To display Intrusion Prevention System (IPS) information such as configured sessions and signatures, use the **show ip ips**command in privileged EXEC mode.

Note Effective with Cisco IOS Release 15.1(4)M, the Cisco Services for IPS on IOS feature is not available in Cisco IOS software. As a result, the **license** keyword was removed from this command.

show ip ips {**all** | **configuration** | **interfaces** | **license** | **name** *name* | **sessions** [**detail**] [**vrf** *vrf-name*] | **signatures** [{[**count**] [{**detail** | **engine** [*engine-name*] | **sigid** [*sigid* [**subid** [*subid*]]]}] | [**statistics**]}] | **statistics** [**reset**] [**vrf** *vrf-name*]}

Syntax Description

all	Displays all available IPS information.
configuration	Displays additional configuration information, including default values that may not be displayed using the **show running-config**command.
interfaces	Displays the interface configuration.
license	Displays license and signature package information.
name *name*	Displays information only for the specified IPS rule.
sessions	Displays IPS session-related information.
detail	(Optional) Shows detailed session information.
vrf *vrf-name*	(Optional) Shows detailed session and latest statistics information per user specific VRF.
signatures	Displays signature information, such as which signatures are disabled and marked for deletion.
count	(Optional) Displays the number of signatures enabled, retired, and compiled.
detail	(Optional) Displays detailed signature information.
engine *engine-name*	(Optional) Displays signatures of a selected engine.
sigid *sigid*	(Optional) Displays signature ID for selected signatures.
subid *subid*	(Optional) Displays the sub ID for selected signatures.
statistics	(Optional) Displays the information such as the number of packets audited and the number of alarms sent.
statistics	Displays the information such as the number of packets audited and the number of alarms sent.
reset	(Optional) Resets sample output to reflect the latest statistics.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.3(8)T	This command was modified. The command name was changed from **show ip audit**to **show ip ips**. Also, all **show ip ips** commands were combined into a single command.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.
12.4(20)T	This command was modified. The **vrf** *keyword and vrf-name argument were added.*
12.4(22)T	This command was modified. The **count**, **detail**, **engine**, **sigid**, **signatures**, and **subid**keywordsandthe *engine-name*, *subid*, and *sigid*arguments were added.
15.0(1)M	This command was modified. The license keyword was added.
15.1(4)M	This command was modified. The **license** keyword was removed.

Usage Guidelines

Use the **show ip ips configuration** command to display additional configuration information, including default values that may not be displayed using the **show running-config** command.

Examples

Sample Output for the show ip ips configuration Command

The following example displays the output of the **show ip ips configuration** command:

```
Router# show ip ips configuration
Event notification through syslog is enabled
Event notification through Net Director is enabled
Default action(s) for info signatures is alarm
Default action(s) for attack signatures is alarm
Default threshold of recipients for spam signature is 25
PostOffice:HostID:5 OrgID:100 Addr:10.2.7.3 Msg dropped:0
HID:1000 OID:100 S:218 A:3 H:14092 HA:7118 DA:0 R:0
    CID:1 IP:172.21.160.20 P:45000 S:ESTAB (Curr Conn)

Audit Rule Configuration
 Audit name AUDIT.1
    info actions alarm
```

Sample Output for the show ip ips interfaces Command

The following example displays the output of the **show ip ips interfaces** command:

```
Router# show ip ips interfaces
Interface Configuration
 Interface Ethernet0
  Inbound IPS audit rule is AUDIT.1
```

```
    info actions alarm
  Outgoing IPS audit rule is not set
 Interface Ethernet1
  Inbound IPS audit rule is AUDIT.1
    info actions alarm
  Outgoing IPS audit rule is AUDIT.1
    info actions alarm
```

Sample Output for the show ip ips statistics Command

The following example displays the output of the **show ip ips statistics** command:

```
Router# show ip ips statistics
Signature audit statistics [process switch:fast switch]
  signature 2000 packets audited: [0:2]
  signature 2001 packets audited: [9:9]
  signature 2004 packets audited: [0:2]
  signature 3151 packets audited: [0:12]
Interfaces configured for audit 2
Session creations since subsystem startup or last reset 11
Current session counts (estab/half-open/terminating) [0:0:0]
Maxever session counts (estab/half-open/terminating) [2:1:0]
Last session created 19:18:27
Last statistic reset never

HID:1000 OID:100 S:218 A:3 H:14085 HA:7114 DA:0 R:0
```

Sample Output for the show ip ips statistics vrf Command

The following example displays the output of the **show ip ips statistics vrf vrf-name**command:

```
Router# show ip ips statistics vrf VRF_600
Signature statistics [process switch:fast switch]
  signature 5170:1 packets checked: [0:2]
Interfaces configured for ips 3
Session creations since subsystem startup or last reset 4
Current session counts (estab/half-open/terminating) [1:0:0]
Maxever session counts (estab/half-open/terminating) [2:1:1]
Last session created 00:02:34
Last statistic reset never
TCP reassembly statistics
  received 8 packets out-of-order; dropped 0
  peak memory usage 12 KB; current usage: 0 KB
  peak queue length 6
```

Sample Output for the show ip ips sessions vrf Command

The following example displays the output of the **show ip ips sessions vrf vrf-name**command:

```
Router# show ip ips sessions vrf VRF_600
Established Sessions
 Session 67D5C744 (10.0.4.2:34000)=>(10.0.6.2:23) tcp SIS_OPEN
```

Sample Output for the show ip ips license Command

The following example displays the output of the **show ip ips license**command:

```
Router# show ip ips license
IPS License Status Valid
Expiration Date: 2009-12-31
Signatures Loaded: 2009-06-25 S375
Signature Package: 2009-06-25 S375
```

The sample output shows the details for a valid IPS license. Note the license expiration date (2009-12-31), the version date of the existing S375 loaded signatures (2009-07-24 S375), and the version date of the last signature package (S375) loaded (2009-07-24 S375). The license is valid as the existing loaded signature version date is the same as the last signature package version date. The last signature package date (2009-07-24) is also before the license expiration date (2009-12-31).

Related Commands

Command	Description
clear ip ips statistics	Resets statistics on packets analyzed and alarms sent.

show ip ips auto-update

To display the automatic signature update configuration, use the **show ip ips auto-update**command in EXEC mode.

show ip ips auto-update

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

EXEC

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Automatic signature updates allow users to override the existing Intrusion Prevention System (IPS) configuration and automatically keep signatures up to date on the basis of a preset time, which can be configured to a preferred setting.

Use the **show ip ips auto-update** command to verify the auto update configuration.

Examples

The following example shows how to configure automatic signature updates and issue the **show ip ips auto-update** command to verify the configuration. In this example, the signature package file is pulled from the TFTP server at the start of every hour or every day, Sunday through Thursday. (Note that adjustments are made for months without 31 days and daylight savings time.)

```
Router# clock set ?
hh:mm:ss Current Time
Router# clock set 10:38:00 20 apr 2006
Router#
*Apr 20 17:38:00.000: %SYS-6-CLOCKUPDATE: System clock has been updated from 10:37:55 MST
Thu Apr 20 2006 to 10:38:00 MST Thu Apr 20 2006, configured from console by cisco on console.
Router(config)# ip ips auto-update
Router(config-ips-auto-update)# occur-at 0 0-23 1-31 1-5
Router(config-ips-auto-update)# $s-auto-update/IOS_reqSeq-dw.xml

Router(config-ips-auto-update)#^Z
Router#
*May 4 2006 15:50:28 MST: IPS Auto Update: setting update timer for next update: 0 hrs 10
min
*May 4 2006 15:50:28 MST: %SYS-5-CONFIG_I: Configured from console by cisco on console
Router#
Router# show ip ips auto-update

IPS Auto Update Configuration
URL : tftp://192.168.0.2/jdoe/ips-auto-update/IOS_reqSeq-dw.xml
Username : not configured
Password : not configured
Auto Update Intervals
  minutes (0-59) : 0
```

```
hours (0-23) : 0-23
days of month (1-31) : 1-31
days of week: (0-6) : 1-5
```

Related Commands

Command	Description
ip ips auto-update	Enables automatic signature updates for Cisco IOS IPS.

show ip ips category

To display the Intrusion Prevention Detection (IPS) categories, use the **show ip ips category** command in user EXEC or privileged EXEC mode.

show ip ips category *category-name* [*subcategory-name*] [**config**]

Syntax Description

category-name	The configured IPS categories. The table in the "Usage Guidelines" lists the *category-name* values.
subcategory-name	(Optional) The configured IPS subcategories. The table in the "Usage Guidelines" lists the *subcategory-name* values.
config	Specifies the configuration values.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.4(11)T	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Usage Guidelines

Use the **show ip ips category** command to display the IPS categories configured in the network.

The table below lists the values for the*category-name* and *subcategory-name* that can be configured for the **show ip ips category** command:

Table 105: Categories and Subcategories for the show ip ips category Command

Category Name	Description
adware/spyware	Displays information about the configured adware and spyware categories. The subcategory-name can be one of the following values: • **all-adware/spyware** --Advertising-supported software or spyware • **config** --Configuration values

Category Name	Description
attack	Displays information about the configured attack categories. The subcategory-name can be one of the following values: • **code_execution** --Code execution attack • **command_execution** --Command execution attack • **config** --Configuration values • **file_access** --File access • **general_attack** --General attack • **ids_evasion** --Intrusion Detection System (IDS) evasion • **informational** --Attack on the information resident in a network • **policy_violation** --Policy violation
ddos	Displays information about the configured Distributed Denial of Service attack categories. The subcategory-name can be one of the following values: • **all-ddos** --All Distributed Denial of Service attacks • **config** --Configuration values
dos	Displays information about the configured Denial of Service attack categories. The subcategory-name can be one of the following values: • **config** --Configuration values • **icmp_floods** --Internet Control Message Protocol flooding of the network • **tcp_floods** --Transmission Control Protocol flooding of the network • **udp_floods** --User Datagram Protocol flooding of the network
email	Displays the configured email clients. The subcategory-name can be one of the following values: • **config** --Configuration values • **imap** --Internet Message Access Protocol • **pop** --Post Office Protocol • **smtp** --Simple Mail Transfer Protocol

Category Name	Description
instant_messaging	Displays the configured instant messaging clients. The subcategory-name can be one of the following values: • **aol** --America Online • **config** --Configuration values • **jabber** --Jabber instant messaging • **msn** --Microsoft Network • **sametime** --IBM Lotus Sametime Connect • **yahoo** --Yahoo messaging service
ios_ips	Displays signature information, such as the signatures that are disabled or marked for deletion. The subcategory-name can be one of the following values: • **advanced** --Advanced category • **basic** --Basic category • **config** --Configuration values • **default** --Default category
l2/l3/l4_protocol	Displays the list of configured Layer 2, Layer 3, and Layer 4 protocols. The subcategory-name can be one of the following values: • **arp** --Address Resolution Protocol • **config** --Configuration values • **general_protocol** --General protocol • **ip** --Internet Protocol. The subcategory-name can be one of the following values: • **config**--Configuration values • **general_ip**--General Internet Protocol • **icmp**--Internet Control Message Protocol • **ip_fragment**--IP Fragment • **ip_v6**--Internet Protocol Version 6 • **tcp**--Transmission Control Protocol • **udp**--User Datagram Protocol

Category Name	Description
network_services	Displays the configured routing protocols. The subcategory-name can be one of the following values: • **bgp** --Border Gateway Protocol • **config** --Configuration values • **dhcp** --Dynamic Host Configuration Protocol • **dns** --Domain Name Server • **finger** --Finger User Information Protocol

os	Displays the configured operating system. The subcategory-name can be one of the following values:
	• **config** --Configuration values
	• **general_os** --General operating system
	• **ios** --Internetwork Operating System
	• **mac_os** --Mac operating system
	• **netware** --Netware operating system
	• **unix** --UNIX operating systems. The subcategory-name can be one of the following values:
	  • **aix**--Advanced Interactive eXecutive operating system
	  • **config**--Configuration values
	  • **general-unix**--UNIX operating system
	  • **hp-ux**--Hewlett-Packard UNIX operating system
	  • **irix**--IRIX operating system
	  • **linux**--Linux operating system
	  • **solaris**--Solaris operating system
	• **windows** --Windows operating systems. The subcategory-name can be one of the following values:
	  • **config**--Configuration values
	  • **general_windows**--General Windows
	  • **windows_nt/2k/xp**--Windows NT, Windows 2000, or Windows XP operating systems. You can specify the following keywords: **config**, **general_windows_nt/2k/xp**, and **winnt**.

Category Name	Description
other_services	Displays the other protocols configured. The subcategory-name can be one of the following values: • **config** --Configuration values • **ftp** --File Transfer Protocol • **general_service** --General service • **http** --Hypertext Transfer Protocol • **https** --Hypertext Transfer Protocol Secure • **ident** --Ident protocol • **lpr** --Line Printer Daemon protocol • **msrpc** --Microsoft Remote Procedural Call • **netbios/smb** --Network Basic Input/Output System or Server Message Block • **nntp** --Network News Transfer Protocol • **ntp** --Network Time Protocol • **r-services** --R services • **rpc** --Remote Procedural Call • **snmp** --Simple Network Management Protocol • **socks** --SOCKS • **sql** --Structured Query Language • **ssh** --Secure Shell Remote Protocol • **telnet** --Telnet Remote Protocol • **tftp** --Trivial File Transport Protocol
p2p	Displays the configured peer-to-peer networks for file sharing. The subcategory-name can be one of the following values: • **bittorrent** --BitTorrent • **config** --Configuration values • **edonkey** --eDonkey • **kazaa** --Kazaa

Category Name	Description
reconnaissance	Displays the configured network reconnaissance categories. The subcategory-name can be one of the following values: • **config** --Configuration values • **icmp_host_sweeps** --Internet Control Message Protocol Host Sweeps • **tcp/udp_combo_sweeps** --Transmission Control Protocol or User Datagram Protocol Combo Sweeps • **tcp_ports_sweeps** --Transmission Control Protocol Port Sweeps • **udp_port_sweeps** --User Datagram Protocol Port Sweeps
viruses/worms/trojans	Displays the viruses, worms, and trojans against which the network is configured. The subcategory-name can be one of the following values: • **all-viruses/worms/trojans** --All viruses, worms, and trojans that attack a network • **config** --Configuration values
web_server	Displays the configured Web servers. The subcategory-name can be one of the following values: • **apache** --Apache Web server • **config** --Configuration values • **internet_information_server_(iis)** --IIS Web server

Examples

The following examples display the output from variations of the **show ip ips category** command. The field names are self-explanatory.

```
Router# show ip ips category attack

Signatures in command_execution:
Signatures in general_attack:
Signatures in informational:
Signatures in file_access:
Signatures in code_execution:
Signatures in policy_violation:
Signatures in ids_evasion:
Router# show ip ips category instant_messaging

Signatures in yahoo:
Signatures in aol:
Signatures in msn:
Signatures in sametime:
Signatures in jabber:
```

Related Commands

Command	Description
ip ips	Applies an IPS rule to an interface.

show ip ips event-action-rules

To display event action rules information, use the **show ip ips event-action-rules** command in privileged EXEC mode.

show ip ips event-action-rules {**filters** | **overrides** | **target-value-rating**}

Syntax Description

filters	Displays the signature event action filters.
overrides	Displays the signature event action overrides.
target-value-rating	Displays the target value rating.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4 (11)T	This command was introduced.

Usage Guidelines

Event action rules are a group of settings you configure for the event action processing component of the sensor. These rules dictate the actions the sensor performs when an event occurs. Use the **show ip ips event-action-rules** command to display event action rules information, including default values that may not be displayed using the **show running-config** command.

Examples

The following example shows the global filter status for the event-action-rules. The output is self-explanatory.

```
Router# show ip ips event-action-rules filters

Filters
Global Filters Status: Enabled
```

The following example shows the global overrides status for the event-action-rules. The output is self-explanatory.

```
Router# show ip ips event-action-rules overrides

Overrides
Global Overrides Status: Enabled
Action to Add                    Enabled  Risk Rating
```

The following example shows the target-value-rating configuration status for the event-action-rules.The output is self-explanatory.

```
Router# show ip ips event-action-rules target-value-rating
No Target Value Ratings are configured
```

Related Commands

Command	Description
category	Displays category information.
configuration	Displays the IPS configuration information.
interfaces	Displays the IPS interfaces information.
ip ips all	Displays all IPS information.
ip ips auto-update	Enables automatic signature updates for Cisco IOS IPS.
name	Displays IPS name.
sessions	Displays IPS sessions.
signature-category	Displays signature category.
signatures	Displays IPS signatures.
statistics	Resets statistics on packets analyzed and alarms sent.

show ip ips signature-category

To display Cisco IOS Intrusion Prevention System (IPS) signature parameters by signature category, use the **show ip ips signature-category** command in privileged EXEC mode.

show ip ips signature-category [**config**]

Syntax Description

config	(Optional) Specifies configuration parameters for the signature categories.

Command Default

All the available signatures for the categories are displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Use the **show ip ips signature-category**command to verify the IPS signature parameters configured on the basis of a signature category.

Examples

The following is sample output from the **show ip ips signature-category** command:

```
Router# show ip ips signature-category
Signatures in basic:
Signatures in advanced:
Signatures in general_unix:
Signatures in general_linux:
Signatures in redhat:
Signatures in gentoo:
Signatures in mandrake:
Signatures in suse:
Signatures in solaris:
Signatures in hp-ux:
Signatures in aix:
Signatures in irix:
Signatures in general_windows:
Signatures in general_windows_nt/2k/xp:
Signatures in winnt:
Signatures in ios:
Signatures in general_os:
Signatures in netware:
Signatures in mac_os:
Signatures in command_execution:
Signatures in general_attack:
Signatures in informational:
Signatures in file_access:
```

The following example shows the **show ip ips signature-category**command output with the configured signature parameters:

```
Router# show ip ips signature-category config
    Category all:
```

```
    Retire: True
Category IOSIPS 256mb:
    Retire: False
```

Related Commands

Command	Description
ip ips signature-category	Tunes IPS signature parameters per category.
show ip ips	Displays IPS configuration information.

show ip nhrp

To display Next Hop Resolution Protocol (NHRP) mapping information, use the **show ip nhrp** command in user EXEC or privileged EXEC mode.

show ip nhrp [{ **dynamic** | **incomplete** | **static** }] [{ *address interface* }] [{ **brief** | **detail** }] [**purge**] [**shortcut**] [**remote**] [**local**]

Syntax Description

dynamic	(Optional) Displays dynamic (learned) IP-to-nonbroadcast multiaccess address (NBMA) mapping entries. Dynamic NHRP mapping entries are obtained from NHRP resolution/registration exchanges. See the table below for types, number ranges, and descriptions.
incomplete	(Optional) Displays information about NHRP mapping entries for which the IP-to-NBMA is not resolved. See the table below for types, number ranges, and descriptions.
static	(Optional) Displays static IP-to-NBMA address mapping entries. Static NHRP mapping entries are configured using the **ip nhrp map** command. See the table below for types, number ranges, and descriptions.
address	(Optional) Displays NHRP mapping entries for specified protocol addresses.
interface	(Optional) Displays NHRP mapping entries for the specified interface. See the table below for types, number ranges, and descriptions.
brief	(Optional) Displays a short output of the NHRP mapping.
detail	(Optional) Displays detailed information about NHRP mapping.
purge	(Optional) Displays NHRP purge information.
shortcut	(Optional) Displays NHRP shortcut information.
remote	Displays the NHRP cache entries for remote networks. **Note** By default, cache entries for both local and remote networks are displayed.
local	Displays the NHRP cache entries for local networks. **Note** By default, cache entries for both local and remote networks are displayed.
self	(Optional) Displays the NHRP fake cache information
summary	(Optional) Displays the summary of NHRP cache

Command Modes

User EXEC (>) Privileged EXEC (#)

Command Default

Information is displayed for all NHRP mappings.

Command History

Release	Modification
10.3	This command was introduced.

Release	Modification
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(22)T	The output of this command was extended to display the NHRP group received from the spoke.
Cisco IOS XE Release 2.5	This command was modified. Support was added for the **shortcut** keyword.
Cisco IOS XE Release 17.7.1.a	The **remote** and **local** keywords were integrated in this release.

Usage Guidelines

The table below lists the valid types, number ranges, and descriptions for the optional *interface* argument.

Note The valid types can vary according to the platform and interfaces on the platform.

Table 106: Valid Types, Number Ranges, and Interface Description

Valid Types	Number Ranges	Interface Descriptions
async	1	Async
atm	0 to 6	ATM
bvi	1 to 255	Bridge-Group Virtual Interface
cdma-ix	1	CDMA Ix
ctunnel	0 to 2147483647	C-Tunnel
dialer	0 to 20049	Dialer
ethernet	0 to 4294967295	Ethernet
fastethernet	0 to 6	FastEthernet IEEE 802.3
lex	0 to 2147483647	Lex
loopback	0 to 2147483647	Loopback
mfr	0 to 2147483647	Multilink Frame Relay bundle
multilink	0 to 2147483647	Multilink-group
null	0	Null
port-channel	1 to 64	Port channel
tunnel	0 to 2147483647	Tunnel

Valid Types	Number Ranges	Interface Descriptions
vif	1	PGM multicast host
virtual-ppp	0 to 2147483647	Virtual PPP
virtual-template	1 to 1000	Virtual template
virtual-tokenring	0 to 2147483647	Virtual Token Ring
xtagatm	0 to 2147483647	Extended tag ATM

Examples

The following is sample output from the **show ip nhrp** command. This output shows the NHRP group received from the spoke:

```
Router# show ip nhrp
10.0.0.2/32 via 10.0.0.2, Tunnel0 created 00:17:49, expire 00:01:30
  Type: dynamic, Flags: unique registered used
  NBMA address: 172.17.0.2
  Group: test-group-0
10.0.0.3/32 via 10.0.0.3, Tunnel0 created 00:00:11, expire 01:59:48
  Type: dynamic, Flags: unique registered used
  NBMA address: 172.17.0.3
  Group: test-group-0
11.0.0.2/32 via 11.0.0.2, Tunnel1 created 00:17:49, expire 00:02:10
  Type: dynamic, Flags: unique registered used
  NBMA address: 172.17.0.2
  Group: test-group-1
```

The following is sample output from the **show ip nhrp shortcut** command:

```
Router#show ip nhrp shortcut
10.1.1.1/24 via 1.1.1.22 Tunnel0 created 00:00:05, expire 00:02:24
   Type: dynamic, Flags: router rib
   NBMA address: 10.12.1.1
10.1.1.2/24 via 1.1.1.22 Tunnel0 created 00:00:05, expire 00:02:24
   Type: dynamic, Flags: router rib nho
   NBMA address: 10.12.1.2
```

The following is sample output from the **show ip nhrp detail** command:

```
Router# show ip nhrp detail
10.1.1.1/8 via 10.2.1.1, Tunnel1 created 00:46:29, never expire
  Type: static, Flags: used
  NBMA address: 10.12.1.1
10.1.1.2/8 via 10.2.1.2, Tunnel1 created 00:00:12, expire 01:59:47
  Type: dynamic, Flags: authoritative unique nat registered used
  NBMA address: 10.12.1.2
10.1.1.4, Tunnel1 created 00:00:07, expire 00:02:57
  Type: incomplete, Flags: negative
  Cache hits: 4
```

The following is sample output from the **show ip nhrp local** command:

```
Router# show ip nhrp local
Load for five secs: 100%/36%; one minute: 99%; five minutes: 99%
No time source, *12:44:19.808 UTC Tue Dec 7 2021
```

```
192.168.0.0/16 via 10.0.0.1
   Tunnel0 created 00:00:08, never expire
   Type: static, Flags: local
   NBMA address: 1.1.1.1
    (no-socket)
```

The following is sample output from the **show ip nhrp local detail** command:

```
Router# show ip nhrp local detail
Load for five secs: 100%/48%; one minute: 99%; five minutes: 99%
No time source, *12:44:52.971 UTC Tue Dec 7 2021

192.168.0.0/16 via 10.0.0.1
   Tunnel0 created 00:00:41, never expire
   Type: static, Flags: local
   NBMA address: 1.1.1.1
   Preference: 255
    (no-socket)
```

The following is sample output from the **show ip nhrp local dynamic** command:

```
Router# show ip nhrp local dynamic
Load for five secs: 99%/29%; one minute: 99%; five minutes: 99%
No time source, *12:45:15.567 UTC Tue Dec 7 2021
```

The following is sample output from the **show ip nhrp remote** command:

```
Router# show ip nhrp remote
Load for five secs: 99%/16%; one minute: 99%; five minutes: 99%
No time source, *12:45:36.789 UTC Tue Dec 7 2021

10.1.0.1/32 via 10.1.0.1
   Tunnel0 created 00:08:41, expire 00:12:55
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.1.1
10.1.0.3/32 via 10.1.0.3
   Tunnel0 created 00:17:30, expire 00:12:36
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.3.1
10.1.0.4/32 via 10.1.0.4
   Tunnel0 created 00:13:01, expire 00:14:31
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.4.1
10.1.0.5/32 via 10.1.0.5
   Tunnel0 created 00:02:08, expire 00:12:51
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.5.1
10.1.0.6/32 via 10.1.0.6
   Tunnel0 created 00:07:19, expire 00:07:41
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.6.1
10.1.0.7/32 via 10.1.0.7
   Tunnel0 created 00:07:27, expire 00:14:57
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.7.1
10.1.0.8/32 via 10.1.0.8
   Tunnel0 created 00:08:30, expire 00:06:31
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.8.1
10.1.0.9/32 via 10.1.0.9
   Tunnel0 created 00:06:22, expire 00:12:34
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.9.1
```

```
10.1.0.10/32 via 10.1.0.10
   Tunnel0 created 00:13:05, expire 00:11:14
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.10.1
10.1.0.11/32 via 10.1.0.11
   Tunnel0 created 00:12:41, expire 00:06:29
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.11.1
10.1.0.12/32 via 10.1.0.12
   Tunnel0 created 00:07:07, expire 00:07:52
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.12.1
10.1.0.13/32 via 10.1.0.13
   Tunnel0 created 00:13:01, expire 00:14:14
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.13.1
10.1.0.14/32 via 10.1.0.14
   Tunnel0 created 00:14:01, expire 00:00:58
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.14.1
10.1.0.15/32 via 10.1.0.15
   Tunnel0 created 00:00:56, expire 00:14:03
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.15.1
10.1.0.16/32 via 10.1.0.16
   Tunnel0 created 00:13:01, expire 00:11:07
```

The following is sample output from the **show ip nhrp remote detail** command:

```
Router# show ip nhrp remote detail
Load for five secs: 99%/27%; one minute: 99%; five minutes: 99%
No time source, *12:45:49.796 UTC Tue Dec 7 2021

10.1.0.1/32 via 10.1.0.1
   Tunnel0 created 00:08:54, expire 00:12:42
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.1.1
   Preference: 192
10.1.0.3/32 via 10.1.0.3
   Tunnel0 created 00:17:43, expire 00:12:23
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.3.1
   Preference: 192
10.1.0.4/32 via 10.1.0.4
   Tunnel0 created 00:13:14, expire 00:14:18
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.4.1
   Preference: 192
10.1.0.5/32 via 10.1.0.5
   Tunnel0 created 00:02:21, expire 00:12:38
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.5.1
   Preference: 192
10.1.0.6/32 via 10.1.0.6
   Tunnel0 created 00:07:32, expire 00:07:28
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.6.1
   Preference: 192
10.1.0.7/32 via 10.1.0.7
  Tunnel0 created 00:07:40, expire 00:14:44
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.7.1
   Preference: 192
10.1.0.8/32 via 10.1.0.8
```

```
   Tunnel0 created 00:08:43, expire 00:14:47
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.8.1
   Preference: 192
10.1.0.9/32 via 10.1.0.9
   Tunnel0 created 00:06:35, expire 00:12:21
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.9.1
   Preference: 192
10.1.0.10/32 via 10.1.0.10
   Tunnel0 created 00:13:18, expire 00:11:01
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.10.1
   Preference: 192
10.1.0.11/32 via 10.1.0.11
   Tunnel0 created 00:12:54, expire 00:06:16
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.11.1
   Preference: 192
10.1.0.12/32 via 10.1.0.12
   Tunnel0 created 00:07:20, expire 00:07:39
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.12.1
   Preference: 192
10.1.0.13/32 via 10.1.0.13
   Tunnel0 created 00:13:14, expire 00:14:01
   Type: dynamic, Flags: registered nhop bfd
```

The following is sample output from the **show ip nhrp remote dynamic** command:

```
Router# show ip nhrp remote dynamic
Load for five secs: 100%/12%; one minute: 99%; five minutes: 99%
No time source, *12:48:52.151 UTC Tue Dec 7 2021

10.1.0.1/32 via 10.1.0.1
   Tunnel0 created 00:11:56, expire 00:12:31
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.1.1
10.1.0.2/32 via 10.1.0.2
   Tunnel0 created 00:02:46, expire 00:12:32
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.2.1
10.1.0.3/32 via 10.1.0.3
   Tunnel0 created 00:20:45, expire 00:12:32
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.3.1
10.1.0.4/32 via 10.1.0.4
   Tunnel0 created 00:16:16, expire 00:12:32
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.4.1
10.1.0.5/32 via 10.1.0.5
   Tunnel0 created 00:05:23, expire 00:12:32
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.5.1
10.1.0.6/32 via 10.1.0.6
   Tunnel0 created 00:10:34, expire 00:12:32
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.6.1
10.1.0.7/32 via 10.1.0.7
   Tunnel0 created 00:10:42, expire 00:12:32
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.7.1
10.1.0.8/32 via 10.1.0.8
   Tunnel0 created 00:11:45, expire 00:12:32
```

```
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.8.1
10.1.0.9/32 via 10.1.0.9
   Tunnel0 created 00:09:38, expire 00:12:32
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.9.1
10.1.0.10/32 via 10.1.0.10
   Tunnel0 created 00:16:20, expire 00:12:32
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.10.1
10.1.0.11/32 via 10.1.0.11
   Tunnel0 created 00:15:56, expire 00:12:32
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.11.1
10.1.0.12/32 via 10.1.0.12
   Tunnel0 created 00:10:23, expire 00:12:32
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.12.1
10.1.0.13/32 via 10.1.0.13
   Tunnel0 created 00:16:16, expire 00:12:32
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.13.1
10.1.0.14/32 via 10.1.0.14
   Tunnel0 created 00:17:16, expire 00:12:32
   Type: dynamic, Flags: registered nhop bfd
   NBMA address: 11.0.14.1
10.1.0.15/32 via 10.1.0.15
   Tunnel0 created 00:04:11, expire 00:12:32
```

The following is sample output from the **show ip nhrp remote self** command:

```
Router# show ip nhrp remote dynamic
Load for five secs: 55%/3%; one minute: 62%; five minutes: 87%
No time source, *12:50:24.793 UTC Tue Dec 7 2021

10.0.0.1/32 via 10.0.0.1
   Tunnel0 created 06:46:47, never expire
   Type: static, Flags: router unique local
   NBMA address: 1.1.1.1
    (no-socket)
Metadata Exchange Framework:
Type State
1   Reset
MEF ext data:0x0
2   Reset
MEF ext data:0x0
3   Reset
MEF ext data:0x0
```

The following is sample output from the **show ip nhrp remote summary** command:

```
Router# show ip nhrp remote summary
Load for five secs: 20%/0%; one minute: 50%; five minutes: 79%
No time source, *12:51:38.026 UTC Tue Dec 7 2021

IP NHRP cache 10000 entries, 7680000 bytes
    1 static   9999 dynamic    0 incomplete
9999 Remote
    0 static   9999 dynamic    0 incomplete
    9999 nhop     9999 bfd
    0 default  0 temporary
    0 route
        0 rib (0 H    0 nho)
```

```
        0 bgp
    0 lfib
1 Local
    1 static   0 dynamic    0 incomplete
    0 lfib
```

The following is sample output from the **show ip nhrp remote static tu1** command:

```
Router# show ip nhrp remote static tu1
10.0.0.1/32 (VPN1) via 10.0.0.1
   Tunnel1 created 1d06h, never expire
   Type: static, Flags: bfd
   NBMA address: 1.1.1.1
spoke1#sh ip nhrp remote static tu11
10.0.0.1/32 (VPN11) via 10.0.0.1
   Tunnel11 created 1d06h, never expire
   Type: static, Flags: bfd
   NBMA address: 1.1.1.1
```

The table below describes the significant fields shown in the displays.

Table 107: show ip nhrp Field Descriptions

Field	Description
10.1.1.1/8	Target network.
via 10.2.1.1	Next Hop to reach the target network.
Tunnel1	Interface through which the target network is reached.
created 00:00:12	Length of time since the entry was created (hours:minutes:seconds).
expire 01:59:47	Time remaining until the entry expires (hours:minutes:seconds).
never expire	Indicates that static entries never expire.
Type	• dynamic--NHRP mapping is obtained dynamically. The mapping entry is created using information from the NHRP resolution and registrations. • static--NHRP mapping is configured statically. Entries configured by the **ip nhrp map** command are marked static. • incomplete--The NBMA address is not known for the target network.
NBMA address	Nonbroadcast multiaccess address of the next hop. The address format is appropriate for the type of network being used: ATM, Ethernet, Switched Multimegabit Data Service (SMDS), or multipoint tunnel.

Field	Description
Flags	• authoritative--Indicates that the NHRP information was obtained directly from the Next Hop Server or router that maintains and is authoritative for the NBMA-to-IP address mapping for a particular destination. • implicit--Indicates that the local node learned about the NHRP mapping entries from the source mapping information of an NHRP resolution request received by the local router, or from an NHRP resolution packet being forwarded through the local router. • local--Indicates NHRP mapping entries that are for networks local to this router (that is, serviced by this router). These flag entries are created when this router answers an NHRP resolution request that has this information and is used to store the transport (tunnel) IP address of all the other NHRP nodes to which it has sent this information. If for some reason this router loses access to this local network (that is, it can no longer service this network), it sends an NHRP purge message to all remote NHRP nodes that are listed in the "local" entry (in **show ip nhrp detail** command output) to tell the remote nodes to clear this information from their NHRP mapping tables. This local mapping entry times out of the local NHRP mapping database at the same time that this information (from the NHRP resolution reply) would time out of the NHRP mapping database on the remote NHRP nodes. • nat--Indicates that the remote node (NHS client) supports the new NHRP NAT extension type for dynamic spoke-spoke tunnels to/from spokes behind a NAT router. This marking does not indicate that the spoke (NHS client) is behind a NAT router.
Flags (continued)	• negative--For negative caching, indicates that the requested NBMA mapping has not yet been or could not be obtained. When NHRP sends an NHRP resolution request, an incomplete (negative) NHRP mapping entry for the address is inserted in the resolution request. This insertion suppresses any more triggering of NHRP resolution requests while the resolution request is being resolved. If configured, any encryption parameters (IKE/IPsec) for the tunnel are negotiated. • (no socket)--Indicates that the NHRP mapping entries will not trigger IPsec to set up encryption because data traffic does not need to use this tunnel. Later, if data traffic needs to use this tunnel, the flag will change from a "(no socket)" to a "(socket)" entry and IPsec will be triggered to set up the encryption for this tunnel. Local and implicit NHRP mapping entries are always initially marked as "(no socket)." By default, NHRP caches source information from NHRP resolution request or replies as they go through the system. To allow this caching to continue, but not have the entry create an IPsec socket, they are marked as (no socket). If this was not done there would be extra IPsec sockets from the hubs to the various spokes that either were not used or were used for only one or two packets while a direct spoke-to-spoke tunnel was being built. Data packets and NHRP packets that arrive on the tunnel interface and are forwarded back out the tunnel interface are not allowed to use the (no socket) NHRP mappings for forwarding. Because, in this case, the router is an intermediate node in the path between the two endpoints and we only want to create short-cut tunnels between the initial entrance and final exit point of the DMVPN (NBMA) network and not between any intermediate nodes. If at some point the router receives a data packet that has a source interface that is not the tunnel interface and it would use the (no socket) mapping entry, the router converts the (no socket) entry to a (socket) entry. In this case, this router is the entrance (or exit) point of the NBMA (for this traffic stream).

Field	Description
Flags (continued)	• (no socket) (continued)--These (no socket) mapping entries are marked (non-authoritative); only mappings from NHRP registrations are marked (authoritative). The NHRP resolution requests are also marked (authoritative), which means that the NHRP resolution request can be answered only from an (authoritative) NHRP mapping entry. A (no socket) mapping entry will not be used to answer an NHRP resolution request and the NHRP resolution request will be forwarded to the NHS of the nodes . • registered--Indicates that the mapping entry was created in response to an NHRP registration request. Although registered mapping entries are dynamic entries, they may not be refreshed through the "used" mechanism. Instead, these entries are refreshed by another NHRP registration request with the same transport (tunnel) IP to NBMA address mapping. The Next Hop Client (NHC) periodically sends NHRP registration requests to keep these mappings from expiring. • router--Indicates that NHRP mapping entries for a remote router (that is accessing a network or host behind the remote router) are marked with the router flag. • unique--NHRP registration requests have the unique flag set on by default. This flag indicates that an NHRP mapping entry cannot be overwritten by a mapping entry that has the same IP address and a different NBMA address. When a spoke has a statically configured outside IP (NBMA) address, this is used to keep another spoke that is mis-configured with the same transport (tunnel) IP address from overwriting this entry. If a spoke has a dynamic outside IP (NBMA) address, you can configure the **ip nhrp registration no-unique** command on the spoke to clear this flag. This configuration allows the registered NHRP mapping entry for that spoke on the hub to be overwritten with a new NBMA address. This is necessary in this case because the spoke's outside IP (NBMA) address can change at any time. If the "unique" flag was set, the spoke would have to wait for the mapping entry on the hub to time out before it could register its new (NBMA) mapping.
Flags (continued)	• used--When data packets are process-switched and this mapping entry was used, the mapping entry is marked as used. The mapping database is checked every 60 seconds. If the used flag is set and more than 120 seconds remain until expire time, the used flag is cleared. If fewer than 120 seconds are left, this mapping entry is "refreshed" by the transmission of another NHRP resolution request. **Note** When using DMVPN Phase 3 in 12.4(6)T, CEF switched packets will also set the "used" flag, and these entries will be timed out and refreshed as described in the "used" flag description above.

Related Commands

Command	Description
ip nhrp group	Configures a NHRP group on a spoke.
ip nhrp map	Statically configures the IP-to-NBMA address mapping of IP destinations connected to an NBMA network.
ip nhrp map group	Adds NHRP groups to QoS policy mappings on a hub.

Command	Description
ip nhrp shortcut	Enables shortcut switching on the tunnel interface.
show dmvpn	Displays DMVPN-specific session information.
show ip nhrp group-map	Displays the details of NHRP group mappings on a hub and the list of tunnels using each of the NHRP groups defined in the mappings.
show ip nhrp multicast	Displays NHRP multicast mapping information.
show ip nhrp nhs	Displays NHRP Next Hop Server information.
show ip nhrp summary	Displays NHRP mapping summary information.
show ip nhrp traffic	Displays NHRP traffic statistics.
show policy-map mgre	Displays statistics about a specific QoS policy as it is applied to a tunnel endpoint.

show ip nhrp nhs

To display Next Hop Resolution Protocol (NHRP) next hop server (NHS) information, use the **show ip nhrp nhs**command in user EXEC or privileged EXEC mode.

show ip nhrp nhs [*interface*] [**detail**]

Syntax Description

interface	(Optional) Displays NHS information currently configured on the interface. See the table below for types, number ranges, and descriptions.
detail	(Optional) Displays detailed NHS information.

Command Modes

User EXEC Privileged EXEC

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS release 12.2(33)SRB.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The table below lists the valid types, number ranges, and descriptions for the optional *interface*argument.

Note The valid types can vary according to the platform and interfaces on the platform.

Table 108: Valid Types, Number Ranges, and Interface Descriptions

Valid Types	Number Ranges	Interface Descriptions
async	1	Async
atm	0 to 6	ATM
bvi	1 to 255	Bridge-Group Virtual Interface
cdma-ix	1	CDMA Ix
ctunnel	0 to 2147483647	C-Tunnel
dialer	0 to 20049	Dialer
ethernet	0 to 4294967295	Ethernet
fastethernet	0 to 6	FastEthernet IEEE 802.3
lex	0 to 2147483647	Lex

Valid Types	Number Ranges	Interface Descriptions
loopback	0 to 2147483647	Loopback
mfr	0 to 2147483647	Multilink Frame Relay bundle
multilink	0 to 2147483647	Multilink-group
null	0	Null
port-channel	1 to 64	Port channel
tunnel	0 to 2147483647	Tunnel
vif	1	PGM multicast host
virtual-ppp	0 to 2147483647	Virtual PPP
virtual-template	1 to 1000	Virtual template
virtual-tokenring	0 to 2147483647	Virtual Token Ring
xtagatm	0 to 2147483647	Extended tag ATM

Examples

The following is sample output from the **show ip nhrp nhs detail** command:

```
Router# show ip nhrp nhs detail
Legend:
  E=Expecting replies
  R=Responding
Tunnel1:
  5.1.1.1           E  req-sent 128  req-failed 1  repl-recv 0
Pending Registration Requests:
Registration Request: Reqid 1, Ret 64  NHS 5.1.1.1
```

The table below describes the significant field shown in the display.

Table 109: show ip nhrp nhs Field Descriptions

Field	Description
Tunnel1	Interface through which the target network is reached.

Related Commands

Command	Description
ip nhrp map	Statically configures the IP-to-NBMA address mapping of IP destinations connected to an NBMA network.
show ip nhrp	Displays NHRP mapping information.
show ip nhrp multicast	Displays NHRP multicast mapping information.
show ip nhrp summary	Displays NHRP mapping summary information.

Command	Description
show ip nhrp traffic	Displays NHRP traffic statistics.

show ip port-map

To display the port-to-application mapping (PAM) information, use the show ip port-map command in privileged EXEC mode.

show ip port-map [{*appl-name* | **port** *port-num* [**detail**]}]

Syntax Description

appl-name	(Optional) Specifies the name of the application to which to apply the port mapping.
port *port-num*	(Optional) Specifies the alternative port number that maps to the application.
detail	(Optional) Shows the port or application details.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.3(14)T	The **detail** keyword was added and command output was modified to display user-defined applications.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to display the port mapping information at the firewall, including the system-defined and user-defined information. Include the application name to display the list of entries by application. Include the port number to display the entries by port.

Examples

The following is sample output from the **show ip port-map** command, including system- and user-defined mapping information. Notice that multiple port numbers display in a series such as 554, 8554, or 1512...1525, or a range such as 55000 to 62000. When there are multiple ports, they all display if they can fit into the fixed-field width. If they cannot fit into the fixed-field width, they display with an ellipse, such as 1512...1525 shown below.

```
Router# show ip port-map
Default mapping:  snmp       udp port 161                    system defined
Host specific:    snmp       udp port 577         in list 55 user defined
Host specific:    snmp       udp port 55000-62000 in list 57 user defined
Default mapping:  echo       tcp port 7                      system defined
Default mapping:  echo       udp port 7                      system defined
Default mapping:  telnet     tcp port 23                     system defined
Default mapping:  wins       tcp port 1512...1525            system defined
Default mapping:  n2h2server tcp port 9285                   system defined
Default mapping:  n2h2server udp port 9285                   system defined
Default mapping:  nntp       tcp port 119                    system defined
Default mapping:  pptp       tcp port 1725                   system defined
```

```
Default mapping:  rtsp       tcp port 554,8554              system defined
Default mapping:  bootpc     udp port 68                    system defined
Default mapping:  gdoi       udp port 848                   system defined
Default mapping:  tacacs     udp port 49                    system defined
Default mapping:  gopher     tcp port 70                    system defined
Default mapping:  icabrowser udp port 1604                  system defined
```

The following sample output from the **show ip port-map snmp** command displays information about the SNMP application:

```
Router# show ip port-map snmp
Default mapping:  snmp    udp port 161                      system defined
Host specific:    snmp    udp port 577          in list 55  user defined
Host specific:    snmp    udp port 55000-62000  in list 57  user defined
```

The following sample output from the **show ip port-map snmp detail** command displays detailed information about the SNMP application:

```
Router# show ip port-map snmp detail
 IP port-map entry for application 'snmp':
     udp 161                    Simple Network Management Protoco system defined
     udp 577             list 55 User's SNMP Port                  user defined
     udp 55000-62000     list 57 User's Another SNMP Port          user defined
```

The following sample output from the **show ip port-map port 577** command displays information about port 577:

```
Router# show ip port-map port 577
Host specific:   snmp  udp port 577    in list 55   user defined
```

The following sample output from the **show ip port-map port 55800**command displays information about port 55800:

```
Router# show ip port-map port 55800
Host specific:   snmp   udp port 55800  in list 57   user defined
```

The following sample output from the **show ip-port-map port 577 detail** command displays detailed information about port 577:

```
Router# show ip port-map port 577 detail

 IP Port-map entry for port 577:
 snmp                 udp list 55                               user defined
```

Related Commands

Command	Description
ip port-map	Establishes PAM entries.

show ip sdee

To display Security Device Event Exchange (SDEE) notification information, use the **show ip sdee**command in privileged EXEC mode.

show ip sdee [**alerts**] [**all**] [**errors**] [**events**] [**configuration**] [**status**] [**subscriptions**]

Syntax Description

alerts	Displays the Intrusion Detection System (IDS) alert buffer.
all	Displays all information available for IDS SDEE notifications.
errors	Displays IDS SDEE error messages.
events	Displays IDS SDEE events.
configuration	Displays SDEE configuration parameters.
status	Displays the status events that are currently in the buffer.
subscriptions	Displays IDS SDEE subscription information.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(8)T	This command was introduced.

Examples

The following is sample output from the **show ip sdee alerts** command. In this example, the alerts are numbered from 1 to 100 (because 100 events are currently in the event buffer). Following the alert number are 3 digits, which indicate whether the alert has been reported for the 3 possible subscriptions. In this example, these alerts have been reported for subscription number 1. The event ID is composed of the alert time and an increasing count, separated by a colon.

```
Router# show ip sdee alerts
Event storage:1000 events using 656000 bytes of memory
                                SDEE Alerts
SigID       SrcIP     DstIP       SrcPort  DstPort  Sev     Event ID        SigName
1:100 2004  10.0.0.2  10.0.0.1    8        0        2       10211478597901  ICMP Echo Req
2:100 2004  10.0.0.2  10.0.0.1    8        0        2       10211478887902  ICMP Echo Req
3:100 2004  10.0.0.2  10.0.0.1    8        0        2       10211479247903  ICMP Echo Req
4:100 2004  10.0.0.2  10.0.0.1    8        0        2       10211479457904  ICMP Echo Req
5:100 2004  10.0.0.2  10.0.0.1    8        0        2       10211479487905  ICMP Echo Req
6:100 2004  10.0.0.2  10.0.0.1    8        0        2       10211480077906  ICMP Echo Req
7:100 2004  10.0.0.2  10.0.0.1    8        0        2       10211480407907  ICMP Echo Req
.....................................................
.....................................................
96:000 2004 10.0.0.2  10.0.0.1    8        0        2       10211750898596  ICMP Echo Req
97:000 2004 10.0.0.2  10.0.0.1    8        0        2       10211750898597  ICMP Echo Req
98:000 2004 10.0.0.2  10.0.0.1    8        0        2       10211750898598  ICMP Echo Req
99:000 2004 10.0.0.2  10.0.0.1    8        0        2       10211750908599  ICMP Echo Req
100:000 2004 10.0.0.2 10.0.0.1    8        0        2       10211750918600  ICMP Echo Req
```

The following is sample output is from the **show ip sdee subscriptions**command. In this example, SDEE is enabled, the maximum event buffer size has been set to 100, and the maximum number of subscriptions that can be open at the same time is 1.

```
Router# show ip sdee subscriptions

SDEE is enabled
Alert buffer size:100 alerts 65600 bytes
Maximum subscriptions:1
SDEE open subscriptions: 1
Subscription ID IDS1720:0:
Client address 10.0.0.2 port 1500
        Subscription opened at 13:21:30 MDT July 18 2003
        Total GET requests:0
        Max number of events:50
        Timeout:30
        Event Start Time:0
        Report alerts:true
        Alert severity level is INFORMATIONAL
        Report errors:false
        Report status:false
```

The table below describes the significant fields shown in the display.

Table 110: show ip sdee subscriptions Field Descriptions

Field	Description
Alert buffer size:100 alerts 65600 bytes	Maximum number of events that can be stored in the buffer. The maximum number of events to be stored refers to all types of events (alert, status, and error). (This value can be changed via the **ip sdee events** command.)
Maximum subscriptions:1	Maximum number of subscriptions that can be open at the same time. (This value can be changed via the **ip sdee subscriptions** command.)

The following is sample output from the **show ip sdee status**command. In this example, the buffer is set to store a maximum of 1000 events.

```
Router# show ip sdee status
Event storage:1000 events using 656000 bytes of memory
                  SDEE Status Messages
Time                           Message              Description
1:000 22:10:58 UTC Apr 18 2003  applicationStarted   STRING.UDP,0 ms
2:000 22:10:58 UTC Apr 18 2003  applicationStarted   STRING.TCP,0 ms
3:000 22:10:58 UTC Apr 18 2003  applicationStarted   OTHER,0 ms
4:000 22:10:58 UTC Apr 18 2003  applicationStarted   SERVICE.FTP,276 ms
5:000 22:11:07 UTC Apr 18 2003  applicationStarted   SERVICE.SMTP,8884 ms
6:000 22:11:07 UTC Apr 18 2003  applicationStarted   SERVICE.RPC,72 ms
7:000 22:11:07 UTC Apr 18 2003  applicationStarted   SERVICE.DNS,132 ms
8:000 22:11:15 UTC Apr 18 2003  applicationStarted   SERVICE.HTTP,7632 ms
9:000 22:11:15 UTC Apr 18 2003  applicationStarted   ATOMIC.TCP,24 ms
10:000 22:11:15 UTC Apr 18 2003  applicationStarted  ATOMIC.UDP,12 ms
11:000 22:11:15 UTC Apr 18 2003  applicationStarted  ATOMIC.ICMP,12 ms
12:000 22:11:15 UTC Apr 18 2003  applicationStarted  ATOMIC.IPOPTIONS,8 ms
13:000 22:11:15 UTC Apr 18 2003  applicationStarted  ATOMIC.L3.IP,8 ms
```

Related Commands

Command	Description
ip ips notify	Specifies the method of event notification.
id sdee events	Sets the maximum number of SDEE events that can be stored in the event buffer.
ip sdee subscriptions	Sets the maximum number of SDEE subscriptions that can be open simultaneously.

show ip ips sig-clidelta

To display the signature parameter tunings configured using the CLI that are stored in the iosips-sig-clidelta.xmz signature file, use the **show ip ips sig-clidelta**command in privileged EXEC mode.

show ip ips sig-clidelta

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **show ip ips sig-clidelta**command displays the tunings configured from the CLI that are stored in the iosips-sig-clidelta.xmz signature file.

Examples

The following is sample output from the **show ip ips sig-clidelta**command. The field descriptions are self-explanatory.

```
Router# show ip ips sig-clidelta
En  - possible values are Y, Y*, N, or N*
      Y:  signature is enabled
      N:  enabled=false in the signature definition file
      *:  retired=true in the signature definition file
Cmp - possible values are Y, Ni, Nr, Nf, or No
      Y:  signature is compiled
      Ni: signature not compiled due to invalid or missing parameters
      Nr: signature not compiled because it is retired
      Nf: signature compile failed
      No: signature is obsoleted
      Nd: signature is disallowed
Action=(A)lert, (D)eny, (R)eset, Deny-(H)ost, Deny-(F)low
Trait=alert-traits             EC=event-count          AI=alert-interval
GST=global-summary-threshold   SI=summary-interval     SM=summary-mode
SW=swap-attacker-victim        SFR=sig-fidelity-rating Rel=release
 SigID:SubID En  Cmp   Action Sev   Trait   EC   AI   GST   SI  SM SW SFR Rel
 ----------- --  ----  ------ ---   -----  ---- ---- -----  --- -- -- --- ---
  5733:0     N   Y     A     HIGH     0     1    0      0    0  FA  N 85  S266
```

Related Commands

Command	Description
ip ips enable-clidelta	Enables the signature tuning settings in the clidelta.xmz file on the router to take precedence over the signature settings in the iosips-sig-delta.xmz file.

show ip source-track

To display traffic flow statistics for tracked IP host addresses, use the **show ip source-track**command in privileged EXEC mode.

show ip source-track [*ip-address*] [{**summary** | **cache**}]

Syntax Description

ip-address	(Optional) Displays the IP address of the tracked host for which traffic flow information is displayed.
summary	(Optional) Displays a summary of traffic flow information that is collected for a specified host address (via the *ip-address* argument) or for all configured hosts.
cache	(Optional) Displays detailed packet and flow information that is collected on line cards and port adapters for all tracked IP addresses or for specified IP address (not displayed in the a distributed platform such as the gigabit route processor (GRP) or route switch processor (RSP)).

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(21)S	This command was introduced.
12.0(22)S	This command was implemented on the Cisco 7500 series routers.
12.0(26)S	This command was implemented on Cisco 12000 series ISE line cards.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example, which is sample output from the show ip source-track summary command, shows how to verify that IP source tracking is enabled for one or more hosts:

```
Router# show ip source-track summary
Address          Bytes    Pkts    Bytes/s   Pkts/s
10.0.0.1          119G   1194M    443535      4432
192.168.1.1       119G   1194M    443535      4432
192.168.42.42     119G   1194M    443535      4432
```

The following example, which is sample output from the show ip source-track summary command, shows how to verify that no traffic has yet to be received for the destination hosts that are being tracked:

```
Router# show ip source-track summary
Address         Bytes   Pkts   Bytes/s   Pkts/s
10.0.0.1            0      0         0        0
192.168.1.1         0      0         0        0
192.168.42.42       0      0         0        0
```

The following example, which is sample output from the show ip source-track command, shows that IP source tracking is processing packets to the hosts and exporting statistics from the line card or port adapter to the route processor:

```
Router# show ip source-track
Address          SrcIF    Bytes   Pkts   Bytes/s   Pkts/s
10.0.0.1         PO0/0    119G   1194M    513009     5127
192.168.1.1      PO0/0    119G   1194M    513009     5127
192.168.42.42    PO0/0    119G   1194M    513009     5127
```

Related Commands

Command	Description
ip source-track	Enables IP source tracking for a specified host.
ip source-track address-limit	Configures the maximum number of destination hosts that can be simultaneously tracked at any given moment.
ip source-track syslog-interval	Sets the time interval (in minutes) in which syslog messages are generated if IP source tracking is enabled on a device.

show ip source-track export flows

To display the last ten packet flows that were exported from the line card to the route processor, use the **show ip source-track export flows**command in privileged EXEC mode.

show ip source-track export flows

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(21)S	This command was introduced.
12.0(22)S	This command was implemented on the Cisco 7500 series routers.
12.0(26)S	This command was implemented on Cisco 12000 series ISE line cards.
12.3(7)T	This command was integrated into Cisco IOS Release 12.3(7)T.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **show ip source-track export flows** command can be issued only on distributed platforms such as the GRP and the RSP.

Examples

The following example displays the packet flow information that is exported from line cards and port adapters to the gigabit route processor (GRP) and the route switch processor (RSP):

```
Router# show ip source-track export flows
SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
PO0/0         10.1.1.0        Null          10.1.1.1        06 0000 0000    88K
PO0/0         10.1.1.0        Null          10.1.1.3        06 0000 0000    88K
PO0/0         10.1.1.0        Null          10.1.1.2        06 0000 0000    88K
```

Related Commands

Command	Description
ip source-track	Enables IP source tracking for a specified host.
ip source-track export-interval	Sets the time interval (in seconds) in which IP source tracking statistics are exported from the line card to the RP.

show ip ssh

To display the version and configuration data for Secure Shell (SSH), use the **show ip ssh** command in privileged EXEC mode.

show ip ssh

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)S	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1 T.
12.1(5)T	This command was modified to display the SSH status--enabled or disabled.
12.2(17a)SX	This command was integrated into Cisco IOS Release 12.2(17a)SX.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.

Usage Guidelines

Use the **show ip ssh** command to view the status of configured options such as retries and timeouts. This command allows you to see if SSH is enabled or disabled.

Examples

The following is sample output from the **show ip ssh** command when SSH has been enabled:

```
Router# show ip ssh
SSH Enabled - version 1.5
Authentication timeout: 120 secs; Authentication retries: 3
The following is sample output from the show ip ssh
 command when SSH has been disabled:
Router# show ip ssh
%SSH has not been enabled
```

Related Commands

Command	Description
show ssh	Displays the status of SSH server connections.

show ip traffic-export

To display information related to router IP traffic export (RITE), use the **show ip traffic-export**command in privileged EXEC mode.

show ip traffic-export [{**interface** *interface-name* | **profile** *profile-name*}]

Syntax Description

interface *interface-name*	(Optional) Only data associated with the monitored ingress interface is shown.
profile *profile-name*	(Optional) Only flow statistics, such as exported packets and number of bytes, are shown.

Command Default

If this command is enabled, all data (both interface- and profile-related data) is shown.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following sample output from the **show ip traffic-export**command is for the profile "one." This example is for a single configured interface. If multiple interfaces are configured, the information shown below is displayed for each interface.

```
Router# show ip traffic-export
```

Router IP Traffic Export Parameters

Monitored Interface FastEthernet0/0

Export Interface FastEthernet0/1

Destination MAC address 0030.7131.abfc

bi-directional traffic export is off

Input IP Traffic Export Information Packets/Bytes Exported 0/0

Packets Dropped 0

Sampling Rate one-in-every 1 packets

```
        No Access List configured
        Profile one is Active
```

The table below describes the significant fields shown in the display.

Table 111: show ip traffic-export Field Descriptions

Field	Description
Monitored Interface	Interface in which the profile was applied. (This interface is specified via the **ip traffic-export apply profile** command.)
Export Interface	Interface in which the profile exports all captured IP traffic. (This interface is specified via the **ip traffic-export profile** command.)
Destination MAC address	Ethernet address of the destination host, which is specified via the **mac-address** command.
bi-directional traffic export is	Incoming and outgoing IP traffic is exported on the monitored interface (via the **bidirectional** command). By default, only incoming traffic is exported.
Input IP Traffic Export Information Packets Dropped Sampling Rate No Access List Configured Profile one is Active	Incoming IP traffic information. The sampling rate and ACL can be defined via the **incoming** command. If the profile is incomplete, the profile will be listed as inactive.

Related Commands

Command	Description
bidirectional	Enables incoming and outgoing IP traffic to be exported across a monitored interface.
ip traffic-export apply profile	Applies an IP traffic export profile to a specific interface.
ip traffic-export profile	Creates or edits an IP traffic export profile and enables the profile on an ingress interface.
incoming	Configures filtering for incoming export traffic.
outgoing	Configures filtering for outgoing export traffic.

show ip trigger-authentication

To display the list of remote hosts for which automated double authentication has been attempted, use the **show ip trigger-authentication** command in privileged EXEC mode.

show ip trigger-authentication

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3 T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Whenever a remote user needs to be user-authenticated in the second stage of automated double authentication, the local device sends a User Datagram Protocol (UDP) packet to the remote user's host. When the UDP packet is sent, the user's host IP address is added to a table. If additional UDP packets are sent to the same remote host, a new table entry is not created; instead, the existing entry is updated with a new time stamp. This remote host table contains a cumulative list of host entries; entries are deleted after a timeout period or after you manually clear the table using the **clear ip trigger-authentication** command. You can change the timeout period with the **ip trigger-authentication**(global) command.

Use this command to view the list of remote hosts for which automated double authentication has been attempted.

Examples

The following example shows output from the **show ip trigger-authentication** command:

```
Router# show ip trigger-authentication
Trigger-authentication Host Table:
Remote Host          Time Stamp
209.165.200.230       2940514234
```

This output shows that automated double authentication was attempted for a remote user; the remote user's host has the IP address 209.165.200.230. The attempt to automatically double authenticate occurred when the local host (myfirewall) sent the remote host (209.165.200.230) a packet to UDP port 7500. (The default port was not changed in this example.)

Related Commands

Command	Description
clear ip trigger-authentication	Clears the list of remote hosts for which automated double authentication has been attempted.

show ip trm subscription status

To display information about the status of the Trend Micro subscription, use the **show ip trm subscription status**command in privileged EXEC mode.

show ip trm subscription status

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(15)XZ	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use the **show ip trm subscription status**command to display the status of the Trend Micro subscription. If the router is registered with the Trend Router Provisioning Server (TRPS), the router displays the subscription status information. If the router is not registered with the TRPS, a message indicating that the router is not registered is displayed.

Examples

The following shows sample output from **show ip trm subscription status**command when the router is registered with the TRPS:

```
Router# show ip trm subscription status

Package Name: Security & Productivity
 ------------------------------------------------
    Status:     Active
 Status Update Time:     08:55:07 MDT Thu Apr 3 2008
    Expiration-Date:     Tue Jul 21 10:12:59 2020

    Last Req Status:     Processed response successfully
 Last Req Sent Time:     08:55:07 MDT Thu Apr 3 2008
```

The table below describes the significant fields shown in the display.

Table 112: show ip trm subscription status Field Descriptions

Field	Description
Status	Displays the status of the Trend Micro subscription.
Status Update Time	Displays the time and date that status of the Trend Micro subscription was last updated.
Expiration Date	Displays the date and time that the Trend Micro subscription expires.
Last Req Status	Displays the status of the most recent request.
Last Req Sent Time	Displays the time and date of the most recent lookup request to the TRPS.

Related Commands

Command	Description
show ip trm config	Displays information about the TRPS.

show ip urlfilter

To display URL filtering information, use the **show ip urlfilter** command in privileged EXEC mode.

Releases Prior to Cisco IOS Release 15.4(3)M

show ip urlfilter {**mib statistics** {**global** | **server** {**address** *ip-address* [**port** *port-number*] | **all**}} | {**cache** | **config** | **statistics** } | [**vrf** *vrf-name*]}

Cisco IOS Release 15.4(3)M and Later Releases

show ip urlfilter {**mib statistics global** | {**cache** | **config** | **statistics**} | [**vrf** *vrf-name*]}

Syntax Description

mib	Displays the firewall MIB-specific URL filtering content.
statistics	Displays URL filtering statistics for the specified parameters.
global	Displays global URL filtering statistics.
server	Displays statistics for the specified server.
address *ip-address*	Displays URL filtering information for the server with the specified IP address.
port *port-number*	(Optional) Displays statistics for the specified server using the service port.
all	Displays statistics for all configured servers.
vrf *vrf-name*	(Optional) Displays information about a specified virtual routing and forwarding (VRF) instance.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(11)YU	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.3(14)T	This command was modified. The **vrf** keyword and *vrf-name* argument were added.
12.4(6)T	This command was modified. The following keywords and arguments were added: **all**, **address**, **global**, *ip-address*, **mib**, **port**, *port-number*, and **server**.
15.4(3)M	This command was modified. The following keywords and arguments were removed: **server**, **address**, *ip-address*, **port**, *port-number*, **all**.

Usage Guidelines

The firewall interacts with URL filtering to prevent users from accessing specified websites on the basis of configured policies such as destination hostname, destination IP address, keyword, and username. Use the **show ip urlfilter** command to display the URL filtering information such as the number of requests that are sent to the vendor server (Websense or N2H2), the number of responses received from the vendor server, the number of pending requests in the system, the number of failed requests, and the number of blocked URLs.

Examples

The following is sample output from the **show ip urlfilter statistics** command:

```
Device# show ip urlfilter statistics

URL filtering statistics
================
Current requests count:25
Current packet buffer count(in use):40
Current cache entry count:3100
Maxever request count:526
Maxever packet buffer count:120
Maxever cache entry count:5000
Total requests sent to URL Filter Server: 44765
Total responses received from URL Filter Server: 44550
Total requests allowed: 44320
Total requests blocked: 224
```

The table below describes the significant fields shown in the display.

Table 113: show ip urlfilter statistics Field Descriptions

Field	Description
Current requests count	Number of requests sent to the vendor server.
Current packet buffer count (in use)	Number of HTTP responses in the packet buffer of the firewall. This value can be specified by using the **ip urlfilter max-resp-pak** command.
Current cache entry count	Number of destination IP addresses cached into the cache table. This value can be specified by using the **ip urlfilter cache** command.
Maxever request count	Maximum number of requests that are sent to the vendor server since power up. This value can be specified by using the **ip urlfilter max-request** command.
Maxever packet buffer count	Maximum number of HTTP responses stored in the packet buffer of the firewall since power up. This value can be specified by using the **ip urlfilter max-resp-pak** command.
Maxever cache entry count	Maximum number of destination IP addresses that are cached in the cache table since power up. This value can be specified by using the **ip urlfilter cache** command.

The following is sample output from the **show ip urlfilter mib statistics global** command when MIBs are enabled to track URL filtering statistics across the entire device (global). The output fields are self-explanatory.

```
Device# show ip urlfilter mib statistics global
```

```
URL Filtering Group Summary Statistics
------------------------------------------------------
URL Filtering Enabled
Requests Processed 260
Requests Processed 1-minute Rate 240
Requests Processed 5-minute Rate 215
Requests Allowed 230
Requests Denied 30
Requests Denied 1-minute Rate 15
Requests Denied 5-minute Rate 0
Requests Cache Allowed 5
Requests Cache Denied 5
Allow Mode Requests Allowed 15
Allow Mode Requests Denied 15
Requests Resource Dropped 0
Requests Resource Dropped 1-minute Rate 0
Requests Resource Dropped 5-minute Rate 0
Server Timeouts 0
Server Retries 0
Late Server Responses 0
Access Responses Resource Dropped 0
```

The following is sample output from the **show ip urlfilter mib statistics server address** command when MIBs are enabled to track URL filtering statistics across the server with the IP address 209.165.201.30. The output fields are self-explanatory.

```
Device# show ip urlfilter mib statistics server address 209.165.201.30

URL Filtering Server Statistics
------------------------------------------------------
URL Server Host Name 209.165.201.30
Server Address 209.165.201.30
Server Port 15868
Server Vendor Websense
Server Status Online
Requests Processed 4
Requests Allowed 1
Requests Denied 3
Server Timeouts 0
Server Retries 9
Responses Received 1
Late Server Responses 12
1 Minute Average Response Time 0
5 Minute Average Response Time 0
```

Related Commands

Command	Description
ip urlfilter cache	Configures cache parameters.
ip urlfilter max-request	Sets the maximum number of outstanding requests that can exist at any given time.
ip urlfilter max-resp-pak	Configures the maximum number of HTTP responses that the firewall can keep in its packet buffer.

show ip urlfilter cache

To display the maximum number of entries that can be cached and the number of entries and destination IP addresses that are cached into the cache table, use the **show ip urlfilter cache** command in privileged EXEC mode.

show ip urlfilter cache [**vrf** *vrf-name*]

Syntax Description

vrf *vrf-name*	(Optional) Displays information about a specified virtual routing and forwarding (VRF) interface.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(11)YU	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.3(14)T	This command was modified. The **vrf** keyword and *vrf-name* argument were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on the feature set, platform, and platform hardware.

Usage Guidelines

The output from the **show ip urlfilter cache** command displays the number of entries cached by a device.

The IP cache table consists of the most recently requested IP addresses and the respective authorization status for each IP address. Use the **show ip urlfilter cache** command to view the contents of the cache table.

Examples

The following is sample output from the **show ip urlfilter cache** command:

```
Device# show ip urlfilter cache

Maximum number of entries allowed: 5000
Number of entries cached: 5
IP addresses cached ....
 10.64.128.54
 172.28.139.21
 10.76.82.25
 192.168.0.1
 10.0.1.2
```

The following table describes the fields shown in the display.

Table 114: show ip urlfilter cache Field Descriptions

Field	Description
Maximum number of entries allowed	Maximum number of destination IP addresses that can be cached into the cache table. This parameter can be configured using the **ip url filter cache** command. The default is 5000.
Number of entries cached	Number of entries that have already been cached into the cache table.
IP addresses cached	IP addresses that have already been cached into the cache table.

Related Commands

Command	Description
clear ip urlfilter cache	Clears the cache table.
ip urlfilter cache	Configures cache parameters.

show ip urlfilter config

To display the size of the cache, the maximum number of outstanding requests, the allow mode state, and the list of configured vendor servers, use the **show ip urlfilter config**command in EXEC mode.

show ip urlfilter config [**vrf** *vrf-name*]

Syntax Description

vrf *vrf-name*	(Optional) Displays the information only for the specified Virtual Routing and Forwarding (VRF) interface.

Command Modes

EXEC

Command History

Release	Modification
12.2(11)YU	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.3(14)T	The **vrf** *vrf-name*keyword/argument pair was added.

Examples

The following example is sample output from the **show ip urlfilter config** command:

```
Router# show ip urlfilter config
URL filter is ENABLED
Primary Websense server configurations
==========================
Websense server IP address: 10.0.0.3
Websense server port: 15868
Websense retransmit time out: 5 (seconds)
Websense number of retransmit:2
Secondary Websense server configurations:
============================
None.
Other configurations
===============
Allow mode: OFF
System Alert: ON
Log message on the router: OFF
Log message on URL filter server:ON
Maximum number of cache entries :5000
Cache timeout :12 (hours)
Maximum number of packet buffers:200
Maximum outstanding requests:1000
```

Related Commands

Command	Description
ip urlfilter allowmode	Turns on the default mode (allow mode) of the filtering algorithm.
ip urlfilter cache	Configures cache parameters.

Command	Description
ip urlfilter max-request	Sets the maximum number of outstanding requests that can exist at any given time.
ip urlfilter server vendor	Configures a vendor server for URL filtering.

show ip virtual-reassembly

To display the configuration and statistical information of the virtual fragment reassembly (VFR) on a given interface, use the **show ip virtual-reassembly** command in privileged EXEC mode.

show ip virtual-reassembly [**interface** *type*]

Syntax Description

interface *type*	(Optional) VFR information is shown only for the specified interface. If an interface is not specified, VFR information for all configured interfaces is shown.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(8)T	This command was introduced.

Examples

The following example is sample output from the **show ip virtual-reassembly** command:

```
Router# show ip virtual-reassembly interface ethernet1/1
Ethernet1/1:
Virtual Fragment Reassembly (VFR) is ENABLED...
Concurrent reassemblies (max-reassemblies):64
Fragments per reassembly (max-fragments):16
Reassembly timeout (timeout):3 seconds
Drop fragments:OFF
Current reassembly count:12
Current fragment count:48
Total reassembly count:6950
Total reassembly failures:9
```

The table below describes the significant fields shown in the display.

Table 115: show ip virtual-reassembly Field Descriptions

Field	Description
Concurrent reassemblies (max-reassemblies):64	Maximum number of IP datagrams that can be reassembled at any given time. Value can be specified via the **max-reassemblies** *number*option from the **ip virtual-reassembly** command.
Fragments per reassembly (max-fragments):16	Maximum number of fragments that are allowed per IP datagram (fragment set). Value can be specified via the **max-fragments** *number* option from the **ip virtual-reassembly** command.
Reassembly timeout (timeout):3 seconds	Timeout value for an IP datagram that is being reassembled. Value can be specified via the **timeout** *seconds* option from the **ip virtual-reassembly** command.

Field	Description
Drop fragments:OFF	Specifies whether the VFR should drop all fragments that arrive on the configured interface. Function can be turned on or off via the **drop-fragments** keyword from the **ip virtual-reassembly** command.
Current reassembly count	Number of IP datagrams that are currently being reassembled
Current fragment count	Number of fragments that have been buffered by VFR for reassembly
Total reassembly count	Total number of datagrams that have been reassembled since the last system reboot.
Total reassembly failures	Total number of reassembly failures since the last system reboot.

Related Commands

Command	Description
ip virtual-reassembly	Enables VFR on an interface.

show ipv6 access-list

To display the contents of all current IPv6 access lists, use the **show ipv6 access-list**command in user EXEC or privileged EXEC mode.

show ipv6 access-list [*access-list-name*]

Syntax Description

access-list-name	(Optional) Name of access list.

Command Default

All IPv6 access lists are displayed.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.0(23)S	The priority field was changed to sequence and Layer 4 protocol information (extended IPv6 access list functionality) was added to the display output.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(50)SY	This command was modified. Information about IPv4 and IPv6 hardware statistics is displayed.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The **show ipv6 access-list** command provides output similar to the **show ip access-list** command, except that it is IPv6-specific.

Examples

The following output from the **show ipv6 access-list**command shows IPv6 access lists named inbound, tcptraffic, and outbound:

```
Router# show ipv6 access-list
IPv6 access list inbound
    permit tcp any any eq bgp reflect tcptraffic (8 matches) sequence 10
    permit tcp any any eq telnet reflect tcptraffic (15 matches) sequence 20
    permit udp any any reflect udptraffic sequence 30
IPv6 access list tcptraffic (reflexive) (per-user)
    permit tcp host 2001:0DB8:1::1 eq bgp host 2001:0DB8:1::2 eq 11000 timeout 300 (time
       left 243) sequence 1
    permit tcp host 2001:0DB8:1::1 eq telnet host 2001:0DB8:1::2 eq 11001 timeout 300
    (time left 296) sequence 2
IPv6 access list outbound
    evaluate udptraffic
    evaluate tcptraffic
```

The following sample output shows IPv6 access list information for use with IPSec:

```
Router#  show ipv6 access-list
IPv6 access list Tunnel0-head-0-ACL (crypto)
     permit ipv6 any any (34 matches) sequence 1
IPv6 access list Ethernet2/0-ipsecv6-ACL (crypto)
     permit 89 FE80::/10 any (85 matches) sequence 1
```

The table below describes the significant fields shown in the display.

Table 116: show ipv6 access-list Field Descriptions

Field	Description
ipv6 access list inbound	Name of the IPv6 access list, for example, inbound.
permit	Permits any packet that matches the specified protocol type.
tcp	Transmission Control Protocol. The higher-level (Layer 4) protocol type that the packet must match.
any	Equal to ::/0.
eq	An equal operand that compares the source or destination ports of TCP or UDP packets.
bgp	Border Gateway Protocol. The lower-level (Layer 3) protocol type that the packet must be equal to.
reflect	Indicates a reflexive IPv6 access list.
tcptraffic (8 matches)	The name of the reflexive IPv6 access list and the number of matches for the access list. The **clear ipv6 access-list** privileged EXEC command resets the IPv6 access list match counters.
sequence 10	Sequence in which an incoming packet is compared to lines in an access list. Lines in an access list are ordered from first priority (lowest number, for example, 10) to last priority (highest number, for example, 80).
host 2001:0DB8:1::1	The source IPv6 host address that the source address of the packet must match.
host 2001:0DB8:1::2	The destination IPv6 host address that the destination address of the packet must match.

Field	Description
11000	The ephemeral source port number for the outgoing connection.
timeout 300	The total interval of idle time (in seconds) after which the temporary IPv6 reflexive access list named tcptraffic will time out for the indicated session.
(time left 243)	The amount of idle time (in seconds) remaining before the temporary IPv6 reflexive access list named tcptraffic is deleted for the indicated session. Additional received traffic that matches the indicated session resets this value to 300 seconds.
evaluate udptraffic	Indicates the IPv6 reflexive access list named udptraffic is nested in the IPv6 access list named outbound.

Related Commands

Command	Description
clear ipv6 access-list	Resets the IPv6 access list match counters.
hardware statistics	Enables the collection of hardware statistics.
show ip access-list	Displays the contents of all current IP access lists.
show ip prefix-list	Displays information about a prefix list or prefix list entries.
show ipv6 prefix-list	Displays information about an IPv6 prefix list or IPv6 prefix list entries.

show ipv6 cga address-db

To display IPv6 cryptographically generated addresses (CGA) from the address database, use the **show ipv6 cga address-db** command in privileged EXEC mode.

show ipv6 cga address-db

Syntax Description

This command has no arguments or keywords.

Command Default

No CGAs are displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(24)T	This command was introduced.

Examples

The following example displays CGAs in the CGA database:

```
Router# show ipv6 cga address-db
2001:0DB8:/64 ::2011:B680:DEF4:A550 - table 0x0
        interface:      Ethernet0/0 (3)
        modifier:       SEND1024e
FE80::/64 ::3824:3CE4:C044:8D65 - table 0x12000003
        interface:      Ethernet0/0 (3)
        modifier:       SEND1024e
```

The table below describes the significant fields shown in the display.

Table 117: show ipv6 cga address-db Field Descriptions

Field	Description
2001:0DB8:/64 ::2011:B680:DEF4:A550 - table 0x0	CGA address for which information is shown.
interface:	Interface on which the address is configured.
modifier:	The CGA modifier.

Related Commands

Command	Description
show ipv6 cga modifier-db	Displays IPv6 CGA modifiers.
show ipv6 nd secured certificates	Displays active SeND certificates.
show ipv6 nd secured counters interface	Displays SeND counters on an interface.
show ipv6 nd secured nonce-db	Displays active SeND nonce entries.
show ipv6 nd secured timestamp-db	Displays active SeND time-stamp entries.

show ipv6 cga modifier-db

To display IPv6 cryptographically generated address (CGA) modifier database entries, use the **show ipv6 cga modifier-db** command in privileged EXEC mode.

show ipv6 cga modifier-db

Syntax Description

This command has no arguments or keywords.

Command Default

No CGA modifiers are displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(24)T	This command was introduced.

Usage Guidelines

The **show ipv6 cga modifier-db** command is used to display the modifiers generated with the **ipv6 cga modifier** command and the addresses generated from them.

Examples

The following example displays CGA modifiers in the CGA modifier database:

```
Router# show ipv6 cga modifier-db
F046:E042:13E8:1661:96E5:DD05:94A8:FADC
        label:          SubCA11
        sec level:      1
        Addresses:
  2001:100::38C9:4A1A:2972:794E
  FE80::289C:3308:4719:87F2
```

The table below describes the significant fields shown in the display.

.

Table 118: show ipv6 cga modifier-db Field Descriptions

Field	Description
D695:5D75:F9B5:9715:DF0A:D840:70A2:84B8	The CGA modifier for which the information is displayed.
label	Name used for the Rivest, Shamir, and Adelman (RSA) key pair.
Addresses: 2001:100::38C9:4A1A:2972:794EFE80::289C:3308:4719:87F2	The CGA address.

Related Commands

Command	Description
ipv6 cga modifier	Generates an IPv6 CGA modifier for a specified RSA key pair.
show ipv6 cga address-db	Displays IPv6 CGAs.
show ipv6 nd secured certificates	Displays active SeND certificates.
show ipv6 nd secured counters interface	Displays SeND counters on an interface.
show ipv6 nd secured nonce-db	Displays active SeND nonce entries.
show ipv6 nd secured timestamp-db	Displays active SeND time-stamp entries.

show ipv6 inspect

To view Context-based Access Control (CBAC) configuration and session information, use the show ipv6 inspect command in privileged EXEC mode.

show ipv6 inspect {**name** *inspection-name* | **config** | **interfaces** | **session** [**detail**] | **all**}

Syntax Description

name *inspection-name*	Displays the configured inspection rule with the name inspection-name.
config	Displays the complete Cisco IOS firewall inspection configuration.
interfaces	Displays interface configuration with respect to applied inspection rules and access lists.
session [**detail**	Displays existing sessions that are currently being tracked and inspected by Cisco IOS firewall. The optional detail keyword causes additional details about these sessions to be shown.
all	Displays all Cisco IOS firewall configuration and all existing sessions that are currently being tracked and inspected by Cisco IOS firewall.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(7)T	This command was introduced.

Examples

The following example asks for information about interfaces currently under inspection:

```
Router# show ipv6 inspect
 interfaces
```

Related Commands

Command	Description
ipv6 inspect	Applies a set of inspection rules to an interface.

show ipv6 nd raguard counters

To display information about RA guard counters, use the **show ipv6 nd raguard policy**command in privileged EXEC mode.

show ipv6 nd raguard counters [**interface** *type number*]

Syntax Description

interface *type number*	(Optional) Displays RA guard policy information for the specified interface type and number.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(5th)SXI	This command was introduced.

Usage Guidelines

The **show ipv6 nd raguard counters** command displays information about RA guard counters, such as packets sent, packets received, and packets droped. This command also provides information on why a packet was dropped.

show ipv6 nd raguard policy

To display a router advertisements (RAs) guard policy on all interfaces configured with the RA guard feature, use the **show ipv6 nd raguard policy** command in privileged EXEC mode.

show ipv6 nd raguard policy [*policy-name*]

Syntax Description

policy-name	(Optional) RA guard policy name.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(50)SY	This command was introduced.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The **show ipv6 nd raguard policy** command displays the options configured for the policy on all interfaces configured with the RA guard feature.

Examples

The following example shows the policy configuration for a policy named raguard1 and all the interfaces where the policy is applied:

```
Router# show ipv6 nd raguard policy interface raguard1

Policy raguard1 configuration:
  device-role host
Policy applied on the following interfaces:
  Et0/0        vlan all
  Et1/0        vlan all
```

The table below describes the significant fields shown in the display.

Table 119: show ipv6 nd raguard policy Field Descriptions

Field	Description
Policy raguard1 configuration:	Configuration of the specified policy.
device-role host	The role of the device attached to the port. This device configuration is that of host.
Policy applied on the following interfaces:	The specified interface on which the RA guard feature is configured.

show ipv6 nd secured certificates

To display active IPv6 Secure Neighbor Discovery (SeND) certificates, use the **show ipv6 nd secured certificates**command in privileged EXEC mode.

show ipv6 nd secured certificates

Syntax Description

This command has no arguments or keywords.

Command Default

No SeND certificates are displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(24)T	This command was introduced.

Usage Guidelines

The **show ipv6 nd secured certificates** command is used on hosts (routers configured in host mode) to display the certifcates received over SeND (via Certificate Path Advertisement) and their state.

Examples

The following example displays active SeND certificates:

```
Router# show ipv6 nd secured certificates
Total number of entries: 1 / 32
Hash                             id         RA  certcnt certrcv state
DC0102E09FAF422D49ED79A846D2EBC1 0x00000778 no  1       1       CERT_VALIDATED
certificate No 0
subject  hostname=sa14-72a,c=FR,st=fr,l=example,o=cisco,ou=nsstg,cn=72a
```

issuer c=FR,st=fr,l=example,o=cisco,ou=nsstg,cn=CA0

The table below describes the significant fields shown in the display.

Table 120: show ipv6 nd secured certificates Field Descriptions

Field	Description
certcnt	Number of certificate for this chain.
certrcv	Number of certifciate received in the chain.
Hash	Key hash.
id	Numero of the certifciate.
RA	Displays Yes if an RA is pending for this certifciate.
state	Current state of the certificate.

Related Commands

Command	Description
show ipv6 cga modifier-db	Displays IPv6 CGA modifiers.
show ipv6 cga address-db	Displays IPv6 CGAs.
show ipv6 nd secured counters interface	Displays SeND counters on an interface.
show ipv6 nd secured nonce-db	Displays active SeND nonce entries.
show ipv6 nd secured timestamp-db	Displays active SeND time-stamp entries.

show ipv6 nd secured counters interface

To display IPv6 Secure Neighbor Discovery (SeND) counters on an interface, use the **show ipv6 nd secured counters interface**command in privileged EXEC mode.

show ipv6 nd secured counters interface *interface*

Syntax Description

interface	(Optional) Specifies the interface on which SeND counters are located.

Command Default

No SeND counter information is displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(24)T	This command was introduced.

Examples

The following example displays SeND counters:

```
Router# show ipv6 nd secured counters interface ethernet0/0
e0/0 Received ND messages on Ethernet0/0:
rcvd    accept  SLLA    TLLA    PREFIX  MTU     CGA     RSA     TS      NONCE   TA CERT
RA      66      65      63      0       62      63      63      63      63      0       0
      0
NS      8       8       8       0       0       0       8       8       8       8       0
      0
NA      20      20      0       8       0       0       19      19      19      14      0
      0
CPA     1       1       0       0       0       0       0       0       0       0       1
      1
Dropped ND messages on Ethernet0/0:
Codes   TIMEOUT: Timed out while waiting for rsp
        drop    TIMEOUT
RA      1       1
Sent ND messages on Ethernet0/0:
sent    aborted SLLA    CGA     RSA     TS      NONCE   TA
NS      14      0       14      14      14      14      14      0
NA      8       0       0       8       8       8       8       0
CPS     43      0       0       0       0       0       0       43
Router#
```

The table below describes the significant fields shown in the display.

Table 121: show ipv6 nd secured counters interface Field Descriptions

Field	Description
accept	Number of neighbor discovery (ND) messages accepted (messages that are not dropped).
CERT	Number of messages received with the certificate option.
CGA	Number of messages received with the CGA option.

Field	Description
MTU	Number of messages received with the MTU option.
NA	Number of NDP neighbor advertisements
NONCE	Number of messages received with the NONCE option.
NS	Number of NDP neighbor solicitions.
PREFIX	Number of messages received with the PREFIX option.
rcvd	Number of ND messages received on the interface.
RA	Number of router advertisements.
REDIR	Number of NDP redirect messages.
RS	Router Solicit.
RSA	Number of messages received with the RSA option.
SLLA	Number of messages received with the ND SLLA option.
TA	Number of messages received with the trust anchor option.
TS	Number of messages received with the time stamp option.

Related Commands

Command	Description
show ipv6 cga address-db	Displays IPv6 CGAs.
show ipv6 cga modifier-db	Displays IPv6 CGA modifiers.
show ipv6 nd secured certificates	Displays active SeND certificates.
show ipv6 nd secured nonce-db	Displays active SeND nonce entries.
show ipv6 nd secured timestamp-db	Displays active SeND timestamp entries.

show ipv6 nd secured nonce-db

To display active IPv6 Secure Neighbor Discovery (SeND) nonce database entries, use the **show ipv6 nd secured nonce-db**command in privileged EXEC mode.

show ipv6 nd secured nonce-db

Syntax Description

This command has no arguments or keywords.

Command Default

No SeND nonce information is displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(24)T	This command was introduced.

Usage Guidelines

The **show ipv6 nd secured nonce-db**command is used to display the pending solicitations. There are rarely any pending solicitations because the solicitations are quickly answered and removed from the database.

Examples

The following example displays active SeND nonce entries. The output is self-explanatory.

```
Router# show ipv6 nd secured nonce-db
Total number of entries: 0
```

Related Commands

Command	Description
show ipv6 cga address-db	Displays IPv6 CGAs.
show ipv6 cga modifier-db	Displays IPv6 CGA modifiers.
show ipv6 nd secured certificates	Displays active SeND certificates.
show ipv6 nd secured counters interface	Displays SeND counters on an interface.
show ipv6 nd secured timestamp-db	Displays active SeND time stamp entries.

show ipv6 nd secured solicit-db

To display pending SEcure Neighbor Discovery (SEND) solicitations from peers, use the **show ipv6 nd secured solicit-db**command in privileged EXEC configuration mode.

show ipv6 nd secured solicit-db

Syntax Description

This command has no arguments or keywords.

Command Default

No pending SEND solicitation information is displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(24)T	This command was introduced.

Usage Guidelines

Use this command to display pending SEND solicitations.

Examples

The following example displays pending SEcure Neighbor Discovery (SEND) solicitations from peers:

```
Router# show ipv6 nd secured solicit-db
```

show ipv6 nd secured timestamp-db

To display active Secure Neighbor Discovery (SeND) time-stamp database entries, use the **show ipv6 nd secured timestamp-db**command in privileged EXEC mode.

show ipv6 nd secured timestamp-db

Syntax Description

This command has no arguments or keywords.

Command Default

No pending SeND solicitation information is displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(24)T	This command was introduced.

Usage Guidelines

The **show ipv6 nd secured timestamp-db** command displays the content of the time-stamp databse, which contains last received messages from peers. It also displays the delta and fuzz values.

Examples

The following example displays active SeND time-stamp database entries:

```
Router# show ipv6 nd secured timestamp-db
Total number of entries: 6 Number of unreached peer entries: 3 / 1024
FE80::289C:3308:4719:87F2 on Ethernet0/0, delta 300s, fuzz 1000ms
        Time to expire: 3h 41m 16s (reached)
        TSlast: 0x4936B97655FF = Wed Dec  3 16:53:10 2008
        RDlast: 0x4936B976438B = Wed Dec  3 16:53:10 2008
FE80::2441:88D1:22FC:3B77 on Ethernet0/0, delta 300s, fuzz 1000ms
        Time to expire: 3h 59m 53s (reached)
        TSlast: 0x4936BDD2E13E = Wed Dec  3 17:11:46 2008
        RDlast: 0x4936BDD2D0D6 = Wed Dec  3 17:11:46 2008
FE80::E2:F012:6F72:9E45 on Ethernet0/0, delta 300s, fuzz 1000ms
        Time to expire: 3h 4m 18s (unreached)
        TSlast: 0x4936B0CBB333 = Wed Dec  3 16:16:11 2008
        RDlast: 0x4936B0CBBD70 = Wed Dec  3 16:16:11 2008 2001:100::38C9:4A1A:2972:794E on
 Ethernet0/0, delta 300s, fuzz 1000ms
        Time to expire: 3h 4m 19s (unreached)
        TSlast: 0x4936BA254FDA = Wed Dec  3 16:56:05 2008
        RDlast: 0x4936BA253F72 = Wed Dec  3 16:56:05 2008 2001:100::383E:6BD5:397:4A50 on
Ethernet0/0, delta 300s, fuzz 1000ms
        Time to expire: 3h 45m 0s (reached)
        TSlast: 0x4936BA55F2AA = Wed Dec  3 16:56:53 2008
        RDlast: 0x4936BA55E036 = Wed Dec  3 16:56:53 2008
2001:100::434:E62D:327D:B1E6 on Ethernet0/0, delta 300s, fuzz 1000ms
        Time to expire: 3h 4m 42s (unreached)
        TSlast: 0x4936B0E422D0 = Wed Dec  3 16:16:36 2008
        RDlast: 0x4936B0E42D0E = Wed Dec  3 16:16:36 2008
```

The table below describes the significant fields shown in the display.

Table 122: show ipv6 nd secured timestamp-db Field Descriptions

Field	Description
Total number of entries	Number of entries (peers) in the cache.
Time to expire	Remaining time before entry expires.
TSlast	Last peer timestamp value.
RDlast	Time when the last message was received from the peer.

Related Commands

Command	Description
show ipv6 cga address-db	Displays IPv6 CGAs.
show ipv6 cga modifier-db	Displays IPv6 CGA modifiers.
show ipv6 nd secured certificates	Displays active SeND certificates.
show ipv6 nd secured counters interface	Displays SeND counters on an interface.
show ipv6 nd secured nonce-db	Displays active SeND nonce entries.

show ipv6 nhrp

To display Next Hop Resolution Protocol (NHRP) mapping information, use the **show ipv6 nhrp** command in user EXEC or privileged EXEC mode.

show ipv6 nhrp [{**dynamic** [*ipv6-address*] | **incomplete** | **static**}] [{**address** | **interface**}] [{**brief** | **detail**}] [**purge**]

Syntax Description

dynamic	(Optional) Displays dynamic (learned) IPv6-to-nonbroadcast multiaccess address (NBMA) mapping entries. Dynamic NHRP mapping entries are obtained from NHRP resolution/registration exchanges. See the table below for types, number ranges, and descriptions.
ipv6-address	(Optional) The IPv6 address of the cache entry.
incomplete	(Optional) Displays information about NHRP mapping entries for which the IPv6-to-NBMA is not resolved. See the table below for types, number ranges, and descriptions.
static	(Optional) Displays static IPv6-to-NBMA address mapping entries. Static NHRP mapping entries are configured using the **ipv6 nhrp map** command. See the table below for types, number ranges, and descriptions.
address	(Optional) NHRP mapping entry for specified protocol addresses.
interface	(Optional) NHRP mapping entry for the specified interface. See the table below for types, number ranges, and descriptions.
brief	(Optional) Displays a short output of the NHRP mapping.
detail	(Optional) Displays detailed information about NHRP mapping.
purge	(Optional) Displays NHRP purge information.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

The table below lists the valid types, number ranges, and descriptions for the optional *interface* argument.

Note The valid types can vary according to the platform and interfaces on the platform.

Table 123: Valid Types, Number Ranges, and Interface Description

Valid Types	Number Ranges	Interface Descriptions
async	1	Async
atm	0 to 6	ATM
bvi	1 to 255	Bridge-Group Virtual Interface
cdma-ix	1	CDMA Ix
ctunnel	0 to 2147483647	C-Tunnel
dialer	0 to 20049	Dialer
ethernet	0 to 4294967295	Ethernet
fastethernet	0 to 6	FastEthernet IEEE 802.3
lex	0 to 2147483647	Lex
loopback	0 to 2147483647	Loopback
mfr	0 to 2147483647	Multilink Frame Relay bundle
multilink	0 to 2147483647	Multilink-group
null	0	Null
port-channel	1 to 64	Port channel
tunnel	0 to 2147483647	Tunnel
vif	1	PGM multicast host
virtual-ppp	0 to 2147483647	Virtual PPP
virtual-template	1 to 1000	Virtual template
virtual-tokenring	0 to 2147483647	Virtual Token Ring
xtagatm	0 to 2147483647	Extended tag ATM

Examples

The following is sample output from the **show ipv6 nhrp** command:

```
Router# show ipv6 nhrp
2001:0db8:3c4d:0015::1a2f:3d2c/48  via
2001:0db8:3c4d:0015::1a2f:3d2c
Tunnel0 created 6d05h, never expire
```

The table below describes the significant fields shown in the display.

Table 124: show ipv6 nhrp Field Descriptions

Field	Description
2001:0db8:3c4d:0015::1a2f: 3d2c/48	Target network.
2001:0db8:3c4d:0015::1a2f:3d2c	Next hop to reach the target network.
Tunnel0	Interface through which the target network is reached.
created 6d05h	Length of time since the entry was created (dayshours).
never expire	Indicates that static entries never expire.

The following is sample output from the **show ipv6 nhrp**command using the **brief** keyword:

```
Router# show ipv6 nhrp brief
2001:0db8:3c4d:0015:0000:0000:1a2f:3d2c/48
 via 2001:0db8:3c4d:0015:0000:0000:1a2f:3d2c
Interface: Tunnel0 Type: static
NBMA address: 10.11.11.99
```

The table below describes the significant fields shown in the display.

Table 125: show ipv6 nhrp brief Field Descriptions

Field	Description
2001:0db8:3c4d:0015:0000:0000: 1a2f:3d2c/48	Target network.
via 2001:0db8:3c4d:0015:0000:0000: 1a2f:3d2c	Next Hop to reach the target network.
Interface: Tunnel0	Interface through which the target network is reached.
Type: static	Type of tunnel. The types can be one of the following: • dynamic--NHRP mapping is obtained dynamically. The mapping entry is created using information from the NHRP resolution and registrations. • static--NHRP mapping is configured statically. Entries configured by the **ipv6 nhrp map** command are marked static. • incomplete--The NBMA address is not known for the target network.

Related Commands

Command	Description
ipv6 nhrp map	Statically configures the IPv6-to-NBMA address mapping of IP destinations connected to an NBMA network.

show ipv6 port-map

To verify port-to-application mapping (PAM) configuration, use the **show ipv6 port-map**command in user EXEC or privileged EXEC mode.

show ipv6 port-map [{*application* | **port** *port-number*}]

Syntax Description

application	(Optional) Specifies the name of the application used in port mapping.
port *port-number*	(Optional) Specifies the port number that maps to the application.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(11)T	This command was introduced.

Usage Guidelines

The **show ipv6 port-map** command displays the entire IPv6 port-mapping table or specific port-mapping information of a particular port number or application (protocol). Enabling the **show ipv6 port-map** command displays the entire IPv6 PAM table, including system-defined, user-defined, and host-specific port-mapping configurations.

To display port-mapping details of a specific port number, use the **show ipv6 port-map** command with the **port***port-number* keyword and argument.

To display the port-mapping details of a specific application, use the **show ipv6 port-map** command with the *application* argument.

Examples

The following example displays the FTP application's PAM information:

```
Router# show ipv6 port-map ftp
```

The following example displays PAM information at port number 21:

```
Router# show ipv6 port-map port 21
```

Related Commands

Command	Description
ipv6 port-map	Establishes PAM for the system.

show ipv6 prefix-list

To display information about an IPv6 prefix list or IPv6 prefix list entries, use the **show ipv6 prefix-list**command in user EXEC or privileged EXEC mode.

show ipv6 prefix-list [{**detail** | **summary**}] [*list-name*]
show ipv6 prefix-list *list-name ipv6-prefix/prefix-length* [{**longer** | **first-match**}]
show ipv6 prefix-list *list-name* **seq** *seq-num*

Syntax Description

detail | **summary**	(Optional) Displays detailed or summarized information about all IPv6 prefix lists.
list-name	(Optional) The name of a specific IPv6 prefix list.
ipv6-prefix	All prefix list entries for the specified IPv6 network. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
/ *prefix-length*	The length of the IPv6 prefix. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.
longer	(Optional) Displays all entries of an IPv6 prefix list that are more specific than the given *ipv6-prefix* / *prefix-length*values.
first-match	(Optional) Displays the entry of an IPv6 prefix list that matches the given *ipv6-prefix* / *prefix-length*values.
seq *seq-num*	The sequence number of the IPv6 prefix list entry.

Command Default

Displays information about all IPv6 prefix lists.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The **show ipv6 prefix-list** command provides output similar to the **show ip prefix-list** command, except that it is IPv6-specific.

Examples

The following example shows the output of the **show ipv6 prefix-list** command with the **detail** keyword:

```
Router# show ipv6 prefix-list detail
Prefix-list with the last deletion/insertion: bgp-in
ipv6 prefix-list 6to4:
   count: 1, range entries: 0, sequences: 5 - 5, refcount: 2
   seq 5 permit 2002::/16 (hit count: 313, refcount: 1)
ipv6 prefix-list aggregate:
   count: 2, range entries: 2, sequences: 5 - 10, refcount: 30
   seq 5 deny 3FFE:C00::/24 ge 25 (hit count: 568, refcount: 1)
   seq 10 permit ::/0 le 48 (hit count: 31310, refcount: 1)
ipv6 prefix-list bgp-in:
   count: 6, range entries: 3, sequences: 5 - 30, refcount: 31
   seq 5 deny 5F00::/8 le 128 (hit count: 0, refcount: 1)
   seq 10 deny ::/0 (hit count: 0, refcount: 1)
   seq 15 deny ::/1 (hit count: 0, refcount: 1)
   seq 20 deny ::/2 (hit count: 0, refcount: 1)
   seq 25 deny ::/3 ge 4 (hit count: 0, refcount: 1)
   seq 30 permit ::/0 le 128 (hit count: 240664, refcount: 0)
```

The table below describes the significant fields shown in the display.

Table 126: show ipv6 prefix-list Field Descriptions

Field	Description
Prefix list with the latest deletion/insertion:	Prefix list that was last modified.
count	Number of entries in the list.
range entries	Number of entries with matching range.
sequences	Sequence number for the prefix entry.
refcount	Number of objects currently using this prefix list.
seq	Entry number in the list.
permit, deny	Granting status.
hit count	Number of matches for the prefix entry.

The following example shows the output of the **show ipv6 prefix-list** command with the **summary**keyword:

```
Router# show ipv6 prefix-list summary
Prefix-list with the last deletion/insertion: bgp-in
ipv6 prefix-list 6to4:
```

```
   count: 1, range entries: 0, sequences: 5 - 5, refcount: 2
ipv6 prefix-list aggregate:
   count: 2, range entries: 2, sequences: 5 - 10, refcount: 30
ipv6 prefix-list bgp-in:
   count: 6, range entries: 3, sequences: 5 - 30, refcount: 31
```

Related Commands

Command	Description
clear ipv6 prefix-list	Resets the hit count of the prefix list entries.
distribute-list in	Filters networks received in updates.
distribute-list out	Suppresses networks from being advertised in updates.
ipv6 prefix-list	Creates an entry in an IPv6 prefix list.
ipv6 prefix-list description	Adds a text description of an IPv6 prefix list.
match ipv6 address	Distributes IPv6 routes that have a prefix permitted by a prefix list.
neighbor prefix-list	Distributes BGP neighbor information as specified in a prefix list.
remark (prefix-list)	Adds a comment for an entry in a prefix list.

show ipv6 snooping capture-policy

To display message capture policies, use the **show ipv6 snooping capture-policy** command in user EXEC or privileged EXEC mode.

show ipv6 snooping capture-policy [**interface** *type number*]

Syntax Description

interface *type number*	(Optional) Displays first-hop message types on the specified interface type and number.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
12.2(50)SY	This command was introduced.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The **show ipv6 snooping capture-policy** command displays IPv6 first-hop message capture policies.

Examples

The following example shows **show ipv6 snooping capture-policy** command output on the Ethernet 0/0 interface, on which the IPv6 Neighbor Discovery Protocol (NDP) Inspection and Router Advertisement (RA) Guard features are configured:

```
Router# show ipv6 snooping capture-policy

Hardware policy registered on Et0/0
Protocol  Protocol value  Message  Value  Action  Feature
ICMP      58              RS       85     punt    RA Guard
                                          punt    ND Inspection
ICMP      58              RA       86     drop    RA guard
                                          punt    ND Inspection
ICMP      58              NS       87     punt    ND Inspection
ICMP      58              NA       88     punt    ND Inspection
ICMP      58              REDIR    89     drop    RA Guard
                                          punt    ND Inspection
```

The table below describes the significant fields shown in the display.

Table 127: show ipv6 snooping capture-policy Field Descriptions

Field	Description
Hardware policy registered on Fa4/11	A hardware policy contains a programmatic access list (ACL), with a list of access control entries (ACEs).
Protocol	The protocol whose packets are being inspected.
Message	The type of message being inspected.
Action	Action to be taken on the packet.
Feature	The inspection feature for this information.

show ipv6 snooping counters

To display information about the packets counted by the interface counter, use the **show ipv6 snooping counters**command in user EXEC or privileged EXEC mode.

show ipv6 snooping counters {**interface** *type number* | **vlan** *vlan-id*}

Syntax Description

interface *type number*	Displays first-hop packets that match the specified interface type and number.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
12.2(50)SY	This command was introduced.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The **show ipv6 snooping counters** command displays packets handled by the switch that are being counted in interface counters. The switch counts packets captured per interface and records whether the packet was received, sent, or dropped. If a packet is dropped, the reason for the drop and the feature that caused the drop are both also provided.

Examples

The following examples shows information about packets counted on Fast Ethernet interface 4/12:

```
Router# show ipv6 snooping counters interface Fa4/12
Received messages on Fa4/12:
Protocol        Protocol message
ICMPv6          RS      RA      NS      NA      REDIR   CPS     CPA
                0       4256    0       0       0       0       0
Bridged messages from Fa4/12:
Protocol        Protocol message
ICMPv6          RS      RA      NS      NA      REDIR   CPS     CPA
                0       4240    0       0       0       0       0
Dropped messages on Fa4/12:
Feature/Message RS      RA      NS      NA      REDIR   CPS     CPA
RA guard        0       16      0       0       0       0       0
Dropped reasons on Fa4/12:
RA guard         16   RA drop - reason:RA/REDIR received on un-authorized port
```

The table below describes the significant fields shown in the display.

Table 128: show ipv6 snooping counters Field Descriptions

Field	Description
Received messages on:	The messages received on an interface.
Protocol	The protocol for which messages are being counted.
Protocol message	The type of protocol messages being counted.
Bridged messages from:	Bridged messages from the interface.
Dropped messages on:	The messages dropped on the interface.
Feature/message	The feature that caused the drop, and the type and number of messages dropped.
RA drop - reason:	The reason that these messages were dropped.

show ipv6 snooping features

To display information about about snooping features configured on the router, use the **show ipv6 snooping features** command in user EXEC or privileged EXEC mode.

show ipv6 snooping features

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
12.2(50)SY	This command was introduced.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S.

Usage Guidelines

The **show ipv6 snooping features** command displays the first-hop features that are configured on the router.

Examples

The following example shows that both IPv6 NDP inspection and IPv6 RA guard are configured on the router:

```
Router# show ipv6 snooping features

Feature name   priority state
RA guard          100   READY
NDP inspection     20   READY
```

The table below describes the significant fields shown in the display.

Table 129: show ipv6 snooping features Field Descriptions

Field	Description
Feature name	The names of the IPv6 global policy features configured on the router.
priority	The priority of the specified feature.
state	The state of the specified feature.

show ipv6 snooping policies

To display information about the configured policies and the interfaces to which they are attached, use the **show ipv6 snooping policies** command in user EXEC or privileged EXEC mode.

show ipv6 snooping policies {**interface** *type number* | **vlan** *vlan-id*}

Syntax Description

interface *type number*	Displays policies that match the specified interface type and number.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
12.2(50)SY	This command was introduced.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.

Usage Guidelines

The **show ipv6 snooping policies** command displays all policies that are configured and lists the interfaces to which they are attached.

Examples

The following example shows information about all policies configured:

```
Device# show ipv6 snooping policies

NDP inspection policies configured:
Policy      Interface    Vlan
------      ---------    ----
trusted      Et0/0        all
             Et1/0        all
untrusted    Et2/0        all
RA guard policies configured:
Policy      Interface    Vlan
------      ---------    ----
host         Et0/0        all
             Et1/0        all
router       Et2/0        all
```

The table below describes the significant fields shown in the display.

Table 130: show ipv6 snooping policies Field Descriptions

Field	Description
NDP inspection policies configured:	Description of the policies configured for a specific feature.
Policy	Whether the policy is trusted or untrusted.
Interface	The interface to which a policy is attached.

show ipv6 spd

To display the IPv6 Selective Packet Discard (SPD) configuration, use the **show ipv6 spd**command in privileged EXEC mode.

show ipv6 spd

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.
15.1(3)T	This command was integrated into Cisco IOS Release 15.1(3)T.

Usage Guidelines

Use the **show ipv6 spd** command to display the SPD configuration, which may provide useful troubleshooting information.

Examples

The following is sample output from the **show ipv6 spd** command:

```
Router# show ipv6 spd
Current mode: normal
Queue max threshold: 74, Headroom: 100, Extended Headroom: 10
IPv6 packet queue: 0
```

The table below describes the significant fields shown in the display.

Table 131: show ipv6 spd Field Description

Field	Description
Current mode: normal	The current SPD state or mode.
Queue max threshold: 74	The process input queue maximum.

Related Commands

Command	Description
ipv6 spd queue max-threshold	Configures the maximum number of packets in the SPD process input queue.

show ipv6 virtual-reassembly

To display Virtual Fragment Reassembly (VFR) configuration and statistical information on a specific interface, use the **show ipv6 virtual-reassembly** command in privileged EXEC mode.

show ipv6 virtual-reassembly interface *interface-type*

Syntax Description

interface *interface-type*	Specifies the interface for which information is requested.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(7)T	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.

Usage Guidelines

This command shows the configuration and statistical information of VFR on the given interface.

Examples

The following example shows a typical display produced by this command:

```
Router# show ipv6 virtual-reassembly
All enabled IPv6 interfaces...
GigabitEthernet0/0/0:
   IPv6 Virtual Fragment Reassembly (IPV6VFR) is ENABLED [in]
   IPv6 configured concurrent reassemblies (max-reassemblies): 64
   IPv6 configured fragments per reassembly (max-fragments): 16
   IPv6 configured reassembly timeout (timeout): 3 seconds
   IPv6 configured drop fragments: OFF

   IPv6 current reassembly count:0
   IPv6 current fragment count:0
   IPv6 total reassembly count:20
   IPv6 total reassembly timeout count:0
```

The display is self-explanatory; it corresponds to the values used when you entered the **ipv6 virtual-reassembly** command.

Related Commands

Command	Description
ipv6 virtual-reassembly	Enables VFR on an interface.

show ipv6 virtual-reassembly features

To display Virtual Fragment Reassembly (VFR) information on all interfaces or on a specified interface, use the **show ipv6 virtual-reassembly features** command in privileged EXEC mode.

show ipv6 virtual-reassembly features [**interface** *interface-type*]

Syntax Description

interface *interface-type*	(Optional) Specifies the interface for which information is requested.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(7)T	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.

Usage Guidelines

This command shows the configuration and statistical information of VFR on a specified interface or on all interfaces. Use the optional **interface** *interface-type* keyword and argument to specify an interface. If you enter the **show ipv6 virtual-reassembly features** command without the keyword and argument, information about all interfaces is displayed.

Examples

The following example displays information about all interfaces:

```
Router# show ipv6 virtual-reassembly features

GigabitEthernet0/0/0:
  IPV6 Virtual Fragment Reassembly (IPV6 VFR) Current Status is ENABLED [in]
  Features to use if IPV6 VFR is Enabled:CLI
GigabitEthernet0/0/0:
  IPV6 Virtual Fragment Reassembly (IPV6 VFR) Current Status is ENABLED [out]
  Features to use if IPV6 VFR is Enabled:CLI
```

The display is self-explanatory; it corresponds to the values used when you entered the **ipv6 virtual-reassembly** command.

Related Commands

Command	Description
ipv6 virtual-reassembly	Enables VFR on an interface.
show ipv6 virtual-reassembly	Displays VFR configuration and statistical information.

show kerberos creds

To display the contents of your credentials cache, use the **show kerberos creds** command in privileged EXEC mode.

show kerberos creds

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **show kerberos creds** command is equivalent to the UNIX klist command.

When users authenticate themselves with Kerberos, they are issued an authentication ticket called a *credential* . The credential is stored in a credential cache.

Examples

The following example displays entries in the credentials cache:

```
Router > show kerberos creds

 Default Principal: user@example.com
 Valid Starting          Expires                 Service Principal
 18-Dec-1995 16:21:07    19-Dec-1995 00:22:24    krbtgt/EXAMPLE.COM@EXAMPLE.COM
```

The following example returns output that acknowledges that credentials do *not* exist in the credentials cache:

```
Router > show kerberos creds
 No Kerberos credentials
```

Related Commands

Command	Description
clear kerberos creds	Deletes the contents of the credentials cache.

show ldap attributes

To display attributes of the Lightweight Directory Access Protocol (LDAP) server, use the **show ldap attributes**command in user EXEC or privileged EXEC mode.

show ldap attributes

Syntax Description

This command has no arguments and keywords.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Usage Guidelines

Use the **show ldap attributes** command to display the default mapping of LDAP attributes to AAA attributes. It displays the dynamic attribute map that is configured on the router.

Examples

The followingis sample output from the **show ldap server** command:

```
Router# show ldap attributes
LDAP Attribute                    Format      AAA Attribute
==============                    ======      =============
airespaceBwDataBurstContract     Ulong       bsn-data-bandwidth-burst-contr
userPassword                     String      password
airespaceBwRealBurstContract     Ulong       bsn-realtime-bandwidth-burst-c
employeeType                     String      employee-type
airespaceServiceType             Ulong       service-type
airespaceACLName                 String      bsn-acl-name
priv-lvl                         Ulong       priv-lvl
memberOf                         String DN   supplicant-group
cn                               String      username
airespaceDSCP                    Ulong       bsn-dscp
policyTag                        String      tag-name
airespaceQOSLevel                Ulong       bsn-qos-level
airespace8021PType               Ulong       bsn-8021p-type
airespaceBwRealAveContract       Ulong       bsn-realtime-bandwidth-average
airespaceVlanInterfaceName       String      bsn-vlan-interface-name
airespaceVapId                   Ulong       bsn-wlan-id
airespaceBwDataAveContract       Ulong       bsn-data-bandwidth-average-con
sAMAccountName                   String      sam-account-name
meetingContactInfo               String      contact-info
telephoneNumber                  String      telephone-number
Map: att_map_1
department                       String DN   element-req-qos
```

The table below describes the significant fields shown in the display.

Table 132: show ldap attributes Descriptions

Field	Description
LDAP Attribute	LDAP distinguished name attribute (or attributes).
Format	Format conversion of the attribute.
AAA Attribute	Authentication, Authorization, and Accounting (AAA) distinguished name attribute (or attributes).

Related Commands

Command	Description
attribute-map	Attaches an attribute map to a particular LDAP server.
ldap attribute-map	Configures a dynamic LDAP attribute map.
map-type	Defines the mapping of an attribute in the LDAP server.
show ldap server	Displays properties of the LDAP server.

show ldap server

To display properties of the Lightweight Directory Access Protocol (LDAP) server, use the **show ldap server** command in user EXEC or privileged EXEC mode.

show ldap server {*name* | **all**} {**connections** | **statistics** | **summary**}

Syntax Description

name	The name of the configured LDAP server for which to display the properties.
all	Displays properties for all LDAP servers.
connections	Displays the number of connections to the LDAP server.
statistics	Displays the LDAP statistics.
summary	Displays the LDAP server information.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
15.1(1)T	This command was introduced.
15.2(2)T	This command was modified. The **connections**, **statistics**, and **summary** keywords were added.

Examples

The following is sample output from the **show ldap server** command:

```
Device# show ldap server ldap1 connections

Sock  Connection Status   Root Bind Status
---------------------------------------------
0     UP                  Root-dn Bind Done
No. of active connections   :1


Device# show ldap server ldap1 statistics

---------------------------------
* LDAP STATISTICS *
Total messages  [Sent:3, Received:7]
Response delay(ms) [Average:543, Maximum:581]
Total search    [Request:1, ResultEntry:4, ResultDone:1]
Total bind      [Request:2, Response:2]
Total extended  [Request:0, Response:0]
Total compare   [Request:0, Response:0]
Search [Success:1, Failures:0]
Bind   [Success:2, Failures:0]
Missing attrs in Entry [0]
---------------------------------
```

```
Device# show ldap server ldap1 summary

Server Information for ldap1
================================
Server name             :ldap1
Server IP               :10.64.67.66
Server listening Port   :389
Bind Root-dn            :cn=admin,dc=ldap,dc=com
Server mode             :Non-Secure
Secure Trustpoint       :MSCA1
Cipher Suite            :0x00
Authentication Seq      :Bind/Compare password first. Search next
Authentication Procedure:Bind with user password
Base-Dn                 :dc=ldap,dc=com
Request timeout         :30
No. of active connections   :1
--------------------------------

Device# show ldap server all

Server Information for ldap1
================================
Server name              :ldap1
Server Address           :2001:DB8:0:0:8:800
Server listening Port    :389
Bind Root-dn             :cn=iosadmin,dc=aaaldap,dc=com
Server mode              :Non-Secure
Cipher Suite             :0x00
Authentication Seq       :Bind/Compare password first. Search next
Authentication Procedure :Bind with user password
Base-Dn                  :dc=aaaldap,dc=com
Object Class             :top
Request timeout          :30
--------------------------------
* LDAP STATISTICS *
Total messages  [Sent:0, Received:0]
Response delay(ms) [Average:0, Maximum:0]
Total search    [Request:0, ResultEntry:0, ResultDone:0]
Total bind      [Request:0, Response:0]
Total extended  [Request:0, Response:0]
Total compare   [Request:0, Response:0]
Search [Success:0, Failures:0]
Bind   [Success:0, Failures:0]
Missing attrs in Entry [0]
--------------------------------
No. of active connections   :0
--------------------------------
```

The following table describes the significant fields shown in the display.

Table 133: show ldap server Field Descriptions

Field	Description
No. of active connections	Total number of connections to the LDAP server.
Total messages	Total number of sent and received LDAP messages.
Response delay (ms)	Maximum and average delay in response, in milliseconds.
Total search	Total number of search requests and results for directory entries.

Field	Description
Total bind	Total number of user credentials verified with the LDAP server.
Total extended	Total number of Transport Layer Security (TLS) extension operations.
Total compare	Total number of requests and results to find if a named entry contains a given attribute value.
Search	Number of successful and failed user search results for directory entries.
Bind	Number of successful and failed user authentication entries.
Missing attrs in Entry	Number of missing attributes in an LDAP entry. LDAP entries contain multiple attributes received from the LDAP server.
Server name	LDAP server name.
Server IP	IP address of the LDAP server.
Server Address	IPv6 address of the LDAP server.
Server listening Port	The transport layer port on which the server is listening.
Bind Root-dn	Distinguished name of the LDAP server.
Server mode	Security mode.
Secure Trustpoint	Secure LDAP server name.
Cipher Suite	Cryptographic algorithms used in the connection.
Authentication Seq	LDAP authentication sequence.
Authentication Procedure	Authentication method.
Base-Dn	Distinguished name of the search base.
Request timeout	Response timeout. The default timeout value is 30 seconds.

Related Commands

Command	Description
show ldap attribute	Displays information about default LDAP attribute mapping.

show logging ip access-list

To display information about the logging IP access list, use the **show logging ip access-list**command in privileged EXEC mode.

show logging ip access-list {**cache** | **config**}

Syntax Description

cache	Displays information about all the entries in the Optimized ACL Logging (OAL) cache.
config	Displays information about the logging IP access-list configuration.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(17d)SXB	Support for this command was introduced on the Supervisor Engine 720.
12.2(18)SXE	This command was changed to include the **config** keyword on the Supervisor Engine 720 only.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is supported on Cisco 7600 series routers that are configured with a Supervisor Engine 720 only.

OAL is supported on IPv4 unicast traffic only.

Examples

This example shows how to display all the entries in the OAL cache:

```
Router# show logging ip access-list cache
Matched flows:
id prot src_ip dst_ip sport dport status count
total lastlog
-------------------------------------------------------------------------------------
1 17 10.2.1.82 10.2.12.2 111 63 Permit 0
3906 2d02h
2 17 10.2.1.82 10.2.12.2 1135 63 Permit 0
3906 2d02h
3 17 10.2.1.82 10.2.12.2 2159 63 Permit 0
3906 2d02h
4 17 10.2.1.82 10.2.12.2 3183 63 Permit 0
3906 2d02h
5 17 10.2.1.82 10.2.12.2 4207 63 Permit 0
3906 2d02h
6 17 10.2.1.82 10.2.12.2 5231 63 Deny 0
3906 2d02h
7 17 10.2.1.82 10.2.12.2 6255 63 Deny 0
3906 2d02h
8 17 10.2.1.82 10.2.12.2 7279 63 Permit 0
3906 2d02h
```

```
9 17 10.2.1.82 10.2.12.2 8303 63 Permit 0
3906 2d02h
10 17 10.2.1.82 10.2.12.2 9327 63 Permit 0
3905 2d02h
11 17 10.2.1.82 10.2.12.2 10351 63 Permit 0
3905 2d02h
12 17 10.2.1.82 10.2.12.2 11375 63 Permit 0
3905 2d02h
13 17 10.2.1.82 10.2.12.2 12399 63 Deny 0
3905 2d02h
14 17 10.2.1.82 10.2.12.2 13423 63 Permit 0
3905 2d02h
15 17 10.2.1.82 10.2.12.2 14447 63 Deny 0
3905 2d02h
16 17 10.2.1.82 10.2.12.2 15471 63 Permit 0
3905 2d02h
17 17 10.2.1.82 10.2.12.2 16495 63 Permit 0
3905 2d02h
18 17 10.2.1.82 10.2.12.2 17519 63 Permit 0
3905 2d02h
19 17 10.2.1.82 10.2.12.2 18543 63 Permit 0
3905 2d02h
20 17 10.2.1.82 10.2.12.2 19567 63 Permit 0
3905 2d02h
Number of entries: 20
Number of messages logged: 112
Number of packets logged: 11200
Number of packets received for logging: 11200
```

This example shows how to display information about the logging IP access-list configuration:

```
Router# show logging ip access-list config
Logging ip access-list configuration
 Maximum number of cached entries: 8192
 Logging rate limiter: 0
 Log-update interval: 300
 Log-update threshold: 0
 Configured on input direction:
        Vlan2
        Vlan1
 Configured on output direction:
        Vlan2
```

Related Commands

Command	Description
clear logging ip access-list cache	Clears all the entries from the OAL cache and sends them to the syslog.
logging ip access-list cache (global configuration)	Configures the OAL parameters.
logging ip access-list cache (interface configuration)	Enables an OAL-logging cache on an interface that is based on direction.

show login

To display login parameters, use the **show login**command in privileged EXEC mode.

show login [**failures**]

Syntax Description

failures	(Optional) Displays information related only to failed login attempts.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

The **show login**command allows users to verify the applied login configuration and present login status on your router.

Examples

The following sample output from the **show login** command verifies that no login parameters have been specified:

```
Router# show login
No login delay has been applied.
No Quiet-Mode access list has been configured.
All successful login is logged and generate SNMP traps.
All failed login is logged and generate SNMP traps
Router NOT enabled to watch for login Attacks
```

The following sample output from the **show login** command verifies that the **login block-for**command is issued. In this example, the command is configured to block login hosts for 100 seconds if 16 or more login requests fail within 100 seconds; 5 login requests have already failed.

```
Router# show login
A default login delay of 1 seconds is applied.
No Quiet-Mode access list has been configured.
All successful login is logged and generate SNMP traps.
All failed login is logged and generate SNMP traps.
Router enabled to watch for login Attacks.
If more than 15 login failures occur in 100 seconds or less, logins will be disabled for
100 seconds.
Router presently in Watch-Mode, will remain in Watch-Mode for 95 seconds.
Present login failure count 5.
```

The following sample output from the **show login** command verifies that the router is in quiet mode. In this example, the **login block-for** command was configured to block login hosts for 100 seconds if 3 or more login requests fail within 100 seconds.

```
Router# show login
A default login delay of 1 seconds is applied.
No Quiet-Mode access list has been configured.
All successful login is logged and generate SNMP traps.
All failed login is logged and generate SNMP traps.
Router enabled to watch for login Attacks.
If more than 2 login failures occur in 100 seconds or less, logins will be disabled for 100
 seconds.
Router presently in Quiet-Mode, will remain in Quiet-Mode for 93 seconds.
```

Denying logins from all sources.

The table below describes the significant fields shown in the proceeding displays.

Table 134: show login Field Descriptions

Field	Description
A default login delay of 1 seconds is applied.	A delay of 1 second is enforced when the **login block-for** command is issued. To specify a different delay value, use the **login delay** command.
No Quiet-Mode access list has been configured.	No access control lists (ACLs) are exempt from the quiet period. To specify an ACL, use the **login quiet-mode access-class** command.
All successful or failed login is logged and generate SNMP traps.	Logging messages and Simple Network Management Protocol (SNMP) traps are configured to be generated upon successful or failed login attempts. To change this setting, use the **login on-success** or **login on-failure** command.
Router enabled to watch for login Attacks.	The Cisco IOS device has been configured with at least the **login block-for** command, which enables default login functionality. **Note** If no login parameters are specified, the following description appears: " Router NOT enabled to watch for login Attacks . "
If more than 2 login failures occur in 100 seconds or less, logins will be disabled for 100 seconds.	Parameters of the **login block-for** *seconds* **attempts** *tries* **within** *seconds* command.
`Router presently in Quiet-Mode, will remain in Quiet-Mode for 93 seconds.`	The router has switched to quiet mode. **Note** If the router is not in quiet mode, the following description appears: " Router presently in Watch-Mode, will remain in Watch-Mode for 95 seconds."

Field	Description
Denying logins from all sources.	The router is in quiet mode and no ACLs are defined, so the router is denying all login requests. **Note** If the router is not in quiet mode, the following description, which allows the user to keep track of the current failed login attempts, appears: "Present login failure count 5."

show login failure Sample Outputs

The following sample output from **show login failures** command shows all failed login attempts on the router:

```
Router# show login failures
Information about login failure's with the device
Username      Source IPAddr  lPort Count  TimeStamp
try1          10.1.1.1        23    1     21:52:49 UTC Sun Mar 9 2003
try2          10.1.1.2        23    1     21:52:52 UTC Sun Mar 9 2003
```

The following sample output from **show login failures** command verifies that no information is presently logged:

```
Router# show login failures
*** No logged failed login attempts with the device.***
```

Related Commands

Command	Description
login block-for	Configures your Cisco IOS device for login parameters that help provide DoS detection.
login delay	Configures a uniform delay between successive login attempts.
login on-failure	Generates system logging messages for every login attempts.
login on-success	Generates system logging messages for successful login attempts.
login quiet-mode access-class	Specifies an ACL that is to be applied to the router when it switches to quiet mode.

show mab

To display MAC Authentication Bypass (MAB) information, use the **show mab** command in privileged EXEC mode.

show mab {**all** | **interface** *type number*} [**detail**]

Syntax Description

all	Specifies all interfaces.
interface *type number*	Specifies a particular interface for which to display MAB information.
detail	(Optional) Displays detailed information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SXI	This command was introduced.
15.2(2)T	This command was integrated into Cisco IOS Release 15.2(2)T.
15.2(3)T	This command was modified. The authorization status of the authentication result is displayed as SUCCESS or FAIL instead of AUTHORIZED or UNAUTHORIZED in the command output.

Usage Guidelines

Use the **show mab** command to display information about MAB ports and MAB sessions.

Examples

The following is sample output from the **show mab interface detail** command where a MAB session has been authorized:

```
Switch# show mab interface
FastEthernet1/0/1
 detail
MAB details for FastEthernet1/0/1
--------------------------------------
Mac-Auth-Bypass           = Enabled
Inactivity Timeout        = None
MAB Client List
---------------
Client MAC                = 000f.23c4.a401
MAB SM state              = TERMINATE
Auth Status               = SUCCESS
```

The table below describes the significant fields shown in the display.

Table 135: show mab Field Descriptions

Field	Description
Mac-Auth-Bypass	Specifies whether MAB is enabled or disabled.

Field	Description
Inactivity Timeout	The period of time of no activity after which the session is ended.
Client MAC	The MAC address of the client.
MAB SM state	The state of the MAB state machine. The possible values, from start to finish, are: • INITIALIZE--the state of the session when it is being initialized. • ACQUIRING--the state of the session when the MAC address is being obtained from the client. • AUTHORIZING--the state of the session when the MAC address is being authorized. • TERMINATE--the state of the session once an authorization result has been obtained.
Auth Status	The authorization status of the MAB session. The possible values are: • SUCCESS--the session has been successfully authorized. • FAIL--the session failed to be authorized.

Related Commands

Command	Description
show authentication interface	Displays information about the Auth Manager for a given interface.
show authentication registrations	Displays information about authentication methods registered with the Auth Manager.
show authentication sessions	Displays information about Auth Manager sessions.

show mac access-group interface

To display the ACL configuration on a Layer 2 interface, use the **show mac access-group interface**command.

show mac access-group interface [*interface interface-number*]

Syntax Description

interface	(Optional) Specifies the interface type; valid values are **gigabitethernet**, **tengigabitethernet**, **longreachethernet**, and **port-channel**.
interface-number	(Optional) Specifies the port number.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC mode

Command History

Release	Modification
12.2(33)SXH	Support for this command was introduced.
12.2(33)SRB	Support for this command was introduced.
12.2(33)SRD3	Support for this command was introduced.

Usage Guidelines

The valid values for the port number depend on the chassis used.

Examples

This example shows how to display the ACL configuration on interface fast 6/1:

```
Switch# show mac access-group interface gigabitethernet 6/1
Interface FastEthernet6/1:
   Inbound access-list is simple-mac-acl
   Outbound access-list is not set
```

Related Commands

Command	Description
access-group mode	Specifies the override modes (for example, VACL overrides PACL) and the non-override modes (for example, merge or strict mode).

show mac-address-table

To display the MAC address table, use the **show mac-address-table** command in privileged EXEC mode.

Cisco 2600, 3600, and 3700 Series Routers
show mac-address-table [{**secure** | **self** | **count**}][{**address***macaddress*}][{**interface***type/number*}]{**fa** | **gi***slot/port*}[{**atm***slot/port*}][{**atm***slot/port* }][{**vlan***vlan-id*}]

Catalyst 4500 Series Switches
show mac-address-table {**assigned** | **ip** | **ipx** | **other**}

Catalyst 6000/6500 Series Switches and 7600 Series Routers
show mac-address-table [**address** *mac-addr* [**all** | **interface** *type/number* | **module** *number* | **vlan** *vlan-id*] | **aging-time** [**vlan** *vlan-id*] | **count**[**module** *number* | **vlan** *vlan-id*] | **interface** *type/number* | **limit** [**vlan** *vlan-id* | **module** *number* | **interface** *type*] | **module** *number* | **multicast** [**count**] [**igmp-snooping** | **mld-snooping** | **user**][**vlan** *vlan-id*] | **notification** {**mac-move**[**counter**[**vlan**]] | **threshold** | **change**}[**interface** [*number*]] | **synchronize statistics** | **unicast-flood** | **vlan** *vlan-id* [{**all** | **module** *number*}]]

Syntax Description

secure	(Optional) Displays only the secure addresses.
self	(Optional) Displays only addresses added by the switch itself.
count	(Optional) Displays the number of entries that are currently in the MAC address table.
address *mac-addr*	(Optional) Displays information about the MAC address table for a specific MAC address. See the ❍Usage Guidelines❍ section for formatting information.
interface *type* / *number*	(Optional) Displays addresses for a specific interface. For the Catalyst 6500 and 6000 series switches, valid values are **atm**, **fastethernet**, **gigabitethernet**, and **port-channel**. For the Cisco 7600 series, valid values are **atm**,**ethernet**, **fastethernet**, **ge-wan**, **gigabitethernet**, **tengigabitethernet**, and **pos**.
fa	(Optional) Specifies the Fast Ethernet interface.
gi	(Optional) Specifies the Gigabit Ethernet interface.
slot / *port*	(Optional) Adds dynamic addresses to the module in slot 1 or 2. The slash mark is required.
atm *slot /port*	(Optional) Adds dynamic addresses to ATM module *slot /port* . Use 1 or 2 for the slot number. Use 0 as the port number. The slash mark is required.
vlan *vlan -id*	(Optional) Displays addresses for a specific VLAN. For the Cisco 2600, 3600, and 3700 series, valid values are from 1 to 1005; do not enter leading zeroes. Beginning with Cisco IOS Release 12.4(15)T, the valid VLAN ID range is from 1 to 4094. For the Catalyst 6500 and 6000 series switches and 7600 series, valid values are from 1 to 4094.

assigned	Specifies the assigned protocol entries.
ip	Specifies the IP protocol entries.
ipx	Specifies the IPX protocol entries.
other	Specifies the other protocol entries.
all	(Optional) Displays every instance of the specified MAC address in the forwarding table.
type / *number*	(Optional) Module and interface number.
module *number*	(Optional) Displays information about the MAC address table for a specific Distributed Forwarding Card (DFC) module.
aging-time	(Optional) Displays the aging time for the VLANs.
limit	Displays MAC-usage information.
multicast	Displays information about the multicast MAC address table entries only.
igmp-snooping	Displays the addresses learned by Internet Group Management Protocol (IGMP) snooping.
mld-snooping	Displays the addresses learned by Multicast Listener Discover version 2 (MLDv2) snooping.
user	Displays the manually entered (static) addresses.
notification mac-move	Displays the MAC-move notification status.
notification mac-move counter	(Optional) Displays the number of times a MAC has moved and the number of these instances that have occurred in the system.
vlan	(Optional) Specifies a VLAN to display. For the Catalyst 6500 and 6000 series switches and 7600 series, valid values are from 1 to 4094.
notification threshold	Displays the Counter-Addressable Memory (CAM) table utilization notification status.
notification change	Displays the MAC notification parameters and history table.
synchronize statistics	Displays information about the statistics collected on the switch processor or DFC.
unicast-flood	Displays unicast-flood information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.2(8)SA	This command was introduced.

Release	Modification
11.2(8)SA3	This command was modified. The **aging-time** ,, **count**, **self** , and **vlan** *vlan -id* keywords and arguments were added.
11.2(8)SA5	This command was modified. The **atm***slot*/*port* keyword-argument pair was added.
12.2(2)XT	This command was modified. This command was implemented on Cisco 2600, 3600, and 3700 series routers.
12.1(8a)EW	This command was modified. This command was implemented on Catalyst 4500 series switches.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T on Cisco 2600, 3600, and 3700 series routers.
12.2(11)T	This command was integrated into Cisco IOS Release 12.2(11)T.
12.2(14)SX	This command was modified. This command was implemented on the Supervisor Engine 720.
12.2(17a)SX	This command was modified. For the Catalyst 6500 and 6000 series switches and 7600 series, this command was changed to support the following optional keywords and arguments: • **count module** *number* • **limit** [**vlan** *vlan-id* | **port** *number* | **interface** *interface-type* • **notification threshold** • **unicast-flood**
12.2(17d)SXB	This command was modified. Support for this command was added for the Supervisor Engine 2.
12.2(18)SXE	This command was modified. For the Catalyst 6500 and 6000 series switches and Cisco 7600 series, support was added for the **mld-snooping** keyword on the Supervisor Engine 720 only.
12.2(18)SXF	This command was modified. For the Catalyst 6500 and 6000 series switches and Cisco 7600 series, support was added for the **synchronizestatistics** keywords on the Supervisor Engine 720 only.
12.2(33)SRA	This command was modified. This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(15)T	This command was modified to extend the range of valid VLAN IDs to 1 to 4094 for specified platforms.
12.2(33)SXH	This command was modified. The **change** keyword was added.
12.2(33)SXI	This command was modified to add the **counter** keyword.
15.4(2)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

Usage Guidelines

Cisco 2600, 3600, and 3700 Series Routers

The **show mac-address-table** command displays the MAC address table for the switch. Specific views can be defined by using the optional keywords and arguments. If more than one optional keyword is used, then all the conditions must be true for that entry to be displayed.

Catalyst 4500 Series Switches

For the MAC address table entries that are used by the routed ports, the routed port name, rather than the internal VLAN number, is displayed in the "vlan" column.

Catalyst 6000 and 6500 Series Switches and Cisco 7600 Series Routers

If you do not specify a module number, the output of the **show mac-address-table** command displays information about the supervisor engine. To display information about the MAC address table of the DFCs, you must enter the module number or the **all** keyword.

The *mac-addr*value is a 48-bit MAC address. The valid format is H.H.H.

The interface *number* argument designates the module and port number. Valid values depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48.

The optional **module** *number* keyword-argument pair is supported only on DFC modules. The **module** *number*keyword-argument pair designate the module number.

Valid values for the *mac-group-address* argument are from 1 to 9.

The optional **count** keyword displays the number of multicast entries.

The optional **multicast** keyword displays the multicast MAC addresses (groups) in a VLAN or displays all statically installed or IGMP snooping-learned entries in the Layer 2 table.

The information that is displayed in the show mac-address-table unicast-flood command output is as follows:

- Up to 50 flood entries, shared across all the VLANs that are not configured to use the filter mode, can be recorded.
- The output field displays are defined as follows:
  - ALERT--Information is updated approximately every 3 seconds.
  - SHUTDOWN--Information is updated approximately every 3 seconds.

Note The information displayed on the destination MAC addresses is deleted as soon as the floods stop after the port shuts down.

- Information is updated each time that you install the filter. The information lasts until you remove the filter.

The dynamic entries that are displayed in the Learn field are always set to Yes.

The **show mac-address-table limit** command output displays the following information:

- The current number of MAC addresses.
- The maximum number of MAC entries that are allowed.

- The percentage of usage.

The show mac-address-table synchronize statistics command output displays the following information:

- Number of messages processed at each time interval.
- Number of active entries sent for synchronization.
- Number of entries updated, created, ignored, or failed.

Examples

The following is sample output from the**show mac-address-table** command:

```
Switch# show mac-address-table

Dynamic Addresses Count:                9
Secure Addresses (User-defined) Count: 0
Static Addresses (User-defined) Count: 0
System Self Addresses Count:           41
Total MAC addresses:                   50
Non-static Address Table:
Destination Address  Address Type  VLAN  Destination Port
-------------------  ------------  ----  --------------------
0010.0de0.e289       Dynamic          1  FastEthernet0/1
0010.7b00.1540       Dynamic          2  FastEthernet0/5
0010.7b00.1545       Dynamic          2  FastEthernet0/5
0060.5cf4.0076       Dynamic          1  FastEthernet0/1
0060.5cf4.0077       Dynamic          1  FastEthernet0/1
0060.5cf4.1315       Dynamic          1  FastEthernet0/1
0060.70cb.f301       Dynamic          1  FastEthernet0/1
00e0.1e42.9978       Dynamic          1  FastEthernet0/1
00e0.1e9f.3900       Dynamic          1  FastEthernet0/1
```

Catalyst 4500 Series Switches

The following example shows how to display the MAC address table entries that have a specific protocol type (in this case, “assigned”):

```
Switch# show mac-address-table protocol assigned

vlan   mac address     type    protocol  qos             ports
-----+---------------+--------+---------+---+--------------------------------
 200  0050.3e8d.6400  static   assigned  --  Switch
 100  0050.3e8d.6400  static   assigned  --  Switch
   5  0050.3e8d.6400  static   assigned  --  Switch
4092  0000.0000.0000  dynamic  assigned  --  Switch
   1  0050.3e8d.6400  static   assigned  --  Switch
   4  0050.3e8d.6400  static   assigned  --  Switch
4092  0050.f0ac.3058  static   assigned  --  Switch
4092  0050.f0ac.3059  dynamic  assigned  --  Switch
   1  0010.7b3b.0978  dynamic  assigned  --  Fa5/9
```

The following example shows the “other” output for the previous example:

```
Switch# show mac-address-table protocol other

Unicast Entries
```

```
 vlan   mac address     type        protocols               port
-------+---------------+--------+---------------------+--------------------
   1    0000.0000.0201   dynamic other                 FastEthernet6/15
   1    0000.0000.0202   dynamic other                 FastEthernet6/15
   1    0000.0000.0203   dynamic other                 FastEthernet6/15
   1    0000.0000.0204   dynamic other                 FastEthernet6/15
   1    0030.94fc.0dff    static ip,ipx,assigned,other  Switch
   2    0000.0000.0101   dynamic other                 FastEthernet6/16
   2    0000.0000.0102   dynamic other                 FastEthernet6/16
   2    0000.0000.0103   dynamic other                 FastEthernet6/16
   2    0000.0000.0104   dynamic other                 FastEthernet6/16
Fa6/1   0030.94fc.0dff    static ip,ipx,assigned,other  Switch
Fa6/2   0030.94fc.0dff    static ip,ipx,assigned,other  Switch
Multicast Entries
 vlan    mac address     type    ports
-------+---------------+-------+-----------------------------------------
   1    ffff.ffff.ffff   system Switch,Fa6/15
   2    ffff.ffff.ffff   system Fa6/16
1002    ffff.ffff.ffff   system
1003    ffff.ffff.ffff   system
1004    ffff.ffff.ffff   system
1005    ffff.ffff.ffff   system
Fa6/1   ffff.ffff.ffff   system Switch,Fa6/1
Fa6/2   ffff.ffff.ffff   system Switch,Fa6/2
```

Catalyst 6000 and 6500 Series Switches and Cisco 7600 Series Routers

The following is sample output from the**show mac-address-table**command:

```
Switch# show mac-address-table

Dynamic Addresses Count:                9
Secure Addresses (User-defined) Count: 0
Static Addresses (User-defined) Count: 0
System Self Addresses Count:            41
Total MAC addresses:                    50
Non-static Address Table:
Destination Address  Address Type  VLAN  Destination Port
-------------------  ------------  ----  --------------------
0010.0de0.e289       Dynamic          1  FastEthernet0/1
0010.7b00.1540       Dynamic          2  FastEthernet0/5
0010.7b00.1545       Dynamic          2  FastEthernet0/5
0060.5cf4.0076       Dynamic          1  FastEthernet0/1
0060.5cf4.0077       Dynamic          1  FastEthernet0/1
0060.5cf4.1315       Dynamic          1  FastEthernet0/1
0060.70cb.f301       Dynamic          1  FastEthernet0/1
00e0.1e42.9978       Dynamic          1  FastEthernet0/1
00e0.1e9f.3900       Dynamic          1  FastEthernet0/1
```

Note In a distributed Encoded Address Recognition Logic (EARL) switch, the asterisk (*) indicates a MAC address that is learned on a port that is associated with this EARL.

The following example shows how to display the information about the MAC address table for a specific MAC address with a Supervisor Engine 720:

```
Switch# show mac-address-table address 001.6441.60ca
```

```
Codes: * - primary entry
  vlan   mac address     type    learn qos            ports
------+---------------+--------+-----+---+--------------------------
Supervisor:
*  ---  0001.6441.60ca    static  No    --  Router
```

The following example shows how to display MAC address table information for a specific MAC address with a Supervisor Engine 720:

```
Router# show mac-address-table address 0100.5e00.0128

Legend: * - primary entry
        age - seconds since last seen
        n/a - not available
  vlan   mac address     type    learn     age              ports
------+---------------+--------+-----+----------+--------------------------
Supervisor:
*   44  0100.5e00.0128    static  Yes          -   Fa6/44,Router
*    1  0100.5e00.0128    static  Yes          -   Router
Module 9:
*   44  0100.5e00.0128    static  Yes          -   Fa6/44,Router
*    1  0100.5e00.0128    static  Yes          -   Router
```

The following example shows how to display the currently configured aging time for all VLANs:

```
Switch# show mac-address-table aging-time

Vlan    Aging Time
----    ----------
*100     300
200     1000
```

The following example shows how to display the entry count for a specific slot:

```
Switch# show mac-address-table count module 1

MAC Entries on slot 1 :
Dynamic Address Count:                4
Static Address (User-defined) Count:  25
Total MAC Addresses In Use:           29
Total MAC Addresses Available:        131072
```

The following example shows how to display the information about the MAC address table for a specific interface with a Supervisor Engine 720:

```
Switch# show mac-address-table interface fastethernet 6/45

Legend: * - primary entry
        age - seconds since last seen
        n/a - not available
  vlan   mac address     type    learn     age              ports
------+---------------+--------+-----+----------+--------------------------
*   45  00e0.f74c.842d   dynamic  Yes          5   Fa6/45
```

Note A leading asterisk (*) indicates entries from a MAC address that was learned from a packet coming from an outside device to a specific module.

The following example shows how to display the limit information for a specific slot:

```
Switch# show mac-address-table limit vlan 1 module 1

vlan    switch   module    action      maximum  Total entries  flooding
-------+--------+---------+-----------+--------+--------------+------------
1          1        7       warning      500      0             enabled
1          1        11      warning      500      0             enabled
1          1        12      warning      500      0             enabled

Router#show mac-address-table limit vlan 1 module 2

vlan    switch   module    action      maximum  Total entries  flooding
-------+--------+---------+-----------+--------+--------------+------------
1          2         7      warning      500      0             enabled
1          2         9      warning      500      0             enabled
```

The following example shows how to display the MAC-move notification status:

```
Switch# show mac-address-table notification mac-move

MAC Move Notification: Enabled
```

The following example shows how to display the MAC move statistics:

```
Router# show mac-address-table notification mac-move counter

--------------------------------------------------------------------------------
Vlan Mac Address From Mod/Port To Mod/Port Count
---- ----------------- ---------------------- ---------------------- ------------
1 00-01-02-03-04-01 2/3 3/1 10
20 00-01-05-03-02-01 5/3 5/1 20
```

The following example shows how to display the CAM-table utilization-notification status:

```
Router# show mac-address-table notification threshold

Status limit Interval
-------------+-----------+-------------
enabled 1 120
```

The following example shows how to display the MAC notification parameters and history table:

```
Switch# show mac-address-table notification change

MAC Notification Feature is Disabled on the switch
MAC Notification Flags For All Ethernet Interfaces :
------------------------------------------------
Interface                   MAC Added Trap MAC Removed Trap
```

```
--------------------         -------------- ----------------
```

The following example shows how to display the MAC notification parameters and history table for a specific interface:

```
Switch# show mac-address-table notification change interface gigabitethernet5/2

MAC Notification Feature is Disabled on the switch
Interface                   MAC Added Trap MAC Removed Trap
--------------------        -------------- ----------------
GigabitEthernet5/2          Disabled       Disabled
```

The following example shows how to display unicast-flood information:

```
Switch# show mac-address-table unicast-flood

> > Unicast Flood Protection status: enabled
> >
> > Configuration:
> > vlan Kfps action timeout
> > ------+----------+-----------------+----------
> > 2 2 alert none
> >
> > Mac filters:
> > No. vlan source mac addr. installed
> > on time left (mm:ss)
> >
> >-----+------+-----------------+------------------------------+------------------
> >
> > Flood details:
> > Vlan source mac addr. destination mac addr.
> >
> >------+---------------+--------------------------------------------------
> > 2 0000.0000.cafe 0000.0000.bad0, 0000.0000.babe,
> > 0000.0000.bac0
> > 0000.0000.bac2, 0000.0000.bac4,
> > 0000.0000.bac6
> > 0000.0000.bac8
> > 2 0000.0000.caff 0000.0000.bad1, 0000.0000.babf,
> > 0000.0000.bac1
> > 0000.0000.bac3, 0000.0000.bac5,
> > 0000.0000.bac7
> > 0000.0000.bac9
```

The following example shows how to display the information about the MAC-address table for a specific VLAN:

```
Switch#show mac-address-table vlan 100

vlan   mac address     type    protocol  qos             ports
-----+---------------+--------+---------+---+--------------------------------
 100  0050.3e8d.6400  static   assigned  --  Router
 100  0050.7312.0cff  dynamic        ip  --  Fa5/9
 100  0080.1c93.8040  dynamic        ip  --  Fa5/9
 100  0050.3e8d.6400  static        ipx  --  Router
 100  0050.3e8d.6400  static      other  --  Router
 100  0100.0cdd.dddd  static      other  --  Fa5/9,Router,Switch
 100  00d0.5870.a4ff  dynamic        ip  --  Fa5/9
 100  00e0.4fac.b400  dynamic        ip  --  Fa5/9
```

```
 100  0100.5e00.0001  static         ip  --  Fa5/9,Switch
 100  0050.3e8d.6400  static         ip  --  Router
```

The following example shows how to display the information about the MAC address table for MLDv2 snooping:

```
Switch# show mac-address-table multicast mld-snooping

vlan mac address type learn qos ports
-----+---------------+--------+-----+---+--------------------------------
--- 3333.0000.0001 static Yes - Switch,Stby-Switch
--- 3333.0000.000d static Yes - Fa2/1,Fa4/1,Router,Switch
--- 3333.0000.0016 static Yes - Switch,Stby-Switch
```

The table below describes the significant fields shown in the displays.

Table 136: show mac-address-table Field Descriptions

Field	Description
Dynamic Addresses Count	Total number of dynamic addresses in the MAC address table.
Secure Addresses (User-defined) Count	Total number of secure addresses in the MAC address table.
Static Addresses (User-defined) Count	Total number of static addresses in the MAC address table.
System Self Addresses Count	Total number of addresses in the MAC address table.
Total MAC addresses	Total MAC addresses in the MAC address table.
Destination Address	Destination addresses present in the MAC address table.
Address Type	Address type: static or dynamic.
VLAN	VLAN number.
Destination Port	Destination port information present in the MAC address table.
mac address	The MAC address of the entry.
protocol	Protocol present in the MAC address table.
qos	Quality of service associated with the MAC address table.
ports	Port type.
age	The time in seconds since last occurrence of the interface.
Aging Time	Aging time for entries.
module	Module number.
action	Type of action.
flooding	Status of the flooding.

Related Commands

Command	Description
clear mac-address-table	Deletes entries from the MAC address table.
mac-address-table aging-time	Configures the aging time for entries in the Layer 2 table.
mac-address-table limit	Enables MAC limiting.
mac-address-table notification mac-move	Enables MAC-move notification.
mac-address-table static	Adds static entries to the MAC address table or configures a static MAC address with IGMP snooping disabled for that address.
mac-address-table synchronize	Synchronizes the Layer 2 MAC address table entries across the PFC and all the DFCs.
show mac-address-table static	Displays only static MAC address table entries.

show management-interface

To display information about management interfaces, use the **show management-interface** command in privileged EXEC mode.

show management-interface [{*interface* | **protocol** *protocol-name*}]

Syntax Description

interface	(Optional) Interface for which you want to view information.
protocol	(Optional) Indicates that a protocol is specified.
protocol-name	(Optional) Protocol for which you want to view information.

Command Default

Information about all dedicated management interfaces is displayed when no interface or protocol is specified.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

The **show management-interface** command allows you to view all management interface configurations and activity on a device and to filter the output by interface or protocol. This flexibility is useful for network monitoring and troubleshooting.

Examples

The following sample output is from a **show management-interface** command when no interface or protocol is specified:

```
Router# show management-interface
Management interface FastEthernet0/0
        Protocol        Packets processed
             ssh                223981
```

The following sample output is from a **show management-interface**commandwith interfaceFastEthernet 0/0specified:

```
Router# show management-interface fastEthernet 0/0
Management interface FastEthernet0/0
        Protocol        Packets processed
             ssh                223981
```

The following sample output is from a **show management-interface**command with protocol Secure Shell (SSH) specified:

```
Router# show management-interface protocol ssh
The following management-interfaces allow protocol ssh
        FastEthernet0/0 Packets processed 223981
```

The table below describes the significant fields shown in the displays.

Table 137: show management-interface Field Descriptions

Field	Description
Management interface <interface>	Interface designated as a management interface.
Protocol	Network management protocols enabled on the interface.
Packets processed	The number of packets processed on the interface.

Related Commands

Command	Description
management-interface allow	Configures an interface to accept only network management packets.

show mka session

To display a summary of active MACsec Key Agreement (MKA) Protocol sessions, use the **show mka session** command in privileged EXEC mode.

show mka session [**interface***interface-id*] [**port-id***port-id*]] [**local-sci***sci*] [**detail**]

Syntax Description

interface *interface-id*	(Optional) Displays status information for active MKA sessions on an interface.
port-id *port-id*	(Optional) Displays a summary of active MKA sessions running on the interface with the specified port ID. To see the port ID, enter the **show mka session interface** *interface-id* command. Port identifier values begin at 2 and monotonically increase for each new session that uses a virtual port on the same physical interface.
local-sci *sci*	(Optional) Displays status information for the MKA session identified by the Local TX-SCI. To determine the Local TX-SCI for a specific session, enter the show mka session command without any keywords. The SCI must be 8 octets (16 hexadecimal digits) long.
detail	(Optional) Displays detailed status information about all active MKA sessions, all sessions on the specified interface, or on the specified interface with the specified port ID.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0	This command was introduced.

Examples

This is sample output of the **show mka session** command:

```
Switch# show mka session

 Total MKA Sessions....... 1
           Secured Sessions... 1
           Pending Sessions... 0

==============================================================================================

           Interface      Local-TxSCI         Policy-Name      Inherited         Key-Server

           Port-ID        Peer-RxSCI          MACsec-Peers     Status            CKN
```

```
==============================================================================================

          Et0/0          aabb.cc00.6600/0002 *DEFAULT POLICY* NO                NO

          2              aabb.cc00.6500/0002 1                Secured           11
```

Table 138: Table 0-6 show mka session Output Fields

Field	Description
Interface	The short name of the physical interface on which the MKA session is active.
Peer-RxSCI	The MAC address of the interface of the peer concatenated with the peer 16-bit Port-ID.
Policy-name	The name of the policy used at session start to set initial configuration values.
Port-ID	The Port-ID used in the Local-TX-SCI.
Local-TxSCI	The MAC address of the physical interface concatenated with the 16-bit Port-ID.
Key Server Status	The key server: has value 'Y' for YES if the MKA session is the key server, otherwise, 'N' for NO.
CKN	Connectivity association key (CAK) name

This is sample output of the **show mka session detail** command:

```
Switch# show mka session detail
MKA Detailed Status for MKA Session
===================================
Status: SECURED - Secured MKA Session with MACsec
Local Tx-SCI..............  a80c.0dee.d702/0012
Interface MAC Address....  a80c.0dee.d702
MKA Port Identifier......  18
Interface Name...........  GigabitEthernet0/0/0.10
Audit Session ID.........
CAK Name (CKN)...........  123456780000000000000000000000000000000000000000000000000000000000000000
Member Identifier (MI)...  67266358A75EC8D235316DDA
Message Number (MN)......  103115
Authenticator............  NO
Key Server...............  YES
MKA Cipher Suite.........  AES-128-CMAC
Latest SAK Status........  Rx & Tx
Latest SAK AN............  3
Latest SAK KI (KN).......  67266358A75EC8D235316DDA00000044 (68)
Old SAK Status...........  No Rx, No Tx
Old SAK AN...............  2
Old SAK KI (KN)..........  RETIRED (67)
SAK Transmit Wait Time...  0s (Not waiting for any peers to respond)
SAK Retire Time..........  0s (No Old SAK to retire)
MKA Policy Name..........  *DEFAULT POLICY*
Key Server Priority......  0
Delay Protection.........  NO
Replay Protection........  YES
Replay Window Size.......  0
Confidentiality Offset...  0
Algorithm Agility........  80C201
SAK Cipher Suite.........  0080C20001000001 (GCM-AES-128)
MACsec Capability........  3 (MACsec Integrity, Confidentiality, & Offset)MACsec
```

```
Desired........... YES
# of MACsec Capable Live Peers............ 5
# of MACsec Capable Live Peers Responded.. 5
Live Peers List:
   MI                                                    MN            Rx-SCI (Peer)
        KS Priority

-----------------------------------------------------------------------------------------------------------

   75FB2095CBCF250C6C385A6D   146558      a80c.0dee.df02/0012   0
   CCD06CFE284D4D6B36DC5F7F  146557      a80c.0dee.df03/0013   0
   AEA06EB8B066448BC83CB6CF   146556      a80c.0dee.df04/0014   0
   533F8C5A0E528137E2C0EF5D    102959      a80c.0dee.de02/0012  0
   BD72C3DDFEACBE46E0E6389A  103025      a80c.0dee.de03/0013  0
Potential Peers List:
   MI                                                     MN            Rx-SCI (Peer)
          KS Priority

-----------------------------------------------------------------------------------------------------------
```

This is sample output of the **show mka session interface** command:

```
Switch# show mka session interface gigabitethernet1/0/25
Summary of All Currently Active MKA Sessions on Interface GigabitEthernet1/0/25.
Interface Peer-RxSCI          Policy-Name      Audit-Session-ID
Port-ID   Local-TxSCI         Key-Svr Status   CKN
================================================================================
Gi1/0/25  001b.2140.ec3c/0000 replay-policy    0A05783B0000001700448BA8
2         001e.bdfe.6d99/0002 YES     Secured  3808F996026DFB8A2FCEC9A88BBD0680
```

Related Commands

Command	Description
clear mka sessions	Clears all MKA sessions or clear MKA sessions on a port-ID, interface, or Local TX-SCI.
macsec	Enables MACsec on an interface.

show mka statistics

To display global MACsec Key Agreement (MKA) Protocol statistics and error counters, use the **show mka statistics** command in privileged EXEC mode.

show mka statistics [**interface***interface-id***port-id***port-id*] | [**local-sci***sci*] }

Syntax Description

interface *interface-id*	(Optional) Displays statistics for an MKA session on an interface. Only physical interfaces are valid.
port-id *port-id*	Displays a summary of active MKA sessions running on the interface with the specified port ID. To see the port ID, enter the show mka session or **show mka session interface** *interface-id* command. Port identifier values begin at 2 and monotonically increase for each new active session using a virtual port on the same physical interface.
local-sci *sci*	(Optional) Shows statistics for an MKA session identified by its Local TX-SCI. To determine the Local TX-SCI for a session, enter the show mka session detail command. The SCI must be 8 octets (16 hexadecimal digits) long.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0	This command was introduced.

Examples

This is an example of the **show mka statistics** command output:

```
Switch# show mka statistics
MKA Global Statistics
=====================
MKA Session Totals
   Secured..................... 32
   Reauthentication Attempts.. 31
   Deleted (Secured)........... 1
   Keepalive Timeouts......... 0
CA Statistics
   Pairwise CAKs Derived...... 32
   Pairwise CAK Rekeys........ 31
   Group CAKs Generated....... 0
   Group CAKs Received........ 0
SA Statistics
   SAKs Generated............. 32
   SAKs Rekeyed............... 31
   SAKs Received.............. 0
   SAK Responses Received..... 32
MKPDU Statistics
   MKPDUs Validated & Rx...... 580
      "Distributed SAK"..... 0
      "Distributed CAK"..... 0
   MKPDUs Transmitted......... 597
```

```
      "Distributed SAK"..... 32
      "Distributed CAK"..... 0
MKA Error Counter Totals
========================
Bring-up Failures................... 0
Reauthentication Failures.......... 0
SAK Failures
   SAK Generation................... 0
   Hash Key Generation.............. 0
   SAK Encryption/Wrap.............. 0
   SAK Decryption/Unwrap............ 0
CA Failures
   Group CAK Generation............. 0
   Group CAK Encryption/Wrap....... 0
   Group CAK Decryption/Unwrap..... 0
   Pairwise CAK Derivation......... 0
   CKN Derivation................... 0
   ICK Derivation................... 0
   KEK Derivation................... 0
   Invalid Peer MACsec Capability.. 2
MACsec Failures
   Rx SC Creation................... 0
   Tx SC Creation................... 0
   Rx SA Installation............... 0
   Tx SA Installation............... 0
MKPDU Failures
   MKPDU Tx......................... 0
   MKPDU Rx Validation.............. 0
   MKPDU Rx Bad Peer MN............. 0
   MKPDU Rx Non-recent Peerlist MN.. 0
```

Table 139: Table 0-7 show mka Global Statistics Output Fields (continued)

Field	Description
Reauthentications	Reauthentications from 802.1x.
Pairwise CAKs Derived	Pairwise secure connectivity association keys (CAKs) derived through EAP authentication.
Pairwise CAK Rekeys	Pairwise CAK rekeys after reauthentication.
Group CAKs Generated	Generated group CAKs while acting as a key server in a group CA.
Group CAKs Received	Received group CAKs while acting as a nonkey server member in a group CA.
SAK Rekeys	Secure association key (SAK) rekeys that have been initiated as key servers or received as nonkey server members.
SAKs Generated	Generated SAKs while acting as a key server in any CA.
SAKs Received	Received SAKs while acting as a nonkey server member in any CA.
MPDUs Validated & Rx	MACsec Key Agreement Protocol Data Units (MPDUs) received and validated.
MPDUs Transmitted	Transmitted MPDUs.

Related Commands

Command	Description
clear mka statistics	Clears all MKA statistics or those on a specified interface port-ID or Local TX-SCI.

show mls acl inconsistency

To display results from the Multi-Link Switching (MLS) Ternary Content Addressable Memory (TCAM) access check list (ACL) consistency checker, use the **show mls acl inconsistency** command in user EXEC or privileged EXEC mode.

show mls acl inconsistency [{**log** | **now**}] [**module** *module-number*]

Syntax Description

log	(Optional) Displays contents of the inconsistency log.
now	(Optional) Runs the consistency checker and displays results.
module *module-number*	(Optional) Restricts output to information about the specified module in your device. The value is 1 to 6.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
15.3(1)S	This command was introduced.

Usage Guidelines

Use this command to verify that the consistency checker is enabled and display the results of the consistency check. The output of this command is self explanatory.

Use this command with the **run** keyword to run a consistency check immediately after the command is issued and to displays the results.

Use this command with the **module** *module-number* keyword and argument combination to display inconsistencies for a specific module in your device.

Examples

```
Device# show mls acl inconsistency

Consistency Check                    : ON
Diagnostics Running                  : NO
Consistency Check Interval(seconds)  : 180
Consistency Check Count              : 4
Last Consistency Check At            : Oct 16 08:48:57.987
TCAM Entry Consistency Check Errors  : 0
TCAM Mask Consistency Check Errors   : 0
Result SRAM Consistency Check Errors : 0

Device# show mls acl inconsistency log

Consistency Check                    : ON
Diagnostics Running                  : NO
Consistency Check Interval(seconds)  : 180
Consistency Check Count              : 459
Last Consistency Check At            : Oct 17 07:32:30.874
TCAM Entry Consistency Check Errors  : 0
TCAM Mask Consistency Check Errors   : 0
Result SRAM Consistency Check Errors : 0
```

```
Device# show mls acl inconsistency now

Running consistency checker now ...
Finished consistency checking
TCAM Entry Consistency Check Errors        : 0
TCAM Mask Consistency Check Errors         : 0
Result SRAM Consistency Check Errors       : 0

Device# show mls acl inconsistency module 1
No forwarding engine in module 1
```

Related Commands

Command	Description
mls acl tcam consistency enable	Enables the MLS ACL TCAM consistency checker.

show mls rate-limit

To display information about the MLS rate limiter in the EXEC command mode, use the **show mls rate-limit** command.

show mls rate-limit [**usage**]

Syntax Description

usage	(Optional) Displays the feature that is used with the rate-limiter register.

Command Default

This command has no default settings.

Command Modes

EXEC

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17a)SX	The command output was changed to include hardware rate-limiting status.
12.2(17b)SXA	The command output was changed to display a hyphen (-) instead of an asterisk (*) to indicate that the multicast partial-SC rate limiter is disabled.
12.2(18)SXD	The command output was changed to display IPv6 information.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

In the command output, the rate-limit status could be one of the following:

- On indicates a rate for that particular case has been set.
- Off indicates that the rate-limiter type has not been configured, and the packets for that case are not rate limited.
- On/Sharing indicates a partic ular case (not manually configured) is affected by the configuration of another rate limiter belonging to the same sharing group.
- A hyphen indicates that the multicast partial-SC rate limiter is disabled.

In the command output, the rate-limit sharing indicates the following information:

- Whether sharing is static or dynamic
- Group dynamic sharing codes

The **show mls rate-limit usage** command displays the hardware register that is used by a rate-limiter type. If the register is not used by any rate-limiter type, Free is displayed in the output. If the register is used by a rate-limiter type, Used and the rate-limiter type are displayed.

Examples

This example shows how to display information about the rate-limit status:

```
Router# show mls rate-limit
Sharing Codes: S - static, D - dynamic
 Codes dynamic sharing: H - owner (head) of the group, g - guest of the group
   Rate Limiter Type       Status     Packets/s   Burst  Sharing
 ---------------------   ----------   ---------   -----  -------
         MCAST NON RPF   Off                  -       -     -
        MCAST DFLT ADJ   On              100000     100  Not sharing
      MCAST DIRECT CON   Off                  -       -     -
        ACL BRIDGED IN   Off                  -       -     -
       ACL BRIDGED OUT   Off                  -       -     -
           IP FEATURES   Off                  -       -     -
          ACL VACL LOG   On                2000       1  Not sharing
            MAC PBF IN   Off                  -       -     -
           CEF RECEIVE   Off                  -       -     -
             CEF GLEAN   Off                  -       -     -
      MCAST PARTIAL SC   On               100000     100  Not sharing
        IP RPF FAILURE   On                  100      10  Group:0 S
           TTL FAILURE   Off                  -       -     -
 ICMP UNREAC. NO-ROUTE   On                  100      10  Group:0 S
 ICMP UNREAC. ACL-DROP   On                  100      10  Group:0 S
          ICMP REDIRECT   Off                  -       -     -
           MTU FAILURE   Off                  -       -     -
       MCAST IP OPTION   Off                  -       -     -
       UCAST IP OPTION   Off                  -       -     -
           LAYER_2 PDU   Off                  -       -     -
            LAYER_2 PT   Off                  -       -     -
       LAYER_2 PORTSEC   Off                  -       -     -
     LAYER_2 MiniProto   Off                  -       -     -
      DHCP Snooping IN   Off                  -       -     -
     DHCP Snooping OUT   Off                  -       -     -
        ARP Inspection   Off                  -       -     -
             IP ERRORS   On                   100      10  Group:0 S
           CAPTURE PKT   Off                  -       -     -
            MCAST IGMP   Off                  -       -     -
 MCAST IPv6 DIRECT CON   Off                  -       -     -
 MCAST IPv6 ROUTE CNTL   Off                  -       -     -
 MCAST IPv6 *G M BRIDG   Off                  -       -     -
  MCAST IPv6 SG BRIDGE   Off                  -       -     -
  MCAST IPv6 DFLT DROP   Off                  -       -     -
 MCAST IPv6 SECOND. DR   Off                  -       -     -
  MCAST IPv6 *G BRIDGE   Off                  -       -     -
        MCAST IPv6 MLD   Off                  -       -     -
  IP ADMIS. ON L2 PORT   Off                  -       -     -
        MCAST IPv4 PIM   Off                  -       -     -
Router#
```

This example shows how to display information about the rate-limit usage:

```
Router # show mls rate-limit usage
Rate Limiter Type     Packets/s   Burst
                      ---------------------   ---------   -----
Layer3 Rate Limiters:
             RL# 0: Free                          -           -       -
             RL# 1: Free                          -           -       -
             RL# 2: Free                          -           -       -
             RL# 3: Free                          -           -       -
             RL# 4: Free                          -           -       -
             RL# 5: Used
                                  IP RPF FAILURE         100      10
                                ICMP UNREAC. NO-ROUTE    100      10
```

```
                          ICMP UNREAC. ACL-DROP         100      10
                                       IP ERRORS        100      10
             RL# 6: Used
                                   ACL VACL LOG        2000       1
             RL# 7: Used
                                 MCAST DFLT ADJ      100000     100
             RL# 8: Rsvd for capture                 -          -       -
Layer2 Rate Limiters:
             RL# 9: Reserved
             RL#10: Reserved
                               MCAST PARTIAL SC      100000     100
             RL#11: Free                             -          -       -
             RL#12: Free                             -          -       -
Router #
```

Related Commands

Command	Description
mls rate-limit multicast ipv4	Enables and sets the rate limiters for the IPv4 multicast packets.
mls rate-limit multicast ipv6	Configures the IPv6 multicast rate limiters.
mls rate-limit unicast acl	Enables and sets the ACL-bridged rate limiters.

show monitor event-trace crypto

To display event trace crypto information, use the **show monitor event-trace crypto** command in privileged EXEC mode.

show monitor event-trace crypto

Syntax Description

all	Displays all event traces in the buffer.
back	Displays trace events from this far back in the past.
clock	Displays trace events from a specific time and date.
from-boot	Displays trace events, in seconds, after the device boots.
ikev2	Displays IKEv2 Traces.
ipsec	Displays IPSEC Trace.
latest	Displays latest trace events since last display.
merged	Displays entries in all event traces sorted by time
PKI	Displays PKI Traces

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS 15.3T	This command was introduced.

Examples

The following is sample output from the **monitor event-trace crypto** command.

```
Need sample output
```

show monitor event-trace crypto ikev2

To display Internet Key Exchange Version 2 (IKEv2) trace information, use the **show monitor event-trace crypto ipsec** command in privileged EXEC mode.

show monitor event-trace crypto ikev2 {**error** | **event** | **exceptions**} {**all** | **back** *time* | **clock** *hh* **:** *mm* [{*daymonth*}] | **from-boot** [**seconds**] | **latest** | **parameters**} [*details*]

Syntax Description

error	Displays IKEv2 errors.
event	Displays IKEv2 events.
exception	Displays IKEv2 exceptions.
all	Displays all event traces in the buffer.
back *time*	Displays trace events from a specific time, specified in milliseconds, hours or minutes.
clock *hh***:***mm* [*day* | *month*]	Displays trace events from a specific time, day, and month.
from-boot [**seconds**]	Displays trace events, in seconds, after the device boots.
latest	Displays latest trace events since last display.
parameters	Displays trace parameters.
detail	Displays detailed information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.1	This command was introduced.

Usage Guidelines

Use this command to view trace information for IKEv2 errors, events, and exceptions.

Examples

The following is a sample output from the **show monitor event-trace crypto ipsec event all** command.

```
Device# show monitor event-trace crypto pki event all
```

show monitor event-trace crypto ikev2 exception

To display Internet Key Exchange Version 2 (IKEv2) trace information exception, use the **show monitor event-trace crypto ikev2 exception** command in privileged EXEC mode.

show monitor event-trace crypto ikev2 exception

Syntax Description

all	Displays all the traces in current buffer
back	Displays trace from this far back in the past.
clock	Displays trace events from a specific time, day, and month.
from-boot	Displays trace events, in seconds, after the device boots.
latest	Displays latest trace events since last display.
parameters	Displays trace parameters.
detail	Displays detailed information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.1	This command was introduced.

Usage Guidelines

Use this command to view trace information for IKEv2 trace events exceptions.

Examples

The following is a sample output from the **show monitor event-trace crypto ikev2 exception** command.

```
need sample output
```

show monitor event-trace crypto ipsec

To display IPsec trace information, use the **show monitor event-trace crypto ipsec** command in privileged EXEC mode.

show monitor event-trace crypto ipsec {**error** | **event** | **exceptions**} {**all** | **back** *time* | **clock** *hh* **:** *mm* [{*daymonth*}] | **from-boot** [**seconds**] | **latest** | **parameters**} [*details*]

Syntax Description

error	Displays IPsec errors.
event	Displays IPsec events.
exception	Displays IPsec exceptions.
all	Displays all event traces in the buffer.
back *time*	Displays trace events from a specific time, specified in milliseconds, hours or minutes.
clock *hh***:***mm* [*day* | *month*]	Displays trace events from a specific time, day, and month.
from-boot [**seconds**]	Displays trace events, in seconds, after the device boots.
latest	Displays latest trace events since last display.
parameters	Displays trace parameters.
detail	Displays detailed information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.1	This command was introduced.

Usage Guidelines

Use this command to view trace information for IPsec errors, events, and exceptions.

Examples

The following is a sample output from the **show monitor event-trace crypto ipsec event all** command.

```
Device# show monitor event-trace crypto pki event all
```

show monitor event-trace crypto pki

To display all the event trace information related to crypto PKI, use the **show monitor event-trace crypto pki** command in privileged EXEC mode.

show monitor event-trace crypto pki

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.1	This command was introduced.

Examples

The following is sample output from the **show monitor event-trace crypto pki** command.

```
Need sample output
```

show monitor event-trace crypto pki error all

To display all the error trace information for PKI events, use the **show monitor event-trace crypto pki error all** command in privileged EXEC mode.

show monitor event-trace crypto pki error all

Syntax Description

This command has no arguments or keywords.

Command Default

PKI event and error traces are enabled by default.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.1	This command was introduced.

Examples

The following is sample output from the **show monitor event-trace crypto pki error all** command when there is no route available to the server via VRF:

```
Router# show monitor event-trace crypto pki error all
 May 30 05:03:48.390: Trustpoint- client:Failed to connect socket via VRF: pki(No route to
 host).
```

show monitor event-trace crypto pki event all

To display all the event trace information related to PKI events, use the **show monitor event-trace crypto pki event all** command in privileged EXEC mode.

show monitor event-trace crypto pki event all

Syntax Description

This command has no arguments or keywords.

Command Default

PKI event and error traces are enabled by default.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.1	This command was introduced.

Examples

The following is sample output from the **show monitor event-trace crypto pki event all** command.

```
Router# show monitor event-trace crypto pki event all

May 30 05:40:07.700: All enrollment requests will be automatically granted.
May 30 05:40:48.745: Trustpoint- subca:Enrollment: SCEP
May 30 05:40:48.745: Trustpoint- subca:Client sending GetCACert request: GET
/cgi-bin/pkiclient.exe?operation=GetCACert&message=subca HTTP/1.0
User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Cisco PKI)
Host: 9.45.3.241


May 30 05:40:48.772: Trustpoint- subca:Client received CA certificate.
May 30 05:40:48.772: Trustpoint- subca:Sending GetCACaps request with msg = GET
/cgi-bin/pkiclient.exe?operation=GetCACaps&message=subca HTTP/1.0
User-Agent: Mozilla/4.0 (compatible; MSIE 5.0; Cisco PKI)
Host: 9.45.3.241


May 30 05:40:48.809: Capabilities received : GET NEXT CA CERT, RENEWAL, SHA1, SHA256, SHA384,
 SHA512,
May 30 05:40:58.827: Trustpoint- subca:A CA certificate has been installed
                     Issuer-name  : cn=RCA1 C=pki
                     Subject-name : cn=RCA1 C=pki
                     Serial-number: 02
                     End-date     : 2018-05-30T11:28:59Z
May 30 05:40:58.835: Trustpoint- subca:CA Certificate will expire in 0 Days 0 hours 18 mins
 1 secs at 2018-05-30T11:28:59Z.
                     Issuer-name  : cn=RCA1 C=pki
                     Subject-name : cn=RCA1 C=pki
                     Serial-number: 02
                     Auto-Renewal : Not Applicable
May 30 05:40:58.836: Trustpoint- subca:Manual enrollment for trustpoint
May 30 05:41:18.868: Trustpoint- subca:CA Certificate request is pending.
May 30 05:41:18.874: Trustpoint- subca:
                     CSR Fingerprint MD5 : 07DEF66E9023EB895E18594458890884
                     CSR Fingerprint SHA1: 9EE814AC715A427B49896FD5C0B32C009735D255
```

```
May 30 05:41:18.896: Trustpoint- subca:Client sending PKCSReq
May 30 05:41:18.934: Trustpoint- subca:Received pki message.
May 30 05:41:18.937: Trustpoint- subca:Client received CertRep - PENDING.
May 30 05:41:18.946: Trustpoint- subca:Client sending GetCertInitial request.
May 30 05:41:18.979: Trustpoint- subca:Received pki message.
May 30 05:41:18.982: Trustpoint- subca:Client received CertRep - PENDING.
May 30 05:42:18.982: Trustpoint- subca:Client sending GetCertInitial(poll) request.
May 30 05:42:19.012: Trustpoint- subca:Received pki message.
May 30 05:42:19.014: Trustpoint- subca:Client received CertRep - PENDING.
May 30 05:43:19.014: Trustpoint- subca:Client sending GetCertInitial(poll) request.
May 30 05:43:19.045: Trustpoint- subca:Received pki message.
May 30 05:43:19.047: Trustpoint- subca:Client received CertRep - GRANTED.
May 30 05:43:19.051: Trustpoint- subca:SUBCA/RA certificate has been installed under
                       Issuer-name  : cn=RCA1 C=pki
                       Subject-name : cn=subca C=pki
                       Serial-number: 03
                       End-date     : 2018-05-30T11:22:28Z
May 30 05:43:19.052: Trustpoint- subca:SUBCS Certificate will expire in 0 Days 0 hours 9
mins 9 secs at 2018-05-30T11:22:28Z.
                       Issuer-name  : cn=RCA1 C=pki
                       Subject-name : cn=subca C=pki
                       Serial-number: 03
                       Auto-Renewal : Not Applicable
May 30 05:43:19.261: Certificate Server is now enabled.
```

show monitor event-trace crypto pki event internal all

To display the internal event trace information for PKI events, use the **show monitor event-trace crypto pki event internal all** command in privileged EXEC mode.

show monitor event-trace crypto pki event internal all

Syntax Description

This command has no arguments or keywords.

Command Default

PKI event internal traces are disabled by default.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.1	This command was introduced.

Examples

The following is sample output from the **show monitor event-trace crypto pki event internal all** command:

```
Router# show monitor event-trace crypto pki event internal all
Jun 20 06:32:09.839: Trustpoint- client:refcount after increment = 1
Jun 20 06:32:09.843: Trustpoint- client:refcount after decrement = 0
Jun 20 06:32:09.843: Trustpoint- client:refcount after increment = 1
Jun 20 06:32:09.849: Trustpoint- client:refcount after decrement = 0
Jun 20 06:32:09.850: Trustpoint- client:refcount after increment = 1
Jun 20 06:32:09.851: Trustpoint- client:refcount after decrement = 0
Jun 20 06:32:09.851: Trustpoint- client:refcount after increment = 1
Jun 20 06:32:09.857: Trustpoint- client:refcount after decrement = 0
Jun 20 06:32:16.058: Trustpoint- client:refcount after increment = 1
Jun 20 06:32:16.169: Trustpoint- client:refcount after decrement = 0
Jun 20 06:32:16.193: Trustpoint- client:refcount after increment = 1
Jun 20 06:32:16.195: Trustpoint- client:refcount after decrement = 0
Jun 20 06:32:16.195: Trustpoint- client:refcount after increment = 1
Jun 20 06:32:16.206: Trustpoint- rootca1:Enrollment request 1 locked. refcount = 1
Jun 20 06:32:16.461: Trustpoint- rootca1:Enrollment request 1 locked. refcount = 0
```

show monitor event-trace dmvpn

To display Dynamic Multipoint VPN (DMVPN) trace information, use the **show monitor event-trace dmvpn** command in privileged EXEC mode.

show monitor event-trace dmvpn [{**merged** | **nhrp** {**event** | **error** | **exception**} | **tunnel** [**parameters**]}] {**all** | **back** *time* | **clock** *hh* **:** *mm* [{*day month* | *month day*}] | **from-boot** [*boot-time*] | **latest**} [**detail**]

Syntax Description

merged	(Optional) Displays all traces in the current buffer.
nhrp	(Optional) Displays Next Hop Resolution Protocol (NHRP) traces.
event	(Optional) Displays NHRP event traces.
error	(Optional) Displays NHRP error traces.
exception	(Optional) Displays NHRP exception traces.
tunnel	(Optional) Displays tunnel events.
parameters	(Optional) Displays parameters of the trace.
all	Displays all traces in the current buffer.
back *time*	Displays traces since the specified time. Time can be specified as minutes (*mmm*) or in hour:minute (*hh* **:** *mm*) format.
clock *hh* **:** *mm*	Displays trace from the specified time.
day	(Optional) Day in a month.
month	(Optional) Month of a year.
from-boot	Displays trace after the specified time after boot.
boot-time	(Optional) Time specified to wait to display trace after boot.
latest	Displays the latest trace events since the previous display.
detail	(Optional) Displays detailed trace information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(4)M	This command was introduced.

Usage Guidelines

You can use the **show monitor event-trace dmvpn** command to verify DMVPN event tracing.

This command displays all the tunnel events, including the DMVPN tunnel events and the non-DMVPN tunnel events.

Note The **show monitor event-trace dmvpn** command output displays all tunnel events. You dare not able to filter only the DMVPN tunnel information in the display.

Examples

The following is sample output from the **show monitor event -trace dmvpn nhrp exception all** command. The fields in the display are self-explanatory.

```
Router# show monitor event-trace dmvpn nhrp exception all

ev_type : NHS-UP trace_type: NHRP-EXCEPTION
*May 17 05:00:09.999: NHRP-EXCEPTION:NHS-UP  Tunnel0 : NHS UP,
(VPN DEST )10.0.0.251 -> (NBMA DEST)172.16.0.251,
(VPN SRC)10.0.0.1 -> (NBMA SRC)172.16.0.1
ev_type : NHS-DOWN trace_type: NHRP-EXCEPTION
*May 17 05:00:09.999: NHRP-EXCEPTION:NHS-DOWN  Tunnel0 : NHS DOWN,
(VPN DEST )10.0.0.251 -> (NBMA DEST)172.16.0.251,
(VPN SRC)10.0.0.1 -> (NBMA SRC)172.16.0.1, reason: External
ev_type : NHC-UP trace_type: NHRP-EXCEPTION
*May 17 05:00:09.999: NHRP-EXCEPTION:NHC-UP  Tunnel0 : NHC UP,
(VPN DEST )10.0.0.251 -> (NBMA DEST)172.16.0.251,
(VPN SRC)10.0.0.1 -> (NBMA SRC)172.16.0.1
ev_type : NHC-DOWN trace_type: NHRP-EXCEPTION
*May 17 05:00:09.999: NHRP-EXCEPTION:NHC-DOWN  Tunnel0 : NHC DOWN,
(VPN DEST )10.0.0.251 -> (NBMA DEST)172.16.0.251,
(VPN SRC)10.0.0.1 -> (NBMA SRC)172.16.0.1, reason: External
ev_type : NHP-UP trace_type: NHRP-EXCEPTION
*May 17 05:00:09.999: NHRP-EXCEPTION:NHP-UP  Tunnel0 : NHP UP,
(VPN DEST )10.0.0.251 -> (NBMA DEST)172.16.0.251,
(VPN SRC)10.0.0.1 -> (NBMA SRC)172.16.0.1
ev_type : NHP-DOWN trace_type: NHRP-EXCEPTION
*May 17 05:00:09.999: NHRP-EXCEPTION:NHP-DOWN  Tunnel0 : NHP DOWN,
(VPN DEST )10.0.0.251 -> (NBMA DEST)172.16.0.251,
(VPN SRC)10.0.0.1 -> (NBMA SRC)172.16.0.1, reason: External
ev_type : NHRP-RATE_LIMIT trace_type: NHRP-EXCEPTION
*May 17 05:00:09.999: NHRP-EXCEPTION:NHRP-RATE_LIMIT  Tunnel0 : Max-send Quota of
10000pkts/500sec exceeded
ev_type : NHS-RECOVERY-NHS-STATE trace_type: NHRP-EXCEPTION
*May 17 05:00:09.999: NHRP-EXCEPTION:NHS-RECOVERY-NHS-STATE  NHS recovery event string
```

Related Commands

Command	Description
monitor event-trace dmvpn	Monitors and controls DMVPN traces.

show monitor event-trace gdoi

To display information about Group Domain of Interpretation (GDOI) event traces, use the **show monitor event-trace gdoi** command in privileged EXEC mode.

show monitor event-trace gdoi [**merged**] {**all** | **back** *trace-duration* | **clock** *time* [*day month*] | **from-boot** [*seconds*] | **latest**} [**detail**]

Syntax Description

merged	(Optional) Displays entries in all event traces sorted by time.
all	(Optional) Displays all traces in the current buffer.
back	(Optional) Displays trace over a specified duration from the present to the past.
trace-duration	(Optional) Duration of trace (in minutes or in hours:minutes format). The range is 0 to 4,294,967,295 minutes (or 0 hours and 0 minutes to 4,294,967,295 hours and 59 minutes when specifying hours and minutes).
clock	(Optional) Displays trace from a specific time and date.
time	(Optional) Time from which to show trace (in hours:minutes format).
day	(Optional) Day of the month. The range is 1 to 31.
month	(Optional) Month of the year. Eligible values are January, February, March, April, May, June, July, August, September, October, November, and December.
from-boot	(Optional) Displays trace from a specific number of seconds after booting.
seconds	(Optional) Time after boot in seconds. The range is 0 to 932221.
latest	(Optional) Displays latest trace events since the last display.
detail	(Optional) Displays detailed trace information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(3)T	This command was introduced.
Cisco IOS XE Release 3.8S	This command was integrated into Cisco IOS XE Release 3.8S.

Examples

The following is sample stack traces from the **show monitor event-trace gdoi rekey** command.

```
Device# show monitor event-trace gdoi rekey

Event[1] Oct 19 18:02:03.055: %GDOI-5-GM_RECV_REKEY: Received Rekey for group gdoigroup1
from 5.5.90.1 to 228.10.10.10 with seq # 2
 -Traceback= 0x36D90 0xDECBC 0x3CC53 0xFC2C320 0xDFC245
```

```
r100#sh monitor event-trace gdoi exit
Event[1] Oct 19 18:02:03.055: Coop Peer not reachable, Peer marked dead.
 -Traceback= 0x3CB04 0xFD2C49 0xFD2C493C
 Event[2] Oct 19 18:02:03.055:  No IKE SA found to peer
 local 16.0.0.1/0 remote 16.0.0.2/500 fvrf 0x0 ivrf 0x0 for SPI 0x120DCC0
 -Traceback= 0x35E90 0xC0CBC 0x3BB54 0xFD2C49 0xFD2C493C
```

Related Commands

Command	Description
monitor event-trace gdoi	Configures event tracing for the GDOI software subsystem component.
monitor event-trace gdoi (privileged EXEC)	Configures event tracing for the GDOI software subsystem component.

show object-group

To display information about configured network or service object groups used in object group access control lists (OGACLs) or user object group information, containing security group or nested group object information, for the class map in a Cisco TrustSec (CTS) Security Group Access (SGA) Zone-Based Policy firewall (ZBPF), use the **show object-group** command in user EXEC or privileged EXEC mode.

show object-group [{*object-group-name*}]

Syntax Description

name	(Optional) Name of the object group, security group, or group object for which information will be displayed.

Command Default

Information is displayed for all object groups.

Command Modes

Privileged EXEC (#) User EXEC (>)

Command History

Release	Modification
12.4(20)T	This command was introduced.
15.2(1)S	This command was introduced in Cisco IOS Release 15.2(1)S.
Cisco IOS XE Release 3.5	This command was introduced in Cisco IOS XE Release 3.5.

Examples

The following example displays **show object-group** command output of network and service object groups in an OGACL configuration:

```
Router# show object-group
Network object group auth_proxy_acl_deny_dest
 host 171.68.225.134
Service object group auth_proxy_acl_deny_services
 tcp eq www
 tcp eq 443
Network object group auth_proxy_acl_permit_dest
 10.34.250.96 255.255.255.224
 171.68.0.0 255.252.0.0
 172.16.0.0 255.240.0.0
 128.107.0.0 255.255.0.0
 10.0.0.0 255.0.0.0
 64.100.0.0 255.253.0.0
 64.104.0.0 255.255.0.0
 144.254.0.0 255.255.0.0
 161.44.0.0 255.255.0.0
 192.168.0.0 255.255.0.0
Service object group auth_proxy_acl_permit_services
 tcp eq www
 tcp eq 443
```

The table below describes the significant fields shown in the command output.

Table 140: show object-group Field Descriptions (OGACL Configuration)

Field	Description
Network object group auth_proxy_acl_deny_dest	Name of the network object group.
host 171.68.225.134	IP address of the host object.
Network object group auth_proxy_acl_deny_services	Name of the service object group.
tcp eq www tcp eq 443	TCP port types.
10.34.250.96 255.255.255.224	Network address and network mask of the subnet object.

The following example displays **show object-group** command output that shows user object group information for the class map in a CTS SGA ZBPF configuration:

```
Router# show object-group

User object group objsgt1
 security-group 120

User object group objsgt2
 group-object objsgt1
```

The table below describes the significant fields shown in the command output.

Table 141: show object-group Field Descriptions (CTS SGA ZBPF Configuration)

Field	Description
User object group	Name of the object group used to identify traffic coming from a specific user or endpoint in the CTS SGA ZBPF.
security-group	The securtiy group, identified by its Security Group Tag (SGT) identification number, that belongs to a user object group in the CTS SGA ZBPF.
group-object	The nested reference to a type of user group within an object group in the CTS SGA ZBPF.

Related Commands

Command	Description
debug object-group event	Enables debug messages for object-group events.
deny	Sets conditions in a named IP access list or OGACL that will deny packets.
group-object	Specifies a nested reference to a type of user group.
ip access-group	Applies an ACL or OGACL to an interface or a service policy map.
ip access-list	Defines an IP access list or OGACL by name or number.

Command	Description
match group-object security	Matches traffic from a user in the security group.
object-group network	Defines network object groups for use in OGACLs.
object-group security	Creates an object group to identify traffic coming from a specific user or endpoint.
object-group service	Defines service object groups for use in OGACLs.
permit	Sets conditions in a named IP access list or OGACL that will permit packets.
security-group	Specifies the membership of the security group for an object group.
show ip access-list	Displays the contents of IP access lists or OGACLs.

show parameter-map type consent through show users

show parameter-map type consent

To display consent parameter map information, use the **show parameter-map type consent**command in privileged EXEC mode.

show parameter-map type consent [{*parameter-map-name* | **default**}]

Syntax Description

parameter-map-name	(Optional) Name of the parameter map.
default	(Optional) Specifies default consent parameter map information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(15)T	This command was introduced.
12.4(20)T	The command was modified. The *parameter-map-name* argument was added.

Examples

The following is sample output from the **show parameter-map type consent**command. The fields are self-explanatory.

```
Router# show parameter-map type consent
parameter-map type consent map1
    Syslog : Enabled
    File download time(in minutes) : 456
    Number of Accepted Users : 0
    Number of Denied Users : 0
```

show parameter-map type inspect

To display user-configured or default inspect-type parameter maps, use the **show parameter-map type inspect** command in privileged EXEC mode.

show parameter-map type inspect [{*parameter-map-name* | **default** | **global**}]

Syntax Description

parameter-map-name	(Optional) Name of the parameter map.
default	(Optional) Displays the default inspect-type parameter-map values. **Note** Use this keyword when no parameter map is attached to the inspect action.
global	(Optional) Displays the global inspect type parameter map values.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(6)T	This command was introduced.
15.1(1)T	This command was modified. The **global** keyword was added.
Cisco IOS XE Release 3.4S	This command was modified. Support for General Packet Radio Service (GPRS) Tunneling Protocol (GTP) was added.
Cisco IOS XE Release 3.9S	This command was modified. The *parameter-map-name* argument was added.
Cisco IOS XE Release 3.11S	This command was modified. The command output was modified to display the number of simultaneous packets per flow.
Cisco IOS XE Release 3.13S	This command was modified. The command output was modified to display the Locator/ID Separation Protocol (LISP) inner-packet inspection information.
Cisco IOS XE Release 3.14S	This command was modified. The command output was modified to display the Network-Based Application Recognition (NBAR) information.

Usage Guidelines

When the **nbar-classify** command is configured, the output of **show parameter-map type inspect global** displays this information.

Examples

The following is sample output from the **show parameter-map type inspect** command. The fields in the output are self-explanatory.

```
Device# show parameter-map type inspect

 audit-trail off
 alert on
 max-incomplete low 2147483647
 max-incomplete high 2147483647
 one-minute low 2147483647
```

```
 one-minute high 2147483647
 udp idle-time 30
 icmp idle-time 10
 dns-timeout 5
 tcp idle-time 3600
 tcp finwait-time 5
 tcp synwait-time 30
 tcp max-incomplete host 4294967295 block-time 0
 tcp window scaling enforcement loose off
 sessions maximum 2147483647
 sessions packet default
```

The following is sample output from the **show parameter-map type inspect** *parameter-map-name* command. The fields in the output are self-explanatory.

```
Device# show parameter-map type inspect pmap1

parameter-map type inspect pmap1
  log dropped-packet off
  audit-trail on
  alert on
  max-incomplete low  unlimited
  max-incomplete high unlimited
  one-minute low  unlimited
  one-minute high unlimited
  sessions rate low  unlimited
  sessions rate high unlimited
  sessions packet default
  udp idle-time 30 ageout-time 30
  udp halfopen idle-time 30000 ms ageout-time 30000 ms
  icmp idle-time 50 ageout-time 50
  dns-timeout 5
  tcp window scaling enforcement loose off
  tcp idle-time 3600 ageout-time 3600
  tcp finwait-time 1 ageout-time 1
  tcp synwait-time 30 ageout-time 30
  tcp half-open on, half-close on, idle on
  tcp max-incomplete host unlimited block-time 0
  sessions maximum 3000
  gtp permit error off
  gtp  request-queue 40000
  gtp  tunnel-limit 40000
  gtp  gsn timeout 30
  gtp  pdp-context timeout 300
  gtp  request-queue timeout 60
  gtp  signaling timeout 30
  gtp  tunnel timeout 60
```

The following is sample output from the **show parameter-map type inspect default** command. The fields in the output are self-explanatory.

```
Device# show parameter-map type inspect default

 parameter-map type inspect default values
  log dropped-packet off
  audit-trail off
  alert on
  max-incomplete low  unlimited
  max-incomplete high unlimited
  one-minute low  unlimited
  one-minute high unlimited
  sessions rate low  unlimited
  sessions rate high unlimited
```

```
 sessions packet default
 udp idle-time 30 ageout-time 30
 udp halfopen idle-time 30000 ms ageout-time 30000 ms
 icmp idle-time 10 ageout-time 10
 dns-timeout 5
 tcp idle-time 3600 ageout-time 3600
 tcp finwait-time 1 ageout-time 1
 tcp synwait-time 30 ageout-time 30
 tcp max-incomplete host unlimited block-time 0
 tcp window scaling enforcement loose off
 sessions maximum unlimited
 gtp permit error off
 gtp  request-queue 40000
 gtp  tunnel-limit 40000
 gtp  gsn timeout 30
 gtp  pdp-context timeout 30
 gtp  request-queue timeout 60
 gtp  signaling timeout 30
 gtp  tunnel timeout 60
```

The following is sample output from the **show parameter-map type inspect global** command. The fields in the output are self-explanatory.

```
Device# show parameter-map type inspect global

alert on
 sessions maximum 2147483647
 waas disabled
 l2-transparent dhcp-passthrough disabled
 log dropped-packets disabled
 log summary disabled
 max-incomplete low 2147483647
 max-incomplete high 2147483647
 one-minute low 2147483647
 one-minute high 2147483647
 vrf vrf2 inspect vrf-default
 lisp inner-packet-inspection
 exporter not-configured
 nbar-classify
```

Related Commands

Command	Description
parameter-map type inspect	Configures an inspect-type parameter map for connecting thresholds, timeouts, and other parameters pertaining to the **inspect** action.
lisp inner-packet-inspection	Enables LISP inner-packet inspection.

show parameter-map type inspect-global

To display global inspect-type parameter map information, use the **show parameter-map type inspect-global** command in user EXEC or privileged EXEC mode.

show parameter-map type inspect-global [{**gtp**}]

Syntax Description

gtp	(Optional) Displays information about the General Packet Radio Service (GPRS) tunneling protocol (GTP).

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.5S	This command was introduced.
Cisco IOS XE Release 3.7S	This command was modified. The **gtp** keyword was added.
Cisco IOS XE Release 3.9S	This command was modified. The output was enhanced to display GTP and GTPv2 configuration.
Cisco IOS XE Release 3.13S	This command was modified. The output was enhanced to display Locator ID Separation Protocol (LISP) inner packet inspection information.

Usage Guidelines

The command output displays all configured parameters and their values and all unconfigured parameters with their box-level default values. (Box refers to the entire firewall session table.)

Examples

The following is sample output from the **show parameter-map type inspect-global** command:

```
Device# show parameter-map type inspect-global

parameter-map type inspect-global
  log dropped-packet off
  alert on
  aggressive aging disabled
  lisp inner-packet-inspection
  syn_flood_limit  unlimited
  tcp window scaling enforcement loose off
  max incomplete unlimited  aggressive aging disabled
  max_incomplete TCP unlimited
  max_incomplete UDP unlimited
  max_incomplete ICMP unlimited
  application-inspect all
  vrf default inspect vrf-default
  vrf vrf2 inspect vrf-default
  vrf vrf3 inspect vrf-defautl
```

The following table describes the fields shown in the display.

Table 142: show parameter-map type inspect-global Field Descriptions

Field	Description
log dropped-packet	Debugging message log of dropped packets is not enabled. If you configure the **log** command in parameter-map type inspect configuration mode, a log of dropped packets is displayed.
alert	Stateful packet inspection of alert messages is on. Valid values are on and off.
aggressive aging	Aggressive aging of half-opened firewall sessions. A half-opened session is a session that has not reached the established state.
lisp inner-packet-inspection	LISP inner-packet packet inspection is enabled.
syn_flood_limit	TCP synchronization (SYN) flood rate limit. When the configured maximum limit is reached, the TCP SYN cookie protection is triggered.
max_incomplete	Maximum half-opened session limit.
max_incomplete TCP	Maximum half-opened TCP connection limit.
max_incomplete UDP	Maximum half-opened UDP connection limit.
max_incomplete ICMP	Maximum half-opened Internet Control Message Protocol (ICMP) connection limit.
vrf default	Default VRF is bound to the inspect-VRF parameter map.

The following is sample output from the **show parameter-map type inspect-global gtp** command:

```
Device# show parameter-map type inspect-global gtp

parameter-map type inspect global-gtp
  gtp request-queue 40000 (default)
  gtp tunnel-limit 40000 (default)
  gtp pdp-context timeout 351
  gtp request-queue timeout 2167
  permit-error Disable (default)
  gtp-in-gtp blocking Disable (default)
  gtpv2 request-queue 40000 (default)
  gtpv2 tunnel-limit 40000 (default)
  gtpv2 echo-rate-limit 10 (default)
```

The following table describes the fields shown in the display.

Table 143: show parameter-map type inspect-global gtp Field Descriptions

Field	Description
gtp request-queue	Displays the number of GTP requests that are queued to wait for a response.
gtp tunnel-limit	Displays the number of GTP tunnels that can be configured.

Field	Description
gtp pdp-context timeout	Displays the timeout, in minutes, for inactive Packet Data Protocol (PDP) contexts.
gtp request-queue timeout	Displays the timeout, in seconds, for inactive request queues.
permit-error	Displays the permissible errors. By default, the permit-error is disabled.
gtpv2 request-queue	Displays the number of GTP requests for GTPv2 protocol that are queued to wait for a response.
gtpv2 tunnel-limit	Displays the number of GTP tunnels that can be configured for gtpv2 protocol.

Related Commands

Command	Description
parameter-map type inspect-global	Configures a global parameter map.
lisp inner-packet-inspection	Enables LISP inner-packet inspection.

show parameter-map type inspect-vrf

To display information about the configured inspect VPN Routing and Forwarding (VRF) type parameter map, use the **show parameter-map type inspect-vrf** command in user EXEC or privileged EXEC mode.

show parameter-map type inspect-vrf [{*name* | **default**}]

Syntax Description

name	(Optional) Name of the inspect VRF type parameter map.
default	(Optional) Specifies the default inspect VRF type parameter map.

Command Default

This command has no default settings.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.3S	This command was introduced.

Examples

The following is sample output from the **show parameter-map type inspect-vrf** command:

```
Router# show parameter-map type inspect-vrf vpmap01
  VRF: vrf001, Parameter-Map: vpmap01
       total_session_cnt: 3500
       exceed_cnt:        40
       tcp_half_open_cnt: 3520
       syn_exceed_cnt:    40
```

The table below describes the significant fields shown in the display.

Table 144: show parameter-map type inspect-vrf Field Descriptions

Field	Description
total_session_cnt	Total session count.
exceed_cnt	Number of sessions that exceeded the configured session count.
tcp_half_open_cnt	TCP half-open sessions configured for each VRF. When the configured session limit is reached, the TCP synchronization (SYN) cookie verifies the source of the half-open TCP sessions before creating more sessions. A TCP half-open session is a session that has not reached the established state.
syn_exceed_count	Number of SYN packets that exceeded the configured SYN flood rate limit.

Related Commands

Command	Description
parameter-map type inspect-vrf	Configures an inspect VRF type parameter map.

show parameter-map type inspect-zone

To display information about the configured inspect zone-type parameter map, use the **show parameter-map type inspect-zone** command in user EXEC or privileged EXEC mode.

show parameter-map type inspect-zone [{*name* | **default**}]

Syntax Description

name	(Optional) Name of the inspect zone-type parameter map.
default	(Optional) Specifies the default inspect zone-type parameter map.

Command Default

This command has no default settings.

Command Modes

User EXEC (>)
Privileged EXEC(#)

Command History

Release	Modification
Cisco IOS XE Release 3.3S	This command was introduced.

Examples

The following is sample output from the **show parameter-map type inspect-zone** command:

```
Router# show parameter-map type inspect-zone zone-pmap

parameter-map type inspect-zone zone-pmap
 tcp syn-flood-rate 400
 max-destination 10000
```

The table below describes the fields shown in the display.

Table 145: show parameter-map type inspect-zone Field Descriptions

Field	Description
parameter-map type inspect-zone	Name of the inspect zone-type parameter map.
tcp syn-flood-rate	TCP synchronization (SYN) flood rate limit. When the configured maximum packet rate is reached, the TCP SYN cookie protection is triggered.
max-destination	Maximum number of destinations that a firewall can track.

Related Commands

Command	Description
parameter-map type inspect-zone	Configures an inspect zone-type parameter map.

show parameter-map type ooo global

To display Out-of-Order (OoO) global parameter-map information, use the **show parameter-map type ooo global** command in privileged EXEC mode.

show parameter-map type ooo global

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

The output of the **show parameter-map type ooo global** command displays configurations related to OoO packet processing. If you do not configure the **parameter-map type ooo global** command, the output of the **show parameter-map type ooo global** command displays default values of the OoO packet-processing parameters.

Examples

The following is sample output from the **show parameter-map type ooo global** command:

```
Device# show parameter-map type ooo global

 parameter-map type ooo global
   tcp reassembly timeout 5
   tcp reassembly queue length 16
   tcp reassembly memory limit 1024
   tcp reassembly alarm off
```

The following table describes the fields shown in the display.

Table 146: show parameter-map type ooo global Field Descriptions

Field	Description
tcp reassembly timeout	Timeout, in seconds, for OoO-TCP queues.
tcp reassembly queue length	Length of the OoO queues.
tcp reassembly memory limit	Limit of the OoO buffer size.
tcp reassembly alarm	Indicates if alert messages for TCP sessions are enabled. Valid values are on and off.

Related Commands

parameter-map type ooo global	Configures an OoO global parameter map for all firewall policies.
tcp reassembly	Changes the default parameters for OoO queue processing of TCP sessions.
tcp reassembly memory limit	Specifies the limit of the OoO queue size for TCP sessions.

show parameter-map type protocol-info

To display protocol parameter map information, use the **show parameter-map type protocol-info**command in privileged EXEC mode.

show parameter-map type protocol-info [{*parameter-map-name* [**dns-cache**] | **dns-cache** | **msrpc** | **zone-pair** *zone-pair-name* | **stun-ice** [*parameter-map-name*]}]

Syntax Description

parameter-map-name	(Optional) Name of the parameter map.
dns-cache	(Optional) Displays the protocol information about the Domain Name System (DNS) cache.
msrpc	(Optional) Displays the protocol information about the Microsoft Remote Procedure Call (MSRPC) parameter map.
zone-pair *zone-pair-name*	(Optional) Specifies the name of the zone pair.
stun-ice	(Optional) Displays the protocol information of Session Traversal Utilities for Network Address Translation (NAT) and Interactive Connectivity Establishment (STUN-ICE). STUN is an Internet standards-track suite of methods, including a network protocol, used in NAT traversal for applications of real-time voice, video, messaging, and other interactive IP communications. ICE is a technique used in computer networking involving NATs in Internet applications of VoIP, peer-to-peer communications, video, instant messaging, and other interactive media. In such applications, NAT traversal is an important component to facilitate communications involving hosts on private network installations, which often are located behind firewalls.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(11)T	This command was introduced.
12.4(22)T	The command was modified. The **stun-ice** keyword was added.
15.1(4)M	This command was modified. The **msrpc** keyword was added.

Examples

The following is sample output from the **show parameter-map type protocol-info** command. The fields are self-explanatory.

```
Router# show parameter-map type protocol-info
parameter-map type protocol-info map2
  server ip 192.168.1.1
```

Related Commands

Command	Description
parameter-map type protocol-info	Creates or modifies a protocol-specific parameter map and enters parameter-map type configuration mode.

show parameter-map type regex

To display regular expression parameter-map information, use the **show parameter-map type regex** command in privileged EXEC mode.

show parameter-map type regex[{*parameter-map-name*}]

Syntax Description

parameter-map-name	(Optional) Name of the parameter map.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(11)T	This command was introduced.
Cisco IOS XE Release 3.2S	This command was integrated into Cisco IOS XE Release 3.2S.

Examples

The following is sample output from the **show parameter-map type regex** command. The output fields are self-explanatory.

```
Router# show parameter-map type regex

parameter-map type regex map3
 pattern x*y
```

Related Commands

Command	Description
parameter-map type regex	Configures a parameter-map type to match a specific traffic pattern.

show parameter-map type trend-global

To display the parameter map for the global parameters for a Trend Micro URL filtering policy, use the **show parameter-map type trend-global** command in privileged EXEC mode.

show parameter-map type trend-global [*parameter-map-name*] [**default**]

Syntax Description

parameter-map-name	(Optional) The name of the parameter map for which to display parameters.
default	(Optional) Specifies that the default values for the global Trend Micro filtering parameters be displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(15)XZ	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use the **show parameter-map type trend-global**command to display the global parameters for Trend Micro URL filtering policies.

Examples

The following is sample output from the **show parameter-map type trend-global default**command:

```
Router# show parameter-map type trend-global
 default
parameter-map type trend-global default values
   server trps.trendmicro.com http-port 80 https-port 443 retrans 3 timeout 60
   alert on
   cache-size 256 KB
   cache-lifetime 24
```

The following is sample output from the **show parameter-map type trend-global**command when the server name and maximum cache size have been specified in the parameter map Global-Parameters:

```
Router# show parameter-map type trend-global
 Global-Parameters

parameter-map type trend-global Global-Parameters
   server trps1.example.com http-port 80 https-port 443 retrans 3 timeout 60
   alert on
   cache-size 300 KB
   cache-lifetime 24
```

Related Commands

Command	Description
show parameter-map type urlfpolicy	Displays the parameters for a URL filtering policy.

show parameter-map type urlf-glob

To display the parameter maps for local URL filtering, use the **show parameter-map type urlf-glob** command in privileged EXEC mode.

show parameter-map type urlf-glob [*parameter-map-name*]

Syntax Description

parameter-map-name	(Optional) Name of the URL filtering parameter map to display.

Command Default

The parameter maps for all local URL filtering policies are displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(15)XZ	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use the **show parameter-map type urlf-glob** command to display the parameter maps for local URL filtering policies.

Examples

The following is sample output from the **show parameter-map type urlf-glob**command when two parameter maps for local URL filtering have been configured:

```
Router# show parameter-map type urlf-glob

parameter-map type urlf-glob trusted-domain-param
 pattern www.example.com
 pattern *.example1.com
parameter-map type urlf-glob untrusted-domain-param
 pattern www.example3.com
 pattern *.example4.com
```

Related Commands

Command	Description
show parameter-map type trend-global	Displays the global parameters for a Trend Micro URL filtering policy.
show parameter-map type urlfpolicy	Displays the parameters for a URL filtering policy.

show parameter-map type urlfilter

Note Effective with Cisco IOS Release 12.4(15)XZ, the **show parameter-map type urlfilter** command is not available in Cisco IOS software.

To display user-configured or default URL filter type parameter maps, use the **show parameter-map type urlfilter**command in privileged EXEC mode.

show parameter-map type urlfilter [**default**]

Syntax Description

default	(Optional) Displays the default urlfilter parameter map values. **Note** If this keyword is not issued, user-configured parameter maps will be displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.4(15)XZ	This command was removed.

Examples

The following example shows sample output from the **show parameter-map type urlfilter** command:

```
Router# show parameter-map type urlfilter
 parameter-map type urlfilter default values
  urlf-server-log off
  audit-trail off
  alert on
  max-request 1000
  max-resp-pak 200
  source-interface default
  allow-mode off
  cache 5000
```

The following example shows sample output from the **show parameter-map type urlfilter default**command:

```
Router# show parameter-map type urlfilter default
parameter-map type urlfilter default values
 urlf-server-log off
 audit-trail off
 alert on
 max-request 1000
 max-resp-pak 200
 source-interface default
 allow-mode off
```

```
cache 5000
```

show parameter-map type urlfpolicy

To display the parameter maps associated with a URL filtering policy, use the **show parameter-map type urlfilter**command in privileged EXEC mode.

show parameter-map type urlfpolicy {**local** | **trend** | **n2h2** | **websense**} [*param-map-name*] [**default**]

Syntax Description

local	Specifies that the parameters for local URL filtering policies be displayed.
trend	Specifies that the parameters for Trend Micro URL filtering policies be displayed.
n2h2	Specifies that the parameters for SmartFilter URL filtering policies be displayed.
websense	Specifies that the parameters for Websense URL filtering policies be displayed.
param-map-name	(Optional) The name of the parameter map for a URL filtering policy to be displayed.
default	(Optional) Displays the default values for the URL filtering policy. **Note** If this keyword is not issued, user-configured values will be displayed.

Command Default

The paramater maps for all URL filtering policies of the type specified (**local**, **trend**, **n2h2**, or **websense**) are displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(15)XZ	This command was introduced.

Examples

The following example shows the default values for a Websense URL filtering policy:

```
Router# show parameter-map type urlfpolicy websense default
 parameter-map type urlfilter websense default values
  urlf-server-log off
  audit-trail off
  alert on
  max-request 1000
  max-resp-pak 200
  source-interface default
  allow-mode off
  cache 5000
```

show parser view

To display command-line interface (CLI) view information, use the **show parser view** command in privileged EXEC mode.

show parser view [**all**]

Syntax Description

all	(Optional) Displays information about all CLI views that are configured on the router.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

The **show parser view**command will display information only about the view that the user is currently in. This command is available for both root view users and lawful intercept view users--except for the **all** keyword, which is available only to root view users. However, the **all** keyword can be configured by a user in root view to be available for users in lawful intercept view.

The **show parser view** command cannot be excluded from any view.

Examples

The following example shows how to display information from the root view and the CLI view "first":

```
Router# enable view
Router#
01:08:16:%PARSER-6-VIEW_SWITCH:successfully set to view 'root'.
Router#
! Enable the show parser view command from the root view
Router# show parser view

Current view is 'root'
! Enable the show parser view command from the root view to display all views
Router# show parser view all

Views Present in System:
View Name:   first
View Name:   second
! Switch to the CLI view "first."
Router# enable view first

Router#
01:08:09:%PARSER-6-VIEW_SWITCH:successfully set to view 'first'.
! Enable the show parser view command from the CLI view "first."
```

```
Router# show parser view
Current view is 'first'
```

Related Commands

Command	Description
parser view	Creates or changes a CLI view and enters view configuration mode.

show platform hardware qfp feature alg

To display application layer gateway (ALG)-specific information in the Cisco Quantum Flow Processor (QFP), use the **show platform hardware qfp feature alg** command in privileged EXEC mode.

show platform hardware qfp {**active** | **standby**} **feature alg** {**debugging** | **memory** | **statistics** [{*protocol* | **clear**}]}

Syntax Description

active	Displays the active instance of the processor.
standby	Displays the standby instance of the processor.
debugging	Displays ALG debugging information.
memory	Displays ALG memory usage information of the processor.
statistics	Displays ALG common statistics information of the processor.

protocol	(Optional) Protocol name. Use one of the following values for the *protocol* argument: • **dns**—Displays Domain Name System (DNS) ALG information in the QFP datapath. • **exec**—Displays exec ALG information in the QFP datapath. • **ftp**—Displays FTP ALG information in the QFP datapath. • **gtp**—Displays General Packet Radio Service (GPRS) Tunneling Protocol (GTP) ALG information in the QFP datapath. • **h323**—Displays H.323 ALG information in the QFP datapath. • **http**—Displays HTTP ALG information in the QFP datapath. • **imap**—Displays Internet Message Access Protocol (IMAP) ALG information in the QFP datapath. • **ldap**—Displays Lightweight Directory Access Protocol (LDAP) ALG information in the QFP datapath. • **login**—Displays login ALG information in the QFP datapath. • **msrpc**—Displays Microsoft Remote Procedure Call (MSRPC) ALG information in the QFP datapath. • **netbios**—Displays Network Basic Input Output System (NetBIOS) ALG information in the QFP datapath. • **pop3**—Displays Post Office Protocol 3 (POP3) ALG information in the QFP datapath. • **pptp**—Displays Point-to-Point Tunneling Protocol (PPTP) ALG information in the QFP datapath. • **rtsp**—Displays Rapid Spanning Tree Protocol (RSTP) ALG information in the QFP datapath. • **shell**—Displays shell ALG information in the QFP datapath. • **sip**—Displays Session Initiation Protocol (SIP) ALG information in the QFP datapath. • **skinny**—Displays Skinny Client Control Protocol (SCCP) ALG information in the QFP datapath. • **smtp**—Displays Simple Mail Transfer Protocol (SMTP) ALG information in the QFP datapath. • **sunrpc**—Displays Sun RPC ALG information in the QFP datapath. • **tftp**—Displays TFTP ALG information in the QFP datapath.
clear	(Optional) Clears common ALG counters after display.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 2.2	This command was introduced.
Cisco IOS XE Release 3.1S	This command was modified. Support for the NetBIOS protocol was added.
Cisco IOS XE Release 3.2S	This command was modified. The **sip** keyword was added.
Cisco IOS XE Release 3.9S	This command was modified. The **gtp** and **pptp** keywords were added.

Usage Guidelines

The **show platform hardware qfp feature alg statistics netbios** command displays the NetBIOS ALG memory usage and statistics information of the processor.

Examples

The following sample output from the **show platform hardware qfp feature alg statistics netbios** command displays the NetBIOS ALG statistics information of the processor:

```
Device# show platform hardware qfp active feature alg statistics netbios

NetBIOS ALG Statistics:
  No. of allocated chunk elements in L7 data pool:0
  No. of times L7 data is allocated:0  No. of times L7 data is freed:0
  Datagram Service statistics
    Total packets            :0
    Direct unique packets    :0
    Direct group packets     :0
    Broadcast packets        :0
    DGM Error packets        :0
    Query request packets    :0
    Positive Qry response packets :0
    Negative Qry response packets:0
    Unknown packets          :0
    Total error packets      :0
  Name Service statistics
    Total packets            :0
    Query request packets    :0
    Query response packets   :0
    Registration req packets :0
    Registration resp packets:0
    Release request packets  :0
    Release response packets :0
    WACK packets             :0
    Refresh packets          :0
    Unknown packets          :0
    Total error packets      :0
  Session Service statistics
    Total packets            :0
    Message packets          :0
    Request packets          :0
    Positive response packets:0
    Negative response packets:0
    Retarget response packets:0
    Keepalive packets        :0
    Unknown packets          :0
    Total error packets      :0
```

The table below describes the significant fields shown in the display.

Table 147: show platform hardware qfp feature alg statistics netbios Field Descriptions

Field	Description
No. of allocated chunk elements in L7 data pool	Number of memory chunks allocated for processing NetBIOS packets.
No. of times L7 data is allocated:0 No. of times L7 data is freed	Number of times memory is allocated and freed for processing NetBIOS packets.
Direct unique packets	Number of direct unique NetBIOS packets processed.
Direct group packets	Number of direct group NetBIOS packets processed.
Broadcast packets	Number of broadcast NetBIOS packets processed.
DGM Error packets	Number of Datagram Error NetBIOS packets processed.
Query request packets	Number of query request NetBIOS packets processed.
Positive Qry response packets	Number of positive query response NetBIOS packets processed.
Negative Qry response packets	Number of negative query response NetBIOS packets processed.
Unknown packets	Number of unknown packets.
Total error packets	Counter tracking number of error packets.

The following sample output from the **show platform hardware qfp feature alg statistics sip** command displays SIP statistics information of the processor.

```
Device# show platform hardware qfp active feature alg statistics sip

SIP info pool used chunk entries number: 6

RECEIVE
Register:           0 -> 200-OK:           0
Invite:             6 -> 200-OK:           6    Re-invite           0
Update:             0 -> 200-OK:           0
Bye:                0 -> 200-OK:           0
Subscribe:          0 -> 200-OK:           0
Refer:              0 -> 200-OK:           0
Prack:              0 -> 200-OK:           0
Trying:             0    Ringing:          6    Ack:                5
Info:               0    Cancel:           0    Sess Prog:          0
Message:            0    Notify:           0
Publish:            0    Options:          0
1xx:                0    2xx:              0
OtherReq:           0    OtherOk:          0    3xx-6xx:            0

Events
Null dport:                  0   Media Port Zero:               0
Malform Media:               0   No Content Length:             0
Cr Trunk Chnls:              6   Del Trunk Chnls:               0
start trunk timer:           6   restart trunk timer:           6
```

```
stop trunk timer:             6   trunk timer timeout:            0
Media Addr Zero:              0   Need More Data:                 0
SIP PKT Alloc:               23   SIP PKT Free:                  23
SIP MSG Alloc:                0   SIP MSG Free:                   0

Errors
Create Token Err:             0    Add portlist Err:              0
Invalid Offset:               0    Invalid Pktlen:                0
Free Magic:                   0    Double Free:                   0
Sess Retmem Failed:           0    Sess Malloc Failed             0
Pkt Retmem Failed:            0    Pkt Malloc Failed:             0
Msg Retmem Failed:            0    Msg Malloc Failed:             0
Bad Format:                   0    Invalid Proto:                 0
Add ALG state Fail:           0    No Call-id:                    0
Parse SIP Hdr Fail:           0    Parse SDP Fail:                0
Error New Chnl:               0    Huge Size:                     0
Create Failed:                0    Not SIP Msg:                   0

Writeback Errors
Offset Err:                   0    PA Err:                        0
No Info:                      0
```

The table below describes the significant fields shown in the display.

Table 148: show platform hardware qfp feature alg statistics sip Field Descriptions

Field	Description
Register	Registers the address listed in the To field of the SIP ALG header with a SIP server.
Invite	Indicates that a user or a service is invited to participate in a call session.
Bye	Terminates a call. This message can be sent either by the caller or the called party.
Refer	Indicates that the user (recipient) should contact a third party for transferring a call.
PRACK	Improves the network reliability by adding an acknowledgment system to the provisional responses. PRACK is a Provisional Response Acknowledgment message.

The following sample output from the **show platform hardware qfp feature alg statistics gtp** command displays GTP (GTPv0, GTPv1, and GTPv2) ALG information. The field descriptions are self-explanatory.

```
Device# show platform hardware qfp active feature alg statistics gtp

Global info:
        Total pkts passed inspection:0
        GTP V0: Request: 0, Response: 0, Data: 0, Unknown: 0
        GTP V1: Request: 0, Response: 0, Data: 0, Unknown: 0
        GTP V2: Request: 0, Response: 0, Data: 0, Unknown: 0
        VFRed packets: 0
Drop counters:
        Total dropped: 0
        Fatal error:
           Internal SW error: 0
        Packets subject to policy inspection:
           Policy not-exist: 0
           Policy dirty-bit set: 0
           Policy-mismatch: 0
        GTP global Info:
           GTP message rejected: 0
```

```
            GTP Request wasn't found: 0
            GTP info element is missing: 0
            GTP info element is incorrect: 0
            GTP info element out of order: 0
            GTP Request retransmit: 0
          GTPv0 Info:
              Message rejected: 0
              Request wasn't found: 0
              Info element is missing: 0
              Info element is incorrect: 0
              Info element out of order: 0
              Request retransmit: 0
          GTPv1 Info:
              Message rejected: 0
              Request wasn't found: 0
              Info element is missing: 0
              Info element is incorrect: 0
              Info element out of order: 0
              Request retransmit: 0
          GTPv2 Info:
              Message rejected: 0
              Request wasn't found: 0
              Info element is missing: 0
              Info element is incorrect: 0
              Info element out of order: 0
              Request retransmit: 0
Memory management:
   GTP ctxt      - allocated: 0, freed: 0, failed: 0
   GTP Primary   - allocated: 0, freed: 0, failed: 0
   GTP Secondary - allocated: 0, freed: 0, failed: 0
   GTP Tunnel DB - allocated: 0, freed: 0, failed: 0
   GTP Req/Res   - allocated: 0, freed: 0, failed: 0
   GTP Req/Resp entry   - allocated: 0, freed: 0, failed: 0
   GTPv2 Session - allocated: 0, freed: 0, failed: 0
   GTPv2 Bearer - allocated: 0, freed: 0, failed: 0
```

Related Commands

Command	Description
debug platform hardware qfp feature	Debugs feature-specific information in the Cisco QFP.

show platform hardware qfp act feature ipsec datapath memory

To display debugging information about the consumption of IPsec datapath memory, use the **show platform hardware qfp act feature ipsec datapath memory** command in privileged EXEC or diagnostic mode.

show platform hardware qfp act feature ipsec datapath memory

Command Default

No default behavior or values

Command Modes

Privileged EXEC (#)

Diagnostic (diag)

Command History

Release	Modification
Cisco IOS XE Release 2.4.2	This command was introduced on the Cisco ASR 1000 Series Routers.

Usage Guidelines

This command displays the consumption of dynamic random access memory (DRAM) on the IPSec Cisco QuantumFlow Processor (QFP) datapath.

```
show platform hardware qfp act feature ipsec datapath memory
pstate chunk totalfree: 80000, allocated: 0
```

Related Commands

Command	Description
show platform software ipsec f0 encryption-processor registers	Displays dubugging information about the crypto engine processor registers.

show platform hardware qfp active feature ipsec

To display IPsec feature-specific information in the IPsec Cisco Quantum Flow Processor (QFP), use the **show platform hardware qfp active feature ipsec** command in the privileged EXEC mode.

show platform hardware qfp active feature ipsec{**event-monitor** | **interface** *interface-name* | **spi** | **sp-obj** *number* | **spd** | **datapath drops** | **clear** | {**all** *qfp-spd-number* | [{**ace** *spd-class-group-id* | [{*qfp-spd-class-id*}]}]}}

Syntax Description

event-monitor	Displays IPsec monitored events and event-count thresholds.
interface *interface-name*	Displays QFP information for the specified interface.
spi	Displays QFP IPsec security parameter index (SPI) information.
sp-obj *number*	Displays security policy information. The range is from 0 to 4294967295.
spd	Displays Security Policy Database (SPD) information.
datapath drops	Displays datapath drop counters, indicating the number of dropped packets, and a code number for the error type. Error codes vary, depending on platform.
clear	Clears the datapath drop counters.
state	Displays QFP IPsec state information.
all	Displays information about all SPDs.
qfp-spd-number	Specific handle in IPsec Cisco QFP.
ace	(Optional) Displays information about QFP IPsec SPD Cisco Application Control Engine (ACE).
spd-class-group-id	(Optional) SPD class group ID in Cisco ACE.
qfp-spd-class-id	(Optional) QFP class ID.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.9S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS 12.2 XN	The **event-monitor type** keyword was added.
Cisco IOS XE Fuji 16.8.1	Updated the error codes in the output when using **datapath drops**.

Usage Guidelines

This command displays information that can help you to troubleshoot issues about IPsec flows.

Examples

The following is a sample output of the **show platform hardware qfp active feature ipsec event-monitor** command. (The fields in the output are self-explanatory.)

```
Device# show platform hardware qfp active feature ipsec event-monitor

AntiReplay Threshold Setting: 1
Decryption Threshold Setting: 1000
Encryption Threshold Setting: 0
```

The following is a sample output from the **show platform hardware qfp active feature ipsec interface** command:

```
Device# show platform hardware qfp active feature ipsec interface gigabitEthernet 1/1/3

QFP ipsec intf sub-block Information

Ingress subblock for interface : 10
                         spd_id : 1
                  flags: 8000 (INTF ENABLED)
           spi tbl ptr: 0x898e4c00
            num labels: 1
                cce_w0: 0x10004
                cce_w1: 0x1084441
                 def_q: 0x0
                 pri_q: 0x0
  Ingress Statistics:

             pkts decrypted: 1
       pkts sent to crypto: 1
      pkts recv from crypt: 1
    pkts failed decryption: 0
  pkts failed policy check: 0

Egress subblock for interface : 10
                         spd_id : 1
                  flags: 8000 (INTF ENABLED)
           spi tbl ptr: 0x0
            num labels: 1
                cce_w0: 0x10004
                cce_w1: 0x1084441
                 def_q: 0x0
                 pri_q: 0x0
  Egress Statistics:

            pkts encrypted : 1
       pkts sent to crypto : 1
       pkts recv from crypt: 1
    pkts failed encryption: 0
```

The following table describes the significant fields shown in the display.

Table 149: show platform hardware qfp active feature ipsec interface Field Descriptions

Field	Description
Ingress subblock for interface	Incoming block for the interface.
spd_id	SPD identifier.
flags	Flags set for the interface.
spi tbl ptr	SPI table pointer.
num labels	Numerical labels.
def_q	Deferral queue.
pri_q	Priority queue.
Ingress Statistics	Incoming statistics.
pkts decrypted	Number of packets decrypted.
pkts sent to crypto	Number of packets sent to the crypto engine.
pkts recv from crypt	Number of packets received from the crypto engine.
pkts failed decryption	Number of packets that failed decryption.
pkts failed policy check	Number of packets that failed security policy check.
Egress subblock for interface	Outgoing block for the interface.
Egress Statistics	Outgoing statistics.
pkts encrypted	Number of packets encrypted.
pkts failed encryption	Number of packets that failed encryption.

The following is a sample output from the **show platform hardware qfp active feature ipsec spi** command:

```
Device# show platform hardware qfp active feature ipsec spi

QFP IPSEC SPI TABLE:

  IDX      SPI          PPE_ADDR     NXT_PPE      PROTO   VRF      SPD        SA
ADDR

-------------------------------------------------------------------------------------------

  0x992    0x95002492   0x89afb420   0x0          0x32    0        1          7
IPV4
```

The following table describes the significant fields shown in the display.

Table 150: show platform hardware qfp active feature ipsec spi Field Descriptions

Field	Description
IDX	Identifier.
SPI	SPI.
PPE_ADDR	Memory address where the SPI is stored in the QFP.
NXT_PPE	Address of the next SPI.
PROTO	IPSec protocol of the SA which is associated with the SPI.
VRF	Virtual routing and forwarding id of the SA.
SPD	QFP handle of the SPD that the SPI belongs to.
SA	QFP handle of the SA that the SPI belongs to.
Addr	Type of address.

The following is a sample output from the **show platform hardware qfp active feature ipsec sp-obj** command for SP ID 1:

```
Device# show platform hardware qfp active feature ipsec sp-obj 4

QFP ipsec sp Information

           QFP sp id: 4
           pal sp id: 6
          QFP spd id: 1
     number of intfs: 0
    cgid.cid.fid.rid: 1.2.2.1
```

The following table describes the significant fields shown in the display.

Table 151: show platform hardware qfp active feature ipsec sp-obj Field Descriptions

Field	Description
QFP sp id	QFP SP identifier.
QFP spd id	QFP SPD identifier.
number of intfs	Number of interfaces.

The following is a sample output from the **show platform hardware qfp active feature ipsec spd all** command:

```
Device# show platform hardware qfp active feature ipsec spd all

Current number CONTEXTs: 8
Current number SPDs: 1
Current number SPs: 5
Current number SAs: 2
    Active IN  SAs: 1          (pending: 0)
```

```
   Active OUT SAs: 1          (pending: 0)

 ---spd_id--------cg_id-----------num of intf---

      1              1              1
```

The following table describes the significant fields shown in the display.

Table 152: show platform hardware qfp active feature ipsec spd all Field Descriptions

Field	Description
Current number CONTEXTs	Number of SPD contexts in the system.
Current number SPDs	Number of SPDs in the system.
Current number SPs	Number of SPs in the system.
Current number SAs	Number of SAs in the system.
Active IN SAs	Number of active SAs.
spd_id	SPD identifier.
cg_id	Class group identifier.
num of intf	Number of interfaces.

The following is a sample output from the **show platform hardware qfp active feature ipsec spd** command for SPD ID 1:

```
Device# show platform hardware qfp active feature ipsec spd 1

             QFP id: 1
             pal id: 1
       num of aces: 6
      num of intfs: 1
   first intf name: GigabitEthernet1/1/3
              cgid: 1
         num of cm: 3
            cce_w0: 0x10004
            cce_w1: 0x1084441

  ---cgid.cid.fid----------num of aces---

       1.1.1                  2
       1.2.2                  2
       1.3.3                  2
```

The following table describes the significant fields shown in the display.

Table 153: show platform hardware qfp active feature ipsec spd Field Descriptions

Field	Description
QFP id	QFP identifier.
num of aces	Number of Cisco Application Control Engines (ACEs).

Field	Description
num of intfs	Number of interfaces.
first intf name	Name of the first interface.

The following is a sample output from the **show platform hardware qfp active feature ipsec state** command:

```
Device# show platform hardware qfp active feature ipsec state

QFP IPSEC state:

Message counter:
  Type                  Request          Reply (OK)       Reply (Error)
  ------------------------------------------------------------------------
  Initialize            1                1                0
  SPD Create            1                1                0
  SPD Intf Bind         1                1                0
  SPD CM Bind           3                3                0
  SP Create             5                5                0
  In SA Add             1                1                0
  Intf Enable           1                1                0
  Bulk SA Stats         128              128              0
  CGM Begin Batch       4                4                0
  CGM End Batch         4                4                0
  Inv SPI Notify        0                2                0
  Out SA Add Bind       1                1                0
```

The following table describes the significant fields shown in the display.

Table 154: show platform hardware qfp active feature ipsec state Field Descriptions

Field	Description
Message counter	Number of messages.
Initialize	Number of messages exchanged to initialize a connection.
SPD Create	Number of messages exchanged to create an SPD.
SPD Intf Bind	Number of messages exchanged to bind the SPD interface.
SPD CM Bind	Number of messages exchanged to bind to the SPD crypto map.
SP Create	Number of messages exchanged to create an SP.
In SA Add	Number of messages exchanged to create an inbound SA.
Intf Enable	Number of messages exchanged to enable an interface.
Bulk SA Stats	SA statistics.
CGM Begin Batch	Number of messages exchanged to start Class Group Manager (CGM).
CGM End Batch	Number of messages exchanged to end CGM.

Field	Description
Inv SPI Notify	Number of messages exchanged to notify an inverse SPI.
Out SA Add Bind	Number of messages exchanged to create an outbound SA.

The following is a sample output from the **show platform hardware qfp active feature ipsec datapath drops** command, showing information about dropped packets. For dropped packets, the **datapath drops** output includes an error code number for the type of packet drop, the name of the error, and the number of dropped packets.

```
Device#show platform hardware qfp active feature ipsec datapath drops
------------------------------------------------------------------------
Drop Type  Name                                        Packets
------------------------------------------------------------------------
30  IN_V4_POST_INPUT_POLICY_FAIL                        25

Device#show platform hard qfp acti feat ipsec datapath drops clear
------------------------------------------------------------------------
Drop Type  Name                                        Packets
------------------------------------------------------------------------
```

The following is a sample output from the **show platform hardware qfp active feature ipsec datapath drops clear** command, which clears the datapath drops counters.

```
Device#show platform hard qfp acti feat ipsec datapath drops clear
------------------------------------------------------------------------
Drop Type  Name                                        Packets
------------------------------------------------------------------------
```

Related Commands

Command	Description
show platform software ipsec fp active flow	Displays information about active instances of IPsec flows in the ESP.
show platform software ipsec fp active spd-map	Displays information about the active instances of IPsec SPD map objects.

show platform hardware qfp feature alg statistics sip

To display Session Initiation Protocol (SIP) application layer gateway (ALG)-specific statistics information in the Cisco Quantum Flow Processor (QFP), use the **show platform hardware qfp feature alg statistics sip** command in privileged EXEC mode.

show platform hardware qfp feature alg statistics sip [{**clear** | **dbl** [{**all** | **clear** | **entry** *entry-string* [{**clear**}]}] | **dblcfg** | **l7data** {**callid** *call-id* | **clear**} | **processor** | **timer**}]

Syntax Description

clear	(Optional) Clears ALG counters after display.
dbl	(Optional) Displays brief information about all SIP blocked list data.
all	(Optional) Displays all dynamic blocked list entries: blocked list and non blocked list entries.
entry *entry-string*	(Optional) Clears the specified blocked list entry.
dblcfg	(Optional) Displays all SIP blocked list settings.
l7data	(Optional) Displays brief information about all SIP Layer 7 data.
callid *call-id*	(Optional) Displays information about the specified SIP call ID.
processor	(Optional) Displays SIP processor settings.
timer	(Optional) Displays SIP timer settings.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.11S	This command was introduced.

Usage Guidelines

This command displays the following error details:

- Session write lock exceeded
- Global write lock exceeded
- Blocked list

This command also displays the following event details:

- Blocked list triggered
- Blocked list timeout

A blocked list is a list of entities that are denied a particular privilege, service, or access.

Examples

The following is sample output from the **show platform hardware qfp active feature alg statistics sip** command:

```
Device#  show platform hardware qfp active feature alg statistics sip
```

```
Events
...
Cr dbl entry:                10   Del dbl entry:                 10
Cr dbl cfg entry:             8   Del dbl cfg entry:              4
start dbl trig tmr:          10   restart dbl trig tmr:        1014
stop dbl trig tmr:           10   dbl trig timeout:            1014
start dbl blk tmr:            0   restart dbl blk tmr:            0
stop dbl blk tmr:             0   dbl blk tmr timeout:            0
start dbl idle tmr:          10   restart dbl idle tmr:         361
stop dbl idle tmr:            1   dbl idle tmr timeout:           9

DoS Errors
Dbl Retmem Failed:            0    Dbl Malloc Failed:             0
DblCfg Retm Failed:           0    DblCfg Malloc Failed:          0
Session wlock ovflw:          0    Global wlock ovflw:            0
Blacklisted:                561
```

The table below describes the significant fields shown in the display.

Table 155: show platform hardware qfp active feature alg statistics sip Field Descriptions

Field	Description
CR dbl entry	Number of dynamic blocked list entries.
start dbl blk tmr	Number of events that have started the dynamic blocked list timer.
stop dbl idle tmr	Number of events that have stopped the dynamic blocked list idle timer.
Del dbl entry	Number of dynamic blocked list entries deleted.
restart dbl trig tmr	Number of dynamic blocked list trigger timers restarted.
dbl trig timeout	Number of dynamic blocked list trigger timers timed out.
restart dbl blk tmr	Number of dynamic blocked list timers to be restarted.
dbl idle tmr timeout	Number of dynamic blocked list idle timers timed out.
DoS Errors	Denial of service (DoS) related errors.
Dbl Retmem Failed	Number of dynamic blocked list return memory failures.
DblCfg Retm Failed	Number of dynamic blocked list configuration return memory failures.
Session wlock ovflw	Number of packets that are dropped because the session-level write lock number is exceeded.
Blocked list	Number of packets dropped by dynamic blocked list.
Dbl Malloc Failed	Number of dynamic blocked list memory allocation failures.
DblCfg Malloc Failed	Number of dynamic blocked list configuration memory allocation failures.

Field	Description
Global wlock ovflw	Number of packets dropped because the global-level write-lock number is exceeded.

The following is sample output from the **show platform hardware qfp active feature alg statistics sip dbl entry** command:

```
Device# show platform hardware qfp active feature alg statistics sip dbl entry a4a051e0a4a1ebd

req_src_addr: 10.74.30.189              req_dst_addr: 10.74.5.30
trigger_period:     1000(ms)            block_timeout:       30(sec)
idle_timeout:       60(sec)             dbl_flags: 0x        1
cfg_trig_cnt:        5                  cur_trig_cnt:        0
```

The table below describes the significant fields shown in the display.

Table 156: show platform hardware qfp active feature alg statistics sip Field Descriptions

Field	Description
req_src_addr	Source IP address of a SIP request message.
trigger_period	Dynamic blocked list trigger period.
idle_timeout	Dynamic blocked list idle timeout entry.
cfg_trig_cnt	Configured trigger counter.
req_dst_addr	Destination IP address of a SIP request message.
block_timeout	Dynamic blocked list block timeout.
dbl_flags	Dynamic blocked list entry flags.
cur_trig_cnt	Current trigger counter.

Related Commands

alg sip blacklist	Configures a dynamic SIP ALG blocked list for destinations.
alg sip processor	Configures the maximum number of backlog messages that wait for shared resources.
alg sip timer	Configures a timer that SIP ALG uses to manage SIP calls.

show platform hardware qfp feature firewall

To display firewall feature-specific information in the Cisco Quantum Flow Processor (QFP), use the **show platform hardware qfp feature firewall** command in privileged EXEC mode.

show platform hardware qfp {**active** | **standby**} **feature firewall** {**memory** | **runtime** | **client** {**l7 policy** {*zone-pair-id layer4-class-id* | **all**} | **statistics**} | **sess-query-context** | **session** {**create** | **delete** | **more**} *session-context number-of-sessions* [{**zonepair** *zonepair-id*}] | **zonepair** *zonepair-id*}

Syntax Description

active	Displays the active instance of the processor.
standby	Displays the standby instance of the processor.
memory	Displays information about the Cisco QFP firewall datapath memory.
runtime	Displays information about the Cisco QFP firewall datapath runtime.
client	Displays information about the Cisco QFP firewall client.
l7 policy *zone-pair-id layer4-class-id*	Displays information about the Layer 7 policy that has the specified zone-pair ID and Layer 4 class ID.
all	Displays information about all Cisco QFP firewall client Layer 7 policies.
statistics	Displays information about Cisco QFP firewall client statistics.
sess-query-context	Displays information about Cisco QFP firewall session query context.
session	Displays information about the Cisco QFP firewall sessions.
create	Creates new show session contexts.
delete	Deletes the specified session context.
more	Reads all configured sessions that have the specified context.
session-context	Session context. Valid values are 0 to 4294967295.
number-of-sessions	Number of sessions to read. Valid values are from 0 to 4294967295.
zonepair *zonepair-id*	Displays information about Cisco QFP firewall zone pairs. Valid values are from 0 to 4294967295.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.9S	This command was introduced.
Cisco IOS XE Release 3.11S	This command was modified. The command output was modified to include the number of simultaneous packets per flow.

Usage Guidelines

Use this command to troubleshoot firewall issues related to memory usage, runtime errors, and so on.

Example

The following is sample output from the **show platform hardware qfp active feature firewall memory** command:

```
Device# show platform hardware qfp active feature firewall memory

                     ==FW memory info==
Chunk-Pool   Allocated     Total_Free   Init-Num     Low_Wat
-------------------------------------------------------------
scb          0             16384        16384        4096
hostdb       0             5120         5120         1024
ICMP Error   0             256          256          128
teardown     0             160          160          80
ha retry     0             2048         2048         512
dst pool     0             5120         5120         1024

                          ------------Total History----------
Chunk-Pool   Inuse       |Allocated    Freed       Alloc_Fail|
-------------------------------------------------------------
scb          0            0            0           0
hostdb       0            0            0           0
ICMP Error   0            0            0           0
dst pool     0            0            0           0

Table-Name   Address      Size
-----------------------------------------
-----------------------------------------
scb          0x8bc80000   65536
hostdb       0x89941c00   1024
zonepair     0x89950400   1024
dchannel     0x8994cc00   2048

FW persona timer tbl address 0x8c271020 entries: 131072 num_tbls 9 stagger 17,
FW persona hostdb mtx (lock address): 0x89942c00
FW persona ICMP Error pool address: 0x89956820
FW persona un-created sessions due to max session limit:  0
FW persona agg-age sess teardown halfopen: 0, non-halfopen: 0
```

The following is sample output from the **show platform hardware qfp active feature firewall runtime** command:

```
Device# show platform hardware qfp active feature firewall runtime

FW internal: stop_traffic 0x0
global 0xa2400021
  HA State                  Allow New Sess
  FW Configured             (0x00000020)
  VRF Rsrc Chk              (0x00400000)
  Syslog Deployed           (0x02000000)
  VRF Enabled               (0x20000000)
```

```
  B2B HA Enabled            (0x80000000)
global2 0x192c0012
  Global number of simultaneous packet per session allowed 44  <<<<<<<<<<<<
  Default number of simultaneous packet per session allowed  25
debug 0x00008041
.
.
.
```

The following is sample output from the **show platform hardware qfp active feature firewall client statistics** command:

```
Device# show platform hardware qfp active feature firewall client statistics

Zonepair table entry count: 1
Filler block count: 0
Action block count: 0
L7 params block count: 0
Statistics table count: 0
Statistics block count: 0
Class name table entry count: 0
Number of vrf interfaces with zone: 0
Number of zoned interfaces: 2
Number of zones: 2
Number of zone pairs with policy: 0
Inspect parameter map count: 3
VRF related objects: VRF-ParameterMap count: 1, VRF-ParameterMap Binding count: 0
Zone related objects: Zone-ParameterMap count: 0, Zone-ParameterMap Binding count: 0
SCB pool: number of entries: 16384, entry limit: 1048576, size: 4719008, number of additions:
 0
Synflood Hostdb pool: number of entries: 5120, entry limit: 0, size: 573856, number of
additions: 0
Session Teardown pool: number of entries: 160, entry limit: 0, size: 5536, number of
additions: 0
Syncookie Destination pool: number of entries: 5120, entry limit: 262144, size: 410016,
number of additions: 0
```

The following is sample output from the **show platform hardware qfp active feature firewall zonepair** command:

```
Device# show platform hardware qfp active feature firewall zonepair 1

Zonepair name:zp-ge000-ge003 | id:1
     Source zone name:ge0-0-0 | id:2
Destination zone name:ge0-0-3 | id:1
     Class group name:policy1 | id:14841376
lookup data in sw: 0x00010003, 0x00084441
lookup data in hw: 0x00010003, 0x00084441

Class name:c-ftp-tcp | id:13549553
Number of Protocols: 4
Protocols: 1, 2, 4, 18
Maxever number of packet per flow: 25
Filler block/Action block/Stats table addresses: 0x8967f400, 0x8d70f400, 0x898d7400
Stats blocks addresses: 0x8d716c00, 0x8d716c40, 0x8d716c80, 0x8d716cc0
Result: 0x08000000, 0x8967f400
Filler block in sw: 0x8d70f400898d7400
Filler block in hw: 0x0000000c00000000
Action block in hw:

Class name:class-default | id:1593
Number of Protocols: 0
Maxever number of packet per flow: 0
Filler block/Action block/Stats table addresses: 0x8967f400, 0x8d70f400, 0x898d7400
```

```
Stats blocks addresses: 0x8d716c00, 0x8d716c40, 0x8d716c80, 0x8d716cc0
Result: 0x08000000, 0x8967f400
Filler block in sw: 0x8d70f400898d7400
Filler block in hw: 0x0000000c00000000
Action block in hw:


Class name:class-default | id:1593
Number of Protocols: 0
Maxever number of packet per flow: 0
Filler block/Action block/Stats table addresses: 0x8967f408, 0x8d70f4f0, 0x898d7520
Result: 0x81000000, 0x8967f408
Filler block in sw: 0x8d70f4f0898d7520
Filler block in hw: 000000000000000000
Action block in hw:
```

The table below describes the significant fields shown in the displays.

Table 157: show platform hardware qfp feature firewall Field Descriptions

Field	Description
scb	Memory allocated for the session control block (SCB) pool.
dst pool	Memory allocated for the destination pool.
HA state	High availability status.
HSL Enabled	Number of sessions for which high-speed logging (HSL) is enabled.
teardowns	Number of queues that were torn down.
Num of ACK exceeds limit	Number of acknowledgment (ACK) requests that exceeded the configured limit.
Num of RST exceeds limit	Number of reset (RST) requests that exceeded the configured limit.
VRF Global Action Block	Information about the global virtual routing and forwarding (VRF) instance.
half-open	Information about the half-opened firewall sessions.
aggr-age high watermark low watermark	Information about the aggressive-aging high and low watermarks. Firewall sessions are aggressively aged to make room for new sessions, thereby protecting the firewall session database from filling. Aggressive aging period starts when the session table crosses the high watermark and ends when it falls below the low watermark.

Related Commands

show platform hardware qfp feature firewall datapath	Displays information about the firewall datapath in the Cisco QFP.
show platform hardware qfp feature firewall drop	Displays information about the firewall packet drops in the Cisco QFP.

show platform hardware qfp feature firewall datapath scb

To display information about the session control block of the Cisco Quantum Flow Processor (QFP), use the **show platform hardware qfp feature firewall datapath scb** command in privileged EXEC mode.

show platform hardware qfp {**active** | **standby**} **feature firewall datapath scb** [{*ipv4-address* | *ipv4-address/mask* | **any** | **ipv6** *source-ipv6-address*}] [{*source-port* | **any**}] [{*destination-ipv4-address destination-ipv6-address* | *ipv4-address/prefix* | **any**}] [{*destination-port* | **any**}] [{*layer4-protocol* | **any**}] [{**all** | **imprecise** | **session**}] [{*vrf-id* | **any**}] [{**detail**}]

Syntax Description

active	Displays the active instance of the processor.
standby	Displays the standby instance of the processor.
ipv4-address mask	(Optional) IPv4 address and prefix mask.
any	(Optional) Specifies any source port, destination port, Layer 4 protocol number, or virtual routing and forwarding (VRF) ID.
ipv6 *source-ipv6-address*	(Optional) Specifies an IPv6 address.
source-port	(Optional) Source port number. The range is from 0 to 65535.
destination-ipv4-address	(Optional) Destination IPv4 address.
destination-ipv6-address	(Optional) Destination IPv6 address.
destination-port	(Optional) Destination port number. The range is from 0 to 65535.
layer4-protocol	(Optional) Layer 4 protocol number. The range is from 0 to 255.
all	(Optional) Specifies all firewall databases.
imprecise	(Optional) Specifies the imprecise database.
session	(Optional) Specifies the firewall session database.
vrf-id	(Optional) VRF ID. The range is from 0 to 65535.
detail	(Optional) Provides detailed information about the firewall session and imprecise databases.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.11S	The command was introduced.

Usage Guidelines

This command provides detailed information about firewall sessions and databases. The **show policy-firewall sessions platform all** command also performs the same action as **show platform hardware qfp active feature firewall datapath scb any any any any any all any detail** command.

Examples

The following is sample output from the **show platform hardware qfp active feature firewall datapath scb any any any any any all any detail** command:

```
Device# show platform hardware qfp active feature firewall datapath scb any any any any any
 all any detail

[s=session  i=imprecise channel  c=control channel  d=data channel]

Session ID:0x00000002  100.0.0.2 8 100.0.0.1 92 proto 1 (0:0)   [sc]
 pscb : 0x8ba00400,  bucket : 55587, fw_flags: 0x204 0x204154c1,

192.168.2.2 1024 192.168.1.2 1024 proto 17 (0:0)       [sd]
 pscb : 0x8bd0ddc0,  bucket : 34846, fw_flags: 0x4 0x20413481,
        scb state: active, scb debug: 0
 nxt_timeout: 360000, refcnt: 1,  ha nak cnt: 0,  rg: 0, sess id: 0
 hostdb: 0x0, L7: 0x0, stats: 0x8d8e3740, child: 0x0
 l4blk0: 29 l4blk1: 1ceabd0a l4blk2: 0 l4blk3: 805a46fd
 l4blk4: 0 l4blk5: 0 l4blk6: 0 l4blk7: 0
 l4blk8: 0 l4blk9: 2
 root scb: 0x0 act_blk: 0x8d8dbde0
 ingress/egress intf: TenGigabitEthernet1/3/0 (1011), TenGigabitEthernet0/3/0 (131057)
 current time 43491794128 create tstamp: 25627209695 last access: 43491799244
 nat_out_local_addr:port: 10.1.1.4:9 nat_in_global_addr:port: 192.0.2.5:7
 syncookie fixup: 0x0
 halfopen linkage: 0x0 0x0
 tw timer: 0x0 0x0 0x37ed5 0xaf32111
 Number of simultaneous packet per session: 70
```

The table below describes the significant fields shown in the display.

Table 158: show platform hardware qfp feature firewall datapath scb Field Descriptions

Field	Description
scb state	State for the SCB; either active or standby.
ingress/egress intf:	Incoming and outgoing interface IP addresses.
nat_out_local_addr:port:	Network Address Translation (NAT) outside local IP address and port number.
nat_in_global_addr:port:	NAT inside global IP address and port number.

Related Commands

Command	Description
parameter-map type inspect	Configures an inspect-type parameter map for connecting thresholds, timeouts, and other parameters pertaining to the **inspect** action.
parameter-map type inspect global	Defines a global parameter map and enter parameter-map type inspect configuration mode.
show parameter-map type inspect	Displays user-configured or default inspect-type parameter maps.

show platform hardware qfp feature td

To display threat-defense-specific information in the Cisco QuantumFlow Processor (QFP), use the **show platform hardware qfp feature td** command in privileged EXEC mode.

show platform hardware qfp {**active** | **standby**} **feature td** {**client** | **datapath**} **memory**

Syntax Description

active	Displays the active instance of the processor.
standby	Displays the standby instance of the processor.
client	Displays information about the threat defense (TD) client.
datapath	Displays TD information in the datapath.
memory	Displays information about the TD memory usage.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.9S	This command was introduced.

Usage Guidelines

Use this command to check the virtual TCP (vTCP) statistics that are triggered by TCP application layer gateway (ALG) sessions.

Examples

The following is sample output from the **show platform hardware qfp active feature td datapath memory** command:

```
Device# show platform hardware qfp active feature td datapath memory

==VTCP ucode info==
info alloc 0, free 0, fail 0
pkt buf alloc 0, free 0, fail 0
buf size alloc 0, free 0
rx drop 0, tx drop 0, tcp drop 0, alg csum 0
sending: rx ack 0, rst 0, hold rst 0 tx payload: seg 0, rexmit 0
vtcp_info_chunk 0x8d54fcb0, totalfree: 2048, allocated: 0
vtcp_pkt_pool 0x8d5d80c0, total: 1048240, free: 1048240
vtcp_timer_wheel 0x8d6d84d0, vtcp_init 1
td_internal debug 0x0
td_global td_init 0x2
alg_debug_vtcp 0x0
```

The table below describes the significant fields shown in the display.

Table 159: show platform hardware qfp feature td datapath memory Field Descriptions

Field	Description
info alloc	vTCP allocated counts.

Field	Description
pkt buf alloc	Allocated packet buffer size.
buf size alloc	Allocated buffer size.
rx drop	Transmit buffer (Rx) drop. Rx is memory spaces allocated by a device to handle traffic bursts.
tx drop	Receive buffer (Tx) drop. Rx is memory spaces allocated by a device to handle traffic bursts.

Related Commands

Command	Description
show platform hardware qfp feature alg	Displays ALG-specific information in the Cisco QFP.
show tech-support alg	Displays ALG-specific information to assist in troubleshooting.

show platform software cerm-information

To display Crypto Export Restrictions Manager (CERM) information, use the **show platform software cerm-information** command in privileged EXEC mode.

show platform software cerm-information

Syntax Description

This command has no keywords or arguments.

Command Default

CERM information is not displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.1	This command was introduced.

Usage Guidelines

This command displays Crypto Export Restrictions Manager (CERM) information of devices running on Cisco IOS XE software.

Examples

The following is a sample output of the **show platform software cerm-information** command:

```
Device# show platform software cerm-information

Crypto Export Restrictions Manager(CERM) Information:
 CERM functionality: ENABLED
 ---------------------------------------------------------------
 Resource                      Maximum Limit           Available
 ---------------------------------------------------------------
 Number of tunnels             1000                    1000
 Number of TLS sessions        1000                    1000
 Resource reservation information:
 D - Dynamic
 ---------------------------------------------------------------------------
 Client         Tunnels    TLS Sessions
 ---------------------------------------------------------------------------
 VOICE           0          0
 IPSEC           0          N/A
 SSLVPN          0          N/A
 Statistics information:
 Failed tunnels:            0
 Failed sessions:           0
 Failed encrypt pkts:                        0
 Failed encrypt pkt bytes:                   0
 Failed decrypt pkts:                        0
 Failed decrypt pkt bytes:                   0
```

show platform software firewall

To display the firewall configuration information, use the **show platform software firewall** command in privileged EXEC mode.

show platform software firewall {**F0** | **F1** } {**bindings** | **pairs** | **parameter-maps** | **port-application-mapping** | **statistics** | **vrf-pmap-bindings** | **zones**}

show platform software firewall {**F0** | **F1** } **sessions** **zone-pair** *zone-pair-name* [{**class-id** *class-id*}] [{**destination** *ip-address* | **ipv6**{**destination** *ipv6-address* | **source** *ipv6-address* [**destination** *ipv6-address*]} | **source** *ip-address* [**destination** *ip-address*]}]

show platform software firewall {**R0** | **R1** } {**bindings** | **pairs** | **parameter-maps** | **port-application-mapping** | **statistics** | **vrf-pmap-bindings** | **zones**}

show platform software firewall {**FP** | **RP**} {**active** | **standby**} {**bindings** | **pairs** | **parameter-maps** | **port-application-mapping** | **statistics** | **vrf-pmap-bindings** | **zones**}

Syntax Description

F0	Displays information about the Embedded Service Processor (ESP) slot 0.
F1	Displays information about the ESP slot 1.
bindings	Displays information about the configured security zone bindings.
pairs	Displays information about configured security zone pairs.
parameter-maps	Displays information about configured parameter maps.
port-application-mapping	Displays information about the configured Port-to-Application Mapping (PAM).
sessions	Displays information about existing firewall sessions.
statistics	Displays firewall statistics.
vrf-pmap-bindings	Displays information about the configured virtual routing and forwarding (VRF) instance and parameter map bindings.
zones	Displays information about configured security zones.
zone-pair *zone-pair*	Displays existing firewall sessions for a zone pair.
class-id *class-id*	Displays sessions in a class.

destination *ip-address*	Displays sessions with specified destination IP address.
ipv6	Displays sessions with specified IPv6 address.
ipv6 destination *ipv6-address*	Displays destination IPv6 address.
ipv6 source *ipv6-address*	Displays source IPv6 address.
source *ip-address*	Displays sessions with specified source IP address.
R0	Displays information about the Route Processor (RP) slot 0.
R1	Displays information about the RP slot 1.
FP	Displays information about the ESP.
RP	Displays information about the RP.
active	Displays information about the active instance of the processor.
standby	Displays information about the standby instance of the processor.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.9S	This command was introduced.
Cisco IOS XE Release 3.11S	This command was modified. The command output was modified to display the number of simultaneous packets per flow.

Usage Guidelines

Use this command to view information about the configured firewall policies, parameter maps, security zones, and security zone-pairs.

Example

The following is sample output from the **show platform software firewall FP active parameter-maps** command:

```
Device# show platform software firewall FP active parameter-maps

Forwarding Manager Inspect Parameter-Maps

  Inspect Parameter Map: global, Index 1
  Parameter Map Type: Parameter-Map
      Global Parameter-Map
      Alerts: On, Audits: Off, Drop-Log: Off
      HSL Mode: V9, Host: 10.1.1.1:9000, Port: 54174, Template: 300 sec
      Session Rate High: 2147483647, Session Rate Low: 2147483647, Time Duration: 60 sec
      Half-Open:
```

```
      High: 2147483647, Low: 2147483647, Host: 4294967295, Host Block Time: 0
    Inactivity Times [sec]:
      DNS: 5, ICMP: 10, TCP: 3600, UDP: 30
    Inactivity Age-out Times [sec]:
      ICMP: 10, TCP: 3600, UDP: 30
    TCP Timeouts [sec]:
      SYN wait time: 30, FIN wait time: 1
    TCP Ageout Timeouts [sec]:
      SYN wait time: 30, FIN wait time: 1
    TCP RST pkt control:
      half-open: On, half-close: On, idle: On
    UDP Timeout [msec]:
      UDP Half-open time: 30000
    UDP Ageout Timeout [msec]:
      UDP Half-open time: 30000

    Max Sessions: Unlimited

    Number of Simultaneous Packet per Sessions: 0
    Syn Cookie and Resource Management:
      Global Syn Flood Limit: 4294967295
      Global Total Session : 4294967295
    Global Total Session Aggressive Aging Disabled
    Global alert : Off
    Global max incomplete : 4294967295
    Global max incomplete TCP: 4294967295
    Global max incomplete UDP: 4294967295
    Global max incomplete ICMP: 4294967295
    Global max incomplete Aggressive Aging Disabled
    Per Box Configuration
      syn flood limit : 4294967295
      Total Session Aggressive Aging Disabled
      max incomplete : 4294967295
      max incomplete TCP: 4294967295
      max incomplete UDP: 4294967295
      max incomplete ICMP: 4294967295
      max incomplete Aggressive Aging Disabled

Inspect Parameter Map: vrf-default, Index 2
Parameter Map Type: VRF-Parameter-Map
VRF PMAP syn flood limit : 4294967295
VRF PMAP total session : 4294967295
VRF PMAP total session Aggressive Aging Disabled
VRF PMAP alert : Off
VRF PMAP max incomplete : 4294967295
VRF PMAP max incomplete TCP: 4294967295
VRF PMAP max incomplete UDP: 4294967295
VRF PMAP max incomplete ICMP: 4294967295
VRF PMAP max incomplete Aggressive Aging Disabled

Inspect Parameter Map: pmap-hsl, Index 3
Parameter Map Type: Parameter-Map
    Alerts: On, Audits: On, Drop-Log: Off
    Session Rate High: 2147483647, Session Rate Low: 2147483647, Time Duration: 60 sec
    TCP Window Scaling Loose: off
    session packet default
    Half-Open:
      High: 2147483647, Low: 2147483647, Host: 4294967295, Host Block Time: 0
    Inactivity Times [sec]:
      DNS: 5, ICMP: 10, TCP: 3600, UDP: 30
    Inactivity Age-out Times [sec]:
      ICMP: 10, TCP: 3600, UDP: 30
    TCP Timeouts [sec]:
      SYN wait time: 30, FIN wait time: 1
```

```
    TCP Ageout Timeouts [sec]:
      SYN wait time: 30, FIN wait time: 1
    TCP RST pkt control:
      half-open: On, half-close: On, idle: On
    UDP Timeout [msec]:
      UDP Half-open time: 30000
    UDP Ageout Timeout [msec]:
      UDP Half-open time: 30000

    Max Sessions: Unlimited

    Number of Simultaneous Packet per Sessions: 0
    Syn Cookie and Resource Management:
      Global Syn Flood Limit: 4294967295
      Global Total Session : 4294967295

 Inspect Parameter Map: pmap1, Index 4
 Parameter Map Type: Parameter-Map
    Alerts: On, Audits: On, Drop-Log: Off
    Session Rate High: 2147483647, Session Rate Low: 2147483647, Time Duration: 60 sec
    TCP Window Scaling Loose: off
    session packet default
    Half-Open:
      High: 2147483647, Low: 2147483647, Host: 4294967295, Host Block Time: 0
    Inactivity Times [sec]:
      DNS: 5, ICMP: 10, TCP: 3600, UDP: 30
    Inactivity Age-out Times [sec]:
      ICMP: 10, TCP: 3600, UDP: 30
    TCP Timeouts [sec]:
      SYN wait time: 30, FIN wait time: 1
    TCP Ageout Timeouts [sec]:
      SYN wait time: 30, FIN wait time: 1
    TCP RST pkt control:
      half-open: On, half-close: On, idle: On
    UDP Timeout [msec]:
      UDP Half-open time: 30000
    UDP Ageout Timeout [msec]:
      UDP Half-open time: 30000

    Max Sessions: 3000

    Number of Simultaneous Packet per Sessions: 0
    Syn Cookie and Resource Management:
      Global Syn Flood Limit: 4294967295
      Global Total Session : 4294967295

Inspect Parameter Map: pmap1, Index 4
 Parameter Map Type: Parameter-Map
    Alerts: On, Audits: On, Drop-Log: Off
    Session Rate High: 2147483647, Session Rate Low: 2147483647, Time Duration: 60 sec
    TCP Window Scaling Loose: off
    session packet default
    Half-Open:
      High: 2147483647, Low: 2147483647, Host: 4294967295, Host Block Time: 0
    Inactivity Times [sec]:
      DNS: 5, ICMP: 10, TCP: 3600, UDP: 30
    Inactivity Age-out Times [sec]:
      ICMP: 10, TCP: 3600, UDP: 30
    TCP Timeouts [sec]:
      SYN wait time: 30, FIN wait time: 1
    TCP Ageout Timeouts [sec]:
      SYN wait time: 30, FIN wait time: 1
    TCP RST pkt control:
      half-open: On, half-close: On, idle: On
```

```
UDP Timeout [msec]:
  UDP Half-open time: 30000
UDP Ageout Timeout [msec]:
  UDP Half-open time: 30000

Max Sessions: 3000

Number of Simultaneous Packet per Sessions: 0
Syn Cookie and Resource Management:
  Global Syn Flood Limit: 4294967295
  Global Total Session : 4294967295
```

The table below describes the significant fields shown in the display.

Table 160: show platform software firewall Field Descriptions

Field	Description
Alerts on	Console display of stateful packet inspection alert messages. Valid values are On and Off.
Audits off	Audit trail messages. Valid values are On and Off.
HSL mode	High-speed logging (HSL) messages are logged.
Host	IP address of the host to which HSL messages are logged.
SYN wait time	Time period the software waits for a TCP session to reach the established state before dropping the session.
FIN wait time	Time period a TCP session is managed after the firewall detects a finish (FIN) exchange.
Global SYN Flood limit	Configured TCP half-open session limit before triggering the synchronization (SYN) cookie processing for new SYN packets.

The following is sample output from the show command **show platform software firewall F0 sessions zone-pairs**

```
Device# show platform software firewall F0 sessions zone-pair in-self

Established Sessions
Session ID 0x00000001 (100.0.0.2:8)=>(100.0.0.1:91) icmp SIS_OPEN
  Created 00:00:02, Last heard 00:00:02
  Bytes sent (initiator:responder) [360:360]
```

The following is sample output from the **show platform software firewall RP active statistics** command:

```
Device# show platform software firewall RP active statistics

Forwarding Manager Firewall Statistics

Zones:
  3 Adds (0 errors), 0 Mods (0 errors), 0 Deletes (0 errors)
  6 Downloads (0 errors)

Zone-pairs:
```

```
  1 Adds (0 errors), 0 Mods (0 errors), 0 Deletes (0 errors)
  2 Downloads (0 errors)

Zone-bindings:
  4 Adds (0 errors), 0 Mods (0 errors), 0 Deletes (0 errors)
  8 Downloads (0 errors)

Inspect Parameter-Maps:
  0 Adds (0 errors), 0 Mods (0 errors), 0 Deletes (0 errors)
  0 Downloads (0 errors)

PAMs(Port Application Mapping):
  0 Adds (0 errors), 0 Mods (0 errors), 0 Deletes (0 errors)
  0 Downloads (0 errors)

VRF Bindings:
  0 Adds (0 errors), 0 Mods (0 errors), 0 Deletes (0 errors)
  0 Downloads (0 errors)
```

Related Commands

Command	Description
parameter-map type inspect	Configures an inspect-type parameter map for connecting thresholds, timeouts, and other parameters pertaining to the **inspect** action.
zone-pair security	Creates a zone pair.

show platform software ipsec policy statistics

To display debugging information about the IP security policy statistics, use the **show platform software ipsec policy statistics** command in Privileged EXEC mode.

show platform software ipsec policy statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.8S	This command was introduced.

The following is sample output from the **show platform software ipsec policy statistics** command:

```
Router# show platform software ipsec policy statistics

PAL CMD                 REQUEST   REPLY OK  REPLY ERR      ABORT
SADB_INIT_START               1          1          0          0
SADB_INIT_COMPLETED           1          1          0          0
SADB_DELETE                   0          0          0          0
SADB_ATTR_UPDATE              1          1          0          0
SADB_INTF_ATTACH              1          1          0          0
SADB_INTF_UPDATE              0          0          0          0
SADB_INTF_DETACH              0          0          0          0
ACL_INSERT                    1          1          0          0
ACL_MODIFY                    0          0          0          0
ACL_DELETE                    0          0          0          0
PEER_INSERT                   3          3          0          0
PEER_DELETE                   2          2          0          0
SPI_INSERT                  151        151          0          0
SPI_DELETE                  150        150          0          0
CFLOW_INSERT                  3        151          0          0
CFLOW_MODIFY                148        148          0          0
CFLOW_DELETE                  2          2          0          0
OUT_SA_DELETE               150        150          0          0
TBAR_CREATE                   0          0          0          0
TBAR_UPDATE                   0          0          0          0
TBAR_REMOVE                   0          0          0          0

PAL NOTIFY   RECEIVE   COMPLETE   PROC ERR     IGNORE
NOTIFY_RP          0          0          0          0
SA_DEAD            2          2          0          0
SA_SOFT_LIFE      80         80          0          0
IDLE_TIMER         0          0          0          0
DPD_TIMER          0          0          0          0
INVALID_SPI        0          0          0          0
```

The following table describes the significant fields shown in the display:

Table 161: show platform software ipsec policy statistics Field Descriptions

Field	Description
PAL CMD	Name of a request sent from the IPsec control plane to the IPsec data plane.

REQUEST	Number of IPsec control plane requests sent.
REPLY OK	Number of successful replies sent by the IPsec data plane for the requests sent by the IPsec control plane.
REPLY ERR	Number of failed replies sent by the IPsec data plane for the requests sent by the IPsec control plane.
ABORT	Number of requests terminated because of a timeout.
PAL NOTIFY	Name of a notification sent from the IPsec data plane to the IPsec control plane.
RECEIVE	Number of IPsec data plane notifications received.
COMPLETE	Number of successful IPsec data plane notifications sent to the IPsec control plane.
PROC ERR	Number of IPsec data plane notifications that were not sent because of a process error.
IGNORE	Number of IPsec data plane notifications that can be safely ignored.

Table 162: Related Commands

Command	Description
show platform software ipsec f0 inventory	Displays the IPsec object counts of a forwarding processor.

show platform software ipsec f0 encryption-processor registers

To display debugging information about the crypto engine processor registers, use the **show platform software ipsec f0 encryption-processor registers** command in privileged EXEC or diagnostic mode.

show platform software ipsec f0 encryption-processor registers

Command Default

No default behavior or values

Command Modes

Privileged EXEC (#)

Diagnostic (diag)

Command History

Release	Modification
Cisco IOS XE Release 2.4.2	This command was introduced on the Cisco ASR 1000 Series Routers.

Usage Guidelines

This command displays debugging information for crypto engine processor registers.

```
show platform software ipsec f0 encryption-processor registers
Forwarding Manager Encryption-processor Registers
     reg_addr : 00000000,    reg_val  : 0000ca5b
     reg_addr : 00000008,    reg_val  : 00000000
     reg_addr : 00000010,    reg_val  : 00000000
     reg_addr : 00000018,    reg_val  : 22f10038
     reg_addr : 00000020,    reg_val  : 00000800
     reg_addr : 00000028,    reg_val  : 00002040
     reg_addr : 00000030,    reg_val  : 00000000
     reg_addr : 00000038,    reg_val  : 23158838
```

Related Commands

Command	Description
show platform hardware qfp act feature ipsec datapath memory	Displays debugging information about the consumption of IPsec datapath memory.

show platform software ipsec fp active flow

To display information about active instances of IPsec flows in the Embedded Service Processor (ESP), use the **show platform software fp ipsec active flow** command in privileged EXEC mode.

show platform software ipsec fp active flow {**all** | **identifier** *number*}

Syntax Description

all	Displays information about all active IPsec flows in the instance.
identifier *number*	Displays information about the specified IPsec flow in the instance. The range is from 0 to 32767.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.9S	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

This command displays information that can help you to troubleshoot issues about IPsec flows.

Examples

The following is sample output from the **show platform software ipsec fp active flow all** command:

```
Device# show platform software ipsec fp active flow all

=========== Flow id: 1
               mode: tunnel
          direction: inbound
           protocol: esp
                SPI: 0x95002492
      local IP addr: 100.0.0.1
     remote IP addr: 100.0.0.2
      crypto map id: 3
             SPD id: 1
    ACE line number: 1
      QFP SA handle: 7
   crypto device id: 0
IOS XE interface id: 11
     interface name: GigabitEthernet1/1/3
       object state: active

=========== Flow id: 2
               mode: tunnel
          direction: outbound
           protocol: esp
                SPI: 0xfd2fa486
      local IP addr: 100.0.0.1
     remote IP addr: 100.0.0.2
      crypto map id: 3
             SPD id: 1
    ACE line number: 1
      QFP SA handle: 8
   crypto device id: 0
IOS XE interface id: 11
     interface name: GigabitEthernet1/1/3
```

```
        object state: active
```

The following table describes the significant fields shown in the display.

Table 163: show platform software ipsec fp active flow all Field Descriptions

Field	Description
Flow id	Flow identifier.
mode	Operation mode. In this case, it is tunnel mode.
direction	Flow direction—inbound or outbound. In this case, it is outbound.
protocol	Protocol used. In this case, it is Encapsulating Security Payloads (ESP).
SPI	Security Parameters Index (SPI) that is used to identify the security association (SA).
local IP addr	IP address of the local host.
remote IP addr	IP address of the remote host.
crypto map id	Crypto map identifier.
SPD id	SPI identifier.
ACE line number	Cisco Application Control Engine (ACE) number.
QFP SA handle	Quantum Flow Processor (QFP) SA identifier.
crypto device id	Crypto device identifier.
IOS XE interface id	Interface ID in Cisco IOS XE software.
interface name	Interface name.
use path MTU	Maximum transmission unit (MTU) size.
object state	Object state.
object bind state	State of the object bound.

The following is sample output from the **show platform software ipsec fp active flow** command for flow ID 1:

```
Device# show platform software ipsec fp active flow identifier 1

========== Flow id: 1
                mode: tunnel
           direction: inbound
            protocol: esp
                 SPI: 0x95002492
      local IP addr: 100.0.0.1
     remote IP addr: 100.0.0.2
   crypto device id: 0
      crypto map id: 3
             SPD id: 1
```

```
    ACE line number: 1
      QFP SA handle: 7
IOS XE interface id: 11
     interface name: GigabitEthernet1/1/3
   Crypto SA ctx id: 0x000000002dc3bfde
             cipher: 3DES
               auth: SHA1
 initial seq.number: 0
      timeout, mins: 0
              flags: exp time;exp traffic;DPD;
   Peer Flow handle: 0x0000000080000014
Time limits

         soft limit: 3537
         hard limit: 3597
Traffic limits

         soft limit: 3686400
         hard limit: 4608000
--------------- DPD

              mode: periodic
    rearm countdown: 0
        next notify: *EXPIRED*
     last in packet: 0
     inline_tagging: DISABLED
 anti-replay window: 64
SPI Selector:

   remote addr low: 0.0.0.0
  remote addr high: 0.0.0.0
    local addr low: 100.0.0.1
   local addr high: 100.0.0.1
Classifier: range

   src IP addr low: 1.0.0.0
  src IP addr high: 1.0.0.255
   dst IP addr low: 2.0.0.0
  dst IP addr high: 2.0.0.255
      src port low: 0
     src port high: 65535
      dst port low: 0
     dst port high: 65535
      protocol low: 0
     protocol high: 255
------- Statistics

             octets: 100
       total octets: 4718591900
            packets: 1
    dropped packets: 0
       replay drops: 0
       auth packets: 1
         auth fails: 0
  encrypted packets: 1
      encrypt fails: 0
---- End statistics

       object state: active
--------------- AOM

         cpp aom id: 145
         cgm aom id: 0
          n2 aom id: 142
```

```
if aom id: 0
```

The following table describes the significant fields shown in the display.

Table 164: show platform software ipsec fp active flow identifier Field Descriptions

Field	Description
Flow id	Flow identifier.
mode	Operation mode. In this case, it is tunnel mode.
direction	Flow direction—inbound or outbound. In this case, it is outbound.
protocol	Protocol used. In this case, it is Encapsulating Security Payloads (ESP).
SPI	Security Parameters Index (SPI) that is used to identify the security association (SA).
local IP addr	IP address of the local host.
remote IP addr	IP address of the remote host.
crypto map id	Crypto map identifier.
SPD id	SPI identifier.
ACE line number	Cisco Application Control Engine (ACE) number.
QFP SA handle	Quantum Flow Processor (QFP) SA identifier.
crypto device id	Crypto device identifier.
IOS XE interface id	Interface ID in Cisco IOS XE software.
interface name	Interface name.
Crypto SA ctx id	Context identifier of the crypto SA.
cipher	Type of encryption algorithm.
auth	Type of authentication algorithm.
initial seq.number	Initial sequence number.
timeout, mins	Timeout, in minutes.
flags	Flags set for the packet flow.
Peer Flow handle	Peer flow identifier.
Time limits soft limit	Minimum permissible time limit.
Time limits hard limit	Maximum permissible time limit.
Traffic limits soft limit	Minimum permissible traffic limit.

Field	Description
Traffic limits hard limit	Maximum permissible traffic limit.
DPD	Dead peer detection (DPD).
mode	DPD mode. In this case, it is periodic.
rearm countdown	Rearm for DPD.
next notify	Status of next notification.
last in packet	Status of the last packet.
inline_tagging	Status of inline tagging.
anti-replay window	Status of anti-replay window.
SPI Selector	Information about SPI selection.
remote addr low	Starting range address of the remote host.
remote addr high	Highest range address of the remote host.
local addr low	Starting range address of the local host.
local addr high	Highest range address of the local host.
Classifier	Type of classification.
src IP addr low	Starting range of the source IP address.
src IP addr high	Highest range of the source IP address.
dst IP addr low	Starting range of the destination IP address.
dst IP addr high	Highest range of the destination IP address.
src port low	Starting range of the source port.
src port high	Highest range of the source port.
dst port low	Starting range of the destination port.
dst port high	Highest range of the destination port.
protocol low	Starting range of the protocol.
protocol high	Highest range of the protocol.
octets	Number of octets in the packet.
total octets	Total number of octets.
packets	Number of packets.
dropped packets	Number of packets dropped.

Field	Description
replay drops	Number of packets that were dropped again.
auth packets	Number of packets authenticated.
auth fails	Number of packets for which authentication failed.
encrypted packets	Number of encrypted packets.
encrypt fails	Number of packets for which encryption failed.
object state	Object state. In this case, it is active.
cpp aom id	Cisco Packet Processor Asynchronous Object Manager (AOM) identifier.
cgm aom id	Class Group Manager AOM identifier.
n2 aom id	Cavium NITROX II cryptographic coprocessor AOM identifier.
if aom id	Interface AOM identifier.

Related Commands

Command	Description
show platform hardware qfp active feature ipsec	Display IPsec feature-specific information in IPsec Cisco QFP.
show platform software ipsec fp active spd-map	Displays information about the active instances of IPsec SPD map objects.

show platform software ipsec fp active spd-map

To display information about the active instances of IPsec Security Policy Database (SPD) map objects in the Embedded Service Processor (ESP), use the **show platform software ipsec fp active spd-map** command in privileged EXEC mode.

show platform software ipsec fp active spd-map {**all** | **identifier** *number*}

Syntax Description

all	Displays information about all active IPsec flows in the instance.
identifier *number*	Displays information about the specified IPsec flow in the instance. The range is from 0 to 4294967295.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.9S	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

SPD is an ordered list of policies applied to traffic. A policy decides if a packet requires IPsec processing, if should be allowed in clear text, or should be dropped. The IPsec SPDs are derived from user configuration of crypto maps. The Internet Key Exchange (IKE) SPD is configured by the user.

Examples

The following is sample output from the **show platform software ipsec fp active spd-map all** command:

```
Device# show platform software ipsec fp active spd-map all

======== SPD map id: 11
             SPD id: 1
       interface id: 11
     interface name: GigabitEthernet1/1/3
     inbound ACL id: 65535
      local address: 0
       object state: active
         bind state: active
       enable state: active
```

The following table describes the significant fields shown in the display.

Table 165: show platform software ipsec fp active spd-map all Field Descriptions

Field	Description
SPD map id	SPD map identifier.
SPD id	SPD identifier.
interface id	Interface identifier.
interface name	Interface name.

Field	Description
inbound ACL id	Inbound access control list (ACL) identifier.
local address	IP address of the local host.
object state	Object status.
bind state	Bind status.
enable state	Enable status.

The following is sample output from the **show platform software ipsec fp active spd-map identifier** command for ID 11:

```
Device# show platform software ipsec fp active spd-map identifier 11

======== SPD map id: 11
             SPD id: 1
       interface id: 11
     interface name: GigabitEthernet1/1/3
     inbound ACL id: 65535
      local address: 0
       object state: active
       tunnel state: new
         bind state: active
       enable state: active
             aom id: 101
```

The following table describes the significant fields shown in the display.

Table 166: show platform software ipsec fp active spd-map identifier Field Descriptions

Field	Description
SPD map id	SPD map identifier.
SPD id	SPD identifier.
interface id	Interface identifier.
interface name	Interface name.
inbound ACL id	Inbound access control list (ACL) identifier.
local address	IP address of the local host.
object state	Object status.
tunnel state	Tunnel status.
bind state	Bind status.
enable state	Enable status.

Field	Description
aom id	Asynchronous Object Manager (AOM) identifier.

Related Commands

Command	Description
show platform hardware qfp active feature ipsec	Display IPsec feature-specific information in IPsec Cisco QFP.
show platform software ipsec fp active flow	Displays information about active instances of IPsec flows in the ESP.

show platform software ipsec modexp-throttle0-stats

To display modexp throttle statistics for IPsec on a device, use the **show platform software ipsec modexp-throttle0-stats**command in privileged EXEC mode.

show platform software ipsec modexp-throttle0-stats

Syntax Description

This command has no keywords or arguments.

Command Default

Modexp throttle statistics for IPsec is not displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.1	This command was introduced.

Usage Guidelines

This command displays modexp throttle statistics information on devices running on Cisco IOS XE software.

Examples

The following is a sample output of the **show platform software ipsec modexp-throttle0-stats** command:

```
Device# show platform software ipsec modexp-throttle0-stats

========= MODEXP Message Statistic Information =======
Window size: 16  Queue max size: 1024
Transmit request total: 59 sent: 59 failed: 0
Transmit send total: 59  without delay: 59  with delay: 0
Queue request total: 0, sent: 0 timeout: 0
Transmit request error: 0
Callback count: 59 pending: 0
Queue max depth: 0 current depth: 0
Transmit request rate (packet per second): 0 average rate: 0 max rate: 0
Callback receive rate (packet per second): 0 average rate: 0 max rate: 0
```

show platform software urpf qfp active configuration

To confirm and display the Unicast Reverse Path Forwarding (uRPF) configuration on a forwarding processor of the Cisco ASR 1000 Series Aggregation Services Routers, use the **show platform software urpf qfp active configuration** command in the privileged EXEC mode.

show platform software urpf qfp active configuration *ip-version interface-name*

Syntax Description

ip-version	Version of the IP. Valid values are, IPv4 and IPv6.
interface-name	Name of the interface.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 2.0S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

The uRPF configuration on an IPv4 or IPv6 interface is downloaded from the route processor to a forwarding processor and the configuration is reflected on the forwarding processor. Use the **show platform software urpf qfp active configuration** command to display the uRPF configuration on a forwarding processor.

Examples

The following is a sample output of the **show platform software urpf qfp active configuration** command:

```
Router# show platform software urpf qfp active configuration ipv6 gigabitethernet 0/0/0.777
Forwarding Manager uRPF IPv6 Configuration on Interface

Interface                Index        FLAGS
------------------------------------------------------------------------------
GigabitEthernet0/0/0.777  13

ACL: 1
ACL Binding AOM id: 152
```

The following table describes the significant fields shown in the display.

Table 167: show platform software urpf qfp active configuration

Field	Description
Interface	Interface number.
Index	Interface ID of the QFP.
ACL	Access Control List (ACL) name on uRPF.
ACL Binding	Asynchronous Object Manager (AOM) ID created to enable uRPF ACL support.

show policy-firewall config

To display the firewall configuration on the router, use the **show policy-firewall config** command in privileged EXEC mode.

show policy-firewall config {**all** | **class-map** [{*class-map-nameprotocol-name*}] | **parameter-map** [{*parameter-map-name* | **default** | **global** | **protocol-info** | **regex** [*protocol-info-name*]}] | **policy-map** [{*policy-map-nameprotocol-name*}] | **zone** [**self**] | **zone-pair**}

Command Syntax for Cisco IOS XE Release 3.14S and later

show policy-firewall config [{**zone-pair** *zone-pair-name* | **platform** [**standby**]}]

Syntax Description

all	Displays the entire firewall configuration on the router.
class-map *class-map-name*	Displays the class-maps configured on the router.
protocol-name	Displays the protocols configured for the class-map.
parameter-map	Displays the parameter-maps configured in the router.
parameter-map-name	Displays configuration information about a specific parameter map.
default	Displays configuration information about the default inspect parameter map.
global	Displays configuration information about the global inspect parameter map.
protocol-info	Displays configuration information about the protocol-specific inspect parameter map.
regex	Displays configuration information about the regex inspect parameter map.
protocol-info-name	Displays configuration information about a specific protocol.
policy-map *policy-map-name*	Displays the policy maps configured on the router.
protocol-name	Displays the protocols configured for the policy map.
zone	Displays configuration information about the zones configured on the router.
self	(Optional) Displays configuration information about the system-defined zone.
zone-pair	Displays configuration information about each zone-pair.
zone-pair-name	Security zone-pair name.
platform	Displays firewall platform information.

standby	Displays platform standby information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(1)T	This command was introduced.
Cisco IOS XE Release 3.14S	This command was modified. The *zone-pair-name* argument was added.

Usage Guidelines

Use this command to display a summary of the firewall configuration on the device.

Examples

The following is the sample output from the **show policy-firewall config all** command. The field descriptions are self-explanatory.

```
Device# show policy-firewall config all

Zone: self
  Description: System defined zone
Parameter-map Config:
 Global:
  alert on
  sessions maximum 2147483647
  waas disabled
  l2-transparent dhcp-passthrough disabled
  dropped-packets disabled
  log summary disabled
  max-incomplete low 2147483647
  max-incomplete high 2147483647
  one-minute low 2147483647
  one-minute high 2147483647
 Default:
  audit-trail off
  alert on
  max-incomplete low 2147483647
  max-incomplete high 2147483647
  one-minute low 2147483647
  one-minute high 2147483647
  udp idle-time 30
  icmp idle-time 10
  dns-timeout 5
  tcp idle-time 3600
  tcp finwait-time 5
  tcp synwait-time 30
  tcp max-incomplete host 4294967295 block-time 0
  sessions maximum 2147483647
```

The following is the sample output from the **show policy-firewall config all** command when a zone-pair is configured. The field descriptions are self-explanatory.

```
Device# show policy-firewall config all

Zone-pair              : z1-z2
Source Zone            : z1
  Member Interfaces:
    GigabitEthernet0/0/0
```

```
Destination Zone       : z2
  Member Interfaces:
    GigabitEthernet0/0/1
Service-policy inspect : pmap
  Class-map : cmap (match-all)
   Match protocol tcp
  Action : inspect
   Parameter-map : Default
  Class-map : class-default (match-any)
   Match any
  Action : drop log
   Parameter-map : Default
---------------------------
Parameter-map Configuration:
  Parameter-map type inspect: pmap
  -------------------------
   alert messages                 : on
   all application inspection     : on
   audit trailing                 : off
   logging dropped-packets        : off
   icmp session idle-time         : 10 sec, ageout-time: 10 sec
   dns session idle-time          : 5 sec
   tcp session half-open          : on, half-close: on, idle: on
   tcp session idle-time          : 3600 sec, ageout-time: 3600 sec
   tcp session FIN wait-time      : 1 sec, FIN ageout-time: 1 sec
   tcp session SYN wait-time      : 30 sec, SYN ageout-time: 30 sec
   tcp loose window scaling enforcement: off
   tcp max-half-open connections/host  : unlimited block-time: 0 min
   udp half-open session idle-time: 30000 ms, ageout-time: 30000 ms
   udp session idle-time          : 30 sec, ageout-time: 30 sec
   sessions, connections/min threshold (low) : unlimited
   sessions, connections/min threshold (high): unlimited
   sessions, connection rate threshold (low) : unlimited
   sessions, connection rate threshold (high): unlimited
   sessions, max-incomplete threshold (low)  : unlimited
   sessions, max-incomplete threshold (high) : unlimited
   sessions, maximum no. of inspect sessions : unlimited
   total number of packets per flow          : default
   zone mismatch drop option           : off
```

The following is the sample output from the **show policy-firewall config zone-pair** *zone-pair-name* command. The field descriptions are self-explanatory.

```
Device# show policy-firewall config zone-pair z1-z2

Zone-pair              : z1-z2
Source Zone            : z1
  Member Interfaces:
    GigabitEthernet0/0/0
Destination Zone       : z2
  Member Interfaces:
    GigabitEthernet0/0/1
Service-policy inspect : pmap
  Class-map : cmap (match-all)
   Match protocol tcp
  Action : inspect
   Parameter-map : Default
  Class-map : class-default (match-any)
   Match any
  Action : drop log
   Parameter-map : Default
```

The following example is a sample output from the **show policy-firewall config class-map** command:

```
Device# show policy-firewall config class-map c1

Class Map type inspect match-all c1 (id 1)
   Match access-group  101
   Match protocol http
```

The following example shows output related to user-defined parameter map:

```
Device# show policy-firewall config parameter-map params1

parameter-map type inspect params1
  audit-trail off
  alert on
  max-incomplete low 2147483647
  max-incomplete high 2147483647
  one-minute low 2147483647
  one-minute high 2147483647
  udp idle-time 30
  icmp idle-time 10
  dns-timeout 5
  tcp idle-time 3600
  tcp finwait-time 5
  tcp synwait-time 30
  tcp max-incomplete host 4294967295 block-time 0
  sessions maximum 2147483647
```

The following example shows output related default parameter map:

```
Device# show policy-firewall config parameter-map default

  audit-trail off
  alert on
  max-incomplete low 2147483647
  max-incomplete high 2147483647
  one-minute low 2147483647
  one-minute high 2147483647
  udp idle-time 30
  icmp idle-time 10
  dns-timeout 5
  tcp idle-time 3600
  tcp finwait-time 5
  tcp synwait-time 30
  tcp max-incomplete host 4294967295 block-time 0
  sessions maximum 2147483647
```

The following example shows output related to global parameter map:

```
Device# show policy-firewall config parameter-map global

  alert on
  sessions maximum 2147483647
  waas disabled
  l2-transparent dhcp-passthrough disabled
  log dropped-packets disabled
  log summary disabled
  max-incomplete low 2147483647
  max-incomplete high 2147483647
  one-minute low 2147483647
  one-minute high 2147483647
```

show policy-firewall mib

To display connection statistics of the firewall policy on the router, use the **show policy-firewall mib** command in privileged EXEC mode.

show policy-firewall mib connection-statistics {**global** | **policy** *policy-name* **zone-pair** *name* | **L4-Protocol** | **L7-Protocol**} {*name* | **all**}

Syntax Description

connection-statistics	Displays the statistics for one of the following selected options.
global	Displays the global connection statistics.
policy *policy-name*	Displays statistics for a specific firewall policy.
zone-pair *name*	Displays statistics for a zone pair in a specific firewall policy.
L4-Protocol *name*	Displays statistics for a specific Layer 4 protocol.
L7-Protocol *name*	Displays statistics for a specific Layer 7 protocol.
all	Displays statistics for all Layer 4 or Layer 7 protocols.

Command Default

Privileged EXEC (#)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Usage Guidelines

Use this command to display the global connection statistics and the statistics per protocol in Layer 4 or Layer 7 for each policy or zone pair. Use the **debug policy-firewall mib** command to toggle on or off the support for MIBs in zone-based policy firewalls.

Examples

The following is sample output from five versios of the **show policy-firewall mib**command:

```
Router# show policy-firewall mib connection-statistics global
-------------------------------------------------
Connections Attempted                           26
Connections Setup Aborted                       0
Connections Policy Declined                     0
Connections Resource Declined                   0
Connections Half Open                           0
Connections Active                              0
Connections Expired                             25
Connections Aborted                             0
Connections Embryonic                           0
Connections 1-min Setup Count                   0
Connections 5-min Setup Count                   0
Router# show policy-firewall mib connection-statistics L4-Protocol all
-------------------------------------------------
Protocol            udp
Connections Attempted                           1
Connections Setup Aborted                       0
```

```
Connections Policy Declined                       0
Connections Resource Declined                     0
Connections Half Open                             0
Connections Active                                0
Connections Aborted                               0
Connections Embryonic                             0
Connections 1-min Setup Count                     0
Connections 5-min Setup Count                     0
-------------------------------------------------
Protocol             tcp
Connections Attempted                            25
Connections Setup Aborted                         0
Connections Policy Declined                       0
Connections Resource Declined                     0
Connections Half Open                             0
Connections Active                                0
Connections Aborted                               0
Connections Embryonic                             0
Connections 1-min Setup Count                     0
Connections 5-min Setup Count                     0
Router# show policy-firewall mib connection-statistics L7-Protocol all
-------------------------------------------------
Protocol             http
Connections Attempted                            14
Connections Setup Aborted                         0
Connections Policy Declined                       0
Connections Resource Declined                     0
Connections Half Open                             0
Connections Active                                0
Connections Aborted                               0
Connections Embryonic                             0
Connections 1-min Setup Count                     0
Connections 5-min Setup Count                     0
-------------------------------------------------
Protocol             tacacs
Connections Attempted                            12
Connections Setup Aborted                         0
Connections Policy Declined                       0
Connections Resource Declined                     0
Connections Half Open                             0
Connections Active                                0
Connections Aborted                               0
Connections Embryonic                             0
Connections 1-min Setup Count                     0
Connections 5-min Setup Count                     0
Router# show policy-firewall mib connection-statistics policy inout-policy zone-pair inout
 L4-Protocol all
-------------------------------------------------
Policy            inout-policy
Zone-pair            inout
-------------------------------------------------
Protocol             udp
Connections Attempted                             1
Connections Setup Aborted                         0
Connections Policy Declined                       0
Connections Resource Declined                     0
Connections Half Open                             0
Connections Active                                0
Connections Aborted                               0
-------------------------------------------------
Protocol             tcp
Connections Attempted                            11
Connections Setup Aborted                         0
Connections Policy Declined                       0
```

```
Connections Resource Declined                    0
Connections Half Open                            0
Connections Active                               0
Connections Aborted                              0
Router# show policy-firewall mib connection-statistics policy inout-policy zone-pair inout
 L7-Protocol all
-------------------------------------------------
Policy            inout-policy
Zone-pair            inout
-------------------------------------------------
Protocol             tacacs
Connections Attempted                           12
Connections Setup Aborted                        0
Connections Policy Declined                      0
Connections Resource Declined                    0
Connections Half Open                            0
Connections Active                               0
Connections Aborted                              0
```

The table below describes the significant fields shown in the displays.

Table 168: show policy-firewall mib Field Descriptions

Field	Description
Connections Attempted	The total number of connection attempts sent to the firewall. This is a cumulative value.
Connections Policy Declined	The number of connection attempts that were declined due to a firewall security policy. This is a cumulative value.
Connections Resource Declined	The number of connection attempts that were declined due to firewall resource constraints. This is a cumulative value.
Connections Half Open	The number of connections that are being established with the firewall. This is a reflection of the current state of the system.
Connections Active	The number of connections that are currently active. This is a reflection of the current state of the system.
Connections Expired	The number of connections that were active and terminated. This is a cumulative value.
Connections Aborted	The number of connections that were abnormally terminated after a successful connection. This is a cumulative value.
Connections Embryonic	The number of embryonic application layer connections. This is a reflection of the current state of the system.
Connections 1-min Setup Count	The number of connections that the firewall attempts to establish per second averaged over the last 60 seconds. This is a reflection of the current state of the system.
Connections 5-min Setup Count	The number of connections that the firewall attempts to establish per second, averaged over the last 300 seconds. This is a reflection of the current state of the system.

Related Commands

Command	Description
debug policy-firewall mib	Toggles on or off the MIB support.

show policy-firewall session

To display the session details of a firewall policy, use the **show policy-firewall session** command in privileged EXEC mode.

show policy-firewall session [{**msrpc** | **ha** | **zone-pair** [{**ha**}]}]

Syntax Description

msrpc	(Optional) Displays the Microsoft Remote Procedure Call (MSRPC) sessions.
ha	(Optional) Displays high availability (HA) sessions pertaining to zone pairs.
zone-pair	(Optional) Displays the sessions pertaining to zone pairs.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
15.1(1)T	This command was introduced.
15.1(4)M	This command was modified. The **msrpc** keyword was added.
15.2(3)T	This command was modified. The **ha** keyword was added.

Usage Guidelines

Use the **show policy-firewall session** command to display session details. Session details can be either global, zone pair-specific, or MSRPC-specific. Global session details incorporate information about all sessions created by the firewall, and zone pair-specific details that pertain to each zone pair.

Examples

The following is sample output from the **show policy-firewall session** command:

```
Router# show policy-firewall session zone-pair

Zone-pair: zone-pair-source2destination
  Service-policy inspect : policy-test
    Class-map: class-test (match-any)
   Inspect
      Number of Established Sessions = 100
      Established Sessions
        Session 3F4DF38 (10.0.0.148:13686)=>(10.0.0.33:80) http:tcp SIS_OPEN
          Created 00:00:02, Last heard 00:00:01
          Bytes sent (initiator:responder) [257:10494]
        Session 43F0F58 (10.0.0.149:13687)=>(10.0.0.33:80) http:tcp SIS_OPEN
          Created 00:00:02, Last heard 00:00:01
          Bytes sent (initiator:responder) [274:10494]
        Session 3F3BD98 (10.0.0.98:13770)=>(10.0.0.33:80) http:tcp SIS_OPEN
          Created 00:00:02, Last heard 00:00:02
          Bytes sent (initiator:responder) [251:0]
        Session 3F2E498 (10.0.0.104:13774)=>(10.0.0.33:80) http:tcp SIS_OPEN
          Created 00:00:02, Last heard 00:00:01
          Bytes sent (initiator:responder) [277:10220]
        Session 3F3B008 (10.0.0.105:13775)=>(10.0.0.33:80) http:tcp SIS_OPEN
          Created 00:00:02, Last heard 00:00:01
```

```
          Bytes sent (initiator:responder) [264:10220]
        Session 3F31AD8 (10.0.0.108:13776)=>(10.0.0.33:80) http:tcp SIS_OPEN
          Created 00:00:02, Last heard 00:00:01
          Bytes sent (initiator:responder) [265:10220]
        Session 2F91030 (10.0.0.113:13780)=>(10.0.0.33:80) http:tcp SIS_OPEN
          Created 00:00:02, Last heard 00:00:01
          Bytes sent (initiator:responder) [257:10220]
        Session 3F35308 (10.0.0.229:13966)=>(10.0.0.33:80) http:tcp SIS_OPEN
          Created 00:00:00, Last heard 00:00:00
          Bytes sent (initiator:responder) [278:10494]
        Session 3F30B58 (10.0.0.231:13968)=>(10.0.0.33:80) http:tcp SIS_OPEN
          Created 00:00:00, Last heard 00:00:00
          Bytes sent (initiator:responder) [257:10494]
        Session 3F30588 (10.0.0.234:13969)=>(10.0.0.33:80) http:tcp SIS_OPEN
          Created 00:00:00, Last heard 00:00:00
          Bytes sent (initiator:responder) [259:10494]
      Number of Half-open Sessions = 8
      Half-open Sessions
        Session 3F32298 (10.0.0.99:13068)=>(10.0.0.33:80) http:tcp SIS_OPENING
          Created 00:00:06, Last heard 00:00:06
          Bytes sent (initiator:responder) [0:0]
        Session 2F8F510 (10.0.0.123:13428)=>(10.0.0.33:80) http:tcp SIS_OPENING
          Created 00:00:04, Last heard 00:00:04
          Bytes sent (initiator:responder) [0:0]
        Session 3F4E128 (10.0.0.125:13430)=>(10.0.0.33:80) http:tcp SIS_OPENING
          Created 00:00:04, Last heard 00:00:04
          Bytes sent (initiator:responder) [0:0]
        Session 3F4E318 (10.0.0.126:13431)=>(10.0.0.33:80) http:tcp SIS_OPENING
          Created 00:00:04, Last heard 00:00:04
          Bytes sent (initiator:responder) [0:0]
        Session 3F4E6F8 (10.0.0.127:13432)=>(10.0.0.33:80) http:tcp SIS_OPENING
          Created 00:00:04, Last heard 00:00:04
          Bytes sent (initiator:responder) [0:0]
        Session 43ECF68 (10.0.0.138:13561)=>(10.0.0.33:80) http:tcp SIS_OPENING
          Created 00:00:03, Last heard 00:00:03
          Bytes sent (initiator:responder) [0:0]
        Session 3F4D968 (10.0.0.130:13674)=>(10.0.0.33:80) http:tcp SIS_OPENING
          Created 00:00:02, Last heard 00:00:02
          Bytes sent (initiator:responder) [0:0]
        Session 3F4DB58 (10.0.0.147:13685)=>(10.0.0.33:80) http:tcp SIS_OPENING
          Created 00:00:02, Last heard 00:00:02
          Bytes sent (initiator:responder) [0:0]

      Number of Terminating Sessions = 3
      Terminating Sessions
        Session 2F9DD90 (10.0.0.203:13603)=>(10.0.0.33:80) http:tcp SIS_CLOSING
          Created 00:00:03, Last heard 00:00:02
          Bytes sent (initiator:responder) [268:10494]
        Session 3F3AA38 (10.0.0.209:13844)=>(10.0.0.33:80) http:tcp SIS_CLOSING
          Created 00:00:01, Last heard 00:00:01
          Bytes sent (initiator:responder) [251:2301]
        Session 43F20C8 (10.0.0.224:14070)=>(10.0.0.33:80) http:tcp SIS_CLOSING
          Created 00:00:00, Last heard 00:00:00
          Bytes sent (initiator:responder) [264:2301]
Zone-pair: zone-pair-destination2source
  Service-policy inspect : policy-test
    Class-map: class-test (match-any)
   Inspect
```

The table below describes the significant fields shown in the display.

Table 169: show policy-firewall session Field Descriptions

Field	Description
Number of Established Sessions	Number of established sessions. A session is established when traffic flows between the sessions.
Number of Half-open Sessions	Number of half-opened sessions. A TCP session that has not yet reached the established state is called a half-opened session.
Number of Terminating Sessions	A link or session between a pair of devices that get closed. The terminating side waits for a timeout and closes the connection between the devices. After the connection is closed, the local port of the terminating side will not be available for new connections.

The following is sample output from the **show policy-firewall session zone-pair ha** command:

```
Router# show policy-firewall session zone-pair ha

Session 3FAF888 (192.168.1.2:14401)=>(10.99.75.1:80) http:tcp SIS_OPEN/TCP_ESTAB
Created 00:00:00, Last heard 00:00:00
Bytes sent (initiator:responder) [252:2301]
HA State: ACTIVE, RG: rg_foo id 1
Session 3FAF888 (192.168.1.3:14401)=>(10.99.175.1:80) http:tcp SIS_OPEN/TCP_ESTAB
Created 00:00:00, Last heard 00:00:00
Bytes sent (initiator:responder) [252:2301]
HA State: STANDBY, RG: rg_fzooid 2
```

show policy-firewall stats

To display the statistics of the firewall activity on the router, use the **show policy-firewall stats** command in privileged EXEC mode.

show policy-firewall stats [{**all** | **drop-counters** | **zone-pair** [**name**]}]

Syntax Description

all	(Optional) Displays all firewall statistics on the router.
drop-counters	(Optional) Displays the number of packets dropped for each error code.
zone-pair *name*	(Optional) Displays statistics pertaining to zone-pair.

Command Default

Privileged EXEC (#)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Usage Guidelines

This command provides the statistics of all the firewall activity on the router. The command displays the box-wide statistics or the statistics for each zone pair. To get all statistics, use the **all** keyword. Use the **drop-counters** keyword to display the packets dropped and grouped by their error codes. The output displays only the error codes for which the drop counter is greater than zero. If the number of packets dropped is similar for multiple error codes, the error codes are sorted in alphabetical order.

Examples

The following is sample output from the **show policy-firewall stats** command. The field descriptions are self-explanatory.

```
Router# show policy-firewall stats drop-counters
REASON                  PACKETS DROPPED
    Invalid Header length               39
    policy match failure               38
    Police rate limiting               37
    Session limiting                36
    Bidirectional traffic disabled              35
    SYN with data or with PSH/URG flags               34
    Segment matching no TCP connection               33
    Invalid Segment               32
    Invalid Seq#               31
    Invalid Ack (or no Ack)               30
    Invalid Flags               29
    Invalid Checksum               28
    SYN inside current window               27
    RST inside current window               26
    Out-Of-Order Segment               25
    Retransmitted Segment               24
    Retransmitted Segment with Invalid Flags               23
    Stray Segment               22
    Internal Error               21
    Invalid Window scale option               20
    Invalid TCP options               19
    No zone-pair between zones               18
    One of the interfaces not being configured for zoning 17
```

```
Policy not present on zone-pair              16
DROP action found in policy-map               15
```

show policy-firewall stats vrf

To display VPN routing and forwarding (VRF)-level policy firewall statistics, use the **show policy-firewall stats vrf** command in user EXEC or privileged EXEC mode.

show policy-firewall stats vrf [*vrf-pmap-name*]

Syntax Description

vrf-pmap-name	(Optional) VRF name.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.3S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was modified. The command output was modified to display UDP and Internet Control Message Protocol (ICMP) half-opened session counts.

Examples

The following is sample output from the **show policy-firewall stats vrf** command:

```
Router# show policy-firewall stats vrf vrf-default

  VRF: default, Parameter-Map: vrf-default
  Interface reference count: 1
       Total Session Count(estab + half-open): 0, Exceed: 0
       Total Session Aggressive Aging Period Off, Event Count: 0

                Half Open
       Protocol Session Cnt     Exceed
       -------- -----------     ------
       All      0               0
       UDP      0               0
       ICMP     0               0
       TCP      0               0

       TCP Syn Flood Half Open Count: 0, Exceed: 0
       Half Open Aggressive Aging Period Off, Event Count: 0
```

The table below describes the significant fields shown in the display.

Table 170: show policy-firewall stats vrf Field Descriptions

Field	Description
Total Session Count	Total session count.
Exceed	Number of sessions that exceeded the configured session count.
Total Session Aggressive Aging Period Off	Indicates whether aggressive aging is enabled (On) or disabled (Off).

Field	Description
Event Count	The number of times the event has been enabled in the past.
TCP Syn Flood Half Open Count	Number of half-open synchronization (SYN) packets that exceeded the configured SYN flood rate limit.
Half Open Aggressive Aging Period Off	Aggressive aging of half-opened sessions is not configured.

Related Commands

Command	Description
clear policy-firewall stats vrf	Clears the policy firewall statistics counter at a VRF level.

show policy-firewall stats vrf global

To display global VPN Routing and Forwarding (VRF) firewall policy statistics, use the **show policy-firewall stats vrf global**command in user EXEC or privileged EXEC mode.

show policy-firewall stats vrf global

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default settings.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.3S	This command was introduced.

Examples

The following is sample output from the **show policy-firewall stats vrf global** command:

```
Router# show policy-firewall stats vrf global

Global table statistics
       total_session_cnt: 0
       exceed_cnt:        0
       tcp_half_open_cnt: 0
       syn_exceed_cnt:    0
```

The table below describes the fields shown in the display.

Table 171: show policy-firewall stats vrf global Field Descriptions

Field	Description
total_session_cnt	Total session count.
exceed_cnt	Number of sessions that exceeded the configured session count.
tcp_half_open_cnt	TCP half-open sessions configured at a global VRF level. When the configured session limit is reached, the TCP synchronization (SYN) cookie verifies the source of the half-open TCP sessions before creating more sessions. A TCP half-open session is a session that has not reached the established state.
syn_exceed_cnt	Number of SYN packets that exceeded the configured SYN flood rate limit.

Related Commands

Command	Description
clear policy-firewall stats vrf global	Clears the global VRF policy firewall statistics.

show policy-firewall stats zone

To display policy firewall statistics at a zone level, use the **show policy-firewall stats zone** command in user EXEC or privileged EXEC mode.

show policy-firewall stats zone [*zone-name*]

Syntax Description

zone-name	(Optional) Zone name.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.3S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was modified. The command output was modified to display threat detection statistics.

Examples

The following is sample output from the **show policy-firewall stats zone** command:

```
Router# show policy-firewall stats zone zone02

Zone: zone02
 Parameter-map: zonepmap
 TCP SYN packet conform limit: 0
 TCP SYN packet exceed limit: 0

 Threat Detection Statistics:
                      Average(eps)   Current(eps)  Threat   Total events
  10-min Basic FW Drop:    0              0           0          20
  10-min Inspection Drop:  0              0           0          70
  10-min Syn Attack:       0              0           0          0
```

The table below describes the significant fields shown in the display.

Table 172: show policy-firewall stats zone Field Descriptions

Field	Description
Zone	Name of the zone.
Parameter-map	Name of the configured zone-type parameter map.
TCP SYN packet conform limit	Number of TCP synchronization (SYN) packets that are within the configured limit.
TCP SYN packet exceed limit	Number of TCP SYN packets that exceeded the configured SYN packet rate limit.

Field	Description
Basic FW Drop	Threat detection rate for firewall drop events.
Inspection Drop	Threat detection rate for firewall inspection-based drop events.
Syn Attack	Threat detection rate for SYN cookie attack events.

Related Commands

Command	Description
clear policy-firewall stats zone	Clears the policy firewall statistics counter at a zone level.
tcp syn-flood limit	Configures a limit to the number of TCP half-open sessions before triggering SYN cookie processing for new SYN packets.
threat-detection	Configures basic threat detection.

show policy-firewall summary-log

To display summary logs, use the **show policy-firewall summary log** command in privileged EXEC mode.

show policy-firewall summary-log

Syntax Description

This command has no arguments or keywords.

Command Default

Summary logs are not displayed.

Command Modes

Privileged EXEC(#)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Usage Guidelines

Use this command to display the summary logs captured as follows:

- Configured flow
- Configured flow value
- Number of flows

Note When the number of flows for the log summary reaches the configured flow value, some flows are not summarized.

Examples

The following is sample output from the **show policy-firewall summary-log**. The field descriptions are self-explanatory.

```
Router# show policy-firewall summary-log
*Apr 1 12:38:29.103: %FW-6-LOG_SUMMARY: 10 http packets were dropped from
10.0.0.1:1024 => 20.0.0.1:23 (target: class)-(z1toz2:C1)
```

Related Commands

Command	Description
clear policy-firewall	Clears the information collected by the firewall.

show policy-map type inspect

To display a specified policy map, use the **show policy-map type inspect** command in privileged EXEC mode.

show policy-map type inspect [*policy-map-name*] [**class** *class-map-name*]

Syntax Description

policy-map-name	(Optional) Name of the policy map.
class *class-map-name*	(Optional) Name of the class map.

Command Default

If a policy-map name is not specified, all Level 7 policy maps are displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(6)T	This command was introduced.

Examples

The following example displays the policy map for policy map p1:

```
Router # show policy-map type inspect p1

 Policy Map type inspect p1
  Class c1
   Inspect
```

The following example shows sample command output:

```
Router# show policy-map type inspect p_inside

Policy Map type inspect p_inside
 Description: Policy map with inspect action
 Class c_permit
  Pass
 Class c_test
 Class class-default
```

The table below describes the significant fields shown in the display.

Table 173: show policy-map type inspect Field Descriptions

Field	Description
p_inside	Name of the policy map.
Description	Description of the policy map.
Class	Name of the class map.
Pass	Allows packets to be sent to the router without being inspected.

show policy-map type inspect urlfilter

To display the details of a URL filtering policy map, use the **show policy-map type inspect urlfilter** command in privileged EXEC mode.

show policy-map type inspect urlfilter [*policy-map-name*]

Syntax Description

policy-map-name	(Optional) Name of the policy map for which details are displayed.

Command Default

The details of all URL filtering policy maps are displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(15)XZ	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use the **show policy-map type inspect urlfilter**command to display the details of all URL filtering policy maps. To display the details of a particular URL filtering policy map, specify the name of the policy map.

The output of the **show ip urlfilter cache** command displays the pages cached by a device.

Examples

The following is sample output from the **show policy-map type inspect urlfilter** command for a policy map named websense-policy:

```
Router# show policy-map type inspect urlfilter websense-policy

policy-map type inspect urlfilter url-websense-policy
  parameter-map urlfpolicy websense websense-parameter-map
  class type urlfilter trusted-domain-lists
   allow
  class type urlfilter untrusted-domain-lists
   reset
  class type urlfilter block-url-keyword-lists
   reset
  class type urlfilter websense websense-map
   server-specified-action
```

show policy-map type inspect zone-pair

To display runtime inspect type policy map statistics and other information such as sessions existing on a specified zone pair, use the **show policy-map type inspect zone-pair** command in privileged EXEC mode.

show policy-map type inspect zone-pair[{*zone-pair-name*[{**sessions**}]}] [**sessions**]
ipv6 | {**destination** *destination-ip* [{**source***source-ip* }] | **source***source-ip*[{**destination** *destination-ip* }]}
destination *destination-ip*[{**source***source-ip*}]
source*source-ip*[{**destination** *destination-ip*}]

Syntax Description

zone-pair-name	(Optional) Zone pair for which the system displays the runtime inspect type policy-map statistics.
sessions	(Optional) Displays stateful packet inspection sessions created because a policy map is applied on the specified zone pair.
ipv6	(Optional) Displays information about the IPv6 session.
destination *destination-ip*	(Optional) Displays information about the destination IPv4 or IPv6 address of the session.
source *source-ip*	(Optional) Displays information about the source IPv4 or IPv6 address of the session.

Command Default

Information about policy maps for all zone pairs is displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.4(9)T	This command was modified. The output was enhanced to display the police action configuration.
12.4(15)XZ	This command was integrated into Cisco IOS Release 12.4(15)XZ and implemented on the following platforms: Cisco 881 and Cisco 888.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.
Cisco IOS XE Release 3.4S	This command was modified. The output was enhanced to display the General Packet Radio Service (GPRS) Tunneling Protocol (GTP) configuration.
Cisco IOS XE Release 3.6S	This command was modified. The output was enhanced to display both IPv4 and IPv6 firewall sessions.
Cisco IOS XE Release 3.9S	This command was modified. The **destination**, **ipv6**, and **source** keywords and the*destination-ip* and *source-ip* arguments were added.

Usage Guidelines

If you do not specify a zone-pair name, policy maps on all zone pairs are displayed.

When packets are matched to an access group (**match access-group**), a protocol (**match protocol**), or a class map (**match class-map**), a traffic rate is generated for these packets. In a zone-based firewall policy, only the first packet that creates a session matches the policy. Subsequent packets in this flow do not match the filters in the configured policy, but instead match the session directly. The statistics related to subsequent packets are shown as part of the "inspect" action and are displayed using the **show policy-map type inspect zone-pair sessions** command.

Command Limitations

The cumulative counters in the **show policy-map type inspect zone-pair** command output do not increment for **match** statements in a nested class map configuration in Cisco IOS Releases 12.4(15)T and 12.4(20)T. The problem with the counters exists regardless of whether the top-level class map uses the **match-any** or **match-all** keyword.

The following configuration example shows the match counter problem:

```
class-map type inspect match-any y
 match protocol tcp
 match protocol icmp
class-map type inspect match-all x
 match class y
```

The following sample output from the **show policy-map type inspect zone-pair** command displays cumulative counters for the above configuration (if the class map matches any class map):

```
Device# show policy-map type inspect zone-pair sessions

policy exists on zp
 Zone-pair: zp
  Service-policy inspect : fw
    Class-map: x (match-any)
      Match: class-map match-any y
        2 packets, 48 bytes   <======== Cumulative class map counters are incrementing.
        30 second rate 0 bps
        Match: protocol tcp
          0 packets, 0 bytes     <===== The match for the protocol is not incrementing.
          30 second rate 0 bps
        Match: protocol icmp
          0 packets, 0 bytes
          30 second rate 0 bps
   Inspect
      Number of Established Sessions = 1
      Established Sessions
        Session 53105C0 (10.1.1.2:19180)=>(10.2.1.2:23) tacacs:tcp SIS_OPEN
          Created 00:00:02, Last heard 00:00:02
          Bytes sent (initiator:responder) [30:69]
    Class-map: class-default (match-any)
      Match: any
      Drop
        0 packets, 0 bytes
```

Examples

The following sample output from the **show policy-map type inspect zone-pair** command shows information about zone pairs zp and trusted-untrusted:

```
Device# show policy-map type inspect zone-pair zp

 Zone-pair: zp
  Service-policy : p1
```

```
   Class-map: c1 (match-all)
    Match: protocol tcp
    Inspect
     Session creations since subsystem startup or last reset 0
     Current session counts (estab/half-open/terminating) [0:0:0]
     Maxever session counts (estab/half-open/terminating) [0:0:0]
     Last session created never
     Last statistic reset never
     Last session creation rate 0
     half-open session total 0
   Class-map: c2 (match-all)
    Match: protocol udp
    Pass
     0 packets, 0 bytes
   Class-map: class-default (match-any)
    Match: any
    Drop
     0 packets, 0 bytes
```

```
Device# show policy-map type inspect zone-pair trusted-untrusted

 Zone-pair: trusted-untrusted
  Service-policy inspect : firewall-policy
Class-map: class_4 (match-any)
      Match: protocol dbcontrol-agent
      Match: protocol ddns-v3
      Match: protocol dhcp-failover
      Match: protocol discard
      Match: protocol dns
      Match: protocol dnsix
      Match: protocol echo
      Match: protocol entrust-svc-handler
      Inspect
        Packet inspection statistics [process switch:fast switch]
        dns packets: [0:28949015]
        Session creations since subsystem startup or last reset 4
        Current session counts (estab/half-open/terminating) [0:0:0]
        Maxever session counts (estab/half-open/terminating) [1:0:0]
        Last session created 00:06:16
        Last statistic reset never
        Last session creation rate 0
        Last half-open session total 0
```

Note Only some protocols that undergo Layer 7 inspections have dedicated statistics; others are grouped into either TCP statistics or UDP statistics.

The following is sample output from the **show policy-map type inspect zone-pair** command for a GTP configuration:

```
Device# show policy-map type inspect zone-pair zp

Zone-pair: zp
  Service-policy inspect : L4-Policy

    Class-map: L4-Class (match-all)
      Match:  protocol gtpv0
      Inspect
        Session creations since subsystem startup or last reset 0
        Current session counts (estab/half-open/terminating) [0:0:0]
```

```
      Maxever session counts (estab/half-open/terminating) [0:0:0]
      Last session created never
      Last statistic reset never
      Last session creation rate 0
      Last half-open session total 0
    Service-policy inspect gtpv0 : L7-Policy

      Class-map: L7-Class (match-any)
        0 packets, 0 bytes
        30 second offered rate 0000 bps, drop rate 0000 bps
        Match:   match mcc 772 mnc 331

      Class-map: class-default (match-any)
        0 packets, 0 bytes
        30 second offered rate 0000 bps, drop rate 0000 bps
        Match:  any

  Class-map: class-default (match-any)
    Match:  any
    Drop (default action)
      0 packets, 0 bytes
```

The following is sample output from the **show policy-map type inspect zone-pair sessions** command:

```
Device# show policy-map type inspect zone-pair sessions

Zone-pair: hi2int
  Service-policy inspect : pg1
    Class-map: c1 (match-any)
      Match: protocol ftp
      Match: protocol telnet
      Match: protocol smtp
      Match: protocol http
      Match: protocol tacacs
      Match: protocol dns
      Match: protocol sql-net
      Match: protocol https
      Match: protocol tftp
      Match: protocol gopher
      Match: protocol finger
      Match: protocol kerberos
      Match: protocol pop3
      Match: protocol sunrpc
      Match: protocol msrpc
      Match: protocol icmp
      Inspect
        Established Sessions
         Session 10E28550 (10.1.1.1:50536)=>(172.16.1.1:111) sunrpc SIS_OPEN
          Created 00:09:44, Last heard 00:09:18
          Bytes sent (initiator:responder) [108:0]
         Session 10E28550 (10.1.1.1:39377)=>(172.16.1.1:150) sql-net SIS_CLOSED
          Created 00:03:01, Last heard 00:03:01
          Bytes sent (initiator:responder) [0:0]
         Session 10E2859C (10.1.1.1:39377)=>(172.16.1.1:110) pop3 SIS_CLOSED
          Created 00:02:59, Last heard 00:02:59
          Bytes sent (initiator:responder) [0:0]
         Session 10E285E8 (10.1.1.1:39377)=>(172.16.1.1:443) https SIS_CLOSED
          Created 00:03:33, Last heard 00:03:33
          Bytes sent (initiator:responder) [0:0]
    Class-map: class-default (match-any)
      Match: any
      Drop (default action)
        147127 packets, 8485742 bytes
```

Note In the preceding sample output, the information displayed below the Class-map field is the traffic rate (bits-per-second) of the traffic belonging to only the connection-initiating traffic. Unless the connection setup rate is significantly high and sustained for multiple intervals over which the rate is computed, no significant data is shown for the connection.

The following sample output from the **show policy-map type inspect zone-pair sessions** command displays IPv6 firewall sessions:

```
Device# show policy-map type inspect zone-pair sessions

Zone-pair: hi2int
  Service-policy inspect : pg1

    Class-map: c1 (match-any)
      Match: protocol ftp
      Match: protocol telnet
      Match: protocol icmp

      Inspect
        Established Sessions
         Session 10E28550 ([2001:DB8::1]:50536)=>( [2001:DB8:2::1]:111) sunrpc SIS_OPEN
          Created 00:09:44, Last heard 00:09:18
          Bytes sent (initiator:responder) [108:0]
        Session 10E28550 ([2001:DB8::1]:39377)=>([2001:DB8:2::1]:150)  sql-net IS_CLOSED
          Created 00:03:01, Last heard 00:03:01
          Bytes sent (initiator:responder) [0:0]

    Class-map: class-default (match-any)
      Match: any
      Drop (default action)
        147127 packets, 8485742 bytes
```

The following sample output from the **show policy-map type inspect zone-pair** command displays the police action configuration:

```
Device# show policy-map type inspect zone-pair

Zone-pair: zp
Service-policy inspect : test-udp
  Class-map: check-udp (match-all)
   Match: protocol udp
   Inspect
    Packet inspection statistics [process switch:fast switch]
    udp packets: [3:4454]
    Session creations since subsystem startup or last reset 92
    Current session counts (estab/half-open/terminating) [5:33:0]
    Maxever session counts (estab/half-open/terminating) [5:59:0]
    Last session created 00:00:06
    Last statistic reset never
    Last session creation rate 61
    Last half-open session total 33
   Class-map: class-default (match-any)
   Match: any
   Drop (default action)
   0 packets, 0 bytes
```

The table below describes the significant fields shown in the display:

Table 174: show parameter-map type inspect zone-pair Field Descriptions

Field	Description
Zone-pair	Name of the configured security zone pair.
Service-policy inspect	Name of the service policy that was inspected.
Class-map	Name of the configured class map and the configured match criterion.
Match	Protocols that were configured as match criteria.
Inspect	Session details such as packets received, current session count, and total session count.

Related Commands

Command	Description
match access-group	Configures the match criteria for a class map on the basis of the specified ACL.
match class-map	Uses a traffic class as a classification policy.
match protocol	Configures the match criterion for a class map on the basis of a specified protocol.
policy-map type inspect	Creates a Layer 3 and Layer 4 or a Layer 7 (protocol-specific) inspect-type policy map.

show policy-map type inspect zone-pair urlfilter

To display the details of a URL filtering policy map--URL filter state, URL filter statistics, and URL filter server details--use the **show policy-map type inspect zone-pair urlfilter** command in privileged EXEC mode.

show policy-map type inspect zone-pair [*zone-pair-name*] **urlfilter cache** [**detail**]

Syntax Description

zone-pair-name	(Optional) Zone pair for which the system will display the runtime inspect type policy-map statistics. Default: The requested information is shown for all zone pairs.
cache	Displays information about the URL filter cache.
detail	(Optional) Displays each entry in the cache. Because cache entries can be long, only the first few bytes are displayed.

Command Default

The URL filter information for all zone pairs is displayed. Details about the URL filtering cache are not displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.4(15)XZ	This command was implemented on the following platforms: Cisco 881 and Cisco 888. The **detail** keyword was added to show more information about the URL filtering cache.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T. The **detail** keyword was added to show more information about the URL filtering cache.

Examples

The following example shows sample output for a Websense URL filtering server:

```
Router# show policy-map type inspect zone-pair urlfilter cache

Zone-pair: zp
 Urlfilter
 Websense URL Filtering is ENABLED

 Websense Primary server: 10.3.3.3(port : 15868)
 recount: 0
 Current packet buffer count(in use): 0
 Current cache entry count: 0
 Maxever request count: 0
 Maxever packet buffer count: 0
 Maxever cache entry count: 0
 Total requests sent to URL Filter Server :0
 Total responses received from URL Filter Server :0
 Total requests allowed: 0
 Total requests blocked: 0
Drop (default action)
```

```
 packets, 0 bytes
 Service-policy inspect : test
  Class-map: test (match-all)
   Match: protocol http
  Class-map: class-default (match-any)
   Match: any
```

The following example shows sample output for a Trend Micro URL filtering server, including the cache details:

```
Router# show policy-map type inspect zone-pair urlfilter cache detail

policy exists on zp zp_in
 Zone-pair: zp_in
 Service-policy inspect : trend-global-policy
  Class-map: http-class (match-all)
   Match: protocol http
   Match: access-group 101
 Inspect
   Packet inspection statistics [process switch:fast switch]
   tcp packets: [3353:0]
   Session creations since subsystem startup or last reset 21
   Current session counts (estab/half-open/terminating) [3:0:0]
   Maxever session counts (estab/half-open/terminating) [4:1:1]
   Last session created 00:00:22
   Last statistic reset never
   Last session creation rate 7
   Maxever session creation rate 14
   Last half-open session total 0
   Maximum number of bytes in cache: 131072000
   Time to live for eache cache entry (in hrs): 1
   Total number of bytes used by cache: 442
   Number of bytes used by domain type cache: 442
   Number of bytes used by directory type cache: 0
   ------------------------------------------------------------
   URL                                  Age   Access #/  Cat::Rep
   (Directory cache end with /)   (day:h:m:s)    Idle Time
   ------------------------------------------------------------
   example.com             0:00:00:23      28   58::100

   example1.com            0:00:00:25       1   56::100

   example.example2.com    0:00:00:34       1   56::100

  Class-map: class-default (match-any)
   Match: any
   Drop
     0 packets, 0 bytes

policy exists on zp zp_out
 Zone-pair: zp_out

 Service-policy inspect : icmp_permit

  Class-map: icmp_permit (match-all)
   Match: access-group 110
   Pass
    0 packets, 0 bytes

  Class-map: class-default (match-any)
   Match: any
   Drop
    0 packets, 0 bytes
```

show port-security

To display information about the port-security setting in EXEC command mode, use the **show port-security** command.

show port-security [**interface** *interface interface-number*]
show port-security [**interface** *interface interface-number*] {**address** | **vlan**}

Syntax Description

interface *interface*	(Optional) Specifies the interface type; possible valid values are **ethernet**, **fastethernet**, **gigabitethernet**, and **longreachethernet**.
interface-number	Interface number. Valid values are 1 to 6.
address	Displays all the secure MAC addresses that are configured on all the switch interfaces or on a specified interface with aging information for each address.
vlan	Virtual LAN.

Command Default

This command has no default settings.

Command Modes

EXEC

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(18)SXE	The **address** keyword was added to display the maximum number of MAC addresses configured per VLAN on a trunk port on the Supervisor Engine 720 only.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.

Usage Guidelines

The **vlan** keyword is supported on trunk ports only and displays per-Vlan maximums set on a trunk port.

The *interface-number* argument designates the module and port number. Valid values for *interface-number* depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48.

Examples

This example shows the output from the **show port-security** command when you do not enter any options:

```
Router# show port-security
Secure Port      MaxSecureAddr  CurrentAddr  SecurityViolation  Security
Action
                    (Count)        (Count)      (Count)
-------------------------------------------------------------------------------
```

```
     Fa5/1           11             11             0             Shutdown
     Fa5/5           15             5              0             Restrict
     Fa5/11          5              4              0             Protect
---------------------------------------------------------------------------

Total Addresses in System: 21
Max Addresses limit in System: 128
Router#
```

This example shows how to display port-security information for a specified interface:

```
Router# show port-security interface fastethernet 5/1
Port Security: Enabled
Port status: SecureUp
Violation mode: Shutdown
Maximum MAC Addresses: 11
Total MAC Addresses: 11
Configured MAC Addresses: 3
Aging time: 20 mins
Aging type: Inactivity
SecureStatic address aging: Enabled
Security Violation count: 0
Router#
```

This example show how to display all the secure MAC addresses that are configured on all the switch interfaces or on a specified interface with aging information for each address:

```
Router# show port-security address
Default maximum: 10
VLAN Maximum Current
1    5       3
2    4       4
3    6       4
Router#
```

Related Commands

Command	Description
clear port-security	Deletes configured secure MAC addresses and sticky MAC addresses from the MAC address table.

show ppp queues

To monitor the number of requests processed by each authentication, authorization, and accounting (AAA) background process, use the **show ppp queues**command inprivilegedEXEC mode.

show ppp queues

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3(2)AA	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **show ppp queues** command to display the number of requests handled by each AAA background process, the average amount of time it takes to complete each request, and the requests still pending in the work queue. This information can help you balance the data load between the network access server and the AAA server.

This command displays information about the background processes configured by the **aaa processes** global configuration command. Each line in the display contains information about one of the background processes. If there are AAA requests in the queue when you enter this command, the requests will be printed as well as the background process data.

Examples

The following example shows output from the **show ppp queues** command:

```
Router# show ppp queues
Proc #0   pid=73  authens=59   avg. rtt=118s. authors=160  avg. rtt=94s.
Proc #1   pid=74  authens=52   avg. rtt=119s. authors=127  avg. rtt=115s.
Proc #2   pid=75  authens=69   avg. rtt=130s. authors=80   avg. rtt=122s.
Proc #3   pid=76  authens=44   avg. rtt=114s. authors=55   avg. rtt=106s.
Proc #4   pid=77  authens=70   avg. rtt=141s. authors=76   avg. rtt=118s.
Proc #5   pid=78  authens=64   avg. rtt=131s. authors=97   avg. rtt=113s.
Proc #6   pid=79  authens=56   avg. rtt=121s. authors=57   avg. rtt=117s.
Proc #7   pid=80  authens=43   avg. rtt=126s. authors=54   avg. rtt=105s.
Proc #8   pid=81  authens=139  avg. rtt=141s. authors=120  avg. rtt=122s.
Proc #9   pid=82  authens=63   avg. rtt=128s. authors=199  avg. rtt=80s.
queue len=0 max len=499
```

The table below describes the fields shown in the example.

Table 175: show ppp queues Field Descriptions

Field	Description
Proc #	Identifies the background process allocated by the **aaa processes** command to handle AAA requests for PPP. All of the data in this row relates to this process.
pid=	Identification number of the background process.
authens=	Number of authentication requests the process has performed.
avg. rtt=	Average delay (in seconds) until the authentication request was completed.
authors=	Number of authorization requests the process has performed.
avg. rtt=	Average delay (in seconds) until the authorization request was completed.
queue len=	Current queue length.
max len=	Maximum length the queue ever reached.

Related Commands

Command	Description
aaa processes	Allocates a specific number of background processes to be used to process AAA authentication and authorization requests for PPP.

show pppoe session

To display information about currently active PPP over Ethernet (PPPoE) sessions, use the **show pppoe session** in privileged EXEC mode.

show pppoe session [{**all** | **interface** *type number* | **packets** [{**all** | **interface** *type number* | **ipv6** }]}]

Syntax Description

all	(Optional) Displays detailed information about the PPPoE session.
interface *type number*	(Optional) Displays information about the interface on which the PPPoE session is active.
packets	(Optional) Displays packet statistics for the PPPoE session.
ipv6	(Optional) Displays PPPoE session packet statistics for IPv6 traffic

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(4)YG	This command was introduced on the Cisco SOHO 76, 77, and 77H routers.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T and was enhanced to display information about relayed PPPoE Active Discovery (PAD) messages.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and support was added for the Cisco 7200, 7301, 7600, and 10000 series platforms.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2 and the output following the use of the **all** keyword was modified to indicate if a session is Interworking Functionality (IWF)-specific or if the **tag ppp-max-payload** tag is in the discovery frame and accepted.
12.4(15)XF	The output was modified to display Virtual Multipoint Interface (VMI) and PPPoE process-level values.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T to support VMIs in Mobile Ad Hoc Router-to-Radio Networks (MANETs).
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
Cisco IOS XE Release 2.5	This command was implemented on Cisco ASR 1000 series routers.
Cisco IOS XE Release 3.5S	This command was modified. The **ipv6** keyword was added.

Single Session: Example

The following is sample output from the show pppoe session command:

```
Router# show pppoe session
     1 session  in FORWARDED (FWDED) State
     1 session  total
```

Uniq ID	PPPoE SID	RemMAC	Port	VT	VA	State	LocMAC	VA-st
26	19	0001.96da.a2c0	Et0/0.1	5	N/A	RELFWD	000c.8670.1006	VLAN:3434

PPPoE Session with IWF and ppp-max-payload Tag Example

The following is sample output from the **show pppoe session** command when there is an IWF session and the ppp-max-payload tag is accepted in the discovery frame (available in Cisco IOS Release 12.2(31)SB2):

```
Router# show pppoe session

     1 session  in LOCALLY_TERMINATED (PTA) State
     1 session  total.  1 session of it is IWF type
```

Uniq ID	PPPoE SID	RemMAC	Port	VT	VA	State	LocMAC	VA-st	Type
26	21	0001.c9f2.a81e	Et1/2	1	Vi2.1	PTA	0006.52a4.901e	UP	IWF

The table below describes the significant fields shown in the displays.

Table 176: show pppoe session Field Descriptions

Field	Description
Uniq ID	Unique identifier for the PPPoE session.
PPPoE SID	PPPoE session identifier.
RemMAC	Remote MAC address.
Port	Port type and number.
VT	Virtual-template interface.
VA	Virtual access interface.

Field	Description
State	Displays the state of the session, which will be one of the following: • FORWARDED • FORWARDING • LCP_NEGOTIATION • LOCALLY_TERMINATED • PPP_START • PTA • RELFWD (a PPPoE session was forwarded for which the Active discovery messages were relayed) • SHUTTING_DOWN • VACCESS_REQUESTED
LocMAC	Local MAC address.

show pppoe session all: Example

The following example shows information per session for the **show pppoe session all** command.

```
Router# show pppoe session all

Total PPPoE sessions 1
session id: 21
local MAC address: 0006.52a4.901e, remote MAC address: 0001.c9f2.a81e
virtual access interface: Vi2.1, outgoing interface: Et1/2, IWF
PPP-Max-Payload tag: 1500
    15942 packets sent, 15924 received
    224561 bytes sent, 222948 received
```

PPPoE Session Including Credit Flow Statistics: Example

The following example shows the output from the **show pppoe session all** command. This version of the display includes PPPoE credit flow statistics for the session.

```
Router# show pppoe session all
Total PPPoE sessions 1
session id: 1
local MAC address: aabb.cc00.0100, remote MAC address: aabb.cc00.0200
virtual access interface: Vi2, outgoing interface: Et0/0
17 packets sent, 24 received
1459 bytes sent, 2561 received
PPPoE Flow Control Stats
Local Credits: 65504 Peer Credits: 65478
Credit Grant Threshold: 28000 Max Credits per grant: 65534
PADG Seq Num: 7 PADG Timer index: 0
PADG last rcvd Seq Num: 7
PADG last nonzero Seq Num: 0
```

```
PADG last nonzero rcvd amount: 0
PADG Timers: [0]-1000 [1]-2000 [2]-3000 [3]-4000
PADG xmit: 7 rcvd: 7
PADC xmit: 7 rcvd: 7
PADQ xmit: 0 rcvd: 0
```

show pppoe session packet ipv6: Example

The following is sample output form the **show pppoe session packet ipv6** command. The output field descriptions are self-explanatory.

```
Device# show pppoe session packet ipv6

SID     Pkts -In         Pkts-Out        Bytes-In        Bytes-Out
1       2800            9               2721600         770
```

Related Commands

Command	Description
clear pppoe relay context	Clears PPPoE relay contexts created for relaying PAD messages.
show pppoe relay context all	Displays PPPoE relay contexts created for relaying PAD messages.

show private-hosts access-lists

To display the access lists for your Private Hosts configuration, use the **show private-hosts access-lists** command in privileged EXEC mode.

show private-hosts access-lists

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Examples

The following example shows how to display the Private Hosts access lists for your configuration:

```
Router# s
how private-hosts access-lists

Promiscuous ACLs
Action Permit   Sequence # 010
    Source:0000.1111.4001 0000.0000.0000 Destination:0000.0000.0000 ffff.ffff.ffff
Action Deny     Sequence # 020
    Source:0000.0000.0000 ffff.ffff.ffff Destination:0000.0000.0000 ffff.ffff.ffff
Isolated ACLs
Action Deny     Sequence # 010
    Source:0000.1111.4001 0000.0000.0000 Destination:0000.0000.0000 ffff.ffff.ffff
Action Permit   Sequence # 020
    Source:0000.0000.0000 ffff.ffff.ffff Destination:0000.1111.4001 0000.0000.0000 Action
Redirect Sequence # 030 Redirect index 6
    Source:0000.0000.0000 ffff.ffff.ffff Destination:ffff.ffff.ffff 0000.0000.0000
Action Permit   Sequence # 040
    Source:0000.0000.0000 ffff.ffff.ffff Destination:0100.5e00.0000 0000.007f.ffff
    Source:0000.0000.0000 ffff.ffff.ffff Destination:3333.0000.0000 0000.ffff.ffff
Action Deny     Sequence # 050
    Source:0000.0000.0000 ffff.ffff.ffff Destination:0000.0000.0000 ffff.ffff.ffff
Mixed ACLs
Action Permit   Sequence # 010
    Source:0000.1111.4001 0000.0000.0000 Destination:ffff.ffff.ffff 0000.0000.0000 Action
Redirect Sequence # 020 Redirect index 6
    Source:0000.0000.0000 ffff.ffff.ffff Destination:ffff.ffff.ffff 0000.0000.0000
Action Permit   Sequence # 030
    Source:0000.1111.4001 0000.0000.0000 Destination:0000.0000.0000 ffff.ffff.ffff
Action Permit   Sequence # 040
    Source:0000.0000.0000 ffff.ffff.ffff Destination:0000.1111.4001 0000.0000.0000
Action Deny     Sequence # 050
    Source:0000.0000.0000 ffff.ffff.ffff Destination:0000.0000.0000 ffff.ffff.ffff
```

Related Commands

Command	Description
show fm private-hosts	Displays information about the Private Hosts feature manager.
show private-hosts configuration	Displays Private Hosts configuration information for the networking device.
show **private-hosts interface configuration**	Displays Private Hosts configuration information for individual interfaces.

show private-hosts configuration

To display information about the Private Hosts configuration on the router, use the **show private-hosts configuration** command in privileged EXEC mode.

show private-hosts configuration

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Examples

The following example shows sample command output:

```
Router# show private-hosts configuration

Private hosts enabled. BR INDEX 6 State 0000000F
Privated hosts vlans lists:
200
Privated promiscuous MAC configuration:
A '*' mark behind the mac list indicates non-existent mac-list
-------------------------------------------------------------------------------
MAC-list                       VLAN list
-------------------------------------------------------------------------------
bras-list                    *** Uses the isolated vlans (if any) ***
```

The following example shows sample command output:

```
Router# show private-hosts configuration
Private-hosts enabled
Isolated vlan-list 10,12,15,200-300
Promiscuous MAC configuration:
-------------------------------------------------------------------------------------
MAC-List               VLAN List
-------------------------------------------------------------------------------
Bras_list              10,12,15,200-300
Mcast_server_list      10,12,15
Router#
```

Related Commands

Command	Description
private-hosts	Enables or configures the Private Hosts feature.
private-hosts mode	Sets the switchport mode.
show fm **private-hosts interface configuration**	Displays the FM-related Private Hosts information.

Command	Description
show **private-hosts interface configuration**	Displays Private Hosts configuration information for individual interfaces.

show private-hosts interface configuration

To display information about the Private Hosts configuration on individual interfaces (ports), use the **show private-hosts interface configuration** command in privileged EXEC mode.

show private-hosts interface configuration

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
12.2(33)SXH	This command was integrated in Cisco IOS Release 12.2(33)SXH.

Examples

The following example shows sample command output:

```
Router# show private-hosts interface configuration

Private hosts enabled
Debug Events: 0 Acl: 0 API: 0
Promiscuous interface list
--------------------------
GigabitEthernet1/1 promiscuous connected Facing BRAS Jupiter
Isolated interface list
-------------------------
FastEthernet3/1-14 isolated connected Facing DSLAM AB-125-1
Mixed mode interface list
-------------------------
GigabitEthernet1/4-5 mixed connected Facing Server Mars
Router#
```

Related Commands

Command	Description
private-hosts	Enables or configures the Private Hosts feature.
private-hosts mode	Sets the switchport mode.
show fm **private-hosts**	Displays the FM-related Private Hosts information.
show private-hosts configuration	Displays Private Hosts configuration information for the router.

show private-hosts mac-list

To display the contents of the MAC address lists defined for Private Hosts, use the **show private-hosts mac-list** command in privileged EXEC mode.

show private-hosts mac-list [*list-name*]

Syntax Description

list-name	(Optional) The name of the MAC address list whose contents you want to display.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Examples

The following example shows sample command output:

```
Router# show private-hosts mac-list

MAC-List: bras-list
-----------------------------------------------------------------
MAC address    Description
-----------------------------------------------------------------
0000.1111.1111 BRAS-SERVER
```

Related Commands

Command	Description
private-hosts mac-list	Creates a MAC address list that identifies a content server that is being used to provide broadband services to isolated hosts.

show privilege

To display your current level of privilege, use the **show privilege** command in EXEC mode.

show privilege

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example shows sample output from the **show privilege** command. The current privilege level is 15.

```
Router# show privilege
Current privilege level is 15
```

Related Commands

Command	Description
enable password	Sets a local password to control access to various privilege levels.
enable secret	Specifies an additional layer of security over the **enable password** command.

show radius local-server statistics

To display the statistics for the local authentication server, use the **show radius local-server statistics**command in privileged EXEC mode.

show radius local-server statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(11)JA	This command was introduced on the Cisco Aironet Access Point 1100 and the Cisco Aironet Access Point 1200.
12.3(11)T	This command was integrated into Cisco IOS Release 12.3(11)T and implemented on the following platforms: Cisco 2600XM, Cisco 2691, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3700, and Cisco 3800 series routers.

Examples

The following output displays statistics for the local authentication server.

```
Router# show radius local-server statistics
Successes              : 11262       Unknown usernames      : 0
Client blocks          : 0           Invalid passwords      : 8
Unknown NAS            : 0           Invalid packet from NAS: 0
NAS : 10.0.0.1
Successes              : 11262       Unknown usernames      : 0
Client blocks          : 0           Invalid passwords      : 8
Corrupted packet       : 0           Unknown RADIUS message : 0
No username attribute  : 0           Missing auth attribute : 0
Shared key mismatch    : 0           Invalid state attribute: 0
Unknown EAP message    : 0           Unknown EAP auth type  : 0
PAC refresh            : 0           Invalid PAC received   : 0
Maximum number of configurable users: 50, current user count: 11
Username                   Successes  Failures  Blocks
vayu-ap-1                       2235         0       0
vayu-ap-2                       2235         0       0
vayu-ap-3                       2246         0       0
vayu-ap-4                       2247         0       0
vayu-ap-5                       2247         0       0
vayu-11                            3         0       0
vayu-12                            5         0       0
vayu-13                            5         0       0
vayu-14                           30         0       0
vayu-15                            3         0       0
scm-test                           1         8       0
```

The first section of statistics lists cumulative statistics from the local authenticator.

The second section lists statistics for each access point (NAS) authorized to use the local authenticator. The EAP-FAST statistics in this section include the following:

- Auto provision success--the number of PACs generated automatically

- Auto provision failure--the number of PACs not generated because of an invalid handshake packet or invalid username or password
- PAC refresh--the number of PACs renewed by clients
- Invalid PAC received--the number of PACs received that were expired, that the authenticator could not decrypt, or that were assigned to a client username not in the authenticator's database

The third section lists stats for individual users. If a user is blocked and the lockout time is set to infinite, blocked appears at the end of the stat line for that user. If the lockout time is not infinite, Unblocked in x seconds appears at the end of the stat line for that user.

Use the **clear radius local-server statistics** command in privileged EXEC mode to reset local authenticator statistics to zero.

Related Commands

Command	Description
block count	Configures the parameters for locking out members of a group to help protect against unauthorized attacks.
clear radius local-server	Clears the statistics display or unblocks a user.
debug radius local-server	Displays the debug information for the local server.
group	Enters user group configuration mode and configures shared setting for a user group.
nas	Adds an access point or router to the list of devices that use the local authentication server.
radius-server host	Specifies the remote RADIUS server host.
radius-server local	Enables the access point or router to be a local authentication server and enters into configuration mode for the authenticator.
reauthentication time	Specifies the time (in seconds) after which access points or wireless-aware routers must reauthenticate the members of a group.
ssid	Specifies up to 20 SSIDs to be used by a user group.
user	Authorizes a user to authenticate using the local authentication server.
vlan	Specifies a VLAN to be used by members of a user group.

show radius server-group

To display properties for the RADIUS server group, use the **show radius server-group** command in user EXEC or privileged EXEC mode.

show radius server-group
{**server-group-name** | **all***123*}

Syntax Description

server-group-name	Displays properties for the server group named. The character string used to name the group of servers must be defined using the **aaa group server radius**command.
all	Displays properties for all the server group.
server	Displays properties for a specific server or servers in the group.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.2(33)SRA	The *server* argument was introduced.

Usage Guidelines

Use the **show radius server-group** command to display the server groups that you defined by using the **aaa group server radius** command.

Examples

The following **show radius server-group** command output displays properties for the server group "rad_sg":

```
Router# show radius server-group rad_sg
server group rad-sg
 Sharecount = 1  sg_unconfigured = FALSE
 Type = standard  Memlocks = 1
```

The following **show radius server-group** command output displays the properties for two server groups, 123 and 456, respectively. Using the **aaa group server radius** command, the configuration of each server group is also shown.

```
Router(config)# aaa new-model
!
!
Router(config)# aaa group server radius 123
 server 10.9.8.1 auth-port 1645 acct-port 1646
!
Router(config)# aaa group server radius 456
 server 10.9.8.2 auth-port 1645 acct-port 1646
Router(config)# exit
Router# show radius server-group all
Server group 123
```

```
 Sharecount = 1  sg_unconfigured = FALSE
 Type = standard
Server group 456
 Sharecount = 1  sg_unconfigured = FALSE
 Type = standard
Router# show radius server-group 123
Server group 123
 Sharecount = 1  sg_unconfigured = FALSE
 Type = standard
```

The table below describes the significant fields shown in the display.

Table 177: show radius server-group command Field Descriptions

Field	Description
Server group	Name of the server group.
Sharecount	Number of method lists that are sharing this server group. For example, if one method list uses a particular server group, the sharecount would be 1. If two method lists use the same server group, the sharecount would be 2.
sg_unconfigured	Server group has been unconfigured.
Type	The type can be either "standard" or "nonstandard". The type indicates whether the servers in the group accept nonstandard attributes. If all servers within the group are configured with the nonstandard option, the type will be shown as "nonstandard".
Memlocks	An internal reference count for the server-group structure that is in memory. The number represents how many internal data structure packets or transactions are holding references to this server group. Memlocks is used internally for memory management purposes.

Related Commands

Command	Description
aaa group server radius	Groups different RADIUS server hosts into distinct lists and distinct methods.
show aaa servers	Displays information about the number of packets sent to and received from AAA servers.
show radius statistics	Displays the RADIUS statistics for accounting and authentication packets.

show radius statistics

To display the RADIUS statistics for accounting and authentication packets, use the **show radius statistics** command in user EXEC or privileged EXEC mode.

show radius statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(1)S	This command was integrated into Cisco IOS Release 15.1(1)S. Support for the CISCO-RADIUS-EXT-MIB was added.
15.1(4)M	This command was modified. Support for the CISCO-RADIUS-EXT-MIB was added.

Usage Guidelines

The values in queue related fields (Maximum inQ length:, Maximum waitQ length:, and Maximum doneQ length:) of the **show radius statistics** command is shown as NA in vEWLC, as these queue related information is applicable only in IOS.

Examples

The following is sample output from the **show radius statistics** command:

```
Router# show radius statistics
                                Auth.      Acct.       Both
Maximum inQ length:              NA         NA         1
Maximum waitQ length:            NA         NA         2
Maximum doneQ length:            NA         NA         1
Total responses seen:            33         67         100
Packets with responses:          33         67         100
Packets without responses:       0          0          0
Access Rejects           :       0
Average response delay(ms) :     1331       124        523
Maximum response delay(ms):      5720       4800       5720
Number of Radius timeouts:       8          2          10
Duplicate ID detects:            0          0           0
Buffer Allocation Failures:      0          0           0
Maximum Buffer Size (bytes):     156        327         327
Malformed Responses        :     0          0           0
Bad Authenticators         :     0          0           0
Source Port Range: (2 ports only)
1645 - 1646
Last used Source Port/Identifier:
```

```
1645/33
1646/69
```

The table below describes significant fields shown in the display.

Table 178: show radius statistics Field Descriptions

Field	Description
Auth.	Statistics for authentication packets.
Acct.	Statistics for accounting packets.
Both	Combined statistics for authentication and accounting packets.
Maximum inQ length	Maximum number of entries allowed in the queue that holds the RADIUS messages not yet sent.
Maximum waitQ length	Maximum number of entries allowed in the queue that holds the RADIUS messages that have been sent and are waiting for a response.
Maximum doneQ length	Maximum number of entries allowed in the queue that holds the messages that have received a response and will be forwarded to the code that is waiting for the messages.
Total responses seen	Number of RADIUS responses seen from the server. In addition to the expected packets, the number includes repeated packets and packets that do not have a matching message in the waitQ.
Packets with responses	Number of packets that received a response from the RADIUS server.
Packets without responses	Number of packets that never received a response from any RADIUS server.
Access Rejects	Number of times access requests have been rejected by a RADIUS server.
Average response delay	Average time, in milliseconds (ms), from when the packet was first transmitted to when it received a response. If the response timed out and the packet was sent again, this value includes the timeout. If the packet never received a response, this value is not included in the average.
Maximum response delay	Maximum delay, in ms, observed while gathering the average response delay information.
Number of RADIUS timeouts	Number of times a server did not respond and the RADIUS server re-sent the packet.
Duplicate ID detects	RADIUS has a maximum of 255 unique IDs. In some instances, there can be more than 255 outstanding packets. When a packet is received, the doneQ is searched from the oldest entry to the youngest. If the IDs are the same, further techniques are used to see if this response matches this entry. If this response does not match, the duplicate ID detect counter is increased.
Buffer Allocation Failures	Number of times the buffer failed to get allocated.

Field	Description
Maximum Buffer Size (bytes)	Displays the maximum size of the buffer.
Malformed Responses	Number of corrupted responses, mostly due to bad authenticators.
Bad Authenticators	Number of authentication failures due to shared secret mismatches.
Source Port Range: (2 ports only)	Displays the port numbers.
Last used Source Port/Identifier	Ports that were last used by the RADIUS server for authentication.

The fields in the output are mapped to Simple Network Management Protocol (SNMP) objects in the CISCO-RADIUS-EXT-MIB and are used in SNMP reporting. The first line of the report is mapped to the CISCO-RADIUS-EXT-MIB as follows:

- Maximum inQ length maps to creClientTotalMaxInQLength
- Maximum waitQ length maps to creClientTotalMaxWaitQLength
- Maximum doneQ length maps to creClientTotalMaxDoneQLength

The field "Both" in the output can be derived from the authentication and accounting MIB objects. The calculation formula for each field, as displayed in the output, is given in the table below.

Table 179: Calculation Formula for the Both field in show radius statistics Command Output

show radius statistics Command Output Data	Calculation Formula for the Both Field
Maximum inQ length	creClientTotalMaxInQLength
Maximum waitQ length	creClientTotalWaitQLength
Maximum doneQ length	creClientDoneQLength
Total responses seen	creAuthClientTotalResponses + creAcctClientTotalResponses
Packets with responses	creAuthClientTotalPacketsWithResponses + creAcctClientTotalPacketsWithResponses
Packets without responses	creAuthClientTotalPacketsWithoutResponses + creAcctClientTotalPacketsWithoutResponses
Access Rejects	creClientTotalAccessRejects
Average response delay	creClientAverageResponseDelay
Maximum response delay	MAX(creAuthClientMaxResponseDelay, creAcctClientMaxResponseDelay)
Number of RADIUS timeouts	creAuthClientTimeouts + creAcctClientTimeouts
Duplicate ID detects	creAuthClientDupIDs + creAcctClientDupIDs

show radius statistics Command Output Data	Calculation Formula for the Both Field
Buffer Allocation Failures	creAuthClientBufferAllocFailures + creAcctClientBufferAllocFailures
Maximum Buffer Size (bytes)	MAX(creAuthClientMaxBufferSize, creAcctClientMaxBufferSize)
Malformed Responses	creAuthClientMalformedResponses + creAcctClientMalformedResponses
Bad Authenticators	creAuthClientBadAuthenticators + creAcctClientBadAuthenticators

Mapping the following set of objects listed in the CISCO-RADIUS-EXT-MIB map to fields displayed by the **show radius statistics**command is straightforward. For example, the creClientLastUsedSourcePort field corresponds to the Last used Source Port/Identifier portion of the report, creAuthClientBufferAllocFailures corresponds to the Buffer Allocation Failures for authentication packets, creAcctClientBufferAllocFailure corresponds to the Buffer Allocation Failures for accounting packets, and so on.

- creClientTotalMaxInQLength
- creClientTotalMaxWaitQLength
- creClientTotalMaxDoneQLength
- creClientTotalAccessRejects
- creClientTotalAverageResponseDelay
- creClientSourcePortRangeStart
- creClientSourcePortRangeEnd
- creClientLastUsedSourcePort
- creClientLastUsedSourceId
- creAuthClientBadAuthenticators
- creAuthClientUnknownResponses
- creAuthClientTotalPacketsWithResponses
- creAuthClientBufferAllocFailures
- creAuthClientTotalResponses
- creAuthClientTotalPacketsWithoutResponses
- creAuthClientAverageResponseDelay
- creAuthClientMaxResponseDelay
- creAuthClientMaxBufferSize
- creAuthClientTimeouts

- creAuthClientDupIDs
- creAuthClientMalformedResponses
- creAuthClientLastUsedSourceId
- creAcctClientBadAuthenticators
- creAcctClientUnknownResponses
- creAcctClientTotalPacketsWithResponses
- creAcctClientBufferAllocFailures
- creAcctClientTotalResponses
- creAcctClientTotalPacketsWithoutResponses
- creAcctClientAverageResponseDelay
- creAcctClientMaxResponseDelay
- creAcctClientMaxBufferSize
- creAcctClientTimeouts
- creAcctClientDupIDs
- creAcctClientMalformedResponses
- creAcctClientLastUsedSourceId

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs .

Related Commands

Command	Description
radius-server host	Specifies a RADIUS server host.
radius-server retransmit	Specifies how many times the Cisco IOS software searches the list of RADIUS server hosts before giving up.
radius-server timeout	Sets the interval for which a router waits for a server host to reply.

show radius table attributes

To display a list of all attributes supported by the RADIUS subsystem, use the **show radius table attributes** command in user EXEC or privileged EXEC mode.

show radius table attributes

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRA	This command was introduced.

Usage Guidelines

This command enables you to verify that a required RADIUS attribute is supported in a specific release.

Examples

The following example displays the complete table attribute list from the **show radius table attributes** command.

```
Router# show radius table attributes

IETF ATTRIBUTE LIST:
    Name User-Name                      Format String
    Name User-Password                  Format Binary
    Name CHAP-Password                  Format Binary
    Name NAS-IP-Address                 Format IPv4 Address
    Name NAS-Port                       Format Ulong
    Name Service-Type                   Format Enum
    Name Framed-Protocol                Format Enum
    Name Framed-IP-Address              Format IPv4 Address
    Name Framed-IP-Netmask              Format IPv4 Address
    Name Framed-Routing                 Format Ulong
    Name Filter-Id                      Format Binary
    Name Framed-MTU                     Format Ulong
    Name Framed-Compression             Format Enum
    Name login-ip-addr-host             Format IPv4 Address
    Name Login-Service                  Format Enum
    Name login-tcp-port                 Format Ulong
    Name Reply-Message                  Format Binary
    Name Callback-Number                Format String
    Name Framed-Route                   Format String
    Name Framed-IPX-Network             Format IPv4 Address
    Name State                          Format Binary
    Name Class                          Format Binary
    Name Vendor-Specific                Format Binary
    Name Session-Timeout                Format Ulong
    Name Idle-Timeout                   Format Ulong
    Name Termination-Action             Format Boolean
    Name Called-Station-Id              Format String
    Name Calling-Station-Id             Format String
    Name Nas-Identifier                 Format String
    Name Acct-Status-Type               Format Enum
```

```
    Name Acct-Delay-Time                Format Ulong
    Name Acct-Input-Octets              Format Ulong
    Name Acct-Output-Octets             Format Ulong
    Name Acct-Session-Id                Format String
    Name Acct-Authentic                 Format Enum
    Name Acct-Session-Time              Format Ulong
    Name Acct-Input-Packets             Format Ulong
    Name Acct-Output-Packets            Format Ulong
    Name Acct-Terminate-Cause           Format Enum
    Name Multilink-Session-ID           Format String
    Name Acct-Link-Count                Format Ulong
    Name Acct-Input-Giga-Words          Format Ulong
    Name Acct-Output-Giga-Words         Format Ulong
    Name Event-Timestamp                Format Ulong
    Name CHAP-Challenge                 Format Binary
    Name NAS-Port-Type                  Format Enum
    Name Port-Limit                     Format Ulong
    Name Tunnel-Type                    Format Enum
    Name Tunnel-Medium-Type             Format Enum
    Name Tunnel-Client-Endpoint         Format String
    Name Tunnel-Server-Endpoint         Format String
    Name Acct-Tunnel-Connection         Format String
    Name Tunnel-Password                Format Binary
    Name Prompt                         Format Enum
    Name Connect-Info                   Format String
    Name EAP-Message                    Format Binary
    Name Message-Authenticator          Format Binary
    Name Tunnel-Private-Group-Id        Format String
    Name Tunnel-Assignment-Id           Format String
    Name Tunnel-Preference              Format Ulong
    Name Acct-Interim-Interval          Format Ulong
    Name Tunnel-Packets-Lost            Format Ulong
    Name NAS-Port-Id                    Format String
    Name Tunnel-Client-Auth-ID          Format String
    Name Tunnel-Server-Auth-ID          Format String
    Name Framed-Interface-Id            Format Binary
    Name Framed-IPv6-Prefix             Format Binary
    Name login-ip-addr-host             Format Binary
    Name Framed-IPv6-Route              Format String
    Name Framed-IPv6-Pool               Format String
    Name Dynamic-Author-Error-Cause     Format Enum
Non Standard ATTRIBUTE LIST:
    Name Old-Password                   Format Binary
    Name Ascend-Filter-Required         Format Enum
    Name Ascend-Cache-Refresh           Format Enum
    Name Ascend-Cache-Time              Format Ulong
    Name Ascend-Auth-Type               Format Ulong
    Name Ascend-Redirect-Number         Format String
    Name Ascend-Private-Route           Format String
    Name Ascend-Shared-Profile-Enable   Format Boolean
    Name Ascend-Client-Primary-DNS      Format IPv4 Address
    Name Ascend-Client-Secondary-DNS    Format IPv4 Address
    Name Ascend-Client-Assign-DNS       Format Ulong
    Name Ascend-Session-Svr-Key         Format String
    Name Ascend-Multicast-Rate-Limit    Format Ulong
    Name Ascend-Multicast-Client        Format Ulong
    Name Ascend-Multilink-Session-ID    Format Ulong
    Name Ascend-Num-In-Multilink        Format Ulong
    Name Ascend-Presession-Octets-In    Format Ulong
    Name Ascend-Presession-Octets-Out   Format Ulong
    Name Ascend-Presession-Packets-In   Format Ulong
    Name Ascend-Presession-Packets-Out  Format Ulong
    Name Ascend-Max-Time                Format Ulong
    Name Ascend-Disconnect-Cause        Format Enum
```

```
    Name Ascend-Connection-Progress     Format Enum
    Name Ascend-Data-Rate               Format Ulong
    Name Ascend-Presession-Time         Format Ulong
    Name Ascend-Require-Auth            Format Ulong
    Name Ascend-PW-Liftime              Format Ulong
    Name Ascend-IP-Direct               Format IPv4 Address
    Name Ascend-PPP-VJ-Slot-Comp        Format Boolean
    Name Ascend-Asyncmap                Format Ulong
    Name Ascend-Send-Secret             Format Binary
    Name ascend_pool_definition         Format String
    Name Ascend-IP-Pool                 Format Ulong
    Name Ascend-Dial-Number             Format String
    Name Ascend-Route-IP                Format Boolean
    Name Ascend-Send-Auth               Format Enum
    Name Ascend-Link-Compression        Format Enum
    Name Ascend-Target-Util             Format Ulong
    Name Ascend-Max-Channels            Format Ulong
    Name Ascend-Data-Filter             Format Binary
    Name Ascend-Call-Filter             Format Binary
    Name Ascend-Idle-Limit              Format Ulong
    Name Ascend-Data-Service            Format Ulong
    Name Ascend-Force-56                Format Ulong
    Name Ascend-Xmit-Rate               Format Ulong
Cisco VSA ATTRIBUTE LIST:
    Name Cisco AVpair                   Format String
    Name cisco-nas-port                 Format String
    Name fax_account_id_origin          Format String
    Name fax_msg_id                     Format String
    Name fax_pages                      Format String
    Name fax_modem_time                 Format String
    Name fax_connect_speed              Format String
    Name fax_mdn_address                Format String
    Name fax_mdn_flag                   Format String
    Name fax_auth_status                Format String
    Name email_server_address           Format String
    Name email_server_ack_flag          Format String
    Name gateway_id                     Format String
    Name call_type                      Format String
    Name port_used                      Format String
    Name abort_cause                    Format String
    Name h323-remote-address            Format String
    Name Conf-Id                        Format String
    Name h323-setup-time                Format String
    Name h323-call-origin               Format String
    Name h323-call-type                 Format String
    Name h323-connect-time              Format String
    Name h323-disconnect-time           Format String
    Name h323-disconnect-cause          Format String
    Name h323-voice-quality             Format String
    Name h323-gw-id                     Format String
    Name Cisco AVpair                   Format Binary
    Name Cisco encrypted string vsa     Format String
    Name Sub_Policy_In                  Format String
    Name Sub_Policy_Out                 Format String
    Name h323-credit-amount             Format String
    Name h323-credit-time               Format String
    Name h323-return-code               Format String
    Name h323-prompt-id                 Format String
    Name h323-time-and-day              Format String
    Name h323-redirect-number           Format String
    Name h323-preferred-lang            Format String
    Name h323-redirect-ip-address       Format String
    Name h323-billing-model             Format String
    Name h323-currency                  Format String
```

```
    Name ssg-account-info               Format String
    Name ssg-service-info               Format String
    Name ssg-command-code               Format Binary
    Name ssg-control-info               Format String
Microsoft VSA ATTRIBUTE LIST:
    Name MS-CHAP-Response               Format Binary
    Name MS-CHAP-ERROR                  Format Binary
    Name MS-CHAP-CPW-1                  Format Binary
    Name MS-CHAP-CPW-2                  Format Binary
    Name MS-CHAP-LM-Enc-PW              Format Binary
    Name MS-CHAP-NT-Enc-PW              Format Binary
    Name MS-MPPE-Enc-Policy             Format Binary
    Name MS-MPPE-Enc-Type               Format Binary
    Name MS-RAS-Vendor                  Format String
    Name MS-CHAP-DOMAIN                 Format String
    Name MSCHAP_Challenge               Format Binary
    Name MS-CHAP-MPPE-Keys              Format Binary
    Name MS-BAP-Usage                   Format Binary
    Name MS-Link-Util-Thresh            Format Binary
    Name MS-Link-Drop-Time-Limit        Format Binary
    Name MS-MPPE-Send-Key               Format Binary
    Name MS-MPPE-Recv-Key               Format Binary
    Name MS-RAS-Version                 Format String
    Name MS-Old-ARAP-Password           Format Binary
    Name New-ARAP-Password              Format Binary
    Name MS-ARAP-PW-Change-Reason       Format Binary
    Name MS-Filter                      Format Binary
    Name MS-Acct-Auth-Type              Format Binary
    Name MS-MPPE-EAP-Type               Format Binary
    Name MS-CHAP-V2-Response            Format Binary
    Name MS-CHAP-V2-Success             Format String
    Name MS-CHAP-CPW-2                  Format Binary
    Name MS-Primary-DNS                 Format IPv4 Address
    Name MS-Secondary-DNS               Format IPv4 Address
    Name MS-1st-NBNS-Server             Format IPv4 Address
    Name MS-2nd-NBNS-Server             Format IPv4 Address
    Name MS-ARAP-Challenge              Format Binary
3GPP VSA ATTRIBUTE LIST:
    Name Charging-ID                    Format Ulong
    Name PDP Type                       Format Enum
    Name Charging-Gateway-Address       Format IPv4 Address
    Name GPRS-QoS-Profile               Format String
    Name SGSN-Address                   Format IPv4 Address
    Name GGSN-Address                   Format IPv4 Address
    Name IMSI-MCC-MNC                   Format String
    Name GGSN-MCC-MNC                   Format String
    Name NSAPI                          Format String
    Name Session-Stop-Ind               Format Binary
    Name Selection-Mode                 Format String
    Name Charging-Characteristics       Format String
3GPP2 VSA ATTRIBUTE LIST:
    Name cdma-reverse-tnl-spec          Format Ulong
    Name cdma-diff-svc-class-opt        Format Ulong
    Name cdma-container                 Format String
    Name cdma-ha-ip-addr                Format IPv4 Address
    Name cdma-pcf-ip-addr               Format IPv4 Address
    Name cdma-bs-msc-addr               Format String
    Name cdma-user-id                   Format Ulong
    Name cdma-forward-mux               Format Ulong
    Name cdma-reverse-mux               Format Ulong
    Name cdma-forward-rate              Format Ulong
    Name cdma-reverse-rate              Format Ulong
    Name cdma-service-option            Format Ulong
    Name cdma-forward-type              Format Ulong
```

```
    Name cdma-reverse-type              Format Ulong
    Name cdma-frame-size                Format Ulong
    Name cdma-forward-rc                Format Ulong
    Name cdma-reverse-rc                Format Ulong
    Name cdma-ip-tech                   Format Ulong
    Name cdma-comp-flag                 Format Enum
    Name cdma-reason-ind                Format Enum
    Name cdma-bad-frame-count           Format Ulong
    Name cdma-num-active                Format Ulong
    Name cdma-sdb-input-octets          Format Ulong
    Name cdma-sdb-output-octets         Format Ulong
    Name cdma-numsdb-input              Format Ulong
    Name cdma-numsdb-output             Format Ulong
    Name cdma-ip-qos                    Format Ulong
    Name cdma-airlink-qos               Format Ulong
    Name cdma-rp-session-id             Format Ulong
    Name cdma-hdlc-layer-bytes-in       Format Ulong
    Name cdma-correlation-id            Format String
    Name cdma-moip-inbound              Format Ulong
    Name cdma-moip-outbound             Format Ulong
    Name cdma-session-continue          Format Ulong
    Name cdma-active-time               Format Ulong
    Name cdma-frame-size                Format Ulong
    Name cdma-esn                       Format String
    Name cdma-mn-ha-spi                 Format Ulong
    Name cdma-mn-ha-shared-key          Format Binary
    Name cdma-sess-term-capability      Format Ulong
    Name cdma-disconnect-reason         Format Ulong
Verizon VSA ATTRIBUTE LIST:
    Name mip-key-data                   Format Binary
    Name aaa-authenticator              Format Binary
    Name public-key-invalid             Format Binary
```

The table below describes the significant fields shown in the display.

Table 180: show radius table attributes Field Descriptions

Field	Description
User-Name	The name of the user on the system. The format is String.
User-Password	The password of the user on the system. The format is Binary.
CHAP-Password	Challenge Handshake Authentication Protocol (CHAP) password. The format is Binary.
NAS-IP-Address	Network-Attached Storage (NAS) IP address. The format is IPv4 Address.
NAS-Port	The RADIUS Attribute 5 (NAS-Port) format specified on a per-server group level. The format is Ulong.
Service-Type	Sets the service type. The format is Enum.
Framed-Protocol	Indicates the framing to be used for framed access. It may be used in both Access-Request and Access-Accept packets. The format is Enum.
Framed-IP-Address	Indicates the address to be configured for the user. It may be used in Access-Accept packets. The format is IPv4 Address.

Field	Description
Framed-IP-Netmask	Indicates the IP netmask to be configured for the user when the user is a router to a network. The format is IPv4 Address.
Framed-Routing	Indicates the routing method for the user when the user is a router to a network. The format is Ulong.
Filter-Id	To disable, enable, get, or set a filter, the filter ID must be valid. The format is Binary.
Framed-MTU	Indicates the maximum transmission unit to be configured for the user, when it is not negotiated by some other means (such as PPP). The format is Ulong.
Framed-Compression	Indicates a compression protocol to be used for the link. The format is Enum.
login-ip-addr-host	Indicates the host to which the user will connect when the Login-Service attribute is included. The format is IPv4 Address.
Login-Service	The Login-IP-Host AVP (AVP Code 14) is of type Address and contains the system with which to connect the user, when the Login-Service AVP is included. The format is Enum.
login-tcp-port	The Login-TCP-Port AVP (AVP Code 16) is of type Integer32 and contains the TCP port with which the user is to be connected, when the Login-Service AVP is also present. The format is Ulong.
Reply-Message	Indicates text that may be displayed to the user. The format is Binary.
Callback-Number	Indicates a dialing string to be used for callback. The format is String.
Framed-Route	Provides routing information to be configured for the user on the NAS. The format is String.
Framed-IPX-Network	The Framed-IPX-Network AVP (AVP Code 23) is of type Unsigned32, and contains the IPX Network number to be configured for the user. The format is Pv4 Address.
State	Is available to be sent by the server to the client in an Access-Challenge and must be sent unmodified from the client to the server in the new Access-Request reply to that challenge, if any. The format is Binary.
Class	Is available to be sent by the server to the client in an Access-Accept and should be sent unmodified by the client to the accounting server as part of the Accounting-Request packet if accounting is supported. The format is Binary.
Vendor-Specific	Is available to allow vendors to support their own extended attributes not suitable for general usage. The format is Binary.
Session-Timeout	Sets the maximum number of seconds of service to be provided to the user before termination of the session or prompt. The format is Ulong.

Field	Description
Idle-Timeout	Sets the maximum number of consecutive seconds of idle connection allowed to the user before termination of the session or prompt. The format is Ulong.
Termination-Action	Indicates what action the NAS should take when the specified service is completed. The format is Boolean.
Called-Station-Id	The Called-Station-Id AVP (AVP Code 30) is of type String and allows the NAS to send in the request the phone number that the user called, using Dialed Number Identification (DNIS) or a similar technology. The format is String.
Calling-Station-Id	The Calling-Station-Id AVP (AVP Code 31) is of type String and allows the NAS to send in the request the phone number that the call came from, using Automatic Number Identification (ANI) or a similar technology. The format is String.
Nas-Identifier	Contains a string identifying the NAS originating the access request. The format is String.
Acct-Status-Type	Indicates whether this Accounting-Request marks the beginning of the user service (Start) or the end (Stop). The format is Enum.
Acct-Delay-Time	Indicates how many seconds the client has been trying to send this record for, and can be subtracted from the time of arrival on the server to find the approximate time of the event generating this Accounting-Request. (Network transit time is ignored.) The format is Ulong.
Acct-Input-Octets	Indicates how many octets have been received from the port over the course of this service being provided, and can only be present in Accounting-Request records where Acct-Status-Type is set to Stop. The format is Ulong.
Acct-Output-Octets	Indicates how many octets have been sent to the port in the course of delivering this service, and can only be present in Accounting-Request records where Acct-Status-Type is set to Stop. The format is Ulong.
Acct-Session-Id	Is a unique accounting ID to make it easy to match start and stop records in a log file. The format is String.
Acct-Authentic	Indicate how the user was authenticated, whether by Radius, the NAS itself, or another remote authentication protocol. It may be included in an Accounting-Request. The format is Enum.
Acct-Session-Time	Indicates how many seconds the user has received service for, and can only be present in Accounting-Request records where Acct-Status-Type is set to Stop. The format is Ulong.
Acct-Input-Packets	Indicates how many packets have been received from the port over the course of this service being provided to a framed user, and can only be present in Accounting-Request records where Acct-Status-Type is set to Stop. The format is Ulong.

Field	Description
Acct-Output-Packets	Indicates how many packets have been sent to the port in the course of delivering this service to a framed user, and can only be present in Accounting-Request records where Acct-Status-Type is set to Stop. The format is Ulong.
Acct-Terminate-Cause	Indicates how the session was terminated, and can only be present in Accounting-Request records where Acct-Status-Type is set to Stop. The format is Enum.
Multilink-Session-ID	Indicates the service to use to connect the user to the login host. It is only used in Access-Accept packets. The format is String.
Acct-Link-Count	Gives the count of links which are known to have been in a given multilink session at the time the accounting record is generated. The format is Ulong.
Acct-Input-Giga-Words	Indicates how many times the Acct-Input-Octets counter has wrapped around 2^32 over the course of this service being provided, and can only be present in Accounting-Request records where the Acct-Status-Type is set to Stop or Interim-Update. The format is Ulong.
Acct-Output-Giga-Words	Indicates how many times the Acct-Output-Octets counter has wrapped around 2^32 in the course of delivering this service, and can only be present in Accounting-Request records where the Acct-Status-Type is set to Stop or Interim-Update. The format is Ulong.
Event-Timestamp	Use to include the Event-Timestamp attribute in Acct-Start or Acct-Stop messages. The format is Ulong.
CHAP-Challenge	The CHAP is used to verify periodically the identity of the peer using a 3-way handshake. The format is Binary.
NAS-Port-Type	Indicates the physical port number of the NAS which is authenticating the user. The format is Enum.
Port-Limit	Sets the maximum number of ports to be provided to the user by the NAS. The format is Ulong.
Tunnel-Type	Indicates the tunneling protocol(s) to be used (in the case of a tunnel initiator) or the the tunneling protocol in use (in the case of a tunnel terminator). The format is Enum.
Tunnel-Medium-Type	Indicates which transport medium to use when creating a tunnel for those protocols (such as L2TP) that can operate over multiple transports. The format is Enum.
Tunnel-Client-Endpoint	Contains the address of the initiator end of the tunnel. The format is String.
Tunnel-Server-Endpoint	Indicates the address of the server end of the tunnel. The format is String.
Acct-Tunnel-Connection	Indicates the identifier assigned to the tunnel session. The format is String.

Field	Description
Tunnel-Password	Can contain a password to be used to authenticate to a remote server. The format is Binary.
Prompt	Used only in Access-Challenge packets, and indicates to the NAS whether it should echo the user's response as it is entered, or not echo it. The format is Enum.
Connect-Info	Is sent from the NAS to indicate the nature of the user's connection. The format is String.
EAP-Message	Encapsulates Extensible Authentication Protocol packets so as to allow the NAS to authenticate dial-in users via EAP without having to understand the protocol. The format is Binary.
Message-Authenticator	Can be used to authenticate and integrity-protect Access-Requests in order to prevent spoofing. The format is Binary.
Tunnel-Private-Group-Id	Indicates the group ID for a particular tunneled session. The format is String.
Tunnel-Assignment-Id	Used to indicate to the tunnel initiator the particular tunnel to which a session is to be assigned. The format is String.
Tunnel-Preference	Should be included in each set to indicate the relative preference assigned to each tunnel if more than one set of tunneling attributes is returned by the RADIUS server to the tunnel initiator. The format is Ulong.
Acct-Interim-Interval	Indicates the number of seconds between each interim update in seconds for this specific session. The format is Ulong.
Tunnel-Packets-Lost	Indicates the number of packets lost on a given link. The format is Ulong.
NAS-Port-Id	Used to identify the IEEE 802.1X Authenticator port which authenticates the Supplicant. The format is String.
Tunnel-Client-Auth-ID	Specifies the name used by the tunnel initiator during the authentication phase of tunnel establishment. The format is String.
Tunnel-Server-Auth-ID	Specifies the name used by the tunnel terminator during the authentication phase of tunnel establishment. The format is String.
Framed-Interface-Id	Indicates the IPv6 interface identifier to be configured for the user. The format is Binary.
Framed-IPv6-Prefix	Indicates an IPv6 prefix (and corresponding route) to be configured for the user. The format is Binary.
Framed-IPv6-Route	Provides routing information to be configured for the user on the NAS. The format is String.
Framed-IPv6-Pool	Contains the name of an assigned pool that should be used to assign an IPv6 prefix for the user. The format is String.

Field	Description
Dynamic-Author-Error-Cause	Specifies the error causes associated with dynamic authorization. The format is Enum.
Old-Password	Is 16 octets in length. It contains the encrypted Lan Manager hash of the old password. The format is Binary.
Ascend-Filter-Required	Specifies whether the call should be permitted if the specified filter is not found. If present, this attribute will be applied after any authentication, authorization, and accounting (AAA) filter method-list. The format is Enum.
Ascend-Cache-Refresh	Specifies whether cache entries should be refreshed each time an entry is referenced by a new session. This attribute corresponds to the **cache refresh** command. The format is Enum.
Ascend-Cache-Time	Specifies the idle time out, in minutes, for cache entries. This attribute corresponds to the **cache clear age** command. The format is Ulong.
Ascend-Auth-Type	Indicates the type of name and password (PPP) authorization to use. The format Ulong.
Ascend-Redirect-Number	Indicates the original number in the information sent to the authentication server when the number dialed by a device is redirected to another number for authentication. The format is String.
Ascend-Private-Route	Specifies whether IP routing is allowed for the user profile. The format is String.
Ascend-Shared-Profile-Enable	Specifies whether multiple incoming callers can share a single RADIUS user profile. The format is Boolean.
Ascend-Client-Primary-DNS	Specifies a primary DNS server address to send to any client connecting to the MAX TNT. The format is IPv4 Address.
Ascend-Client-Secondary-DNS	Specifies a secondary DNS server address to send to any client connecting to the MAX TNT. The format is IPv4 Address.
Ascend-Client-Assign-DNS	Specifies whether or not the MAX TNT sends the Ascend-Client-Primary-DNS and Ascend-Client-Secondary-DNS values during connection negotiation. The format is Ulong.
Ascend-Session-Svr-Key	Specifies the session key that identifies the user session. You can specify up to 16 characters. The default value is null. The format is String.
Ascend-Multicast-Rate-Limit	Specifies how many seconds the MAX waits before accepting another packet from the multicast client. The format is Ulong.
Ascend-Multicast-Client	Specifies whether the user is a multicast client of the MAX. The format is Ulong.
Ascend-Multilink-Session-ID	Specifies the ID number of the Multilink bundle when the session closes. A Multilink bundle is a multichannel MP or MP+ call. The format is Ulong.

Field	Description
Ascend-Num-In-Multilink	Indicates the number of sessions remaining in a Multilink bundle when the session closes. A Multilink bundle is a multichannel MP or MP+ call. The format is Ulong.
Ascend-Presession-Octets-In	Reports the number of octets received before authentication. The value reflects only the data delivered by PPP or other encapsulation. It does not include the header or other protocol-dependent components of the packet. The format is Ulong.
Ascend-Presession-Octets-Out	Reports the number of octets transmitted before authentication. The value reflects only the data delivered by PPP or other encapsulation. It does not include the header or other protocol-dependent components of the packet. The format is Ulong.
Ascend-Presession-Packets-In	Reports the number of packets received before authentication. The packets are counted before the encapsulation is removed. The attribute's value does not include maintenance packets, such as keepalive or management packets. The format is Ulong.
Ascend-Presession-Packets-Out	Reports the number of packets transmitted before authentication. The packets are counted before the encapsulation is removed. The attribute's value does not include maintenance packets, such as keepalive or management packets. The format is Ulong.
Ascend-Max-Time	Specifies the maximum length of time in seconds that any session can remain online. Once a session reaches the time limit, its connection goes offline. The format is Ulong.
Ascend-Disconnect-Cause	Indicates the reason a connection went offline. The format is Enum.
Ascend-Connection-Progress	Indicates the state of the connection before it disconnects. The format is Enum.
Ascend-Data-Rate	Specifies the rate of data received on the connection in bits per second. The format is Ulong.
Ascend-Presession-Time	Reports the length of time in seconds from when a call connected to when it completes authentication. The format is Ulong.
Ascend-Require-Auth	Specifies whether the MAX TNT requires additional authentication after Calling-Line ID (CLID) or called-number authentication. The format is Ulong.
Ascend-PW-Liftime	Specifies the number of days that a password is valid. The format is Ulong.
Ascend-IP-Direct	Specifies the IP address to which the MAX TNT redirects packets from the user. When you include this attribute in a user profile, the MAX TNT bypasses all internal routing tables, and simply sends all packets it receives on the connection's WAN interface to the specified IP address. The format is IPv4 Address.

Field	Description
Ascend-PPP-VJ-Slot-Comp	Instructs the MAX TNT to not use slot compression when sending VJ-compressed packets. The format is Boolean.
Ascend-Asyncmap	The format is Ulong.
Ascend-Send-Secret	Specifies the password that the RADIUS server sends to the remote end of a connection on an outgoing call. It is encrypted when passed between the RADIUS server and the MAX TNT. The format is Binary.
Ascend_pool_definition	Specifies all the addresses in the pool. The format is String.
Ascend-IP-Pool	Specifies the first address in an IP address pool, as well as the number of addresses in the pool. The format is Ulong.
Ascend-Dial-Number	Specifies the phone number the MAX TNT dials to reach the router or node at the remote end of the link. The format is String.
Ascend-Route-IP	Specifies whether IP routing is allowed for the user profile. The format is Boolean.
Ascend-Send-Auth	Specifies the authentication protocol that the MAX TNT requests when initiating a PPP or MP+ connection. The answering side of the connection determines which authentication protocol, if any, the connection uses. The format is Enum.
Ascend-Link-Compression	Turns data compression on or off for a PPP link. The format is Enum.
Ascend-Target-Util	Specifies the percentage of bandwidth use at which the MAX TNT adds or subtracts bandwidth. The format is Ulong.
Ascend-Max-Channels	Specifies the maximum number of channels allowed on an MP+ call. The format is Ulong.
Ascend-Data-Filter	Specifies the characteristics of a data filter in a RADIUS user profile. The MAX TNT uses the filter only when it places or receives a call associated with the profile that includes the filter definition. The format is Binary.
Ascend-Call-Filter	Specifies the characteristics of a call filter in a RADIUS user profile. The MAX TNT uses the filter only when it places a call or receives a call associated with the profile that includes the filter definition. The format is Binary.
Ascend-Idle-Limit	Specifies the number of seconds the MAX TNT waits before clearing a call when a session is inactive. The format is Ulong.
Ascend-Data-Service	Specifies the type of data service the link uses for outgoing calls. The format is Ulong.
Ascend-Force-56	Indicates whether the MAX uses only the 56-kbps portion of a channel, even when all 64-kbps appear to be available. The format is Ulong.

Field	Description
Ascend-Xmit-Rate	Specifies the rate of data transmitted on the connection in bits per second. For ISDN calls, Ascend-Xmit-Rate indicates the transmit data rate. For analog calls, it indicates the modem baud rate at the time of the initial connection. The format is Ulong.
Cisco AVpair	The Cisco RADIUS implementation supports one vendor-specific option using the format recommended in the specification. Cisco's vendor-ID is 9, and the supported option has vendor-type 1, which is named "cisco-avpair". The format is String.
cisco-nas-port	Enables the display of physical interface information and parent interface details as part of the of the cisco-nas-port vendor-specific attribute (VSA) for login calls. The format is String.
fax_account_id_origin	Indicates the account ID origin as defined by system administrator for the **mmoip aaa receive-id** or the **mmoip aaa send-id** command. The format is String.
fax_msg_id	Indicates a unique fax message identification number assigned by Store and Forward Fax. The format is String.
fax_pages	Indicates the number of pages transmitted or received during this fax session. This page count includes cover pages. The format is String.
fax_modem_time	Indicates the amount of time in seconds the modem sent fax data (x) and the amount of time in seconds of the total fax session (y), which includes both fax-mail and PSTN time, in the form x/y. For example, 10/15 means that the transfer time took 10 seconds, and the total fax session took 15 seconds. The format is String.
fax_connect_speed	Indicates the modem speed at which this fax-mail was initially transmitted or received. Possible values are 1200, 4800, 9600, and 14400. The format is String.
fax_mdn_address	Indicates the address to which message delivery notifications (MDNs) will be sent. The format is String.
fax_mdn_flag	Indicates whether or not MDNs has been enabled. True indicates that MDN had been enabled; false means that MDN had not been enabled. The format is String.
fax_auth_status	Indicates whether or not authentication for this fax session was successful. Possible values for this field are success, failed, bypassed, or unknown. The format is String.
email_server_address	Indicates the IP address of the e-mail server handling the on-ramp fax-mail message. The format is String.
email_server_ack_flag	Indicates that the on-ramp gateway has received a positive acknowledgment from the e-mail server accepting the fax-mail message. The format is String.

Field	Description
gateway_id	Indicates the name of the gateway that processed the fax session. The name appears in the following format: hostname.domain-name. The format is String.
call_type	Describes the type of fax activity: fax receive or fax send. The format is String.
port_used	Indicates the slot/port number of the Cisco AS5300 used to either transmit or receive this fax-mail. The format is String.
abort_cause	If the fax session terminates, it indicates the system component that signaled the termination. Examples of system components that could trigger a termination are FAP (Fax Application Process), TIFF (the TIFF reader or the TIFF writer), fax-mail client, fax-mail server, ESMTP client, or ESMTP server. The format is String.
h323-remote-address	Indicates the IP address of the remote gateway. The format is String.
Conf-Id	Indicates a unique call identifier generated by the gateway. Used to identify the separate billable events (calls) within a single calling session. The format is String.
h323-setup-time	Indicates the setup time in NTP format: hour, minutes, seconds, microseconds, time_zone, day, month, day_of_month, year. The format is String.
h323-call-origin	Indicates the gateway's behavior in relation to the connection that is active for this leg. The format is String.
h323-call-type	Indicates the protocol type or family used on this leg of the call. The format is String.
h323-connect-time	Indicates the connect time in Network Time Protocol (NTP) format: hour, minutes, seconds, microseconds, time_zone, day, month, day_of_month, and year. The format is String.
h323-disconnect-time	Indicates the disconnect time in NTP format: hour, minutes, seconds, microseconds, time_zone, day, month, day_of_month, year. The format is String.
h323-disconnect-cause	Indicates the Q.931 disconnect cause code retrieved from CCAPI. The source of the code is the disconnect location such as a PSTN, terminating gateway, or SIP. The format is String.
h323-voice-quality	Indicates the ICPIF of the voice quality. The format is String.
h323-gw-id	Indicate the name of the tenor. The format is String.
Cisco AVpair	The Cisco RADIUS implementation supports one vendor-specific option using the format recommended in the specification. Cisco's vendor-ID is 9, and the supported option has vendor-type 1, which is named "cisco-avpair". The format is String.

Field	Description
Cisco encrypted string vsa	Cisco allows several forms of sub-attribute encryption. The only method supported is the Cisco Encrypted String VSA Format also supported by an IETF draft for Salt-Encryption of RADIUS attributes. The format is String.
Sub_Policy_In	Defines the service policy input. The format is String.
Sub_Policy_Out	Defines the service policy output. The format is String.
h323-credit-amount	Indicates the amount of credit (in currency) that the account contains. The format is String.
h323-credit-time	Indicates the number of seconds for which the call is authorized. The format is String.
h323-return-code	Return codes are instructions from the RADIUS server to the voice gateway. The format is String.
h323-prompt-id	Indexes into an array that selects prompt files used at the gateway. The format is String.
h323-time-and-day	Indicates the time of day at the dialed number or at the remote gateway in the format: hour, minutes, seconds. The format is String.
h323-redirect-number	Indicates the phone number to which the call is redirected; for example, to a toll-free number or a customer service number. The format is String.
h323-preferred-lang	Indicates the language to use when playing the audio prompt specified by the h323-prompt-id. The format is String.
h323-redirect-ip-address	Indicates the IP address for an alternate or redirected call. The format is String.
h323-billing-model	Indicates the type of billing service for a specific call. The format is String.
h323-currency	Indicates the currency to use with h323-credit-amount. The format is String.
ssg-account-info	Subscribes the subscriber to the specified service and indicates that the subscriber should be automatically connected to this service after successful logon. The format is String.
ssg-service-info	SSG redirects the user's HTTP traffic to a server in the specified server group. All the service features (such as quality of service (QoS) and prepaid billing) are applied to the HTTP traffic. The format is String.
ssg-command-code	Specifies account logon and logoff, session query, and service activate and deactivate information. The format is Binary.
ssg-control-info	Indicates the control-info code for prepaid quota. The format is String.
MS-CHAP-Response	This attribute contains the response value provided by a PPP Microsoft Challenge-Handshake Authentication Protocol (MS-CHAP) user in response to the challenge. The format is Binary.

Field	Description
MS-CHAP-ERROR	Contains error data related to the preceding MS-CHAP exchange. The format is Binary.
MS-CHAP-CPW-1	Allows the user to change their password if it has expired. The format is Binary.
MS-CHAP-CPW-2	Allows the user to change their password if it has expired. The format is Binary.
MS-CHAP-LM-Enc-PW	Contains the new Windows NT password encrypted with the old LAN Manager password hash. The format is Binary.
MS-CHAP-NT-Enc-PW	Contains the new Windows NT password encrypted with the old Windows NT password hash. The format is Binary.
MS-MPPE-Enc-Policy	The MS-MPPE-Encryption-Policy attribute may be used to signify whether the use of encryption is allowed or required. The format is Binary.
MS-MPPE-Enc-Type	The MS-MPPE-Encryption-Types attribute is used to signify the types of encryption available for use with Microsoft Point-to-Point Encryption (MPPE). The format is Binary.
MS-RAS-Vendor	Used to indicate the manufacturer of the RADIUS client machine. The format is Binary.
MS-CHAP-DOMAIN	Indicates the Windows NT domain in which the user was authenticated. The format is Binary.
MSCHAP_Challenge	Contains the challenge sent by a NAS to a MS-CHAP user. The format is Binary.
MS-CHAP-MPPE-Keys	Contains two session keys for use by the MPPE. The format is Binary.
MS-BAP-Usage	Describes whether the use of Bandwidth Allocation Protocol (BAP) is allowed, disallowed or required on new multilink calls. The format is Binary.
MS-Link-Util-Thresh	Represents the percentage of available bandwidth utilization below which the link must fall before the link is eligible for termination. The format is Binary.
MS-Link-Drop-Time-Limit	Indicates the length of time (in seconds) that a link must be underutilized before it is dropped. The format is Binary.
MS-MPPE-Send-Key	Contains a session key for use by the MPPE. The format is Binary.
MS-MPPE-Recv-Key	Contains a session key for use by the MPPE. The format is Binary.
MS-RAS-Version	Used to indicate the version of the RADIUS client software. The format is Binary.
MS-Old-ARAP-Password	Used to transmit the old Apple Remote Access Protocol (ARAP) password during an ARAP password change operation. The format is Binary.

Field	Description
New-ARAP-Password	Used to transmit the new ARAP password during an ARAP password change operation. The format is Binary.
MS-ARAP-PW-Change-Reason	Used to indicate reason for a server-initiated password change. The format is Binary.
MS-Filter	Used to transmit traffic filters. The format is Binary.
MS-Acct-Auth-Type	Used to represent the method used to authenticate the dial-up user. The format is Binary.
MS-MPPE-EAP-Type	Used to represent the EAP type used to authenticate the dial-up user. The format is Binary.
MS-CHAP-V2-Response	This attribute is identical in format to the standard CHAP Response packet. The format is Binary.
MS-CHAP-V2-Success	Contains a 42-octet authenticator response string and must be included in the Message field packet sent from the NAS to the peer. The format is Binary.
MS-CHAP-CPW-2	Allows the user to change their password if it has expired. The format is Binary.
MS-Primary-DNS	Used to indicate the address of the primary DNS server to be used by the PPP peer. The format is IPv4 Address.
MS-Secondary-DNS	Used to indicate the address of the secondary DNS server to be used by the PPP peer. The format is IPv4 Address.
MS-1st-NBNS-Server	Used to indicate the address of the primary NetBIOS Name Server (NBNS) server to be used by the PPP peer. The format is IPv4 Address.
MS-2nd-NBNS-Server	Used to indicate the address of the secondary NBNS server to be used by the PPP peer. The format is IPv4 Address.
MS-ARAP-Challenge	Only present in an Access-Request packet containing a Framed-Protocol Attribute with the value 3 (ARAP). The format is Binary.
Charging-ID	Generated for each activated context. It is a unique four octet value generated by the GGSN when a PDP Context is activated. The format is Ulong.
PDP Type	Indicates the Packet Data Protocol (PDP) is to be used by the mobile for a certain service. The format is Enum.
Charging-Gateway-Address	The IP address of the recommended Charging Gateway Functionality to which the SGSN should transfer the Charging Detail Records (CDR) for this PDP Context. The format is IPv4 Address.
GPRS-QoS-Profile	Controls the QoS negotiated values. The format is String.
SGSN-Address	This is the IP address of the SGSN that is used by the GTP control plane for handling control messages. The format is IPv4 Address.

Field	Description
GGSN-Address	IP address of the GGSN that is used by the GTP control plane for the context establishment. This address is the same as the GGSN IP address used in G-CDRs. The format is IPv4 Address.
IMSI-MCC-MNC	The MCC and MNC extracted from the user's IMSI number (the first 5 or 6 digits depending on the IMSI). The format is String.
GGSN-MCC-MNC	The MCC and MNC of the network to which the GGSN belongs. The format is String.
NSAPI	Identifies a particular PDP context for the associated PDN and MSISDN/IMSI from creation to deletion. The format is String.
Session-Stop-Ind	Indicates to the AAA server that the last PDP context of a session is released and that the PDP session has been terminated. The format is Binary
Selection-Mode	Contains the selection mode for this PDP Context received in the Create PDP Context Request Message. The format is String.
Charging-Characteristics	Contains the charging characteristics for this PDP Context received in the Create PDP Context Request Message (only available in R99 and later releases). The format is String.
cdma-reverse-tnl-spec	Indicates the style of reverse tunneling that is required, and optionally appears in a RADIUS Access-Accept message. The format is Ulong.
cdma-diff-svc-class-opt	This attribute is deprecated and is replaced by the Allowed Differentiated Services Marking attribute. The Home RADIUS server authorizes differentiated services via the Differentiated Services Class Options attribute, and optionally appears in a RADIUS Access-Accept message. The format is Ulong.
cdma-container	Contains embedded 3GPP2 VSAs and/or RADIUS accounting attributes. The format is String.
cdma-ha-ip-addr	A Home Agent (HA) IP address used during a MIP session by the user as defined in IETF RFC 2002. The format is IPv4 Address.
cdma-pcf-ip-addr	The IP address of the serving PCF (the PCF in the serving RN). The format is IPv4 Address.
cdma-bs-msc-addr	The Base Station (BS) Mobile Switching Center (MSC) address. The format is String.
cdma-user-id	The name of the user on the system. The format is Ulong.
cdma-forward-mux	Forwards FCH multiplex option. The format is Ulong.
cdma-reverse-mux	Reverses FCH multiplex option. The format is Ulong.

Field	Description
cdma-forward-rate	The format and structure of the radio channel in the forward Dedicated Control Channel. A set of forward transmission formats that are characterized by data rates, modulation characterized, and spreading rates. The format is Ulong.
cdma-reverse-rate	The format and structure of the radio channel in the reverse Dedicated Control Channel. A set of reverse transmission formats that are characterized by data rates, modulation characterized, and spreading rates. The format is Ulong.
cdma-service-option	Code Division Multiple Access (CDMA) service option as received from the RN. The format is Ulong.
cdma-forward-type	Forward direction traffic type. It is either Primary or Secondary. The format is Ulong.
cdma-reverse-type	Reverse direction traffic type. It is either Primary or Secondary. The format is Ulong.
cdma-frame-size	Specifies the Fundamental Channel (FCH) frame size. The format is Ulong.
cdma-forward-rc	The format and structure of the radio channel in the forward FCH. A set of forward transmission formats that are characterized by data rates, modulation characterized, and spreading rates. The format is Ulong.
cdma-reverse-rc	The format and structure of the radio channel in the reverse FCH. A set of reverse transmission formats that are characterized by data rates, modulation characterized, and spreading rates. The format is Ulong.
cdma-ip-tech	Identifies the IP technology to use for the call: Simple IP or Mobile IP. The format is Ulong.
cdma-comp-flag	Indicates the type of compulsory tunnel. The format is Ulong.
cdma-reason-ind	Indicates the reasons for a stop record. The format is Ulong.
cdma-bad-frame-count	The total number of PPP frames from the MS dropped by the Packet Data Serving Node (PDSN) due to uncorrectable errors. The format is Ulong.
cdma-num-active	The number of active transitions. The format is Ulong.
cdma-sdb-input-octets	This is the Short Data Burst (SDB) octet count reported by the RN in the SDB Airlink Record. The format is Ulong.
cdma-sdb-output-octets	The SDB octet count reported by the RN in the SDB Airlink Record. The format is Ulong.
cdma-numsdb-input	The number of terminating SDBs. The format is Ulong.
cdma-numsdb-output	The number of originating SDBs. The format is Ulong.
cdma-ip-qos	Indicates the IP Quality of Service (QoS). The format is Ulong.

Field	Description
cdma-airlink-qos	Identifies Airlink Priority associated with the user. This is the user's priority associated with the packet data service. The format is Ulong.
cdma-rp-session-id	Identifies the resource reservation protocol type session identifier. The format is Ulong.
cdma-hdlc-layer-bytes-in	The count of all octets received in the reverse direction by the High-Level Data Link Control (HDLC) layer in the PDSN. The format is Ulong.
cdma-correlation-id	Indicates a unique accounting ID created by the Serving PDSN for each packet data session that allows multiple accounting events for each associated R-P connection or P-P connection to be correlated.The format is String.
cdma-moip-inbound	This is the total number of octets in registration requests and solicitations sent by the MS. The format is Ulong.
cdma-moip-outbound	This is the total number of octets in registration replies and agent advertisements, sent to the MS. The format is Ulong.
cdma-session-continue	This attribute when set to "true" means it is not the end of a Session and an Accounting Stop is immediately followed by an Account Start Record. "False" means end of a session. The format is Ulong.
cdma-active-time	The total active connection time on traffic channel in seconds. The format is Ulong.
cdma-frame-size	Specifies the FSH frame size. The format is Ulong.
cdma-esn	Indicates the Electronic Serial Number (ESN). The format is String.
cdma-mn-ha-spi	The SPI for the MN-HA shared key that optionally appears in a RADIUS Access-Request message. It is used to request an MN-HA shared key. The format is Ulong.
cdma-mn-ha-shared-key	A shared key for MN-HA that may appear in a RADIUS Access-Accept message. The MN-HA shared key is encrypted using a method based on the RSA Message Digest Algorithm MD5 [RFC 1321] as described in Section 3.5 of RFC 2868. The format is Binary.
cdma-sess-term-capability	The value shall be bitmap encoded rather than a raw integer. This attribute shall be included in a RADIUS Access-Request message to the Home RADIUS server and shall contain the value 3 to indicate that the PDSN and HA support both Dynamic authorization with RADIUS and Registration Revocation for Mobile IPv4. The attribute shall also be included in the RADIUS Access-Accept message and shall contain the preferred resource management mechanism by the home network, which shall be used for the session and may include values 1 to 3. The format is Ulong.
cdma-disconnect-reason	Indicates the reason for disconnecting the user. This attribute may be included in a RADIUS Disconnect-Request message from Home RADIUS server to the PDSN. The format is Ulong.

Field	Description
mip-key-data	This is the key data payload containing the encrypted MN_AAA key, MN_HA key, CHAP key, MN_Authenticator, and AAA_Authenticator. The format is Binary.
aaa-authenticator	This is the 64-bit AAA_Authenticator value decrypted by the Home RADIUS AAA Server. The format is Binary.
public-key-invalid	The home RADIUS AAA Server includes this attribute to indicate that the Public key used by the MN is not valid. The format is Binary.

Related Commands

Command	Description
show radius	Displays information about the RADIUS servers that are configured in the system.

show redundancy application asymmetric-routing

To display asymmetric routing information for a redundancy group, use the **show redundancy application asymmetric-routing** command in user EXEC or privileged EXEC mode.

show redundancy application asymmetric-routing {**interface** | **tunnel**} **group** *id*

Syntax Description

interface	Displays asymmetric routing interface information.
tunnel	Displays asymmetric routing tunnel information.
group *id*	Displays information about the redundancy group.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
15.2(3)T	This command was introduced.

Examples

The following is sample output from the **show redundancy application asymmetric-routing interface group** command:

```
Device# show redundancy application asymmetric-routing interface group 1

AR Group ID:1 interface Ethernet1/1
neighbor 10.3.3.2,
  transport context:
    my ip 10.9.9.1, my port 53000
    peer ip 10.9.9.2, peer port 53000
```

The following is sample output from the **show redundancy application asymmetric-routing tunnel group** command:

```
Device# show redundancy application asymmetric-routing tunnel group 1

Group ID:1
  rii  1000, idb Ethernet1/2
        packet sent: 0, packet received: 0
        byte sent:   0, byte recv:       0
        encap: length 32
         IP :45 00 00 00 00 00 00 00 FF 11 00 00 09 09 09 01 09 09 09 02
         UDP:CF 08 CF 08 00 00 00 00
         AR :00 01 03 E8
```

The following table describes the significant fields shown in the displays.

Table 181: show redundancy application asymmetric-routing Field Descriptions

Field	Description
AR Group ID	The identifier for the asymmetric routing redundancy group.

Field	Description
interface	The interface type and number.
neighbor	The IP address of the peer redundancy group's control interface.
transport context:	The IP address of the asymmetric routing interface and the IP address of the peer asymmetric routing interface are displayed under the transport context.
Group ID	The identifier for the asymmetric routing redundancy group.
rii	The redundancy interface identifier.

Related Commands

Command	Description
redundancy application asymmetric-routing	Associates a redundancy group with an interface that is used for asymmetric routing.

show redundancy application control-interface group

To display control interface information for a redundancy group, use the **show redundancy application control-interface group** command in privileged EXEC mode.

show redundancy application control-interface group [*group-id*]

Syntax Description

group-id	(Optional) Redundancy group ID. Valid values are 1 and 2.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Usage Guidelines

The **show redundancy application control-interface**command shows information for the redundancy group control interfaces.

Examples

The following is sample output from the **show redundancy application control-interface** command:

```
Router# show redundancy application control-interface group 2
The control interface for rg[2] is GigabitEthernet0/1/0
Interface is Control interface associated with the following protocols: 2 1
BFD Enabled
Interface Neighbors:
```

Related Commands

Command	Description
show redundancy application faults	Displays fault-specific information for a redundancy group.
show redundancy application group	Displays redundancy group information.
show redundancy application if-mgr	Displays if-mgr information for a redundancy group.
show redundancy application protocol	Displays protocol-specific information for a redundancy group.

show redundancy application data-interface

To display data interface-specific information, use the **show redundancy application data-interface**command in privileged EXEC mode.

show redundancy application data-interface group [*group-id*]

Syntax Description

group	Specifies the redundancy group.
group-id	(Optional) Redundancy group ID. Valid values are 1 and 2.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Usage Guidelines

The **show redundancy application data-interface** command displays information about the redundancy group data interfaces.

Examples

The following is sample output from the **show redundancy application data-interface** command:

```
Router# show redundancy application data-interface group 1
The data interface for rg[1] is GigabitEthernet0/1/1
```

Related Commands

Command	Description
show redundancy application control-interface	Displays control interface information for a redundancy group.
show redundancy application faults	Displays fault-specific information for a redundancy group.
show redundancy application group	Displays redundancy group information.
show redundancy application if-mgr	Displays if-mgr information for a redundancy group.
show redundancy application protocol	Displays protocol-specific information for a redundancy group.

show redundancy application faults group

To display fault-specific information for a redundancy group, use the **show redundancy application faults group**command in privileged EXEC mode.

show redundancy application faults group [*group-id*]

Syntax Description

group-id	(Optional) Redundancy group ID. Valid values are 1 and 2.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Usage Guidelines

The **show redundancy application faults**command shows information returned by redundancy group faults.

Examples

The following is sample output from the **show redundancy application faults** command:

```
Router# show redundancy application faults group 2
Faults states Group 2 info:
        Runtime priority: [150]
                RG Faults RG State: Up.
                        Total # of switchovers due to faults:          2
                        Total # of down/up state changes due to faults: 2
```

Related Commands

Command	Description
show redundancy application control-interface	Displays control interface information for a redundancy group.
show redundancy application group	Displays redundancy group information.
show redundancy application if-mgr	Displays if-mgr information for a redundancy group.
show redundancy application protocol	Displays protocol-specific information for a redundancy group.

show redundancy application group

To display the redundancy group information, use the **show redundancy application group** command in privileged EXEC mode.

show redundancy application group [{*group-id* | **all**}]

Syntax Description

group-id	(Optional) Redundancy group ID. Valid values are 1 and 2.
all	(Optional) Display information about all redundancy groups.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.
15.3(2)T	This command was integrated into Cisco IOS Release 15.3(2)T.

Usage Guidelines

Use the **show redundancy application group** command to display the current state of each interbox redundancy group on the device and the peer device.

Examples

The following is sample output from the **show redundancy application group all** command:

```
Device# show redundancy application group all

Faults states Group 1 info:
        Runtime priority: [200]
                RG Faults RG State: Up.
                        Total # of switchovers due to faults:           3
                        Total # of down/up state changes due to faults: 2
Group ID:1
Group Name:grp2
Administrative State: No Shutdown
Aggregate operational state : Up
My Role: ACTIVE
Peer Role: UNKNOWN
Peer Presence: No
Peer Comm: No
Peer Progression Started: No
RF Domain: btob-one
         RF state: ACTIVE
         Peer RF state: DISABLED
RG Protocol RG 1
------------------
        Role: Active
        Negotiation: Enabled
        Priority: 200
        Protocol state: Active
        Ctrl Intf(s) state: Down
        Active Peer: Local
        Standby Peer: Not exist
        Log counters:
```

```
                role change to active: 2
                role change to standby: 0
                disable events: rg down state 1, rg shut 0
                ctrl intf events: up 0, down 2, admin_down 1
                reload events: local request 3, peer request 0
RG Media Context for RG 1
--------------------------
        Ctx State: Active
        Protocol ID: 1
        Media type: Default
        Control Interface: GigabitEthernet0/1/0
        Hello timer: 5000
        Effective Hello timer: 5000, Effective Hold timer: 15000
         LAPT values: 0, 0
        Stats:
                Pkts 0, Bytes 0, HA Seq 0, Seq Number 0, Pkt Loss 0
                Authentication not configured
                Authentication Failure: 0
                Reload Peer: TX 0, RX 0
                Resign: TX 1, RX 0
        Standby Peer: Not Present.
Faults states Group 2 info:
        Runtime priority: [150]
                RG Faults RG State: Up.
                        Total # of switchovers due to faults:           2
                        Total # of down/up state changes due to faults: 2
Group ID:2
Group Name:name1
Administrative State: No Shutdown
Aggregate operational state : Up
My Role: ACTIVE
Peer Role: UNKNOWN
Peer Presence: No
Peer Comm: No
Peer Progression Started: No
RF Domain: btob-two
         RF state: ACTIVE
         Peer RF state: DISABLED
RG Protocol RG 2
------------------
        Role: Active
        Negotiation: Enabled
        Priority: 150
        Protocol state: Active
        Ctrl Intf(s) state: Down
        Active Peer: Local
        Standby Peer: Not exist
        Log counters:
                role change to active: 1
                role change to standby: 0
                disable events: rg down state 1, rg shut 0
                ctrl intf events: up 0, down 2, admin_down 1
                reload events: local request 2, peer request 0
RG Media Context for RG 2
--------------------------
        Ctx State: Active
        Protocol ID: 2
        Media type: Default
        Control Interface: GigabitEthernet0/1/0
        Hello timer: 5000
        Effective Hello timer: 5000, Effective Hold timer: 15000
         LAPT values: 0, 0
        Stats:
                Pkts 0, Bytes 0, HA Seq 0, Seq Number 0, Pkt Loss 0
```

```
            Authentication not configured
            Authentication Failure: 0
            Reload Peer: TX 0, RX 0
            Resign: TX 0, RX 0
    Standby Peer: Not Present.
```

The table below describes the significant fields shown in the display.

Table 182: show redundancy application group all Field Descriptions

Field	Description
Faults states Group 1 info	Redundancy group faults information for Group 1.
Runtime priority	Current priority of the redundancy group.
RG Faults RG State	Redundancy group state returned by redundancy group faults.
Total # of switchovers due to faults	Number of switchovers triggered by redundancy group fault events.
Total # of down/up state changes due to faults	Number of down and up state changes triggered by redundancy group fault events.
Group ID	Redundancy group ID.
Group Name	Redundancy group name.
Administrative State	Redundancy group state configured by users.
Aggregate operational state	Current redundancy group state.
My Role	Current role of the device.
Peer Role	Current role of the peer device.
Peer Presence	Indicates if the peer device is detected or not.
Peer Comm	Indicates the communication state with the peer device.
Peer Progression Started	Indicates if the peer device has started Redundancy Framework (RF) progression.
RF Domain	Name of the RF domain for the redundancy group.

Related Commands

Command	Description
show redundancy application control-interface	Displays control interface information for a redundancy group.
show redundancy application faults	Displays fault-specific information for a redundancy group.
show redundancy application if-mgr	Displays if-mgr information for a redundancy group.

Command	Description
show redundancy application protocol	Displays protocol-specific information for a redundancy group.

show redundancy application if-mgr

To display interface manager information for a redundancy group, use the **show redundancy application if-mgr** command in privileged EXEC mode.

show redundancy application if-mgr group [*group-id*]

Syntax Description

group	Specifies the redundancy group.
group-id	(Optional) Redundancy group ID. Valid values are 1 to 2.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Usage Guidelines

The **show redundancy application if-mgr** command shows information of traffic interfaces protected by redundancy groups. When a traffic interface is functioning with the redundancy group, the state is no shut on the active device, and shut on the standby device. On the other hand, it is always shut on the standby device.

Examples

The following is sample output from the **show redundancy application if-mgr** command:

```
Router# show redundancy application if-mgr group 2
RG ID: 2
 Interface       VIP         VMAC        Shut   Decrement
 ============================================================
 GigabitEthernet0/1/7 10.1.1.3 0007.b422.0016  no shut    50
 GigabitEthernet0/3/1 11.1.1.3 0007.b422.0017  no shut    50
```

The table below describes the significant fields shown in the display.

Table 183: show redundancy application if-mgr Field Descriptions

Field	Description
RG ID	Redundancy group ID.
Interface	Interface name.
VIP	Virtual IP address for this traffic interface.
VMAC	Virtual MAC address for this traffic interface.
Shut	The state of this interface. **Note** It is always “shut” on the standby box.
Decrement	The decrement value for this interface. When this interface goes down, the runtime priority of its redundancy group decreases.

Related Commands

Command	Description
show redundancy application control-interface	Displays control interface information for a redundancy group.
show redundancy application faults	Displays fault-specific information for a redundancy group.
show redundancy application group	Displays redundancy group information.
show redundancy application protocol	Displays protocol-specific information for a redundancy group

show redundancy application protocol

To display protocol-specific information for a redundancy group, use the **show redundancy application protocol**command in privileged EXEC mode.

show redundancy application protocol {*protocol-id* | **group** [*group-id*] }

Syntax Description

protocol-id	Protocol ID. The range is from 1 to 8.
group	Specifies the redundancy group.
group-id	(Optional) Redundancy group ID. Valid values are 1 and 2.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Usage Guidelines

The **show redundancy application protocol**command shows information returned by redundancy group protocol.

Examples

The following is sample output from the **show redundancy application protocol** command:

```
Router# show redundancy application protocol 3

Protocol id: 3, name:
 BFD: ENABLE
 Hello timer in msecs: 0
 Hold timer in msecs: 0
```

The table below describes the significant fields shown in the display.

Table 184: show redundancy application protocol Field Descriptions

Field	Description
Protocol id	Redundancy group protocol ID.
BFD	Indicates whether the BFD protocol is enabled for the redundancy group protocol.
Hello timer in msecs	Redundancy group hello timer, in milliseconds, for the redundancy group protocol. The default is 3000 msecs.
Hold timer in msecs	Redundancy group hold timer, in milliseconds, for the redundancy group protocol. The default is 10000 msecs.

Related Commands

Command	Description
show redundancy application group	Displays redundancy group information.
show redundancy application control-interface	Displays control interface information for a redundancy group.
show redundancy application faults	Displays fault-specific information for a redundancy group.
show redundancy application if-mgr	Displays if-mgr information for a redundancy group.

show redundancy application transport

To display transport-specific information for a redundancy group, use the **show redundancy application transport**command in privileged EXEC mode.

show redundancy application transport {**client** | **group** [*group-id*]}

Syntax Description

client	Displays transport client-specific information.
group	Displays the redundancy group name.
group-id	(Optional) Redundancy group ID. Valid values are 1 and 2.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Usage Guidelines

The **show redundancy application transport** command shows information for redundancy group transport.

Examples

The following is sample output from the **show redundancy application transport group** command:

```
Router# show redundancy application transport group 1
Transport Information for RG (1)
```

Related Commands

Command	Description
show redundancy application control-interface	Displays control interface information for a redundancy group.
show redundancy application faults	Displays fault-specific information for a redundancy group.
show redundancy application group	Displays redundancy group information.
show redundancy application if-mgr	Displays if-mgr information for a redundancy group.
show redundancy application protocol	Displays protocol-specific information for a redundancy group.

show redundancy linecard-group

To display the components of a Blade Failure Group, use the **show redundancy linecard-group** command in privileged EXEC mode.

show redundancy linecard-group *group-id*

Syntax Description

group-id	Group ID.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)SXE2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

The following example shows the components of a Blade Failure Group:

```
Router# show redundancy linecard-group

1
Line Card Redundancy Group:1 Mode:feature-card
Class:load-sharing
Cards:
Slot:3 Subslot:0
Slot:5 Subslot:0
```

Related Commands

Command	Description
linecard-group feature card	Assigns a group ID to a Blade Failure Group.

show running-config

To display the contents of the current running configuration file or the configuration for a specific module, Layer 2 VLAN, class map, interface, map class, policy map, or virtual circuit (VC) class, use the **show running-config** command in privileged EXEC mode.

show running-config [*options*]

Syntax Description

options	(Optional) Keywords used to customize output. You can enter more than one keyword. • **all** --Expands the output to include the commands that are configured with default parameters. If the **all** keyword is not used, the output does not display commands configured with default parameters. • **brief** --Displays the configuration without certification data and encrypted filter details. The **brief** keyword can be used with the **linenum** keyword. • **class-map** [*name*][**linenum**]--Displays class map information. The **linenum** keyword can be used with the **class-map** *name* option. • **control-plane** [**cef-exception**| **host**| **transit**]--Displays control-plane information. The **cef-exception**, **host**, and **transit** keywords can be used with the **control-plane** option. • **flow** {**exporter**	**monitor**	**record**}--Displays global flow configuration commands. The **exporter**, **monitor**, and **record**keywords can be used with the **flow** option. • **full** --Displays the full configuration. • **interface** *type number* -- Displays interface-specific configuration information. If you use the **interface** keyword, you must specify the interface type and the interface number (for example, **interface ethernet 0**). Keywords for common interfaces include **async**, **ethernet**, **fastEthernet**, **group-async**, **loopback**, **null**, **serial**, and **virtual-template**. Use the **show run interface ?**command to determine the interfaces available on your system. • **linenum** --Displays line numbers in the output. The **brief** or **full** keyword can be used with the **linenum** keyword. The **linenum**keyword can be used with the **class-map**, **interface**, **map-class**, **policy-map**, and **vc-class** keywords. • **map-class** [**atm**	**dialer**	**frame-relay**] [**name**] [**linenum**]--Displays map class information. This option is described separately; see the **show running-config map-class** command page.
	• **partition types** -- Displays the configuration corresponding to a partition. The **types** keyword can be used with the **partition**option. • **policy-map** [*name*][**linenum**]--Displays policy map information. The **linenum** keyword can be used with the **policy-map** *name* option. • **vc-class** [*name*] [**linenum**]--Displays VC-class information (the display is available only on certain devices such as the Cisco 7500 series devices). The **linenum** keyword can be used with the **vc-class** *name* option.

	• **view full** --Enables the display of a full running configuration. This is for view-based users who typically can only view the configuration commands that they are entitled to access for that particular view. • **vrf** *name* --Displays the Virtual routing and forwarding (VRF)-aware configuration module number . • **vlan** [*vlan-id*]--Displays the specific VLAN information ; valid values are from 1 to 4094.

Command Default

The default syntax, **show running-config**, displays the contents of the running configuration file, except commands configured using the default parameters.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.0	This command was introduced.
12.0	This command was replaced by the **more system:running-config** command.
12.0(1)T	This command was integrated into Cisco IOS Release 12.0(1)T, and the output modifier (|) was added.
12.2(4)T	This command was modified. The **linenum** keyword was added.
12.3(8)T	This command was modified. The **view full**option was added.
12.2(14)SX	This command was integrated into Cisco IOS Release 12.2(14)SX. The **module** *number* and **vlan** *vlan-id* keywords and arguments were added for the Supervisor Engine 720.
12.2(17d)SXB	This command was integrated into Release 12.2(17d)SXB and implemented on the Supervisor Engine 2.
12.2(33)SXH	This command was modified. The **all**keyword was added.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2. This command was enhanced to display the configuration information for traffic shaping overhead accounting for ATM and was implemented on the Cisco 10000 series device for the PRE3.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SB	This command was modified. Support for the Cisco 7300 series device was added.
12.4(24)T	This command was modified in a release earlier than Cisco IOS Release 12.4(24)T. The **partition** and **vrf** keywords were added. The **module** and **vlan** keywords were removed.
15.0(1)M	This command was modified. The output was modified to include encrypted filter information.
12.2(33)SXI	This command was modified. The output was modified to display Access Control List (ACL) information.

Usage Guidelines

The **show running-config** command is technically a command alias (substitute or replacement syntax) of the **more system:running-config** command. Although the use of more commands is recommended (because of

their uniform structure across platforms and their expandable syntax), the **show running-config** command remains enabled to accommodate its widespread use, and to allow typing shortcuts such as **show run**.

The **show running-config interface** command is useful when there are multiple interfaces and you want to look at the configuration of a specific interface.

The **linenum** keyword causes line numbers to be displayed in the output. This option is useful for identifying a particular portion of a very large configuration.

You can enter additional output modifiers in the command syntax by including a pipe character (|) after the optional keyword. For example, **show running-config interface serial 2/1 linenum | begin 3**. To display the output modifiers that are available for a keyword, enter **| ?** after the keyword. Depending on the platform you are using, the keywords and the arguments for the *options* argument may vary.

Prior to Cisco IOS Release 12.2(33)SXH, the **show running-config**command output omitted configuration commands set with default values. Effective with Cisco IOS Release 12.2(33)SXH, the **show running-config all** command displays complete configuration information, including the default settings and values. For example, if the Cisco Discovery Protocol (abbreviated as CDP in the output) hold-time value is set to its default of 180:

- The **show running-config** command does not display this value.
- The **show running-config all** displays the following output: cdp holdtime 180.

If the Cisco Discovery Protocol holdtime is changed to a nondefault value (for example, 100), the output of the **show running-config** and **show running-config all**commands is the same; that is, the configured parameter is displayed.

Note In Cisco IOS Release 12.2(33)SXH, the **all**keyword expands the output to include some of the commands that are configured with default values. In subsequent Cisco IOS releases, additional configuration commands that are configured with default values will be added to the output of the **show running-config all**command.

Effective with Cisco IOS Release 12.2(33)SXI, the **show running-config** command displays ACL information. To exclude ACL information from the output, use the **show running | section exclude ip access | access list**command.

Cisco 7600 Series Device

In some cases, you might see a difference in the duplex mode that is displayed between the **show interfaces** command and the **show running-config** command. The duplex mode that is displayed in the **show interfaces** command is the actual duplex mode that the interface is running. The **show interfaces** command displays the operating mode of an interface, and the **show running-config** command displays the configured mode of the interface.

The **show running-config** command output for an interface might display the duplex mode but no configuration for the speed. This output indicates that the interface speed is configured as auto and that the duplex mode that is displayed becomes the operational setting once the speed is configured to something other than auto. With this configuration, it is possible that the operating duplex mode for that interface does not match the duplex mode that is displayed with the **show running-config** command.

Examples

The following example shows the configuration for serial interface 1. The fields are self-explanatory.

```
Device# show running-config interface serial 1
```

```
Building configuration...
Current configuration:
!
interface Serial1
 no ip address
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
 shutdown
end
```

The following example shows the configuration for Ethernet interface 0/0. Line numbers are displayed in the output. The fields are self-explanatory.

```
Device# show running-config interface ethernet 0/0 linenum
Building configuration...
Current configuration : 104 bytes
 1 : !
 2 : interface Ethernet0/0
 3 :  ip address 10.4.2.63 255.255.255.0
 4 :  no ip route-cache
 5 :  no ip mroute-cache
 6 : end
```

The following example shows how to set line numbers in the command output and then use the output modifier to start the display at line 10. The fields are self-explanatory.

```
Device# show running-config linenum | begin 10

   10 : boot-start-marker
   11 : boot-end-marker
   12 : !
   13 : no logging buffered
   14 : enable password #####
   15 : !
   16 : spe 1/0 1/7
   17 :  firmware location bootflash:mica-modem-pw.172.16.0.0.bin
   18 : !
   19 : !
   20 : resource-pool disable
   21 : !
   22 : no aaa new-model
   23 : ip subnet-zero
   24 : ip domain name cisco.com
   25 : ip name-server 172.16.11.48
   26 : ip name-server 172.16.2.133
   27 : !
   28 : !
   29 : isdn switch-type primary-5ess
   30 : !
   .
   .
   .
   126 : end
```

The following example shows how to display the module and status configuration for all modules on a Cisco 7600 series device. The fields are self-explanatory.

```
Device#
show running-config
Building configuration...
Current configuration:
```

```
!
version 12.0
service timestamps debug datetime localtime
service timestamps log datetime localtime
no service password-encryption
!
hostname device
!
boot buffersize 126968
boot system flash slot0:7600r
boot bootldr bootflash:c6msfc-boot-mz.120-6.5T.XE1.0.83.bin
enable password lab
!
clock timezone Pacific -8
clock summer-time Daylight recurring
redundancy
 main-cpu
  auto-sync standard
!
ip subnet-zero
!
ip multicast-routing
ip dvmrp route-limit 20000
ip cef
mls flow ip destination
mls flow ipx destination
cns event-service server
!
spanning-tree portfast bpdu-guard
spanning-tree uplinkfast
spanning-tree vlan 200 forward-time 21
port-channel load-balance sdip
!
!
!
 shutdown
!
!
.
.
.
```

In the following sample output from the **show running-config** command, the **shape average**command indicates that the traffic shaping overhead accounting for ATM is enabled. The BRAS-DSLAM encapsulation type is qinq and the subscriber line encapsulation type is snap-rbe based on the ATM adaptation layer 5 (AAL5) service. The fields are self-explanatory

```
Device# show running-config
.
.
.
subscriber policy recording rules limit 64
no mpls traffic-eng auto-bw timers frequency 0
call rsvp-sync
!
controller T1 2/0
framing sf
linecode ami
!
controller T1 2/1
framing sf
linecode ami
!
```

```
!
policy-map unit-test
class class-default
shape average percent 10 account qinq aal5 snap-rbe
!
```

The following is sample output from the **show running-config class-map** command. The fields in the display are self-explanatory.

```
Device# show running-config class-map
Building configuration...
Current configuration : 2910 bytes
!
class-map type stack match-all ip_tcp_stack
 match field IP protocol eq 0x6 next TCP
class-map type access-control match-all my
 match field UDP dest-port eq 1111
 match encrypted
  filter-version 0.1, Dummy Filter 2
  filter-id      123
  filter-hash    DE0EB7D3C4AFDD990038174A472E4789
  algorithm      aes256cbc
  cipherkey      realm-cisco.sym
  ciphervalue    #
oeahb4L6JK+XuC0q8k9AqXvBeQWzVfdg8WV67WEXbiWdXGQs6BEXqQeb4Pfow570zM4eDw0gxlp/Er8w
/lXsmolSgYpYuxFMYb1KX/H2iCXvA76VX7w5TElb/+6ekgbfP/d5ms6DEzKa8DlOpl+Q95lP194PsIlU
wCyfVCwLS+T8p3RDLi8dKBgQMcDW4Dha1ObBJTpV4zpwhEdMvJDu5PATtEQhFjhN/UYeyQiPRthjbkJn
LzT8hQFxwYwVW8PCjkyqEwYrr+R+mFG/C7tFRiooaW9MU9PCpFd95FARvlU=#
  exit
class-map type stack match-all ip_udp_stack
 match field IP protocol eq 0x11 next UDP
class-map type access-control match-all psirt1
 match encrypted
  filter-version 0.0_DummyVersion_20090101_1830
  filter-id      cisco-sa-20090101-dummy_ddts_001
  filter-hash    FC50BED10521002B8A170F29AF059C53
  algorithm      aes256cbc
  cipherkey      realm-cisco.sym
  ciphervalue    #
DkGbVq0FPAsVJKguU15lQPDfZyTcHUXWsj8+tD+dCSYW9cjkRU9jyST4vO4u69/L62QlbyQuKdyQmb10
6sAeY5vDsDfDV05k4o5eD+j8cMt78iZT0Qg7uGiBSYBbak3kKn/5w2gDd1vnivyQ7g4Ltd9+XM+GP6XL
27RrXeP5A5iGbzC7KI9t6riZXk0gmR/vFw1a5wck0D/iQHIlFa/yRPoKMSFlqfIlLTe5NM7JArSTKET2
pu7wZammTz4FF6rY#
  exit
 match start TCP payload-start offset 0 size 10 regex "abc.*def"
 match field TCP source-port eq 1234
class-map type access-control match-all psirt2
 match encrypted
  filter-version 0.0_DummyVersion_20090711_1830
  filter-id      cisco-sa-20090711-dummy_ddts_002
  filter-hash    DE0EB7D3C4AFDD990038174A472E4789
  algorithm      aes256cbc
  cipherkey      realm-cisco.sym
```

The following example shows that the teletype (tty) line 2 is reserved for communicating with the 2nd core:

```
Device# show running
Building configuration...

Current configuration:
!
```

```
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname device
!
enable password lab
!
no ip subnet-zero
!
!
!
interface Ethernet0
 ip address 172.25.213.150 255.255.255.128
 no ip directed-broadcast
 no logging event link-status
!
interface Serial0
 no ip address
 no ip directed-broadcast
 no ip mroute-cache
 shutdown
 no fair-queue
!
interface Serial1
 no ip address
 no ip directed-broadcast
 shutdown
!
ip default-gateway 172.25.213.129
ip classless
ip route 0.0.0.0 0.0.0.0 172.25.213.129
!
!
line con 0
 transport input none
line 1 6
 no exec
 transport input all
line 7
 no exec
 exec-timeout 300 0
 transport input all
line 8 9
 no exec
 transport input all
line 10
 no exec
 transport input all
 stopbits 1
line 11 12
 no exec
 transport input all
line 13
 no exec
 transport input all
 speed 115200
line 14 16
 no exec
 transport input all
line aux 0
line vty 0 4
 password cisco
```

```
 login
!
end
```

Related Commands

Command	Description
bandwidth	Specifies or modifies the bandwidth allocated for a class belonging to a policy map, and enables ATM overhead accounting.
boot config	Specifies the device and filename of the configuration file from which the device configures itself during initialization (startup).
configure terminal	Enters global configuration mode.
copy running-config startup-config	Copies the running configuration to the startup configuration. (Command alias for the **copy system:running-config nvram:startup-config** command.)
shape	Shapes traffic to the indicated bit rate according to the algorithm specified, and enables ATM overhead accounting.
show interfaces	Displays statistics for all interfaces configured on the device or access server.
show policy-map	Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps, and displays ATM overhead accounting information, if configured.
show startup-config	Displays the contents of NVRAM (if present and valid) or displays the configuration file pointed to by the CONFIG_FILE environment variable. (Command alias for the **more:nvram startup-config** command.)

show running-config vrf

To display the subset of the running configuration of a router that is linked to a specific VPN routing and forwarding (VRF) instance or linked to all VRFs configured on the router, use the **show running-config vrf** command in privileged EXEC mode.

show running-config vrf [*vrf-name*]

Syntax Description

vrf-name	(Optional) Name of the VRF configuration that you want to display.

Command Default

If you do not specify the name of a VRF configuration, the running configurations of all VRFs on the router are displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
Cisco IOS XE Release 3.5S	This command was modified. The output of the command was modified to display the Network Address Translation (NAT) configuration.

Usage Guidelines

Use the **show running-config vrf** command to display a specific VRF configuration or to display all VRF configurations on the router. To display the configuration of a specific VRF, specify the name of the VRF.

This command displays the following elements of the VRF configuration:

- The VRF submode configuration.
- The routing protocol and static routing configurations associated with the VRF.
- The configuration of interfaces in the VRF, which includes the configuration of any owning controller and physical interface for a subinterface.

Examples

The following is sample output from the **show running-config vrf** command. It includes a base VRF configuration for VRF vpn3 and Border Gateway Protocol (BGP) and Open Shortest Path First (OSPF) configurations associated with VRF vpn3.

```
Router# show running-config vrf vpn3

Building configuration...

Current configuration : 720 bytes
```

```
ip vrf vpn3
 rd 100:1
 route-target export 100:1
 route-target import 100:1
!
!
interface GigabitEthernet0/0/1
 description connected to nat44-1ru-ce1 g0/0/0
 ip vrf forwarding vpn3
 ip address 172.17.0.1 255.0.0.0
 ip nat inside
 shutdown
 negotiation auto
!
interface GigabitEthernet0/0/3
 no ip address
 negotiation auto
!
interface GigabitEthernet0/0/3.2
 encapsulation dot1Q 2
 ip vrf forwarding vpn3
 ip address 10.0.0.1 255.255.255.0
 ip nat inside
!
router bgp 100
 !
 address-family ipv4 vrf vpn3
  redistribute connected
  redistribute static
 exit-address-family
ip nat inside source route-map rm-vpn3 pool shared-pool vrf vpn3 match-in-vrf overload
ip nat pool shared-pool 10.0.0.2 10.0.0.254 prefix-length 24
!
router ospf 101 vrf vpn3
 log-adjacency-changes
 area 1 sham-link 10.43.43.43 10.23.23.23 cost 10
 network 172.17.0.0 0.255.255.255 area 1
.
.
.
end
```

The table below describes the significant fields shown in the display.

Table 185: show running-config vrf Field Descriptions

Field	Description
Current configuration: 720 bytes	Indicates the number of bytes (720) in the VRF vpn3 configuration.
ip vrf vpn3	Indicates the name of the VRF (vpn3) for which the configuration is displayed.
rd 100:1	Identifies the route distinguisher (100:1) for VRF vpn3.
route-target export 100:1 route-target import 100:1	Specifies the route-target extended community for VRF vpn3. • Routes tagged with route-target export 100:1 are exported from VRF vpn3. • Routes tagged with the route-target import 100:1 are imported into VRF vpn3.

Field	Description
interface GigabitEthernet0/0/1	Specifies the interface associated with VRF vpn3.
ip vrf forwarding vpn3	Associates VRF vpn3 with the named interface.
ip address 172.17.0.1 255.0.0.0	Configures the IP address of the Gigabit Ethernet interface.
ip nat inside	Enables NAT of inside addresses.
router bgp 100	Sets up a BGP routing process for the router with the autonomous system number as 100.
address-family ipv4 vrf vpn3	Sets up a routing session for VRF vpn3 using the standard IPv4 address prefixes.
redistribute connected	Redistributes routes that are automatically established by the IP on an interface into the BGP routing domain.
ip nat pool	Defines a pool of IP addresses for NAT.
router ospf 101 vrf vpn3	Sets up an OSPF routing process and associates VRF vpn3 with OSPF VRF processes.
area 1 sham-link 10.43.43.43 10.23.23.23 cost 10	Configures a sham-link interface on a provider edge (PE) router in a Multiprotocol Label Switching (MPLS) VPN backbone. • 1 is the ID number of the OSPF area assigned to the sham-link. • 10.43.43.43 is the IP address of the source PE router. • 10.23.23.23 is the IP address of the destination PE router. • 10 is the OSPF cost to send IP packets over the sham-link interface.
network 172.17.0.0 0.255.255.255 area 1	Defines the interfaces on which OSPF runs and defines the area ID for those interfaces.

Related Commands

Command	Description
ip vrf	Configures a VRF routing table.
show ip interface	Displays the usability status of interfaces configured for IP.
show ip vrf	Displays the set of defined VRFs and associated interfaces.
show running-config interface	Displays the configuration for a specific interface.

show sasl

To display Simple Authentication and Security Layer (SASL) information, use the **show sasl** command in user EXEC or privileged EXEC mode.

show sasl {**all** | **context** | **mechanisms** | **profile** {*profile-name* | **all**}}

Syntax Description

all	Displays detailed information for all SASL profiles.
context	Displays context information for SASL profiles.
mechanisms	Displays the mechanisms applied for all SASL profiles.
profile *profile-name*	Displays detailed information for the specified SASL profile.
profile all	Displays all configured profiles.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.3(1)	This command was introduced.
12.2(33)SRC	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRC.
12.2(33)SXI	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Examples

The following is sample output from the **show sasl profile all** command:

```
Router# show sasl profile all
SASL profile 'sgw_sasl' Refs:0 Mechs:0x2
    client:  <NONE>/<NONE>
    servers: ravi/ravi

SASL profile 'sgw_1' Refs:0 Mechs:0x1
    client:  us1/pw1
    servers: server1/user
```

The table below describes the significant fields shown in the display.

Table 186: show sasl profile all Field Descriptions

Field	Description
SASL profile	Indicates the name of the SASL profile.

Field	Description
Refs	Indicates the number of active sessions.
Mechs	Indicates the profile mechanisms configured.
client	Indicates the SASL client configured for the specified profile.
servers	Indicates the SASL server configured for the specified profile.

Related Commands

Command	Description
sasl	Configures SASL.

show secure bootset

To display the status of Cisco IOS image and configuration resilience, use the **show secure**command in privileged EXEC mode.

show secure bootset

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

Use the **show secure bootset**command, instead of the Cisco IOS directory listing **dir** command, to verify the existence of an image archive. This command also displays output that specifies whether the image or configuration archive is ready for an upgrade.

Examples

The following is sample output from the **show secure bootset** command. The field descriptions are self-explanatory:

```
Router# show secure bootset
%IOS image and configuration resilience is not active
Router# show secure bootset
IOS resilience router id JMX0704L5GH
IOS image resilience version 12.3 activated at 08:16:51 UTC Sun Jun 16 2002
Secure archive slot0:c3745-js2-mz type is image (elf) []
  file size is 25469248 bytes, run size is 25634900 bytes
  Runnable image, entry point 0x80008000, run from ram
IOS configuration resilience version 12.3 activated at 08:17:02 UTC Sun Jun 16 2002
Secure archive slot0:.runcfg-20020616-081702.ar type is config
configuration archive size 1059 bytes
```

Related Commands

Command	Description
dir	Displays a list of files on a file system.
secure boot-config	Saves a secure copy of the router running configuration in persistent storage.
secure boot-image	Enables Cisco IOS image resilience.

show smm

To display string matching module (SMM) information, use the **show smm** command in privileged EXEC mode.

show smm {**counters** | **timing** | **tree** [{*tree-index* | **details**}]}

Syntax Description

counters	Displays information about SMM counters.
timing	Displays timing information about the SMM.
tree	Displays the AVL tree containing the string information.
tree-index	(Optional) Specifies the tree index.
details	(Optional) Displays detailed information about the AVL tree.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)	This command was introduced in a release earlier than Cisco IOS Release 15.0(1) on Cisco 3845 series routers.

Examples

The following is sample output from the **show smm counters** command. Fields in the output are self-explanatory.

```
Router# show smm counters

Number of non-matching packets processed   - 0
Number of cache hits                       - 0
Number of cache misses                     - 0
Cache full instances                       - 0
Number of matching packets processed       - 0
Number of matches for Stage0               - 0
Number of matches for Stage1               - 0
Number of matches for Stage2               - 0
Number of matches for Stage3               - 0
Number of signatures in signature database - 0
```

The following is sample output from the **show smm timing** command:

```
Router# show smm timing
Packet processing stats (in microseconds) :
-------------------------------------------
Minimum processing time per packet - 0
Maximum processing time per packet - 0
Average processing time for non-matching packets - 0
Average processing time for matching packets     - 0
```

Related Commands

Command	Description
action string match	Returns 1 to the $_string_result, if the string matches the pattern when an EEM applet is triggered.

show snmp mib nhrp status

To display status information about the Next Hop Resolution Protocol (NHRP) MIB, use the **show snmp mib nhrp** status command in privileged EXEC mode.

show snmp mib nhrp status

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

This command is used to display the status of the MIB for NHRP and whether the NHRP MIB is enabled or disabled.

Examples

The following output is from the show snmp mib nhrp status command:

```
Spoke_103# show snmp mib nhrp status
NHRP-SNMP Agent Feature: Enabled
NHRP-SNMP Tree State: Good
ListEnqueue Count = 0 Node Malloc Counts = 1
Spoke_103#
```

Table 1 describes the significant fields shown in the display.

Table 187: show snmp mib nhrp status Field Descriptions

Field	Description
NHRP-SNMP Agent Feature:	Shows the status of the NHRP MIB. "Enabled" indicates that the NHRP MIB is enabled. If the NHRP MIB was disabled, it would display "Disabled".
ListEnqueue Count	Indicates how many nodes have been queued for freeing.
Node Malloc Counts	Indicates how many nodes are allocated.

Related Commands

Command	Description
show snmp mib	Displays a list of the MIB OIDs registered on the system.

show ssh

To display the status of Secure Shell (SSH) server connections on the router, use the **show ssh** command in user EXEC or privileged EXEC mode.

show ssh vty [*ssh-number*]

Syntax Description

vty	Displays virtual terminal line (VTY) connection details.
ssh-number	(Optional) The number of SSH server connections on the router. Range is from 0 to 1510. The default value is 0.

Command Modes

User Exec (>)
Privileged EXEC (#)

Command History

Release	Modification
12.1(15)T	This command was introduced.
12.2(33)SRA	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXI	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.1	This command was modified. It was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

Use the **show ssh** command to display the status of the SSH connections on your router. This command does not display any SSH configuration data. Use the **show ip ssh** command for SSH configuration information such as timeouts and retries.

Examples

The following is sample output from the **show ssh** command with SSH enabled:

```
Router# show ssh
Connection     Version      Encryption     State                Username
0               1.5         3DES           Session Started       guest
```

The table below describes the significant fields shown in the display.

Table 188: show ssh Field Descriptions

Field	Description
Connection	Number of SSH connections on the router.
Version	Version number of the SSH terminal.
Encryption	Type of transport encryption.

Field	Description
State	The status of SSH connection to indicate if the session has started or stopped.
Username	Uesrname to log in to the SSH.

Related Commands

Command	Description
show ip ssh	Displays version and configuration data for SSH.

show ssl-proxy module state

To display the spanning-tree state for the specified VLAN, enter the **showssl-proxymodulestate** command in user EXEC mode.

show ssl-proxy module *mod* **state**

Syntax Description

mod	Module number.

Command Modes

User EXEC (>)

Command History

Release	Modification
12.2(18)SXD	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is supported on Cisco 7600 series routers that are configured with a Secure Sockets Layer (SSL) Services Module only.

Examples

This example shows how to verify that the VLAN information displayed matches the VLAN configuration. The fields shown in the display are self-explanatory.

```
Router# show ssl-proxy module 6 state
SSL-services module 6 data-port:
 Switchport:Enabled
Administrative Mode:trunk
Operational Mode:trunk
Administrative Trunking Encapsulation:dot1q
Operational Trunking Encapsulation:dot1q
Negotiation of Trunking:Off
Access Mode VLAN:1 (default)
Trunking Native Mode VLAN:1 (default)
Trunking VLANs Enabled:100
Pruning VLANs Enabled:2-1001
Vlans allowed on trunk:100
Vlans allowed and active in management domain:100
Vlans in spanning tree forwarding state and not pruned:
100
Allowed-vlan :100
Router#
```

Related Commands

Command	Description
ssl-proxy module allowed-vlan	Adds the VLANs allowed over the trunk to the SSL Services Module.

show tacacs

To display statistics for a TACACS+ server, use the **show tacacs** command in privileged EXEC mode.

show tacacs [{**private** | **public**}]

Syntax Description

private	(Optional) Displays private tacacs+ server statistics.
public	(Optional) Displays public tacacs+ server statistics.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.3	This command was integrated into Cisco IOS XE Release 2.3. The **private** and **public** keywords were added.

Examples

The following example is sample output for the **show tacacs** command:

```
Router# show tacacs

Tacacs+ Server            : 172.19.192.80/49
              Socket opens:          3
             Socket closes:          3
             Socket aborts:          0
             Socket errors:          0
          Socket Timeouts:           0
   Failed Connect Attempts:          0
        Total Packets Sent:          7
        Total Packets Recv:          7
          Expected Replies:          0
  No current connection
```

he following is sample output from the **show tacacs** command for the private IP address 192.168.0.0:

```
Router# show tacacs private 192.168.0.0
Tacacs+ Server -  private  :  192.168.0.0
              Socket opens:          0
             Socket closes:          0
             Socket aborts:          0
             Socket errors:          0
          Socket Timeouts:           0
   Failed Connect Attempts:          0
```

```
        Total Packets Sent:          0
        Total Packets Recv:          0
```

The following is sample output from the **show tacacs** command for the public IP address 209.165.200.224:

```
Router# show tacacs public 209.165.200.224
Tacacs+ Server -  public  :  209.165.200.224
              Socket opens:          0
             Socket closes:          0
             Socket aborts:          0
             Socket errors:          0
          Socket Timeouts:           0
   Failed Connect Attempts:          0
        Total Packets Sent:          0
        Total Packets Recv:          0
```

The table below describes the significant fields shown in the display.

Table 189: show tacacs Field Descriptions

Field	Description
Tacacs+ Server	IP address of the TACACS+ server.
Socket opens	Number of successful TCP socket connections to the TACACS+ server.
Socket closes	Number of successfully closed TCP socket attempts.
Socket aborts	Number of premature TCP socket closures to the TACACS+ server; That is, the peer did not wait for a reply from the server after a the peer sent its request.
Socket errors	Any other socket read or write errors, such as incorrect packet format and length.
Failed Connect Attempts	Number of failed TCP socket connections to the TACACS+ server.
Total Packets Sent	Number of packets sent to the TACACS+ server.
Total Packets Recv	Number of packets received from the TACACS+ server.
Tacacs+ Server	IP address of the TACACS+ server.

Related Commands

Command	Description
tacacs-server host	Specifies a TACACS+ host.

show tcp intercept connections

To display TCP incomplete and established connections, use the **show tcp intercept connections**command in EXEC mode.

show tcp intercept connections

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.2 F	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **show tcp intercept connections** command to display TCP incomplete and established connections.

Examples

The following is sample output from the **show tcp intercept connections** command:

```
Router# show tcp intercept connections

Incomplete:
Client                Server                State    Create   Timeout  Mode
172.19.160.17:58190   10.1.1.30:23          SYNRCVD  00:00:09 00:00:05 I
172.19.160.17:57934   10.1.1.30:23          SYNRCVD  00:00:09 00:00:05 I

Established:
Client                Server                State    Create   Timeout  Mode
172.16.232.23:1045    10.1.1.30:23          ESTAB    00:00:08 23:59:54 I
```

The table below describes significant fields shown in the display.

Table 190: show tcp intercept connections Field Descriptions

Field	Description
Incomplete:	Rows of information under "Incomplete" indicate connections that are not yet established.
Client	IP address and port of the client.
Server	IP address and port of the server being protected by TCP intercept.
State	SYNRCVD--establishing with client. SYNSENT--establishing with server. ESTAB--established with both, passing data.

Field	Description
Create	Hours:minutes:seconds since the connection was created.
Timeout	Hours:minutes:seconds until the retransmission timeout.
Mode	I--intercept mode. W--watch mode.
Established:	Rows of information under "Established" indicate connections that are established. The fields are the same as those under "Incomplete" except for the Timeout field described below.
Timeout	Hours:minutes:seconds until the connection will timeout, unless the software sees a FIN exchange, in which case this indicates the hours:minutes:seconds until the FIN or RESET timeout.

Related Commands

Command	Description
ip tcp intercept connection-timeout	Changes how long a TCP connection will be managed by the TCP intercept after no activity.
ip tcp intercept finrst-timeout	Changes how long after receipt of a reset or FIN-exchange the software ceases to manage the connection.
ip tcp intercept list	Enables TCP intercept.
show tcp intercept statistics	Displays TCP intercept statistics.

show tcp intercept statistics

To display TCP intercept statistics, use the **show tcp intercept statistics**command in EXEC mode.

show tcp intercept statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.2 F	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **show tcp intercept statistics**command to display TCP intercept statistics.

Examples

The following is sample output from the **show tcp intercept statistics** command:

```
Router# show tcp intercept statistics
intercepting new connections using access-list 101
2 incomplete, 1 established connections (total 3)
1 minute connection request rate 2 requests/sec
```

Related Commands

Command	Description
ip tcp intercept connection-timeout	Changes how long a TCP connection will be managed by the TCP intercept after no activity.
ip tcp intercept finrst-timeout	Changes how long after receipt of a reset or FIN-exchange the software ceases to manage the connection.
ip tcp intercept list	Enables TCP intercept.
show tcp intercept connections	Displays TCP incomplete and established connections.

show tech-support alg

To display application layer gateway (ALG)-specific information to assist in troubleshooting, use the **show tech-support alg** command in privileged EXEC mode.

show tech-support alg platform

Syntax Description

platform	Displays platform-specific ALG information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.9S	This command was introduced.

Usage Guidelines

The **show tech-support alg** command is useful for collecting a large amount of information about ALGs for troubleshooting purposes. The output of this command can be provided to technical support representatives when reporting a problem. The command output displays the output of a number of **show** commands at once. The output from this command varies depending on your platform and configuration.

Examples

The following is sample output from the **show tech-support alg platform** command:

```
Device# show tech-support alg platform

show platform hardware qfp active feature alg memory

Pool information:
Pool-Name                Num-Entries  Entry-Limit  Size(bytes)  Num-Additions
-----------------------------------------------------------------------------
FTP pool                 640          0            41376        0
SCCP pool                160          0            8096         0
SIP pool                 640          0            348576       0
SIP pkt pool             160          0            18336        0
SIP msg pool             320          0            26016        0
RTSP pool                160          0            10656        0
H323 info pool           100          5000         61216        0
H323 fs olc pool         100          5000         3616         0
H323 pkt sb pool         100          5000         3616         0
H323 indus pool          1000         2000         4112416      0
H323 tl olc pool         100          5000         3616         0
H323 msg info pool       100          5000         8416         0
DNS pool                 1024         0            82336        0
LDAP pool                128          5000         4512         0
LDAP pkt info pool       32           160          670624       0
RCMD pool                160          5000         5536         0
HTTP info pool           2400         1048576      192416       0
HTTP req ctxt pool       6400         2097152      1638816      0
HTTP resp ctxt pool      6400         2097152      1331616      0
HTTP hdr fld pool        6400         2097152      307616       0
HTTP MIME ctxt pool      6400         2097152      819616       0
NetBIOS L7 data pool     1024         5000         33184        0
Act token pool           640          0            143776       0
Ext state pool           160          0            5536         0
ALG HA ntuple hdr pool   10000        0            640416       0
```

```
Sun RPC info pool        1024         7168         33184        0
MS RPC info pool         1024         7168         49568        0
MS RPC extended toke...  1024         7168         82336        0
SMTP l7 info pool        2400         524288       1075616      0
SMTP command pool        6400         1048576      307616       0
SMTP log filter pool     6400         1048576      307616       0
SMTP mask pool           6400         1048576      307616       0
IMAP info pool           2400         524288       154016       0
POP3 info pool           2400         524288       154016       0
GTP AIC ctxt pool        2400         1048576      154016       0
GTP request response...  2400         524288       154016       0
GTP hash info pool       2400         2097152      192416       0
GTP master pdp pool      2400         524288       1421216      0
GTP secondary pdp pool   2400         524288       269216       0
GTP req_resp hash en...  2400         1048576      192416       0

Table information:
Ha hash table: Num-Entries: 10000, Size(bytes): 40000

show platform hardware qfp active feature td datapath memory
==VTCP ucode info==
info alloc 0, free 0, fail 0
pkt buf alloc 0, free 0, fail 0
buf size alloc 0, free 0
rx drop 0, tx drop 0, tcp drop 0, alg csum 0
sending: rx ack 0, rst 0, hold rst 0 tx payload: seg 0, rexmit 0
vtcp_info_chunk 0x8d54fcb0, totalfree: 2048, allocated: 0
vtcp_pkt_pool 0x8d5d80c0, total: 1048240, free: 1048240
vtcp_timer_wheel 0x8d6d84d0, vtcp_init 1
td_internal debug 0x0
td_global td_init 0x2
alg_debug_vtcp 0x0

show platform hardware qfp active feature alg statistics
ALG counters:
ALG         Cntrl-Pkt        Parser-Err&Drop  Parser-No-Act
FTP         0                0                0
SIP         0                0                0
SKINNY      0                0                0
H225        0                0                0
H245        0                0                0
H225ras     0                0                0
RTSP        0                0                0
DNS         0                0                0
LDAP        0                0                0
TFTP        0                0                0
HTTP        0                0                0
SHELL       0                0                0
LOGIN       0                0                0
NETBIOS-NS  0                0                0
NETBIOS-SSN 0                0                0

ALG chunk pool:
Pool-Name                  Used-Entries     Free-Entries
FTP pool                   0                640
SCCP pool                  0                160
SIP pool                   0                640
SIP pkt pool               0                160
SIP msg pool               0                320
RTSP pool                  0                160
H323 info pool             0                100
H323 fs olc pool           0                100
H323 pkt sb pool           0                100
H323 indus pool            50               950
```

```
H323 tl olc pool            0               100
H323 msg info pool          0               100
DNS pool                    0               1024
LDAP pool                   0               128
LDAP pkt info pool          0               32
HTTP info pool              0               0
HTTP req ctxt pool          0               0
HTTP resp ctxt pool         0               0
HTTP hdr fld pool           0               0
HTTP MIME ctxt pool         0               0
NetBIOS L7 data pool        0               1024

Common ALG chunk pool:
Pool-Name                   Used-Entries    Free-Entries
Act Token Pool              0               640
Ext State Pool              0               160
HA ntuple hdr Pool          0               10000
Sun RPC info pool           0               1024
MS RPC info pool            0               1024
SMTP l7 info pool           0               0
SMTP command pool           0               0
SMTP log filter pool        0               0
SMTP mask pool              0               0
IMAP info pool              0               0
POP3 info pool              0               0
GTP AIC ctxt pool           0               0
GTP Req/Res pool            0               0
GTP hash info pool          0               0
GTP master pdp pool         0               0
GTP secondary pdp pool      0               0
GTP req_res hash entry pool 0               0
.
.
.
```

The table below describes the significant fields shown in the display.

Table 191: show tech-support alg platform Field Descriptions

Field	Description
Pool information	Detailed information about ALG pools.
Pool-Name	Name of the ALG pool.
Num-Entries	Number of pool entries.
Entry-Limit	Configured limit for the number of packets that can access the pool.
info alloc	Virtual TCP (vTCP) allocated counts.
pak buf alloc	Allocated packet buffer.
buf siz alloc	Allocated buffer size.

Related Commands

Command	Description
show platform hardware qfp feature alg	Displays ALG-specific information in the QFP.

show tech-support ipsec

To display IPsec information to assist in troubleshooting, use the **show tech-support ipsec** command in privileged EXEC mode.

show tech-support ipsec [{**peer** *ipv4-address* | **vrf** *vrf-name* | **platform**}]

Syntax Description

peer *ipv4-address*	(Optional) Displays information about the specified IPv4 peer.
vrf *vrf-name*	(Optional) Displays information about the specified VPN routing and forwarding (VRF) instance.
platform	(Optional) Displays platform specific information about the IPsec flow.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 Series Aggregation Service Routers.
Cisco IOS XE Release 3.7S	This command was modified. The **platform** keyword was added. The output was enhanced to display platform specific information about the IPsec flow.

Usage Guidelines

The **show tech-support ipsec** command simplifies the collection of IPsec-related information if you are troubleshooting a problem.

The **show tech-support ipsec** command without any keywords displays the output from the following **show** commands, as listed in the order below:

- **show version**
- **show running-config**
- **show crypto isakmp sa count**
- **show crypto ipsec sa count**
- **show crypto session summary**
- **show crypto session detail**
- **show crypto isakmp sa detail**
- **show crypto ipsec sa detail**
- **show crypto isakmp peers**
- **show crypto ruleset detail**
- **show processes memory | include Crypto IKMP**

- **show processes cpu | include Crypto IKMP**
- **show crypto eli**
- **show crypto engine accelerator statistic**

The **show tech-support ipsec** command with the **peer** keyword and the *ipv4-address* argument displays the output from the following **show** commands, as listed in the order below:

- **show version**
- **show running-config**
- **show crypto session remote** *ipv4address* **detail**
- **show crypto isakmp sa peer** *ipv4address* **detail**
- **show crypto ipsec sa peer** *ipv4address* **detail**
- **show crypto isakmp peers** *ipv4address*
- **show crypto ruleset detail**
- **show processes memory** | **include Crypto IKMP**
- **show processes cpu** | **include Crypto IKMP**
- **show crypto eli**
- **show crypto engine accelerator statistic**

The **show tech-support ipsec** command with the **vrf** *vrf-name* keyword and argument displays the output from the following **show** commands as listed in the order below:

- **show version**
- **show running-config**
- **show crypto isakmp sa count vrf** *vrf-name*
- **show crypto ipsec sa count vrf** *vrf-name*
- **show crypto session ivrf** *ivrf-name* **detail**
- **show crypto session fvrf** *fvrf-name* **detail**
- **show crypto isakmp sa vrf** *vrf-name* **detail**
- **show crypto ipsec sa vrf** *vrf-name* **detail**
- **show crypto ruleset detail**
- **show processes memory** | **include Crypto IKMP**
- **show processes cpu** | **include Crypto IKMP**
- **show crypto eli**
- **show crypto engine accelerator statistic**

The **show tech-support ipsec platform** command displays the output from the following **show** commands, as listed in the order below:

- **show clock**
- **show version**
- **show running-config**
- **show crypto tech-support**
- **show crypto isakmp sa count**
- **show crypto ipsec sa count**
- **show crypto isakmp sa detail**
- **show crypto ipsec sa detail**
- **show crypto session summary**
- **show crypto session detail**
- **show crypto isakmp peers**
- **show crypto ruleset detail**
- **show processes memory**
- **show processes cpu**
- **show crypto eli**
- **show crypto engine accelerator statistic**
- **show crypto isakmp diagnose error**
- **show crypto isakmp diagnose error count**
- **show crypto call admission statistics**

Related Commands

Command	Description
show tech-support	Displays information about the device when the device reports a problem.

show tech-support pki

To display public key infrastructure (PKI)-specific information to assist in troubleshooting, use the **show tech-support pki** command in privileged EXEC mode.

show tech-support pki

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.8.1	This command was introduced.
Cisco IOS XE Fuji 16.9.1	This command was modified to display the clock, version and other configuration details.

Usage Guidelines

The **show tech-support pki** command is useful for collecting the complete set of PKI-related information for troubleshooting purposes. The output of this command can be provided to technical support representatives when reporting a problem.

Examples

The following is sample output from the **show tech-support pki** command:

```
Device# show tech-support pki

------------------ show clock ------------------


07:07:35.291 IST Sun Jun 3 2018

------------------ show version ------------------

Cisco IOS XE Software, Version 2018-05-31_14.33_sudsirig
Cisco IOS Software [Fuji], IOS-XE Virtual XE Software (X86_64_LINUX_IOSD-UNIVERSALK9-M),
Experimental Version 16.10.20180531:085308
[polaris_dev-/nobackup/sudsirig/poldev_cflow_devtest 105]
Copyright (c) 1986-2018 by Cisco Systems, Inc.
Compiled Thu 31-May-18 14:26 by sudsirig


Cisco IOS-XE software, Copyright (c) 2005-2018 by cisco Systems, Inc.
All rights reserved.  Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0.  The
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY.  You can redistribute and/or modify such
GPL code under the terms of GPL Version 2.0.  For more details, see the
documentation or "License Notice" file accompanying the IOS-XE software,
or the applicable URL provided on the flyer accompanying the IOS-XE
software.


ROM: IOS-XE ROMMON

pki_a uptime is 6 hours, 53 minutes
```

```
Uptime for this control processor is 6 hours, 54 minutes
System returned to ROM by reload
System restarted at 00:14:18 IST Sun Jun 3 2018
System image file is "cdrom0:packages.conf"
Last reload reason: reload



This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

License Level: ax
License Type: Default. No valid license found.
Next reload license Level: ax

cisco CSR1000V (VXE) processor (revision VXE) with 2372442K/3075K bytes of memory.
Processor board ID 9VJK6T4IQMT
4 Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
8113356K bytes of physical memory.
16162815K bytes of virtual hard disk at bootflash:.
0K bytes of WebUI ODM Files at webui:.

Configuration register is 0x2102


------------------ show running-config ------------------


Building configuration...

Current configuration : 6003 bytes
!
! Last configuration change at 07:07:18 IST Sun Jun 3 2018
!
version 16.10
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
platform qfp utilization monitor load 80
no platform punt-keepalive disable-kernel-core
platform console serial
!
hostname pki_a
!
boot-start-marker
boot-end-marker
!
!
logging buffered 1000000
no logging console
!
no aaa new-model
```

```
clock timezone IST 5 30
clock calendar-valid
!
!
ip admission watch-list expiry-time 0
!
subscriber templating
!
multilink bundle-name authenticated
!
crypto pki server rootca
no database archive
issuer-name CN=RCA1 C=pki
grant auto
hash sha512
lifetime certificate 364
lifetime ca-certificate 364
!
crypto pki trustpoint TP-self-signed-777972883
enrollment selfsigned
subject-name cn=IOS-Self-Signed-Certificate-777972883
revocation-check none
rsakeypair TP-self-signed-777972883
!
crypto pki trustpoint rootca
revocation-check none
rsakeypair rootca 1024
hash sha512
!
crypto pki trustpoint test
enrollment url http://9.45.3.241:80
usage ike
subject-name CN=R1 C=pki
revocation-check crl
rsakeypair test 1024
auto-enroll 3
hash sha512
!
!
crypto pki certificate chain TP-self-signed-777972883
crypto pki certificate chain rootca
certificate ca 02
  30820203 3082016C A0030201 02020102 300D0609 2A864886 F70D0101 0D050030
  15311330 11060355 0403130A 52434131 20433D70 6B69301E 170D3138 30363033
  30313334 35365A17 0D313930 36303230 31333435 365A3015 31133011 06035504
  03130A52 43413120 433D706B 6930819F 300D0609 2A864886 F70D0101 01050003
  818D0030 81890281 8100AD12 BD3E2CA7 3B3F1C19 A18CD53B DF618277 00512357
  A95C141E 4DE7B147 EF4FC9DC C0EB8B7D A81D20E3 25A4B53C 87D19F61 F63AE52A
  82724182 F3DE33AE A59ABB7B 9C6F4D9D F944B0AB 789F635C 740CC101 73CE3043
  7EA692F4 DCFAB15B 99782B0C 0143EFA4 BA4242CD E20F77DD B968C0C8 B5EF2A3F
  D3313C6F 49D93E12 D98D0203 010001A3 63306130 0F060355 1D130101 FF040530
  030101FF 300E0603 551D0F01 01FF0404 03020186 301F0603 551D2304 18301680
  1446E428 7A45971E 1904AB57 D78E8249 54FF9C1F 90301D06 03551D0E 04160414
  46E4287A 45971E19 04AB57D7 8E824954 FF9C1F90 300D0609 2A864886 F70D0101
  0D050003 8181005A CC810010 60BB1DD5 6847F3CE AAE871C9 6E214C60 FD5C56C1
  05A15C67 99CB7464 B518897E 2FE96C87 5FF54631 1224BCE2 AEF599DB 61CB0576
  A70757E6 183A3238 863E54FB 959333C8 562150DE F6FA68D8 DE2526D6 8F41BE72
  26C30292 042D16D3 ADA81A98 CC1D94CD ED06A9EA 6B2BE946 82760C7F A7146306
  D95D07A6 F1ADF6
            quit
crypto pki certificate chain test
certificate 04
  30820203 3082016C A0030201 02020104 300D0609 2A864886 F70D0101 0D050030
  15311330 11060355 0403130A 52434131 20433D70 6B69301E 170D3138 30363033
```

```
  30313336 31395A17 0D313930 36303230 31333435 365A3029 3111300F 06035504
  03130852 3120433D 706B6931 14301206 092A8648 86F70D01 09021605 706B695F
  6130819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281 8100CDB7
  98AF2475 DF4A4DD5 26C602CD C27358F2 D90A4BE7 FA58F5AB 2E5495C7 EEB55513
  A357339C 319392CD FD28F607 BDBDBB77 21261F94 A623B694 A966F9F6 0327582B
  6A6CA0EE C0E8AD8E 7715FFB5 01BCBE7D 2DE0ECD2 D985A524 BFDEAA21 47D7D45A
  19820585 B314EAA7 E939AC85 2A2385AF F9DE5871 3C9A41DF 683BAFD5 D2D30203
  010001A3 4F304D30 0B060355 1D0F0404 030205A0 301F0603 551D2304 18301680
  1446E428 7A45971E 1904AB57 D78E8249 54FF9C1F 90301D06 03551D0E 04160414
  EFBBABD1 EECCC80E 3CAE59B0 C6AC6333 91070AC1 300D0609 2A864886 F70D0101
  0D050003 81810086 59F8185A 5B769128 C37F1C7B 1A32D024 438BC872 1AC6AD50
  F1E9E96F C8DC9413 9ACDFA82 4858F4FA 829F7BAC 09A040AF 5A5A53AB AC6EA5E6
  EADC2BFC BFB33036 C4295B18 C5CC141D A3BCE791 6E25123F 4ABC5746 E569F072
  51AC1E71 0E872A09 8012E547 820E229E F73D8C0E 8818BB5C 8F9E49D6 22EE9BF3
  028A40BB D0EAE0
        quit
certificate ca 02
  30820203 3082016C A0030201 02020102 300D0609 2A864886 F70D0101 0D050030
  15311330 11060355 0403130A 52434131 20433D70 6B69301E 170D3138 30363033
  30313334 35365A17 0D313930 36303230 31333435 365A3015 31133011 06035504
  03130A52 43413120 433D706B 6930819F 300D0609 2A864886 F70D0101 01050003
  818D0030 81890281 8100AD12 BD3E2CA7 3B3F1C19 A18CD53B DF618277 00512357
  A95C141E 4DE7B147 EF4FC9DC C0EB8B7D A81D20E3 25A4B53C 87D19F61 F63AE52A
  82724182 F3DE33AE A59ABB7B 9C6F4D9D F944B0AB 789F635C 740CC101 73CE3043
  7EA692F4 DCFAB15B 99782B0C 0143EFA4 BA4242CD E20F77DD B968C0C8 B5EF2A3F
  D3313C6F 49D93E12 D98D0203 010001A3 63306130 0F060355 1D130101 FF040530
  030101FF 300E0603 551D0F01 01FF0404 03020186 301F0603 551D2304 18301680
  1446E428 7A45971E 1904AB57 D78E8249 54FF9C1F 90301D06 03551D0E 04160414
  46E4287A 45971E19 04AB57D7 8E824954 FF9C1F90 300D0609 2A864886 F70D0101
  0D050003 8181005A CC810010 60BB1DD5 6847F3CE AAE871C9 6E214C60 FD5C56C1
  05A15C67 99CB7464 B518897E 2FE96C87 5FF54631 1224BCE2 AEF599DB 61CB0576
  A70757E6 183A3238 863E54FB 959333C8 562150DE F6FA68D8 DE2526D6 8F41BE72
  26C30292 042D16D3 ADA81A98 CC1D94CD ED06A9EA 6B2BE946 82760C7F A7146306
  D95D07A6 F1ADF6
        quit
!
license udi pid CSR1000V sn 9VJK6T4IQMT
no license smart enable
diagnostic bootup level minimal
!
spanning-tree extend system-id
!
redundancy
!
interface GigabitEthernet1
no ip address
shutdown
negotiation auto
no mop enabled
no mop sysid
!
interface GigabitEthernet2
ip address 9.45.3.241 255.255.0.0
negotiation auto
no mop enabled
no mop sysid
!
interface GigabitEthernet3
no ip address
shutdown
negotiation auto
no mop enabled
no mop sysid
!
```

```
interface GigabitEthernet4
ip address 33.33.33.1 255.255.0.0
negotiation auto
no mop enabled
no mop sysid
!
ip forward-protocol nd
ip http server
ip http secure-server
ip tftp source-interface GigabitEthernet2
ip route 202.153.0.0 255.255.0.0 9.45.0.1
!
control-plane
!
line con 0
exec-timeout 0 0
stopbits 1
line vty 0 4
login
!
end


------------------ show crypto pki certificate verbose ------------------

Certificate
  Status: Available
  Version: 3
  Certificate Serial Number (hex): 04
  Certificate Usage: General Purpose
  Issuer:
    cn=RCA1 C=pki
  Subject:
    Name: pki_a
    hostname=pki_a
    cn=R1 C=pki
  Validity Date:
    start date: 07:06:19 IST Jun 3 2018
    end   date: 07:04:56 IST Jun 2 2019
  Subject Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (1024 bit)
  Signature Algorithm: SHA512 with RSA Encryption
  Fingerprint MD5: 11BC5664 377EEEDC 665FD807 FC9FB976
  Fingerprint SHA1: 5DE8E5B9 EDD3F73B 37A0FF8B E4F6397E 19B6B124
  X509v3 extensions:
    X509v3 Key Usage: A0000000
      Digital Signature
      Key Encipherment
    X509v3 Subject Key ID: EFBBABD1 EECCC80E 3CAE59B0 C6AC6333 91070AC1
    X509v3 Authority Key ID: 46E4287A 45971E19 04AB57D7 8E824954 FF9C1F90
    Authority Info Access:
  Associated Trustpoints: test
  Key Label: test

CA Certificate
  Status: Available
  Version: 3
  Certificate Serial Number (hex): 02
  Certificate Usage: Signature
  Issuer:
    cn=RCA1 C=pki
  Subject:
    cn=RCA1 C=pki
```

```
  Validity Date:
    start date: 07:04:56 IST Jun 3 2018
    end   date: 07:04:56 IST Jun 2 2019
  Subject Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (1024 bit)
  Signature Algorithm: SHA512 with RSA Encryption
  Fingerprint MD5: 0C61C633 C72CE9EC 45E86045 03611E16
  Fingerprint SHA1: 3737DC2B 576D41F5 86ABCD44 F8D05B95 FC2661DF
  X509v3 extensions:
    X509v3 Key Usage: 86000000
      Digital Signature
      Key Cert Sign
      CRL Signature
    X509v3 Subject Key ID: 46E4287A 45971E19 04AB57D7 8E824954 FF9C1F90
    X509v3 Basic Constraints:
        CA: TRUE
    X509v3 Authority Key ID: 46E4287A 45971E19 04AB57D7 8E824954 FF9C1F90
    Authority Info Access:
  Associated Trustpoints: test rootca



------------------ show clock detail ------------------


07:07:35.514 IST Sun Jun 3 2018
Time source is user configuration

------------------ show crypto pki timers detail ------------------

PKI Timers
|        1:44.647  (2018-06-03T07:09:19Z)
  |        1:44.647  (2018-06-03T07:09:19Z) SHADOW test
  |       11:11.420  (2018-06-03T07:18:46Z) SESSION CLEANUP
Expiry Alert Timers
|303d23:57:20.646  (2019-04-03T07:04:55Z)
  |303d23:57:20.646  (2019-04-03T07:04:55Z) ID(test)
  |303d23:57:21.325  (2019-04-03T07:04:56Z) CS(test)
Trustpool Timers
|3693d22:22:24.339  (2028-07-14T05:29:59Z)
  |3693d22:22:24.339  (2028-07-14T05:29:59Z) TRUSTPOOL
CS Timers
|     5:57:21.277  (2018-06-03T13:04:56Z)
  |     5:57:21.277  (2018-06-03T13:04:56Z) CS CRL UPDATE
  |363d23:57:20.995  (2019-06-02T07:04:55Z) CS CERT EXPIRE

------------------ show crypto pki trustpoint ------------------


Trustpoint TP-self-signed-777972883:
    Subject Name:
    cn=IOS-Self-Signed-Certificate-777972883
          Serial Number (hex): 01
    Persistent self-signed certificate trust point
    Using key label TP-self-signed-777972883


Trustpoint rootca:
    Subject Name:
    cn=RCA1 C=pki
          Serial Number (hex): 02
    Certificate configured.
```

```
Trustpoint test:
    Subject Name:
    cn=RCA1 C=pki
          Serial Number (hex): 02
    Certificate configured.
    SCEP URL: http://9.45.3.241:80/cgi-bin


------------------ show crypto pki counters ------------------


PKI Sessions Started: 9
PKI Sessions Ended: 9
PKI Sessions Active: 0
Successful Validations: 1
Failed Validations: 0
Bypassed Validations: 0
Pending Validations: 0
CRLs checked: 0
CRL - fetch attempts: 0
CRL - failed attempts: 0
CRL - rejected busy fetching: 0
AAA authorizations: 0

------------------ show crypto pki crls ------------------


------------------ show crypto pki sessions ------------------


------------------ show crypto key mypubkey all ------------------


% Key pair was generated at: 03:41:10 IST Jun 3 2018
Key name: rootca#
Key type: RSA KEYS
Storage Device: not specified
Usage: General Purpose Key
Key is not exportable.
Key Data:
  30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00B2A2CB
  981220AC 5148C520 B3758EF2 FD00534D E8ECFAA1 C22F9680 C184C785 7FAB0DA1
  505FFB68 E66BD1B6 2560849E 071A3AA8 77B2CA36 00DB9F0A 6DEF0067 C7F95031
  41825E0F C0000417 28A31029 0E0AEF25 BF3C3425 DB03E4D0 7C338411 41873EC7
  044A9EF0 FEB11A07 484F0B26 6BF83C80 21D89FB2 85B2CFD4 3C571D2C D7020301
  0001
% Key pair was generated at: 07:04:56 IST Jun 3 2018
Key name: rootca
Key type: RSA KEYS
Storage Device: not specified
Usage: General Purpose Key
Key is not exportable. Redundancy enabled.
Key Data:
  30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00AD12BD
  3E2CA73B 3F1C19A1 8CD53BDF 61827700 512357A9 5C141E4D E7B147EF 4FC9DCC0
  EB8B7DA8 1D20E325 A4B53C87 D19F61F6 3AE52A82 724182F3 DE33AEA5 9ABB7B9C
  6F4D9DF9 44B0AB78 9F635C74 0CC10173 CE30437E A692F4DC FAB15B99 782B0C01
  43EFA4BA 4242CDE2 0F77DDB9 68C0C8B5 EF2A3FD3 313C6F49 D93E12D9 8D020301
  0001
% Key pair was generated at: 07:04:56 IST Jun 3 2018
```

```
Key name: rootca.server
Key type: RSA KEYS
Temporary key
Usage: Encryption Key
Key is not exportable.
Key Data:
  307C300D 06092A86 4886F70D 01010105 00036B00 30680261 00DB008C C1220131
  2ABB976F 1210B31D 0F84E5AE 24840A01 7A459228 7BB785C4 98DABB13 A8FCE70D
  13A38E40 0FFAC835 A294348C FAC36445 5D128775 8526BE2F D68539C6 91584899
  915BDB10 E963CB56 2FBCFAF1 76CA6C42 C004D778 81A5C614 AD020301 0001
% Key pair was generated at: 07:06:03 IST Jun 3 2018
Key name: client
Key type: RSA KEYS
Storage Device: not specified
Usage: General Purpose Key
Key is not exportable. Redundancy enabled.
Key Data:
  30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 009E6F1C
  B3748AFA 5679B076 A7D3F692 C9F560BB BD61BE66 4DD01B53 9EB5B633 96BC6E63
  A5485193 B9651CA6 09CF2E07 F4841313 E5191B54 011C10DC A639093E 55A015CA
  15B73B31 829D6E55 A69A93E6 9BF321AB 06A2A3C8 547A7F25 DFDF0421 0F9F53B5
  7AFB72BB D65CB226 50515468 23E0D057 7F9675EA 30845D72 F1BB2BB0 85020301
  0001
% Key pair was generated at: 07:06:19 IST Jun 3 2018
Key name: test
Key type: RSA KEYS
Storage Device: not specified
Usage: General Purpose Key
Key is not exportable. Redundancy enabled.
Key Data:
  30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00CDB798
  AF2475DF 4A4DD526 C602CDC2 7358F2D9 0A4BE7FA 58F5AB2E 5495C7EE B55513A3
  57339C31 9392CDFD 28F607BD BDBB7721 261F94A6 23B694A9 66F9F603 27582B6A
  6CA0EEC0 E8AD8E77 15FFB501 BCBE7D2D E0ECD2D9 85A524BF DEAA2147 D7D45A19
  820585B3 14EAA7E9 39AC852A 2385AFF9 DE58713C 9A41DF68 3BAFD5D2 D3020301
  0001

------------------ show crypto pki certificate storage ------------------

Trustpool - certificates will be stored in nvram:
TP-self-signed-777972883 - certificates will be stored in nvram:
rootca - certificates will be stored in nvram:
test - certificates will be stored in nvram:


------------------ show crypto pki certificate pem ------------------


------Trustpoint: TP-self-signed-777972883------
% The specified trustpoint is not enrolled (TP-self-signed-777972883).
% Only export the CA certificate in PEM format.
% Error: failed to get CA cert.
------Trustpoint: rootca------
% The specified trustpoint is not enrolled (rootca).
% Only export the CA certificate in PEM format.
% CA certificate:
-----BEGIN CERTIFICATE-----
MIICAzCCAWygAwIBAgIBAjANBgkqhkiG9w0BAQ0FADAVMRMwEQYDVQQDEwpSQ0Ex
IEM9cGtpMB4XDTE4MDYwMzAxMzQ1NloXDTE5MDYwMjAxMzQ1NlowFTETMBEGA1UE
AxMKUkNBMSBDPXBraTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEArRK9Piyn
Oz8cGaGM1TvfYYJ3AFEjV6lcFB5N57FH70/J3MDri32oHSDjJaS1PIfRn2H2OuUq
gnJBgvPeM66lmrt7nG9NnflEsKt4n2NcdAzBAXPOMEN+ppL03PqxW5l4KwwBQ++k
ukJCzeIPd925aMDIte8qP9MxPG9J2T4S2Y0CAwEAAaNjMGEwDwYDVR0TAQH/BAUw
AwEB/zAOBgNVHQ8BAf8EBAMCAYYwHwYDVR0jBBgwFoAURuQoekWXHhkEq1fXjoJJ
```

```
VP+cH5AwHQYDVR0OBBYEFEbkKHpFlx4ZBKtX146CSVT/nB+QMA0GCSqGSIb3DQEB
DQUAA4GBAFrMgQAQYLsd1WhH886q6HHJbiFMYP1cVsEFoVxnmct0ZLUYiX4v6WyH
X/VGMRIkvOKu9ZnbYcsFdqcHV+YYOjI4hj5U+5WTM8hWIVDe9vpo2N4lJtaPQb5y
JsMCkgQtFtOtqBqYzB2Uze0GqeprK+lGgnYMf6cUYwbZXQem8a32
-----END CERTIFICATE-----

------Trustpoint: test------
% CA certificate:
-----BEGIN CERTIFICATE-----
MIICAzCCAWygAwIBAgIBAjANBgkqhkiG9w0BAQ0FADAVMRMwEQYDVQQDEwpSQ0Ex
IEM9cGtpMB4XDTE4MDYwMzAxMzQ1NloXDTE5MDYwMjAxMzQ1NlowFTETMBEGA1UE
AxMKUkNBMSBDPXBraTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEArRK9Piyn
Oz8cGaGM1TvfYYJ3AFEjV6lcFB5N57FH70/J3MDri32oHSDjJaS1PIfRn2H2OuUq
gnJBgvPeM66lmrt7nG9NnflEsKt4n2NcdAzBAXPOMEN+ppL03PqxW5l4KwwBQ++k
ukJCzeIPd925aMDIte8qP9MxPG9J2T4S2Y0CAwEAAaNjMGEwDwYDVR0TAQH/BAUw
AwEB/zAOBgNVHQ8BAf8EBAMCAYYwHwYDVR0jBBgwFoAURuQoekWXHhkEq1fXjoJJ
VP+cH5AwHQYDVR0OBBYEFEbkKHpFlx4ZBKtX146CSVT/nB+QMA0GCSqGSIb3DQEB
DQUAA4GBAFrMgQAQYLsd1WhH886q6HHJbiFMYP1cVsEFoVxnmct0ZLUYiX4v6WyH
X/VGMRIkvOKu9ZnbYcsFdqcHV+YYOjI4hj5U+5WTM8hWIVDe9vpo2N4lJtaPQb5y
JsMCkgQtFtOtqBqYzB2Uze0GqeprK+lGgnYMf6cUYwbZXQem8a32
-----END CERTIFICATE-----

% General Purpose Certificate:
-----BEGIN CERTIFICATE-----
MIICAzCCAWygAwIBAgIBBDANBgkqhkiG9w0BAQ0FADAVMRMwEQYDVQQDEwpSQ0Ex
IEM9cGtpMB4XDTE4MDYwMzAxMzYxOVoXDTE5MDYwMjAxMzQ1NlowKTERMA8GA1UE
AxMIUjEgQz1wa2kxFDASBgkqhkiG9w0BCQIWBXBraV9hMIGfMA0GCSqGSIb3DQEB
AQUAA4GNADCBiQKBgQDNt5ivJHXfSk3VJsYCzcJzWPLZCkvn+lj1qy5UlcfutVUT
o1cznDGTks39KPYHvb27dyEmH5SmI7aUqWb59gMnWCtqbKDuwOitjncV/7UBvL59
LeDs0tmFpSS/3qohR9fUWhmCBYWzFOqn6TmshSojha/53lhxPJpB32g7r9XS0wID
AQABo08wTTALBgNVHQ8EBAMCBaAwHwYDVR0jBBgwFoAURuQoekWXHhkEq1fXjoJJ
VP+cH5AwHQYDVR0OBBYEFO+7q9HuzMgOPK5ZsMasYzORBwrBMA0GCSqGSIb3DQEB
DQUAA4GBAIZZ+BhaW3aRKMN/HHsaMtAkQ4vIchrGrVDx6elvyNyUE5rN+oJIWPT6
gp97rAmgQK9aWlOrrG6l5urcK/y/szA2xClbGMXMFB2jvOeRbiUSP0q8V0blafBy
UawecQ6HKgmAEuVHgg4invc9jA6IGLtcj55J1iLum/MCikC70Org
-----END CERTIFICATE-----


------------------ show crypto pki server ------------------


Certificate Server rootca:
    Status: enabled
    State: enabled
    Server's configuration is locked  (enter "shut" to unlock it)
    Issuer name: CN=RCA1 C=pki
    CA cert fingerprint: 0C61C633 C72CE9EC 45E86045 03611E16
    Granting mode is: auto
    Last certificate issued serial number (hex): 4
    CA certificate expiration timer: 07:04:56 IST Jun 2 2019
    CRL NextUpdate timer: 13:04:56 IST Jun 3 2018
    Current primary storage dir: nvram:
    Database Level: Minimum - no cert data written to storage

------------------ show crypto pki server rootca certificates ------------------

Serial Issued date              Expire date               Subject Name
1       <cert file not accessible>
2       <cert file not accessible>
3       <cert file not accessible>
4       <cert file not accessible>


------------------ show crypto pki server rootca crl ------------------
```

```
Certificate Revocation List:
    Issuer: cn=RCA1 C=pki
    This Update: 07:04:56 IST Jun 3 2018
    Next Update: 13:04:56 IST Jun 3 2018
    Number of CRL entries: 0
    CRL size: 220 bytes


------------------ show crypto pki server rootca requests ------------------

The Enrollment Request Database is empty.
```

Related Commands

Command	Description
show tech-support	Displays information about the device when the device reports a problem.

show tunnel endpoints

To display the contents of the tunnel endpoint database that is used for tunnel endpoint address resolution, when running a tunnel in multipoint generic routing encapsulation (mGRE) mode, use the **show tunnel endpoints**command in privileged EXEC mode.

show tunnel endpoints [**tunnel** *tunnel-number*]

Syntax Description

tunnel	(Optional) Specifies the tunnel interface. If a tunnel is specified, only the endpoint database for that tunnel is displayed. If a tunnel is not specified, endpoint databases for all tunnels are displayed.
tunnel-number	(Optional) Tunnel interface number. The range is from 0 to 2147483647.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(27)S	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.(33)SRA.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
Cisco IOS XE Release 2.1	This command was implemented on the Cisco ASR 1000 series routers.

Usage Guidelines

The output of **show tunnel endpoints** command displays the tunnel destination and transport address together with any overlay or virtual private network (VPN) address that resolves to it.

Examples

The following example shows that there are two tunnel endpoints in the database that are associated with tunnel 1 (192.0.2.0 and 192.0.2.1). Through these endpoints, VPN destination 192.0.2.3 is reachable by tunneling to endpoint 192.0.2.0 and VPN destination 192.0.2.2 is reachable by tunneling to endpoint 192.0.2.1.

```
Router# show tunnel endpoints
Tunnel0 running in multi-GRE/IP mode

 Endpoint transport 20.20.20.20 Refcount 4 Base 0x55BCC5E8 Create Time 00:01:08
   overlay ::FFFF:20.20.20.20 Refcount 2 Parent 0x55BCC5E8 Create Time 00:01:08
   overlay 20.20.20.20 Refcount 2 Parent 0x55BCC5E8 Create Time 00:01:08
```

The table below describes the significant fields shown in the display..

Table 192: show tunnel endpoints Field Descriptions

Field	Description
Transport	Displays the transport address.
Refcount	Number of overlay addresses that are resolving through the destination address.
Base	Displays the base address.
Overlay	Displays the overlay address.
Parent	Reference to the tunnel endpoint.

Related Commands

Command	Description
tunnel mode	Sets the encapsulation mode for the tunnel interface.
tunnel protection	Associates a tunnel interface with an IPSec profile.

show usb controllers

To display USB host controller information, use the **show usb controllers**command in privileged EXEC mode.

show usb controllers [*controller-number*]

Syntax Description

controller-number	(Optional) Displays information only for the specified controller.

Command Default

Information about all controllers on the system are displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(11)T	This command was integrated into the Cisco 7200VXR NPE-G2 platform.

Usage Guidelines

Use the **show usb controllers**command to display content such as controller register specific information, current asynchronous buffer addresses, and period scheduling information. You can also use this command to verify that copy operations are occurring successfully onto a USB flash module.

Examples

The following example is sample output from the **show usb controllers** command:

```
Router# show usb controllers
Name:1362HCD
Controller ID:1
Controller Specific Information:
    Revision:0x11
    Control:0x80
    Command Status:0x0
    Hardware Interrupt Status:0x24
    Hardware Interrupt Enable:0x80000040
    Hardware Interrupt Disable:0x80000040
    Frame Interval:0x27782EDF
    Frame Remaining:0x13C1
    Frame Number:0xDA4C
    LSThreshold:0x628
    RhDescriptorA:0x19000202
    RhDescriptorB:0x0
    RhStatus:0x0
    RhPort1Status:0x100103
    RhPort2Status:0x100303
    Hardware Configuration:0x3029
    DMA Configuration:0x0
    Transfer Counter:0x1
    Interrupt:0x9
    Interrupt Enable:0x196
    Chip ID:0x3630
    Buffer Status:0x0
    Direct Address Length:0x80A00
    ATL Buffer Size:0x600
```

```
    ATL Buffer Port:0x0
    ATL Block Size:0x100
    ATL PTD Skip Map:0xFFFFFFFF
    ATL PTD Last:0x20
    ATL Current Active PTD:0x0
    ATL Threshold Count:0x1
    ATL Threshold Timeout:0xFF
Int Level:1
Transfer Completion Codes:
         Success              :920             CRC              :0
         Bit Stuff            :0               Stall            :0
         No Response          :0               Overrun          :0
         Underrun             :0               Other            :0
         Buffer Overrun       :0               Buffer Underrun :0
Transfer Errors:
         Canceled Transfers   :2               Control Timeout :0
Transfer Failures:
         Interrupt Transfer   :0               Bulk Transfer   :0
         Isochronous Transfer :0               Control Transfer:0
Transfer Successes:
         Interrupt Transfer   :0               Bulk Transfer   :26
         Isochronous Transfer :0               Control Transfer:894
USBD Failures:
         Enumeration Failures :0               No Class Driver Found:0
         Power Budget Exceeded:0
USB MSCD SCSI Class Driver Counters:
         Good Status Failures :3               Command Fail    :0
         Good Status Timed out:0               Device not Found:0
         Device Never Opened  :0               Drive Init Fail :0
         Illegal App Handle   :0               Bad API Command :0
         Invalid Unit Number  :0               Invalid Argument:0
         Application Overflow :0               Device in use   :0
         Control Pipe Stall   :0               Malloc Error    :0
         Device Stalled       :0               Bad Command Code:0
         Device Detached      :0               Unknown Error   :0
         Invalid Logic Unit Num:0
USB Aladdin Token Driver Counters:
         Token Inserted       :1               Token Removed   :0
         Send Insert Msg Fail :0               Response Txns   :434
         Dev Entry Add Fail   :0               Request Txns    :434
         Dev Entry Remove Fail:0               Request Txn Fail:0
         Response Txn Fail    :0               Command Txn Fail:0
         Txn Invalid Dev Handle:0
USB Flash File System Counters:
         Flash Disconnected   :0               Flash Connected :1
         Flash Device Fail    :0               Flash Ok        :1
         Flash startstop Fail :0               Flash FS Fail   :0
USB Secure Token File System Counters:
         Token Inserted       :1               Token Detached  :0
         Token FS success     :1               Token FS Fail   :0
         Token Max Inserted   :0               Create Talker Failures:0
         Token Event          :0               Destroy Talker Failures:0
         Watched Boolean Create Failures:0
```

show usb device

To display USB device information, use the **show usb device**command in privileged EXEC mode.

show usb device [*controller-ID* [*device-address*]]

Syntax Description

controller-ID	(Optional) Displays information only for the devices under the specified controller.
device-address	(Optional) Displays information only for the device with the specified address.

Command Default

Information for all devices attached to the system are displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(11)T	This command was integrated into the Cisco 7200VXR NPE-G2 platform.

Usage Guidelines

Use the **show usb device** command to display information for either a USB flash drive or a USB eToken, as appropriate.

Examples

The following example is sample output from the **show usb device** command:

```
Router# show usb device

Host Controller:1
Address:0x1
Device Configured:YES
Device Supported:YES
Description:DiskOnKey
Manufacturer:M-Sys
Version:2.0
Serial Number:0750D84030316868
Device Handle:0x1000000
USB Version Compliance:2.0
Class Code:0x0
Subclass Code:0x0
Protocol:0x0
Vendor ID:0x8EC
Product ID:0x15
Max. Packet Size of Endpoint Zero:64
Number of Configurations:1
Speed:Full
Selected Configuration:1
Selected Interface:0
Configuration:
    Number:1
    Number of Interfaces:1
    Description:
    Attributes:None
    Max Power:140 mA
    Interface:
```

```
        Number:0
        Description:
        Class Code:8
        Subclass:6
        Protocol:80
        Number of Endpoints:2
        Endpoint:
            Number:1
            Transfer Type:BULK
            Transfer Direction:Device to Host
            Max Packet:64
            Interval:0
        Endpoint:
            Number:2
            Transfer Type:BULK
            Transfer Direction:Host to Device
            Max Packet:64
            Interval:0
Host Controller:1
Address:0x11
Device Configured:YES
Device Supported:YES
Description:eToken Pro 4254
Manufacturer:AKS
Version:1.0
Serial Number:
Device Handle:0x1010000
USB Version Compliance:1.0
Class Code:0xFF
Subclass Code:0x0
Protocol:0x0
Vendor ID:0x529
Product ID:0x514
Max. Packet Size of Endpoint Zero:8
Number of Configurations:1
Speed:Low
Selected Configuration:1
Selected Interface:0
Configuration:
    Number:1
    Number of Interfaces:1
    Description:
    Attributes:None
    Max Power:60 mA
    Interface:
        Number:0
        Description:
        Class Code:255
        Subclass:0
        Protocol:0
        Number of Endpoints:0
```

The following table describes the significant fields shown in the display.

Table 193: show usb device Field Descriptions

Field	Description
Device handle	Internal memory handle allocated to the device.

Field	Description
Device Class code	The class code supported by the device. This number is allocated by the USB-IF. If this field is reset to 0, each interface within a configuration specifies its own class information, and the various interfaces operate independently. If this field is set to a value between 1 and FEH, the device supports different class specifications on different interfaces, and the interfaces may not operate independently. This value identifies the class definition used for the aggregate interfaces. If this field is set to FFH, the device class is vendor-specific.
Device Subclass code	The subclass code supported by the device. This number is allocated by the USB-IF.
Device Protocol	The protocol supported by the device. If this field is set to 0, the device does not use class-specific protocols on a device basis. If this field is set to 0xFF, the device uses a vendor-specific protocol on a device basis.
Interface Class code	The class code supported by the interface. If the value is set to 0xFF, the interface class is vendor specific. All other values are allocated by the USB-IF.
Interface Subclass code	The subclass code supported by the interface. All values are allocated by the USB-IF.
Interface Protocol	The protocol code supported by the interface. If this field is set to 0, the device does not use a class-specific protocol on this interface. If this field is set to 0xFF, the device uses a vendor-specific protocol for this interface.
Max Packet	Maximum data packet size, in bytes.

show usb driver

To display information about registered USB class drivers and vendor-specific drivers, use the **show usb driver**command in privileged EXEC mode.

show usb driver [*index*]

Syntax Description

index	(Optional) Displays information only for drivers on the specified index.

Command Default

Information about all drivers is displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(11)T	This command was integrated into the Cisco 7200VXR NPE-G2 platform.
Cisco IOS XE Release 3.6	This command was integrated into Cisco IOS XE Release 3.6.

Examples

The following example is sample output for the **show usb driver** command:

```
Router# show usb driver

Index:0
Owner Mask:0x6
Class Code:0x0
Subclass Code:0x0
Protocol:0x0
Interface Class Code:0x8
Interface Subclass Code:0x6
Interface Protocol Code:0x50
Product ID:0x655BD598
Vendor ID:0x64E90000
Attached Devices:
    Controller ID:1, Device Address:1
Index:1
Owner Mask:0x1
Class Code:0x0
Subclass Code:0x0
Protocol:0x0
Interface Class Code:0x0
Interface Subclass Code:0x0
Interface Protocol Code:0x0
Product ID:0x514
Vendor ID:0x529
Attached Devices:
    Controller ID:1, Device Address:17
Index:2
Owner Mask:0x5
Class Code:0x9
Subclass Code:0x6249BD58
Protocol:0x2
```

```
Interface Class Code:0x5DC0
Interface Subclass Code:0x5
Interface Protocol Code:0xFFFFFFFF
Product ID:0x2
Vendor ID:0x1
Attached Devices:
    None
Index:3
Owner Mask:0x10
Class Code:0x0
Subclass Code:0x0
Protocol:0x0
Interface Class Code:0x0
Interface Subclass Code:0x0
Interface Protocol Code:0x0
Product ID:0x0
Vendor ID:0x0
Attached Devices:
    None
```

The following table describes the significant field shown in the display.

Table 194: show usb driver Field Descriptions

Field	Description
Owner Mask	Indicates the fields that are used in enumeration comparison. The driver can own different devices on the basis of their product or vendor IDs and device or interface class, subclass, and protocol codes.

show usb port

To sisplay USB root hub port information, use the **show usb port**command in privileged EXEC mode.

show usb port [*port-number*]

Syntax Description

port-number	(Optional) Displays information only for a specified. If the *port-number* is not issued, information for all root ports will be displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(14)T	This command was introduced.

Examples

The following sample from the **show usb port** command shows the status of the port 1 on the router:

```
Router# show usb port
Port Number:0
Status:Enabled
Connection State:Connected
Speed:Full
Power State:ON
Port Number:1
Status:Enabled
Connection State:Connected
Speed:Low
Power State:ON
```

show usb-devices summary

To display USB device summary information for all USB devices attached to the router, use the **show usb-devices summary**command in privileged EXEC mode.

show usb-devices summary

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.6	This command was integrated into Cisco IOS XE Release 3.6.

Usage Guidelines

Use the **show usb-devices summary** command to display information for either a USB flash drive or a USB eToken, as appropriate.

Examples

The following example is sample output from the **show usb-devices summary** command, which shows that a USB token device is supported by Cisco (see the text in bold).:

```
Router# show usb-devices summary

USB Device: OHCI Host Controller
Bus: 03 Port: 00 Cnt: 00 Speed: 12
Vendor: 1d6b ProdID: 0001 Rev: 2.06
Serial Number: 0001:01:11.1

USB Device: OHCI Host Controller
Bus: 02 Port: 00 Cnt: 00 Speed: 12
Vendor: 1d6b ProdID: 0001 Rev: 2.06
Serial Number: 0001:01:11.0

USB Device: Token 4.28.1.1 2.7.195
Bus: 02 Port: 00 Cnt: 01 Speed: 12
Vendor: 0529 ProdID: 0600 Rev: 1.00
Serial Number:

USB Device: EHCI Host Controller
Bus: 01 Port: 00 Cnt: 00 Speed: 480
Vendor: 1d6b ProdID: 0002 Rev: 2.06
Serial Number: 0001:01:11.2

USB Device: eUSB
Bus: 01 Port: 03 Cnt: 01 Speed: 480
Vendor: 0e39 ProdID: 2b00 Rev: b9.00
Serial Number: 1E884812183636210510
```

show usb tree

To display information about the port state and all attached devices, use the **show usb tree**command in privileged EXEC mode.

show usb tree

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
12.3(14)T	This command was introduced.

Examples

The following example is sample output from the **show usb tree** command. This output shows that both a USB flash module and a USB eToken are currently enabled.

```
Router# show usb tree

[Host Id:1, Host Type:1362HCD, Number of RH-Port:2]
<Root Port0:Power=ON      Current State=Enabled>
  Port0:(DiskOnKey) Addr:0x1 VID:0x08EC PID:0x0015 Configured (0x1000000)
<Root Port1:Power=ON      Current State=Enabled>
  Port1:(eToken Pro 4254) Addr:0x11 VID:0x0529 PID:0x0514 Configured (0x1010000)
```

show usbtoken

To display information about the USB eToken (such as the eToken ID), use the **show usbtoken**command in privileged EXEC mode.

show usbtoken [**0-9**]**:**{**all***filesystem*}

Syntax Description

0-9	(Optional) One of the ten available flash drives you can choose from; valid values: 0-9. If you do not specify a number, 0 is used by default
all	(Optional) All configuration files stored on the eToken.
filesystem	(Optional) Name of a configuration file.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(11)T	This command was integrated into the Cisco 7200VXR NPE-G2 platform.
Cisco IOS XE Release 3.6	This command was integrated into Cisco IOS XE Release 3.6.

Usage Guidelines

Use the **show usbtoken** command to verify whether a USB eToken is inserted in the router.

Examples

The following example is sample output from the **show usbtoken** command:

```
Router# show usbtoken0
Token ID           :43353334
Token device name  : token0
Vendor name        : Vendor34
Product Name       :Etoken Pro
Serial number      : 22273a334353
Firmware version   :   4.1.3.2
Total memory size  : 32 KB
Free memory size   : 16 KB
FIPS version       :  Yes/No
Token state        :  "Active" | "User locked" | "Admin locked" | "System Error" | "Uknown"
ATR (Answer To Reset) :"3B F2 98 0  FF C1 10 31 FE 55 C8 3"
```

The following table describes the significant fields shown in the display.

Table 195: show usbtoken Field Descriptions

Field	Description
Token ID	Token identifier.
Token device name	A unique name derived by the token driver.
ATR (Answer to Reset)	Information replied by Smart cards when a reset command is issued.

show user-group

To display information about user groups, use the **show user-group**command in privileged EXEC mode.

show user-group [{*group-name* | **count**}]

Syntax Description

group-name	(Optional) Name of the user-group.
count	(Optional) Displays the total number of user groups, the names of the user groups, and the number of members in each.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Examples

The following is sample output from the show user-group command when the auth_proxy_ug user group is specified.

```
Router# show user-group auth_proxy_ug
!
Usergroup: auth_proxy_ug
------------------------------------------------------------
User Name     Type  Interface   Learn   Age (min)
------------------------------------------------------------
192.168.101.131     IPv4  Vlan333   Dynamic   0
```

!

The following is sample output from the show user-group command when the **count** keyword is used.

```
Router# show user-group count
!
Total Usergroup: 2
--------------------------
User Group    Members
--------------------------
auth_proxy_ug    1
eng_group_ug    1
!
```

The table below describes the significant fields shown in the displays.

Table 196: show user-group Field Descriptions

Field	Description
User Name	IP address of the user-group.
Learn	Describes how the mapping of source IP addresses to user groups is learned.

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
user-group	Defines the user-group associated with the identity policy.

show users

To displa y information about the active lines on the router, use the **show users**command in user EXEC or privileged EXEC mode.

show users [{[**all**] [**wide**] | **slot** {*slot-number* | **all**} | **summary**}] [**lawful-intercept**]

Syntax Description

all	(Optional) Specifies that all lines be displayed, regardless of whether anyone is using them.
wide	(Optional) Specifies that the wide format be used.
slot	(Optional) Displays information about remote logins to other processes in the chassis.
slot-number	(Optional) The slot number.
summary	(Optional) Displays a summary of user sessions.
lawful-intercept	(Optional) Displays lawful-intercept users.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
10.0	This command was introduced.
12.3(2)T	The **summary** keyword was introduced.
12.3(7)T	The **lawful-intercept** keyword was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXI	This command was modified in a release earlier than Cisco IOS Release 12.2(33)SXI. The **slot** keyword and *slot-number* argument were added.
Cisco IOS XE Release 2.1	This command was implemented on the Cisco ASR 1000 Series Aggregation Sevices Routers.

Usage Guidelines

This command displays the line number, connection name, idle time, hosts (including virtual access interfaces), and terminal location. An asterisk (*) indicates the current terminal session.

If the **lawful-intercept** keyword is issued, the names of all users who have access to a configured lawful intercept view will be displayed. To access the **show users lawful-intercept** command, you must be an authorized lawful-intercept-view user.

When an idle timeout is configured on a full virtual access interface and a subvirtual access interface, the **show users** command displays the idle time for both the interfaces. However, if the idle timeout is not configured on both the interfaces, then the **show users** command will display the idle time for the full virtual access interface only.

Examples

The following is sample output from the **show users** command:

```
Router# show users
      Line           User            Host(s)        Idle Location
      0 con 0                        idle
*     2 vty 0        user1           idle            0   SERVICE1.CISCO.COM
```

The following is sample output identifying an active virtual access interface:

```
Router# show users
Line         User      Host(s)                Idle    Location
*  0 con 0             idle                   01:58
  10 vty 0             Virtual-Access2         0      1212321
```

The following is sample output from the **show users all** command:

```
Router# show users all
    Line       User          Host(s)      Idle  Location
*   0 vty 0    user1         idle         0    SERVICE1.CISCO.COM
    1 vty 1
    2 con 0
    3 aux 0
    4 vty 2
```

The table below describes the significant fields shown in the displays.

Table 197: show users Field Descriptions

Field	Description
Line	Contains three subfields: • The first subfield (0 in the sample output) is the absolute line number. • The second subfield (vty in the sample output) indicates the type of line. Possible values follow: aux--auxiliary port con--console tty--asynchronous terminal port vty--virtual terminal • The third subfield (0 in the * sample output) indicates the relative line number within the type.
User	User using the line. If no user is listed in this field, no one is using the line.
Host(s)	Host to which the user is connected (outgoing connection). A value of idle means that there is no outgoing connection to a host.
Idle	Interval (in minutes) since the user has entered something.
Location	Either the hard-wired location for the line or, if there is an incoming connection, the host from which the incoming connection came.

The following sample output from the **show users lawful intercept**command shows three LI-View users on the system--li_admin, li-user1, and li-user2:

```
Router# show users lawful-intercept

li_admin
li-user1
li-user2
Router#
```

Related Commands

Command	Description
line	Identifies a specific line for configuration and starts the line configuration command collection mode.
li-view	Initializes a lawful intercept view.
show line	Displays the parameters of a terminal line.
username	Establishes a username-based authentication system.

show vlan group through switchport port-security violation

show vasi pair

To display the status of a VRF-Aware Service Infrastructure (VASI) pair, use the **show vasi pair**command in privileged EXEC mode.

show vasi pair status [*number*]

Syntax Description

status	Displays the VASI pair status.
number	(Optional) VASI pair number. The range is from 1 to 256.

Command Default

If no interface is specified, all VASI interfaces are displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 2.6	This command was introduced.

Examples

The following is sample output from the **show vasi pair** command:

```
Router# show vasi pair status 100
Pair name     Left state             Right state            Pair state
------------------------------------------------------------------------------
VASIPair100   down                   not configured         need vasiright100
```

The table below describes the significant fields shown in the display.

Table 198: show vasi pair status Field Descriptions

Field	Description
Pair name	Name of the VASI interface pair.
Left state	State of the vasileft interface. The values are as follows: • admin down--interface is administratively down. • down--interface is down. • not configure--interface is not configured. • up--interface is operational and up.

Field	Description
Right state	State of the vasiright interface. The values are as follows: • admin down--interface is administratively down. • down--interface is down. • not configure--interface is not configured. • up--interface is operational and up.
Pair state	Vasi pair status. Possible values are as follows: • need vasileft--vasileft interface is not configured. • need vasiright--vasiright interface is not configured. • up-- both interfaces are up and operational. • vasileft down--vasileft interface state is down • vasiright down--vasiright interface state is down

Related Commands

debug adjacency (vasi)	Displays debugging information for VASI adjacency.
debug interface (vasi)	Displays debugging information for VASI interface descriptor block.
debug vasi	Displays VASI debugging information.
interface (vasi)	Configures a VASI virtual interface.

show vlan group

To display the VLANs mapped to VLAN groups, use the **show vlan group** command in privileged EXEC mode.

show vlan group [**group-name** *group-name*]

Syntax Description

group-name *group-name*	(Optional) Displays the VLANs mapped to the specified VLAN group.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SXI1	This command was introduced.

Usage Guidelines

The **show vlan group** command displays the existing VLAN groups and lists the VLANs and VLAN ranges that are members of each VLAN group. If the **group-name**keyword is entered, only the members of the VLAN group specified by the *group-name* argument are displayed.

Examples

This example shows how to display the members of a specified VLAN group:

```
Router# show vlan group group-name ganymede
Group Name Vlans Mapped
---------------- -------------------
ganymede         7-9
```

Related Commands

Command	Description
vlan group	Creates or modifies a VLAN group.

show vtemplate

To display information about all configured virtual templates, use the **show vtemplate**command in privileged EXEC mode.

show vtemplate

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(7)DC	This command was introduced on the Cisco 6400 NRP.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3(14)T	The show display was modified to display the interface type of the virtual template and to provide counters on a per-interface-type basis for IPsec virtual tunnel interfaces.
12.2(33)SRA	This comand was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This comand was integrated into Cisco IOS Release 12.2(33)SXH.

Examples

The following is sample output from the **show vtemplate** command:

```
Router# show vtemplate
Virtual access subinterface creation is globally enabled
         Active     Active    Subint  Pre-clone Pre-clone Interface
       Interface Subinterface Capable Available   Limit     Type
       --------- ------------ ------- --------- --------- ---------
Vt1            0            0   Yes          --        --   Serial
Vt2            0            0   Yes          --        --   Serial
Vt4            0            0   Yes          --        --   Serial
Vt21           0            0    No          --        --   Tunnel
Vt22           0            0   Yes          --        --   Ether
Vt23           0            0   Yes          --        --   Serial
Vt24           0            0   Yes          --        --   Serial
Usage Summary
                              Interface   Subinterface
                              ---------   ------------
Current Serial  in use                1              0
Current Serial  free                  0              3
Current Ether   in use                0              0
Current Ether   free                  0              0
Current Tunnel  in use                0              0
Current Tunnel  free                  0              0
Total                                 1              3
Cumulative created                    8              4
Cumulative freed                      0              4
Base virtual access interfaces: 1
Total create or clone requests: 0
Current request queue size: 0
Current free pending: 0
```

```
Maximum request duration: 0 msec
Average request duration: 0 msec
Last request duration: 0 msec
Maximum processing duration: 0 msec
Average processing duration: 0 msec
Last processing duration: 0 msec
Last processing duration:0 msec
```

The table below describes the significant fields shown in the example.

Table 199: show vtemplate Field Descriptions

Field	Description
Virtual access subinterface creation is globally...	The configured setting of the **virtual-template**command. Virtual access subinterface creation may be enabled or disabled.
Active Interface	The number of virtual access interfaces that are cloned from the specified virtual template.
Active Subinterface	The number of virtual access subinterfaces that are cloned from the specified virtual template.
Subint Capable	Specifies if the configuration of the virtual template is supported on the virtual access subinterface.
Pre-clone Available	The number of precloned virtual access interfaces currently available for use for the particular virtual template.
Pre-clone Limit	The number of precloned virtual access interfaces available for that particular virtual template.
Current in use	The number of virtual access interfaces and subinterfaces that are currently in use.
Current free	The number of virtual access interfaces and subinterfaces that are no longer in use.
Total	The total number of virtual access interfaces and subinterfaces that exist.
Cumulative created	The number of requests for a virtual access interface or subinterface that have been satisfied.
Cumulative freed	The number of times that the application using the virtual access interface or subinterface has been freed.
Base virtual-access interfaces	This field specifies the number of base virtual access interfaces. The base virtual access interface is used to create virtual access subinterfaces. There is one base virtual access interface per application that supports subinterfaces. A base virtual access interface can be identified from the output of the **show interfaces virtual-access** command.
Total create or clone requests	The number of requests that have been made through the asynchronous request API of the virtual template manager.
Current request queue size	The number of items in the virtual template manager work queue.

Field	Description
Current free pending	The number of virtual access interfaces whose final freeing is pending. These virtual access interfaces cannot currently be freed because they are still in use.
Maximum request duration	The maximum time that it took from the time that the asynchronous request was made until the application was notified that the request was done.
Average request duration	The average time that it took from the time that the asynchronous request was made until the application was notified that the request was done.
Last request duration	The time that it took from the time that the asynchronous request was made until the application was notified that the request was done for the most recent request.
Maximum processing duration	The maximum time that the virtual template manager spent satisfying the request.
Average processing duration	The average time that the virtual template manager spent satisfying the request.
Last processing duration	The time that the virtual template manager spent satisfying the request for the most recent request.

Related Commands

Command	Description
clear counters	Clears interface counters.
show interfaces virtual-access	Displays status, traffic data, and configuration information about a specified virtual access interface.
virtual-template	Specifies which virtual template will be used to clone virtual access interfaces.

show webvpn context

To display the operational status and configuration parameters for Secure Socket Layer (SSL) virtual private network (VPN) context configurations, use the **show webvpn context** command in privileged EXEC mode.

show webvpn context [{*name* | **brief**}]

Syntax Description

name	(Optional) Name of the context for which output will be filtered to display detailed information.
brief	(Optional) Filters the output to display a summary of SSL VPN context configuration.

Command Default

If no arguments or keywords are specified, the output displays general information about the operational status of all SSL VPN contexts.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(6)T	This command was introduced.
15.0(1)M	This command was modified. The **brief**keyword was added.

Usage Guidelines

Entering a context name displays more detailed information, such as the operational status and specific configuration information for the named context.

Examples

The following output is an example of brief information that can be displayed for system security officer (SSO) servers configured for the SSL VPN context:

```
Router# show webvpn context brief
Codes: AS - Admin Status, OS - Operation Status
       VHost - Virtual Host
Context Name        Gateway  Domain/VHost      VRF      AS    OS
------------        -------  ------------      -------  ----  --------
Default_context     n/a      n/a               n/a      down  down
con-1               gw-1     one               -        up    up
con-2               -        -                 -        down  down
```

The table below describes the significant fields shown in the display.

Table 200: show webvpn context brief Field Descriptions

Field	Description
Context Name	Displays the name of the context.
Gateway	Displays the name of the associated gateway. n/a is displayed if no gateway is associated.
Domain/VHost	Displays the SSL VPN domain or virtual hostname.

Field	Description
VRF	Displays the VPN routing and forwarding (VRF) instance, if configured, that is associated with the context configuration.
AS	Displays the administrative status of the SSL VPN context. The status is displayed as "up" or "down."
OS	Displays the operational status of the SSL VPN context. The status is displayed as "up" or "down."

The following is sample output from the **show webvpn context** command entered with the name of a specific SSL VPN context:

```
Router# show webvpn context 1234567891234567891second
Admin Status: down
Operation Status: down
Error and Event Logging: Disabled
CSD Status: Disabled
Certificate authentication type: All attributes (like CRL) are verified
AAA Authentication List not configured
AAA Authorization List not configured
AAA Accounting List not configured
AAA Authentication Domain not configured
Authentication mode: AAA authentication
Default Group Policy not configured
Not associated with any WebVPN Gateway
Domain Name and Virtual Host not configured
Maximum Users Allowed: 1000 (default)
NAT Address not configured
VRF Name not configured
Virtual Template not configured
```

The table below describes the significant fields shown in the display.

Table 201: show webvpn context (Specific WebVPN Context) Field Descriptions

Field	Description
Admin Status	Administrative status of the context. The status is displayed as "up" or "down." The **inservice** command is used to configure this configuration parameter.
Operation Status	Displays the operational status of the SSL VPN. The status is displayed as "up" or "down." The context and the associated gateway must both be in an enabled state for the operational status to be "up."
CSD Status	Displays the status of Cisco Secure Desktop (CSD). The status is displayed as "Enabled" or "Disabled."
Certificate authentication type	Displays the certification authority (CA) type.
AAA Authentication List...	Displays the authentication list if configured.
AAA Authentication Domain...	Displays the authentication, authorization, and accounting (AAA) domain if configured.

Field	Description
Default Group Policy	Name of the group policy configured under the named context.
Domain Name	Domain name or virtual hostname configured under the named context.
Maximum Users Allowed	Displays the maximum number of user sessions that can be configured.
NAT Address...	Displays the Network Address Translation (NAT) address if configured.
VRF	Displays the VRF, if configured, that is associated with the context configuration.

Related Commands

Command	Description
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

show webvpn gateway

To display the status of a SSL VPN gateway, use the **show webvpn gateway** command in privileged EXEC mode.

show webvpn gateway [{*name*}]

Syntax Description

name	(Optional) Filters the output to display more detailed information about the named gateway.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

Entering this command without specifying a gateway name, displays general the operational status of all SSL VPN gateways. Entering a gateway name displays the IP address and CA trustpoint.

Examples

The following is sample output from the **show webvpn gateway** command:

```
Device# show webvpn gateway

Gateway Name                        Admin  Operation
------------                        -----  ---------
GW_1                                up     up
GW_2                                down   down
```

The table below describes the significant fields shown in the display.

Table 202: show webvpn gateway Field Descriptions

Field	Description
Gateway Name	Name of the gateway.
Admin	The administrative status of the gateway, displayed as “up” or “down.” Administrative status is configured with the **inservice** command.
Operation	The operational status of the gateway, displayed as “up” or “down.” The gateway must be “inservice” and configured with a valid IP address to be in an “up” state.

The following is sample output from the **show webvpn gateway**command, entered with a specific SSL VPN gateway name:

```
Device# show webvpn gateway

 GW_1
 Admin Status: up
 Operation Status: up
 IP: 10.1.1.1, port: 443
 SSL Trustpoint: TP-self-signed-26793562
```

The table below describes the significant fields shown in the display.

Table 203: show webvpn gateway name Field Descriptions

Field	Description
Admin Status	The administrative status of the gateway, displayed as “up” or “down.” Administrative status is configured with the **inservice** command.
Operation Status	The operational status of the gateway, displayed as “up” or “down.” The gateway must be "inservice" and configured with a valid IP address to be in an “up” state.
IP: ... port: ...	The configured IP address and port number of the WebVPN gateway. The default port number 443.
SSL Trustpoint:	Configures the CA certificate trust point.

Related Commands

Command	Description
webvpn gateway	Enters webvpn gateway configuration mode to configure a SSL VPN gateway.

show webvpn install

To display the installation status of SVC or CSD client software packages, use the **show webvpn install** command in EXEC mode.

show webvpn install {**file** *name* | **package** {**csd** | **svc**} | **status** {**csd** | **svc**}}

Syntax Description

file *name*	Displays file attribute information about the named software package file.
package {**csd** | **svc**	Displays information about either the CSD or SVC software installation package.
status {**csd** | **svc**}	Displays file attribute information about the CSD or SVC software package.

Command Default

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

This command is used to display information about Cisco Secure Desktop (CSD) and SSL VPN Client (SVC) software pages that are locally cached for distribution to remote SSL VPN clients. This information includes software versions and build dates.

Examples

The following is sample output from the **show webvpn install** command, entered with the **file** keyword:

```
Router# show webvpn install file \webvpn\stc\version.txt

SSLVPN File \webvpn\stc\version.txt installed:
CISCO STC win2k+ 1.0.0
1,1,0,116
Fri 06/03/2005 03:02:46.43
```

The table below describes the significant fields shown in the display.

Table 204: show webvpn install file Field Descriptions

Field	Description
SSLVPN File	The local path to the specified installation package file. File attributes, such as the name, build number, and installation date are deployed following this line.

The following is sample output from the **show webvpn install** command, entered with the **package svc**keywords:

```
Router# show webvpn install package svc
```

```
SSLVPN Package SSL-VPN-Client installed:
File: \webvpn\stc\1\binaries\detectvm.class, size: 555
File: \webvpn\stc\1\binaries\java.htm, size: 309
File: \webvpn\stc\1\binaries\main.js, size: 8049
File: \webvpn\stc\1\binaries\ocx.htm, size: 244
File: \webvpn\stc\1\binaries\setup.cab, size: 176132
File: \webvpn\stc\1\binaries\stc.exe, size: 94696
File: \webvpn\stc\1\binaries\stcjava.cab, size: 7166
File: \webvpn\stc\1\binaries\stcjava.jar, size: 4846
File: \webvpn\stc\1\binaries\stcweb.cab, size: 13678
File: \webvpn\stc\1\binaries\update.txt, size: 11
File: \webvpn\stc\1\empty.html, size: 153
File: \webvpn\stc\1\images\alert.gif, size: 2042
File: \webvpn\stc\1\images\buttons.gif, size: 1842
File: \webvpn\stc\1\images\loading.gif, size: 313
File: \webvpn\stc\1\images\title.gif, size: 2739
File: \webvpn\stc\1\index.html, size: 4725
File: \webvpn\stc\2\index.html, size: 325
File: \webvpn\stc\version.txt, size: 63
Total files: 18
```

The table below describes the significant fields shown in the display.

Table 205: show webvpn install package Field Descriptions

Field	Description
SSLVPN Package SSL-VPN-Client installed:	Displays the installation status of the CSD or SVC software package as "installed" or "NONE."
File: ... size: ...	The path, name, and size of each installation file.
Total files:	Total number in the package.

The following is sample output from the **show webvpn install** command, entered with the **status svc** keywords:

```
Router# show webvpn install status svc

SSLVPN Package SSL-VPN-Client version installed:
CISCO STC win2k+ 1.0.0
1,0,2,127
Fri 07/22/2005 12:14:45.43
```

The table below describes the significant fields shown in the display.

Table 206: show webvpn install stats Field Descriptions

Field	Description
SSLVPN Package	The SVC or CSD package file status is displayed as "installed" or "NONE." File attributes, such as the name, build number, and installation date are displayed following this line.

Related Commands

Command	Description
webvpn install	Installs a CSD or SVC package file to a WebVPN gateway for distribution to remote users.

show webvpn license

To display the available count and the current usage, use the **show webvpn license**command in privileged EXEC mode.

show webvpn license

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

Use the **show webvpn license** command to display the available count and the current usage. To display the current license type and time period left in the case of a nonpermanent licence, use the **show license**command.

Examples

The following is sample output from the **show webvpn license** command:

```
Router# show webvpn license
Available license count : 200
Reserved license count  : 200
In-use count : 3
```

The above output is self-explanatory.

Related Commands

Command	Description
debug webvpn license	Displays debug messages related to license operations, events, and errors.

show webvpn nbns

To display information in the NetBIOS Name Service (NBNS) cache, use the **show webvpn nbns** command in privileged EXEC mode.

show webvpn nbns context {**all***name*}

Syntax Description

context *name*	Filters the output to display NBNS information for the named context.
context all	Displays NBNS information for all contexts.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

This command is used to display information about NBNS cache entries. The NetBIOS name, IP address of the Windows Internet Name Service (WINS) server, and associated time stamps.

Examples

The following is sample output from the **show webvpn nbns** command, entered with the **context** and **all** keywords:

```
Router# show webvpn nbns context all

NetBIOS name        IP Address       Timestamp
0 total entries
NetBIOS name        IP Address       Timestamp
0 total entries
NetBIOS name        IP Address       Timestamp
0 total entries
```

The table below describes the significant fields shown in the display.

Table 207: show webvpn nbns context all Field Descriptions

Field	Description
NetBIOS name	NetBIOS name.
IP Address	The IP address of the WINs server.
Timestamp	Time stamp for the last entry.
... total entries	Total number of NetBIOS cache entries.

Related Commands

Command	Description
nbns-list	Enters webvpn NBNS list configuration mode to configure a NBNS server list for CIFS name resolution.
webvpn install	Installs a CSD or Cisco AnyConnect VPN Client package file to a SSL VPN gateway for distribution to end users.

show webvpn policy

To display the context configuration associated with a policy group, use the **show webvpn policy** command in user EXEC or privileged EXEC mode.

show webvpn policy group *name* **context** {**all***name*} [**detail**]

Syntax Description

group *name*	Displays information for the named policy group.
context all	Displays information for all context configurations with which the policy group is associated.
context *name*	Displays information for the named context configuration.
detail	(Optional) Displays detailed information about the user session.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.4(11)T	This command was modified. An output example was added for Single SignOn (SSO) server information.
15.1(1)T	This command was modified. The **detail** keyword was added. The output was modified to display the webvpn home page configuration.

Usage Guidelines

This command is used to display configuration settings that apply only to the policy group. This command can also be used to display all contexts for which the policy group is configured.

Examples

The following is sample output from the **show webvpn policy**command:

```
Router# show webvpn policy group group1 context all
WEBVPN: group policy = group1 ; context = context1
      url list name = "web-url"
      cifs url list name = "cifs-url"
      idle timeout = 2100 sec
      session timeout = Disabled
      port forward name = "pflist"
      functions =
                file-access
                file-browse
                file-entry
                svc-enabled
      citrix disabled
      address pool name = "70pool"
      svc home page = "http://wiki-eng.cisco.com/engwiki/SSLVPNTech"
      webvpn home page = "http://192.0.2.0", redirection time = 10
      dpd client timeout = 300 sec
```

```
      dpd gateway timeout = 300 sec
      keepalive interval = 30 sec
      SSLVPN Full Tunnel mtu size = 1406 bytes
      keep sslvpn client installed = enabled
      rekey interval = 3600 sec
      rekey method =
      lease duration = 43200 sec
      msie-proxy = auto
      ie proxy server = "test.com:80"
      split include = 209.165.200.225 255.255.255.224
      split include = 209.165.200.226 255.255.255.224
```

See the table below for the field description.

```
The following sample output displays information about an SSO server configured for a policy
 group of the SSL VPN context:
Router# show webvpn policy group ONE context all
WV: group policy = sso ; context = test_sso
  idle timeout = 2100 sec
  session timeout = 43200 sec
  sso server name = "server2
  citrix disabled
  dpd client timeout = 300 sec
  dpd gateway timeout = 300 sec
  keep sslvpn client installed = disabled
  rekey interval = 3600 sec
  rekey method =
  lease duration = 43200 sec
```

The table below describes the significant fields shown in the displays.

Table 208: show webvpn policy Field Descriptions

Field	Description
group policy	Name of the policy group.
context	Name of the Secure Socket Layer (SSL) Virtual Private Network (VPN) context.
url list name	Name of the URL list.
cifs url list name	Name of the Common Internet File System (CIFS) URL list.
idle timeout	Length of time that a remote-user session can remain idle.
session timeout	Length of time that a remote-user session can remain active.
port forward name	Name of the port-forwarding list configured with the **port-forward** command.
citrix	Support for Citrix applications, shown as "disabled" or "enabled."
address pool name	Name of the address pool configured.
svc home page	URL of the SSL VPN Client (SVC) configured.
webvpn home page	URL of the WebVPN configured using the **webvpn-homepage** command.

Field	Description
dpd client timeout	Length of time that a session will be maintained with a nonresponsive end user (remote client).
dpd gateway timeout	Length of the time that a session will be maintained with a nonresponsive SSL VPN gateway.
keepalive interval	Keepalive interval, in seconds.
SSLVPN Full Tunnel mtu size	MTU, in bytes.
keep sslvpn client installed	Cisco AnyConnect VPN Client software installation policy on the end user (remote PC). "enabled" indicates that Cisco AnyConnect VPN Client software remains installed after the SSL VPN session is terminated. "disabled" indicates that Cisco AnyConnect VPN Client software is pushed to the end user each time a connection is established.
rekey interval	Length of time between tunnel key refresh cycles.
rekey method	Tunnel key authentication method.
lease duration	Tunnel key lifetime.
sso server name	Name of the SSO server.

Related Commands

Command	Description
policy group	Enters SSL VPN group policy configuration mode to configure a group policy.

show webvpn session

To display Secure Sockets Layer Virtual Private Network (SSL VPN) user session information, use the **show webvpn session** command in user EXEC or privileged EXEC mode.

show webvpn session [**user** *user-name*] **context** {*context-name* | **all**} [**detail**]

Syntax Description

user	(Optional) Displays detailed information about the named user session.
user-name	(Optional) Name of the user.
context	Displays a list of active users for only the named context.
context-name	Name of the context.
all	Displays a list of active users sessions for all locally configured contexts.
detail	(Optional) Displays detailed information about the user session.

Command Default

Session information is not displayed.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.4(6)T	This command was introduced.
15.1(1)T	This command was modified. The **detail**keyword was added.

Usage Guidelines

This command is used to list active SSL VPN connections or to display context configuration policies that apply to the specified end user.

The **show webvpn session** command provides detailed information about the user session. These details include the username, assigned IP addess, group policy, login time, hash algorithms used for the session, number of clientless tunnels, and the number of full tunnels enabled for the user.

This command is applicable only for user session statistics and tunnel statistics.

Examples

The following is sample output from the **show webvpn session** command. The output is filtered to display user session information for only the specified context.

```
Router# show webvpn session context context1

WebVPN context name: context1
Client_Login_Name  Client_IP_Address  No_of_Connections  Created  Last_Used
user1              192.0.2.1                  2         04:47:16  00:01:26
user2              192.0.2.2                  2         04:48:36  00:01:56
```

The table below describes the significant fields shown in the display.

Table 209: show webvpn session Field Descriptions

Field	Description
WebVPN context name	Name of the context.
Client_Login_Name	Login name for the end user (remote PC or device).
Client_IP_Address	IP address of the remote user.
No_of_Connections	Number of times the remote user has connected.
Created	Time, in hh:mm:ss, when the remote connection was established.
Last_Used	Time, in hh:mm:ss, that the user connection last generated network activity.

The following is sample output from the **show webvpn session** command. The output is filtered to display session information for a specific user.

```
Router# show webvpn session user user1 context all

Session Type      : Full Tunnel
Client User-Agent : Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.1.5)
Username          : test                 Num Connection : 1
Public IP         : 192.0.2.0            VRF Name       : None
Context           : context1             Policy Group   : default
Last-Used         : 00:00:42             Created        : *09:50:38.191 UTC Thu Jan 21 2010
Session Timeout   : Disabled             Idle Timeout   : 2100
DPD GW Timeout    : 300                  DPD CL Timeout : 300
Address Pool      : varun                MTU Size       : 1206
Rekey Time        : 3600                 Rekey Method   :
Lease Duration    : 43200
Tunnel IP         : 209.165.200.225      Netmask        : 255.255.255.224
Rx IP Packets     : 0                    Tx IP Packets  : 1
CSTP Started      : 00:01:42             Last-Received  : 00:01:42
CSTP DPD-Req sent : 0                    Virtual Access : 1
Msie-ProxyServer  : None                 Msie-PxyPolicy : Disabled
Msie-Exception    :
Split Include     : 209.165.200.224 255.255.255.224
Client Ports      : 2538
DTLS Port         : 2547
```

The table below describes the significant fields shown in the display.

Table 210: show webvpn session user context all Field Descriptions

Field	Description
Session Type	Mode used to access SSL VPN.
Client User-Agent	The client user-agent header.
Username	Name of the end user.
Num Connection	Number of times the remote user has connected.
Public IP	Public IP address.
VRF Name	Name of the virtual routing and forwarding (VRF) interface.

Field	Description
Context	Name of the context to which user policies apply.
Policy Group	Name of the policy group to which the user belongs.
Last-Used	Time, in hh:mm:ss, that the user connection last generated network activity.
Created	Time, in hh:mm:ss, when the remote connection was established.
Session Timeout	Length of time that a remote-user session can remain active.
Idle Timeout	Length of time that a remote-user session can remain idle.
DPD GW Timeout	Length of time that a Dead Peer Detection (DPD) gateway can remain idle.
DPD CL Timeout	Length of time that a DPD client can remain idle.
Address Pool	Name of the address pool configured.
MTU Size	Size of the maximum transmission unit (MTU).
Rekey Time	Time at which the tunnel key is refreshed.
Rekey Method	Tunnel key authentication method.
Lease Duration	Tunnel key lifetime.
Tunnel IP	IP address of the SSL VPN tunnel.
Netmask	Network mask used.
Rx IP Packets	Number of IP packets sent.
Tx IP Packets	Number of IP packets received.
CSTP Started	Time at which the Cisco SSL Tunnel Protocol (CSTP) frames were sent to the client.
Last-Received	Time when the CSTP frame was received.
CSTP DPD-Req sent	Time at which the CSTP request was sent to the client.
Virtual Access	Total number of virtual access interfaces created.
Msie-ProxyServer	Number of Microsoft Internet Explorer (MSIE) proxy servers configured for policy group end users.
Msie-PxyPolicy	Status of the MSIE policy: Enabled or Disabled.
Msie-Exception	MS Proxy exceptions.
Split Include	IP address from which the traffic is resolved through the Cisco AnyConnect VPN Client tunnel.
Client Ports	Local TCP port used on the client host.
DTLS Port	Datagram Transport Layer Security (DTLS) port.

The following is sample output from the show webvpn session user context all detail command:

```
Router# show webvpn session user user1 context all detail
Session Type      : Full Tunnel
Client User-Agent : Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:10.0.0.1)
Username          : user1                Num Connection : 1
Public IP         : 209.165.200.225      VRF Name       : None
Context           : context1             Policy Group   : default
Last-Used         : 00:00:02             Created        : *09:50:38.191 UTC Thu Jan 21 2010
Session Timeout   : Disabled             Idle Timeout   : 2100
DPD GW Timeout    : 300                  DPD CL Timeout : 300
Address Pool      : varun                MTU Size       : 1206
Rekey Time        : 3600                 Rekey Method   :
Lease Duration    : 43200
Tunnel IP         : 209.165.200.249      Netmask        : 255.255.255.224
Rx IP Packets     : 0                    Tx IP Packets  : 2
CSTP Started      : 00:02:03             Last-Received  : 00:02:03
CSTP DPD-Req sent : 0                    Virtual Access : 1
Msie-ProxyServer  : None                 Msie-PxyPolicy : Disabled
Msie-Exception    :
Split Include     : 209.165.200.250 255.255.255.224
Client Ports      : 2538
DTLS Port         : 2547

Detail Session Statistics for User:: user1
-----------------------------------
CSTP Statistics::
Rx CSTP Frames    : 4                  Tx CSTP Frames   : 0
Rx CSTP Bytes     : 32                 Tx CSTP Bytes    : 0
Rx CSTP Data Fr   : 0                  Tx CSTP Data Fr  : 0
Rx CSTP CNTL Fr   : 4                  Tx CSTP CNTL Fr  : 0
Rx CSTP DPD Req   : 0                  Tx CSTP DPD Req  : 0
Rx CSTP DPD Res   : 0                  Tx CSTP DPD Res  : 0
Rx Addr Renew Req : 0                  Tx Address Renew : 0
Rx CDTP Frames    : 2                  Tx CDTP Frames   : 0
Rx CDTP Bytes     : 122                Tx CDTP Bytes    : 0
Rx CDTP Data Fr   : 2                  Tx CDTP Data Fr  : 0
Rx CDTP CNTL Fr   : 0                  Tx CDTP CNTL Fr  : 0
Rx CDTP DPD Req   : 0                  Tx CSTP DPD Req  : 0
Rx CDTP DPD Res   : 0                  Tx CDTP DPD Res  : 0
Rx IP Packets     : 0                  Tx IP Packets    : 2
Rx IP Bytes       : 0                  Tx IP Bytes      : 10
CEF Statistics::
Rx CSTP Data Fr   : 0                  Tx CSTP Data Fr  : 0
Rx CSTP Bytes     : 0                  Tx CSTP Bytes    : 0
```

The table below describes the significant fields shown in the display.

Table 211: show webvpn session user context all detail Field Descriptions

Field	Description
Rx CSTP Frames	Number of CSTP frames received from the client.
Rx CSTP Bytes	Number of CSTP bytes (data plus control frames) received from the client.
Rx CSTP Data Fr	Number of CSTP data frames received from the client.
Rx CSTP CNTL Fr	Number of CSTP control frames received from the client.
Rx CSTP DPD Req	Number of DPD requests received at the gateway.

Field	Description
Rx CSTP DPD Res	Number of times the gateway processed a CSTP DPD request frame.
Rx Addr Renew Req	Number of address renew requests received at the gateway.
Rx CDTP Frames	Number of Cisco Dynamic Trunking Protocol (CDTP) frames received from the client.
Rx CDTP Bytes	Number of CDTP bytes received from the client.
Rx CDTP Data Fr	Number of CDTP data frames received from the client.
Rx CDTP CNTL Fr	Number of CDTP control frames received from the client.
Rx CDTP DPD Req	Number of CDTP DPD requests received at the gateway.
Rx CDTP DPD Res	Number of times the gateway processed a CDTP DPD request frame.
Rx IP Packets	Total number of IP packets received.
Rx IP Bytes	Total number of IP bytes received.
Tx CSTP Frames	Number of CSTP frames transmitted to the client.
Tx CSTP Bytes	Number of CSTP bytes (data plus control frames) transmitted to the client.
Tx CSTP Data Fr	Number of CSTP data frames transmitted to the client.
Tx CSTP CNTL Fr	Number of CSTP control frames transmitted to the client.
Tx CSTP DPD Req	Number of DPD requests transmitted from the gateway.
Tx CSTP DPD Res	Number of times the gateway processed a CSTP DPD request frame.
Tx Address Renew	Number of address renew requests transmitted at the gateway.
Tx CDTP Frames	Number of CDTP frames transmitted to the client.
Tx CDTP Bytes	Number of CDTP bytes transmitted to the client.
Tx CDTP Data Fr	Number of CDTP data frames transmitted to the client.
Tx CDTP CNTL Fr	Number of CDTP control frames transmitted to the client.
Tx CDTP DPD Req	Number of CDTP DPD requests transmitted to the gateway.
Tx CDTP DPD Res	Number of times the gateway processed a CDTP DPD request frame.
Tx IP Packets	Total number of IP packets transmitted.
Tx IP Bytes	Total number of IP bytes transmitted.
CEF Statistics	Cisco Express Forwarding statistics.

show webvpn sessions

Note Effective with Cisco IOS Release 12.4(6)T, the **show webvpn sessions** command is replaced by the **show webvpn session** command. See the **show webvpn session** command for more information.

To display information about WebVPN sessions, use the **show webvpn sessions** command in privileged EXEC mode.

show webvpn sessions

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(6)T	This command was replaced by the **show webvpn session** command.

Examples

The following output example displays information about a WebVPN session:

```
Router# show webvpn sessions
WebVPN domain name: cisco.com
Client Login Name          Client IP Address     Number of Connections
webuser                    172.16.163.142       4
    Created 00:14:25, Last-used 00:00:10
    Client Port: 2366
    Client Port: 2386
    Client Port: 2396
    Client Port: 2486
browseruser                172.16.163.142      2
    Created 00:00:09, Last-used 00:00:08
    Client Port: 2431
    Client Port: 2432
```

The table below describes the significant fields shown in the display

Table 212: show webvpn sessions Field Descriptions

Field	Description
Client Login Name	Username used to log in to the WebVPN gateway.
Client IP Address	IP address of the host from which the user is connecting.
Number of Connections	Number of active TCP connections by the user at this point.
Created	Provides the time that has elapsed since the user logged in (in HH:MM:SS format).

Field	Description
Client Port	Local TCP port used on the client host.

Related Commands

Command	Description
show webvpn statistics	Displays WebVPN statistics.

show webvpn statistics

Note Effective with Cisco IOS Release 12.4(6)T, the **show webvpn statistics** command is replaced by the **show webvpn stats**command. See the **show webvpn stats** command for more information.

To display WebVPN statistics, use the **show webvpn statistics** command in privileged EXEC mode.

show webvpn statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(6)T	This command was replaced by the **show webvpn stats**command.

Examples

The following is sample output using the **show webvpn statistics** command:

```
Router# show webvpn statistics
Active user sessions: 2
Active user TCP connections: 6
Authentication failures: 3
Terminated user sessions: 0
```

The table below describes the significant fields shown in the display.

Table 213: show webvpn statistics Field Descriptions

Field	Description
Active user sessions	Number of users who are logged into the system.
Active user TCP connections	Number of TCP user connections that are used by the user session.
Authentication failures	Number of authentication failures to the gateway.
Terminated user sessions	Number of users who logged in and logged out after the statistics were cleared.

Related Commands

Command	Description
show webvpn sessions	Displays information about WebVPN sessions.

show webvpn stats

To display Secure Socket Layer Virtual Private Network (SSL VPN) application and network statistics, use the **show webvpn stats** command in privileged EXEC mode.

show webvpn stats [{**cifs** | **citrix** | **mangle** | **port-forward** | **sso** | **tunnel**}] [**detail**] [**context** {**all***name*}]

Syntax Description

cifs	(Optional) Displays Windows file share (Common Internet File System [CIFS]) statistics.
citrix	(Optional) Displays Citrix application statistics.
mangle	(Optional) Displays URL mangling statistics.
port-forward	(Optional) Displays port forwarding statistics.
sso	(Optional) Displays statistics for the Single SignOn (SSO) server.
tunnel	(Optional) Displays VPN tunnel statistics.
detail	(Optional) Displays detailed information.
context all | *name*	(Optional) Displays information for a specific context or all contexts.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.4(11)T	The **sso** keyword was added for Cisco 6500 Catalyst switches.
12.4(15)T	Output information was added for Cisco Express Forwarding (CEF).

Usage Guidelines

This command is used to display SSL VPN application, authentication, and network statistics and counters.

Examples

The following is sample output from the **show webvpn stats** command entered with the **detail** and **context** keywords:

```
Router# show webvpn stats detail context context1
WebVPN context name : context1
User session statistics:
    Active user sessions     : 0          AAA pending reqs         : 0
    Peak user sessions       : 0          Peak time                : never
    Active user TCP conns    : 0          Terminated user sessions : 0
    Session alloc failures   : 0          Authentication failures  : 0
    VPN session timeout      : 0          VPN idle timeout         : 0
    User cleared VPN sessions: 0          Exceeded ctx user limit  : 0
```

```
    CEF switched packets - client: 0         , server: 0
    CEF punted packets - client: 0         , server: 0
Mangling statistics:
    Relative urls            : 0          Absolute urls            : 0
    Non-http(s) absolute urls: 0          Non-standard path urls   : 0
    Interesting tags         : 0          Uninteresting tags       : 0
    Interesting attributes   : 0          Uninteresting attributes : 0
    Embedded script statement: 0          Embedded style statement : 0
    Inline scripts           : 0          Inline styles            : 0
    HTML comments            : 0          HTTP/1.0 requests        : 0
    HTTP/1.1 requests        : 0          Unknown HTTP version     : 0
    GET requests             : 0          POST requests            : 0
    CONNECT requests         : 0          Other request methods    : 0
    Through requests         : 0          Gateway requests         : 0
    Pipelined requests       : 0          Req with header size >1K : 0
    Processed req hdr bytes  : 0          Processed req body bytes : 0
    HTTP/1.0 responses       : 0          HTTP/1.1 responses       : 0
    HTML responses           : 0          CSS responses            : 0
    XML responses            : 0          JS responses             : 0
    Other content type resp  : 0          Chunked encoding resp    : 0
    Resp with encoded content: 0          Resp with content length : 0
    Close after response     : 0          Resp with header size >1K: 0
    Processed resp hdr size  : 0          Processed resp body bytes: 0
    Backend https response   : 0          Chunked encoding requests: 0
CIFS statistics:
  SMB related Per Context:
    TCP VC's                 : 0          UDP VC's                 : 0
    Active VC's              : 0          Active Contexts          : 0
    Aborted Conns            : 0
  NetBIOS related Per Context:
    Name Queries             : 0          Name Replies             : 0
    NB DGM Requests          : 0          NB DGM Replies           : 0
    NB TCP Connect Fails     : 0          NB Name Resolution Fails : 0
  HTTP related Per Context:
    Requests                 : 0          Request Bytes RX         : 0
    Request Packets RX       : 0          Response Bytes TX        : 0
    Response Packets TX      : 0          Active Connections       : 0
    Active CIFS context      : 0          Requests Dropped         : 0

Socket statistics:
    Sockets in use           : 0          Sock Usr Blocks in use   : 0
    Sock Data Buffers in use : 0          Sock Buf desc in use     : 0
    Select timers in use     : 0          Sock Select Timeouts     : 0
    Sock Tx Blocked          : 0          Sock Tx Unblocked        : 0
    Sock Rx Blocked          : 0          Sock Rx Unblocked        : 0
    Sock UDP Connects        : 0          Sock UDP Disconnects     : 0
    Sock Premature Close     : 0          Sock Pipe Errors         : 0
    Sock Select Timeout Errs : 0
Port Forward statistics:
    Connections serviced     : 0          Server Aborts (idle)     : 0
  Client                                Server
    in pkts                  : 0          out pkts                 : 0
    in bytes                 : 0          out bytes                : 0
    out pkts                 : 0          in pkts                  : 0
    out bytes                : 0          in bytes                 : 0
WEBVPN Citrix statistics:
Connections serviced : 0
               Server                   Client
  Packets in  : 0                        0
  Packets out : 0                        0
  Bytes in    : 0                        0
  Bytes out   : 0                        0
Tunnel Statistics:
    Active connections       : 0
```

```
  Peak connections         : 0          Peak time                : never
  Connect succeed          : 0          Connect failed           : 0
  Reconnect succeed        : 0          Reconnect failed         : 0
  SVCIP install IOS succeed: 0          SVCIP install IOS failed : 0
  SVCIP clear IOS succeed  : 0          SVCIP clear IOS failed   : 0
  SVCIP install TCP succeed: 0          SVCIP install TCP failed : 0
  DPD timeout              : 0
Client                                Server
  in  CSTP frames          : 0          out IP pkts              : 0
  in  CSTP data            : 0          out stitched pkts        : 0
  in  CSTP control         : 0          out copied pkts          : 0
  in  CSTP Addr Reqs       : 0          out bad pkts             : 0
  in  CSTP DPD Reqs        : 0          out filtered pkts        : 0
  in  CSTP DPD Resps       : 0          out non fwded pkts       : 0
  in  CSTP Msg Reqs        : 0          out forwarded pkts       : 0
  in  CSTP bytes           : 0          out IP bytes             : 0
  out CSTP frames          : 0          in  IP pkts              : 0
  out CSTP data            : 0          in  invalid pkts         : 0
  out CSTP control         : 0          in  congested pkts       : 0
  out CSTP Addr Resps      : 0          in  bad pkts             : 0
  out CSTP DPD Reqs        : 0          in  nonfwded pkts        : 0
  out CSTP DPD Resps       : 0          in  forwarded pkts       : 0
  out CSTP Msg Reqs        : 0
  out CSTP bytes           : 0          in  IP bytes             : 0
```

The table below describes significant fields in the **show webvpn stats detail context**display.

Table 214: show webvpn stats detail context Field Descriptions

Field	Description
WebVPN context name	Name of the context.
User session statistics:	
Active user sessions	Total number of currently active user sessions on the gateway.
Peak user sessions	Maximum number of simultaneous user sessions on the gateway since the gateway came up.
Active user TCP conns	Total number of currently active TCP connections that were initiated from the client side toward the SSL VPN gateway.
Session alloc failures	Total number of session allocation failures that were initiated from the client side. These failures occur because of a lack of memory on the gateway. Examples: • No free slot in session table • No memory for session allocation • No memory for gateway cookie allocation • Not enough memory on the gateway

Field	Description
VPN session timeout	Information about the number of times the web VPN session timer has expired. This value reflects the full total for all the contexts that are configured at the gateway. The session timer is off by default, and it is enabled when an administrator intentionally uses the command-line interface (CLI) timeout session *number* argument under the **group policy** command submode.
User cleared VPN sessions	Total number of user-removed (or cleared) VPN sessions on the gateway. For example, if any user sessions are cleared using the CLI command **clear webvpn session** *user-name* **context** *context-name*, the counter is incremented by one.
AAA pending reqs	Total number of pending authentication, authorization, and accounting (AAA) requests on the gateway.
Peak time	Time elapsed since the peak number of simultaneous user sessions were observed on the gateway.
Terminated user sessions	Total number of expired user sessions on the gateway. Examples: • User logout sessions • Session cookie removed
Authentication failures	Total number of authentication failures on the gateway. Examples: • Wrong username and password • Empty username and password field
VPN idle timeout	Number of times the idle timer expired for all the contexts configured at the security gateway. Idle time refers to the time for which an active session can be left unattended (maximum time for which a session is up even though no traffic flows through the connection).
Exceeded ctx user limit	Total number of denied logins on the gateway that exceeded the context maximum user limit.
CEF switched packets (for client and server)	Packets that were CEF-switched.
CEF punted packets (for client and server)	Packets that could not be CEF-switched in a box with CEF switching enabled and that were "punted" to the next switching level.
Mangling statistics:	
Relative urls	Number of URLs that point to a file/directory in relation to the present file/directory.

Field	Description
Non-http(s) absolute urls	Number of non-HTTP- relative URLs that are mangled.
Interesting tags	Number of HTTP, Cascade Style Sheets (CSS), or JavaScript tags that are mangled.
Interesting attributes	HTTP attributes, JavaScript, or CSS attributes that are mangled.
Embedded script statement	Embedded JavaScripts that were mangled.
Inline scripts	Number of inline CSSs that were mangled.
HTML comments	Number of HTML comments that were encountered.
HTTP/1.1 requests	Number of HTTP 1.1 requests that were encountered.
GET requests	Number of HTTP 1.0 or 1.1 GET requests that were encountered.
CONNECT requests	Number of HTTP 1.0 or 1.1 CONNECT requests that were encountered.
Pipelined requests	Number of requests dropped due to pipelines (pipelined requests are currently not supported).
Processed req hdr bytes	Total number of bytes in the requests made by the HTTP header to the backend server.
HTML /1.0 responses	Number of HTTP 1.0 responses that were encountered.
HTML responses	Total number of HTML pages that were received at the gateway.
XML responses	Total number of XML pages/responses that were received at the gateway.
Other content type resp	Total number of responses that were received other than HTML, XML, JavaScript, or CSS.
Resp with encoded content	Number of supported responses that were already encoded by the backend server.
Processed resp hdr size	Number of bytes in the headers of HTTP responses that were processed at the gateway.
Backend https response	Number of HTTP pages sent to the client by the backend server.
Absolute urls	Number of absolute HTTP URLs that were mangled.
Non-standard path urls	Number of non-HTTP-relative URLs that were mangled.
Uninteresting tags	HTTP attributes, JavaScript, or CSS attributes that were mangled.
Uninteresting attributes	Number of attributes that were not mangled (for instance, XML attributes).
Embedded style statement	Embedded CSS and other styling sheets that were mangled.

Field	Description
Inline styles	Number of inline CSSs that were mangled.
HTTP/1.0 requests	Number of HTTP 1.0 requests that were encountered.
Unknown HTTP version	Number of HTTP version requests other than 1.0 and 1.1.
POST requests	Number of HTTP 1.0 or 1.1 POST requests that were encountered.
Other request methods	Number of non- (1.0 or 1.1) HTTP requests plus the number of requests other than GET, POST, or CONNECT.
Gateway requests	Number of requests made explicitly to the gateway.
Req with header size >1K	Number of requests to the backend server having a header size greater than 1024 bytes.
Processed req body bytes	Total number of bytes processed while parsing HTML requests (body means the total bytes processed or read in an HTML request excluding the header).
HTTP/1.1 responses	Number of HTTP 1.1 responses that were received at the gateway.
CSS responses	Total number of CSS tags that were received.
JS responses	Total number of JavaScript responses that were received at the gateway.
Chunked encoding resp	Number of times transfer encoding was set to "chunked" in an HTTP response.
Resp with content length	Number of non-zero content-length responses.
Resp with header size > 1K	Responses received at the gateway with a header size greater than 1 kilobyte.
Processed resp body bytes	Total number of bytes that were processed in responses (number of bytes in the bodies of the messages).
Chunked encoding requests	Number of requests that were chunk encoded.
CIFS statistics:	
SMB related Per Context:	
TCP VC’s	Backend TCP connections established successfully (thus far).
Active VC’s	Currently active TCP/User Datagram Protocol (UDP) connections.
Aborted Conns	Number of TCP-terminated connections (thus far).
UDP VC’s	Backend TCP connections established successfully (thus far).
Active Contexts	Currently active Server Message Block (SMB) contexts.
NetBIOS related Per Context:	

Field	Description
Name Queries	NetBIOS name service (NBNS) name queries that have been sent.
NB DGM Requests	NetBios datagram service-related GET backup browser-list queries that have been sent.
NB TCP Connect Fails	NetBios TCP connections that failed.
Name Replies	NBNS name-query replies that have been received. Mismatch indicates that browsers/primary domain controller (PDC)/servers could not be contacted.
NB DGM Replies	NetBIOS datagram service-related GET backup browser replies were received. Request/reply mismatch indicates that a browse domain attempt would not work.
NB Name Resolution Fails	NetBIOS name resolution requests sent to the PDC failed.
HTTP related Per Context:	
Requests	Number of HTTP requests made per a CIFS application context.
Request Packets RX	Number of HTTP packets received per a CIFS application context.
Response Packets TX	Number of HTTP packets sent per a CIFS application context.
Active CIFS context	Number of active CIFS application module contexts on which CIFS requests are being processed.
Request Bytes RX	Number of HTTP bytes received per a CIFS application context.
Response Bytes TX	Number of HTTP bytes sent per a CIFS application context.
Active Connections	Number of active CIFS connections.
Requests Dropped	Number of HTTP requests dropped per CIFS application context.
Socket statistics:	
Sockets in use	Number of sockets that are in use by SSL VPN socket layer.
Sock Data Buffers in use	Number of data buffers that are used by the socket layer.
Select timers in use	Number of socket select timers that are in use.
Sock TX Blocked	Number of times an application send was blocked by TCP congestion control.
Sock Rx Blocked	Number of times an application blocked further reception of data from the TCP layer. The blocking indicates application buffer starvation or a processing limit.
Sock UDP Connects	Number of UDP connects to the gateway.

Field	Description
Sock Premature Close	Number of times an application received a Closed connection before it could be established.
Sock Select Timeout Errs	Number of times a socket select timeout error occurred.
Sock Usr Blocks in use	Number of user blocks in use.
Sock Buf desc in use	Number of socket buffer descriptors in use.
Sock Select Timeouts	Number of times an application timed out while waiting for a reply in a request/reply exchange or while waiting for a TCP connection to be established.
Sock Tx Unblocked	Number of times an application send resumed after being blocked due to TCP congestion control. If the transmit blocked and unblocked do not match after a sufficient period of time, the transaction is stalled.
Sock Rx Unblocked	Number of times an application resumed further reception of data from the TCP layer. If receive blocked and unblocked do not match after a sufficient period of time, the transaction is stalled.
Sock UDP Disconnects	Number of UDP disconnects to the gateway.
Sock Pipe Errors	Number of times socket pipe establishment failed.
WEBVPN Citrix statistics:	
Server	
Packets in	Number of packets received from the server.
Packets out	Number of packets sent to the server.
Bytes in	Number of bytes received from the server.
Bytes out	Number of bytes sent to the server.
Client	
Packets in	Number of packets received from the client.
Packets out	Number of packets sent to the client.
Bytes in	Number of bytes received from the server.
Bytes out	Number of bytes sent to the client.
Tunnel Statistics:	
Active connections	Number of active tunnels.
Peak connections	Maximum number of simultaneously active tunnels as observed since the last reboot of the Cisco IOS router or last counter reset.

Field	Description
Connect succeed	Number of tunnel connections that have succeeded since the last reboot of the Cisco IOS router or last counter reset.
Reconnect succeed	Number of tunnel connections that have succeeded in reconnecting since the last reboot of the Cisco IOS router or last counter reset.
SVCIP install IOS succeed	Number of times, during the SSL VPN Client (SVC)/AnyConnect package installation, that the frame IP address or allocated IP address is used (IP address sticky).
SVCIP clear IOS succeed	Number of times an SVC IP address is successfully removed from the IP alias on the core.
SVCIP install TCP succeed	Number of tunnel connections that have succeeded since the last reboot of the Cisco IOS router or last counter reset.
DPD timeout	Number of Dead Peer Detection (DPD) timeout sessions.
Peak time	Absolute timestamp when the peak full-tunnel connections were observed.
Connect failed	Number of tunnel connections that have failed since the last reboot of the Cisco IOS router or last counter reset.
Reconnect failed	Number of tunnel connections that have failed in reconnecting since the last reboot of the Cisco IOS router or last counter reset.
SVCIP install IOS failed	Total number of times, during the SVC/AnyConnect installation, that an IP assignment from the pool fails or failed to configure an IP address to the virtual route forwarding (VRF) table.
SVCIP clear IOS failed	Number of times an STC IP address could not be removed from the IP alias on the core.
SVCIP install TCP failed	Number of tunnel connections that have failed since the last reboot of the Cisco IOS router or last counter reset.
Client	
in CSTP frames	Number of Cisco SSL Tunnel Protocol (CSTP) frames from the client.
in CSTP data	Number of CSTP data frames from the client.
in CSTP control	Number of CSTP control frames from the client.
in CSTP Addr Reqs	Number of IP address renewal requests received by the gateway.
in CSTP DPD Reqs	Number of DPD requests received at the gateway.
in CSTP DPD Resps	Number of DPD responses received at the gateway (The client sends the DPD requests, the gateway responds to the transmission, and the client responds back. It is this response that is counted here.)

Field	Description
in CSTP Msg Reqs	Number of times a CSTP message control frame is received at the gateway.
in CSTP bytes	Number of CSTP bytes (data+control frames) from the client.
out CSTP frames	Number of CSTP frames to the client.
out CSTP data	Number of CSTP data frames to the client.
out CSTP control	Number of CSTP control frames to the client.
out CSTP DPD Reqs	Number of times at-gateway CSTP control frames were generated.
out CSTP DPD Resps	Number of times the gateway processed a CSTP DPD request frame.
out CSTP Msg Reqs	Number of times the gateway generated a CSTP message (MSG) frame.
out CSTP bytes	Number of CSTP bytes (data+control frames) to the client.
Server	
out IP pkts	IP datagrams that are successfully forwarded to the server.
out bad pkts	Number of times a bad tunneled IP packet was dropped at the gateway.
out filtered pkts	Number of times a tunneled IP packet was dropped at the gateway due to a named or numbered ACL that was configured at the gateway.
out non fwded pkts	Number of times a tunneled IP packet could not be forwarded due to routing issues.
out forwarded pkts	Number of times a tunneled IP packet was successfully forwarded by the gateway.
out IP bytes	IP datagram bytes that are successfully forwarded to the server.
in IP pkts	IP datagrams that are successfully received from the server.
in IP bytes	IP datagram bytes that are successfully received from the server.

The following example displays SSO statistics:

```
Router# show webvpn stats sso
   Auth Requests            : 4          Pending Auth Requests      : 0
   Successful Requests      : 1          Failed Requests            : 3
   Retranmissions           : 0          DNS Errors                 : 0
   Connection Errors        : 0          Request Timeouts           : 0
   Unknown Responses        : 0
```

The table below describes significant fields in the **show webvpn stats sso**display.

Table 215: show webvpn stats sso Field Descriptions

Field	Description
Auth Requests	Number of SSO authentication requests.
Successful Requests	Number of SSO authentication requests that passed successfully.
Retransmissions	Total number of times authentication requests were resent for authentication. The resending occurs when the SSO timer expires and no response is received from the SSO server for authentication requests.
Connection Errors	Number of failures to sign on to the SSO server.
Unknown Responses	Number of times an SSO authentication request yielded results other than failure or success (includes errors, such as access control list [ACL] errors).
Pending Auth Requests	Total number of SSO authentication requests pending to be processed for authentication.
Failed Requests	Number of times SSO authentication failed.
DNS Errors	Number of times an SSO server could not be resolved.
Request Timeouts	Number of times an SSO authentication request timed out.

The following example displays information about CEF:

```
Router# show webvpn stats
User session statistics:
   Active user sessions     : 1           AAA pending reqs         : 0
   Peak user sessions       : 1           Peak time                : 00:12:01
   Active user TCP conns    : 1           Terminated user sessions : 1
   Session alloc failures   : 0           Authentication failures  : 0
   VPN session timeout      : 0           VPN idle timeout         : 0
   User cleared VPN sessions: 0           Exceeded ctx user limit  : 0
   Exceeded total user limit: 0
   Client process rcvd pkts : 37          Server process rcvd pkts : 0
   Client process sent pkts : 1052        Server process sent pkts : 0
   Client CEF received pkts : 69          Server CEF received pkts : 0
   Client CEF rcv punt pkts : 1           Server CEF rcv punt pkts : 0
   Client CEF sent pkts     : 1102        Server CEF sent pkts     : 0
   Client CEF sent punt pkts: 448         Server CEF sent punt pkts: 0

   SSLVPN appl bufs inuse   : 0           SSLVPN eng  bufs inuse   : 0
  Active server TCP conns   : 0
```

The table below describes fields in the **show webvpn stats** display.

Table 216: show webvpn stats Field Descriptions

Field	Description
User session statistics:	
Active user sessions	Total number of currently active user sessions on the gateway.

Field	Description
Peak user sessions	Maximum number of simultaneous user sessions on the gateway since the gateway came up.
Active user TCP conns	Total number of currently active TCP connections that were initiated from the client side toward the SSL VPN gateway.
Session alloc failures	Total number of session allocation failures that were initiated from the client side. These failures occur because of a lack of memory on the gateway. Examples: • No free slot in session table • No memory for session allocation • No memory for gateway cookie allocation Not enough memory on the gateway
VPN session timeout	Information about the number of times the web VPN session timer has expired. This value reflects the full total for all the contexts that are configured at the gateway. The session timer is OFF by default, and it is enabled when an administrator intentionally uses the CLI timeout session *number* argument under the **group policy** command submode.
User cleared VPN sessions	Total number of user-removed (or cleared) VPN sessions on the gateway. For example, if any user sessions are cleared using the CLI command **clear webvpn session** *user-name* **context** *context-name*, the counter is incremented by one.
Exceeded total user limit	Total number of denied logins on the gateway. An SSL VPN gateway can support the maximum user sessions (up to 1000).
Client process rcvd pkts	Total number of packets that were received from the client on the SSL VPN gateway.
Client process sent pkts	Total number of data packets that were sent to the client side from the SSL VPN gateway.
Client CEF received pkts	Total number of CEF-related packets that were received from the client on the gateway.
Client CEF rcv punt pkts	Total number of punt packets that were received from the client on the gateway. Punting is defined as the handling of CEF-intended data on the slower path (called the process path). Punting occurs when the data is not handled by the CEF path. Example: • If any control packets are received on the CEF path, those packets will punt to the slower path (process path), which is not handled by the CEF path.

Field	Description
Client CEF sent pkts	Total number of data packets that were sent via the CEF path to the client side from the gateway.
Client CEF sent punt pkts	Total number of punt packets (data sent via a slow path) that were sent to the client from the gateway.
SSLVPN appl bufs inuse	Total number of buffers that are allocated for data or application processing on the gateway.
Active server TCP conns	Total number of currently active TCP connections on the gateway that were initiated from the server side toward the SSL VPN gateway.
AAA pending reqs	Total number of pending AAA requests on the gateway.
Peak time	Time elapsed since the peak number of simultaneous user sessions were observed on the gateway.
Terminated user sessions	Total number of expired user sessions on the gateway. Examples: • User logout sessions • Session cookie removed
Authentication failures	Total number of authentication failures on the gateway. Examples: • Wrong username and password • Empty username and password field
VPN idle timeout	Number of times the idle timer expired for all the contexts configured at the security gateway. Idle time refers to the time for which an active session can be left unattended (maximum time for which a session is up even though no traffic flows through the connection).
Exceeded ctx user limit	Total number of denied logins on the gateway that exceeded the context maximum user limit.
Server process rcvd pkts	Total number of control packets that were received from the server side of the SSL VPN gateway.
Server process sent pkts	Total number of control packets that were sent to the server side from the SSL VPN gateway.
Server CEF received pkts	Total number of data CEF-related packets that were received from the server side of the SSL VPN gateway.
Server CEF rcv punt pkts	Total number of punt packets that were received from the server on the SSL VPN gateway.

Field	Description
Server CEF sent pkts	Total number of data (CEF-related) packets that were sent to the server from the SSL VPN gateway.
Server CEF sent punt pkts	Total number of punt packets that were sent to the server side from the SSL VPN gateway.
SSLVPN eng bufs inuse	Total number of buffers that were allocated for engine processing on the gateway.

Related Commands

Command	Description
clear webvpn stats	Clears application and access counters on an SSL VPN gateway.

show wlccp wds

To display information either about the wireless domain services (WDS) device or about client devices, use the **show wlccp wds**command in privileged EXEC mode.

show wlccp wds [{**ap** | **mn**}] [**detail**] [**mac-addr mac-address**]

Syntax Description

ap	(Optional) Displays access points participating in Cisco Centralized Key Management.
mn	(Optional) Displays cached information about client devices, also called mobile nodes.
detail	(Optional) Displays the lifetime of the client, the service set identifier (SSID), and the virtual VLAN ID.
mac-addr	(Optional) Displays information about a specific client device.
mac-address	Client's MAC address.

Command Default

If you do not enter any options with the **show wlccp wds** command, this command displays the IP address of the WDS device, the MAC address, the priority, and the interface state. If the interface state is backup, the command also displays the IP address of the current WDS device, the MAC address, and the priority.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(11)JA	This command was introduced.
12.3(11)T	This command was implemented on the following platforms: Cisco 2600XM, Cisco 2691, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3700, and Cisco 3800 series routers.

Usage Guidelines

To show information about the WDS device, do not enter any keywords with this command.

Examples

The following command entry displays information about the WDS device:

```
Router# show wlccp wds ap
```

The following command entry displays cached information, including details, about the client device with the specified MAC address:

```
Router# show wlccp wds mn detail mac-addr 00-05-C2-00-01-F5
```

The following is sample output from the **show wlccp wds** command:

```
Router# show wlccp wds
      MAC:0001.28e0.a400, IP-ADDR:10.0.0.1       , Priority:255
      Interface Vlan1, State:Administratively StandAlone - ACTIVE
      AP Count:1   , MN Count:0   , MAX AP Count:50
```

The table below describes the significant fields shown in the display.

Table 217: show wlccp wds Field Descriptions

Field	Description
MAC	MAC address of the interface on which the WDS is configured.
IP-ADDR	IP address of the interface on which the WDS is configured.
Priority	Priority of the WDS.
Interface	Interface on which the WDS is configured.
State	State of the WDS. The state can be INITIALIZATION, BACKUP, or ACTIVE.
AP Count	Number of access points registered to the WDS.
MN Count	Number of mobile nodes registered to the WDS.
MAX AP Count	Maximum number of access points that can be registered.

Related Commands

Command	Description
debug wlccp packet	Displays packet traffic to and from the WDS router.
debug wlccp wds	Displays either WDS debug state or WDS statistics messages.
wlccp authentication-server client	Configures the list of servers to be used for 802.1X authentication.
wlccp authentication-server infrastructure	Configures the list of servers to be used for 802.1X authentication for the wireless infrastructure devices.
wlccp wds priority interface	Enables a wireless device such as an access point or a wireless-aware router to be a WDS candidate.

show xsm status

To display information and subscription status of the XML Subscription Manager (XSM) server and clients (such as VPN Device Manager [VDM]), and to display a list of XML data from the XSM server, use the **show xsm status**command in privileged EXEC mode.

show xsm status

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(6)E	This command was introduced.
12.2(9)YE	This command was integrated into Cisco IOS Release 12.2(9)YE.
12.2(9)YO1	This command was integrated into Cisco IOS Release 12.2(9)YO1.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to display the following information: which subsystems and histories are enabled or disabled (XSM, Embedded Device Manager [EDM], VDM), XSM client version, number of XSM sessions, duration of XSM session, session IDs, client version and IP address, configuration and monitor privilege levels, and list of subscribed XML Request Descriptors (XRDs).

Examples

The following example shows one XSM session (Session ID = 2) active on the Cisco device for the XSM client at IP address 172.17.129.134, and how long this session has been connected to the XSM server (Session 2: Connected since 22:47:07 UTC Mon Jan 8 2001). The output shows that the XSM, VDM, and EDM subsystems, and EDM and VDM history collecting are enabled. XSM configuration privilege level is set at 15, with XSM monitor privilege level set at 1.

This output also shows the active XRDs (and their version) for Session 2:

```
Router# show xsm status
XSM subsystem is Enabled.
VDM subsystem is Enabled.
EDM subsystem is Enabled.
EDM History is Enabled.
VDM History is Enabled.
XSM privilege configuration level 15.
XSM privilege monitor level 1.
Number of XSM Sessions : 1.
```

```
Session ID = 2.
  XSM Client v0.0(0.0)- @ 172.17.129.134
  Connected since 22:47:07 UTC Mon Jan 8 2001
  List of subscribed xrds:
  0 ) device-about                              v1.0
  1 ) ios-image                                 v1.0
  2 ) if-list                                   v1.0
  3 ) device-health                             v1.0
  4 ) ike-stats                                 v1.0
  5 ) ike                                       v1.0
  6 ) ipsec-topn-tunnels-by-traffic             v1.0
  7 ) ipsec-topn-tunnels-by-duration            v1.0
  8 ) ipsec-stats                               v1.0
  9 ) crypto-maps                               v1.0
  10) ipsec                                     v1.0
```

The table below describes the significant fields shown in the display. (See documention of the **show xsm xrd-list** command for a full description of subscribed XRDs).

Table 218: show xsm status Field Descriptions

Field	Description
XSM privilege configuration level	XSM configuration privilege level.
XSM privilege monitor level	XSM monitor privilege level.
Number of XSM Sessions	Total number of concurrent XSM sessions.
Session ID	Specific XSM session number.
XSM Client	Version and IP address of the XSM client.
Connected since	Start time for each session connection to the XSM server.
List of subscribed xrds	Details XRDs available from the XSM server (see **show xsm xrd-list** command for complete list of XRDs).

Related Commands

Command	Description
clear xsm	Clears XSM client sessions.
show xsm xrd-list	Displays all XRDs for clients subscribed to the XSM server.
xsm	Enables XSM client access to the router.
xsm privilege configuration level	Enables configuration privilege level to subscribe to XRDs.
xsm privilege monitor level	Enables monitor privilege level to subscribe to XRDs.

show xsm xrd-list

To display all XML Request Descriptors (XRDs) for XML Subscription Manager (XSM) clients (such as the VPN Device Manager [VDM]) made available by subscription to the XSM server and to identify the required privilege levels, use the **show xsm xrd-list** command in privileged EXEC mode.

show xsm xrd-list

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(6)E	This command was introduced.
12.2(9)YE	This command was integrated into Cisco IOS Release 12.2(9)YE.
12.2(9)YO1	This command was integrated into Cisco IOS Release 12.2(9)YO1.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to display the XRD version and minimum privilege level and type (configuration or monitor) required to view each XRD.

Examples

The following example shows some active XRDs on the XSM server. The end of each line displays the following:

- XRD version number.
- XRD privilege type (configuration or monitor), indicating the privilege level required.

This example displays all available XRDs because both relevant commands (**xsm edm** and **xsm vdm**) have been configured. However, if one command is not configured, only an abbreviated XRD list will appear.

```
Router# show xsm xrd-list

List of all available xrds:
0 ) vlan-db                                 v1.0  privilege=configuration
1 ) entity                                  v1.0  privilege=configuration
2 ) ip                                      v1.0  privilege=configuration
3 ) ios-users                               v1.0  privilege=configuration
4 ) device-about                            v1.0  privilege=monitor
```

```
5 ) ios-image                                v1.0  privilege=configuration
6 ) if-stats                                 v1.0  privilege=monitor
7 ) if-list                                  v1.0  privilege=configuration
8 ) device-health                            v1.0  privilege=monitor
9 ) time                                     v1.0  privilege=monitor
10) access-lists                             v1.0  privilege=configuration
11) ike-topn-tunnels-by-traffic              v1.0  privilege=monitor
12) ike-topn-tunnels-by-errors               v1.0  privilege=monitor
13) ike-topn-tunnels-by-duration             v1.0  privilege=monitor
14) ike-stats                                v1.0  privilege=monitor
15) ike                                      v1.0  privilege=configuration
16) certificate-authorities                  v1.0  privilege=configuration
17) ipsec-topn-tunnels-by-traffic            v1.0  privilege=monitor
18) ipsec-topn-tunnels-by-errors             v1.0  privilege=monitor
19) ipsec-topn-tunnels-by-duration           v1.0  privilege=monitor
20) ipsec-stats                              v1.0  privilege=monitor
21) crypto-maps                              v1.0  privilege=configuration
22) ipsec                                    v1.0  privilege=configuration
23) vdm-history                              v1.0  privilege=configuration
24) gre-tunnels                              v1.0  privilege=monitor
end list.
```

The table below describes (in alphabetical order) typical XRDs shown in the display.

Table 219: show xsm xrd-list Field Descriptions

Field	Descriptions
access-lists	IOS access control list (ACL) configuration.
certificate-authorities	IOS certificate authority (CA) configuration.
crypto-maps	IOS Crypto Map configuration.
device-about	General network device information.
device-health	General network device health statistics.
edm-history	Selected, historical statistics related to general embedded device management. (This field is not shown in the example above.)
entity	Summary of all physical and logical entities within a device.
gre-tunnels	All current GRE tunnels and respective statistics.
if-list	List of all interfaces and their respective IOS configurations.
if-stats	Statistics for all interfaces and their respective IOS configurations.
ike	IOS Internet Key Exchange (IKE) configuration.
ike-stats	Statistics related to IKE.
ike-topn-tunnels-by-duration	Top 10 IKE tunnels by duration (time).
ike-topn-tunnels-by-errors	Top 10 IKE tunnels by errors.
ike-topn-tunnels-by-traffic	Top 10 IKE tunnels by traffic volume.

Field	Descriptions
ios-image	Information about the current running IOS image.
ios-users	Local IOS user configuration.
ip	IOS IP configuration statistics.
ipsec	IOS IPSec configuration.
ipsec-stats	Interface name and IPSec input and output statistics including: number of packets, dropped packets, octets and errors.
ipsec-topn-tunnels-by-duration	Top 10 IPSec tunnels by duration.
ipsec-topn-tunnels-by-errors	Top 10 IPSec tunnels by errors.
ipsec-topn-tunnels-by-traffic	Top 10 IPSec tunnels by traffic.
time	Device's clock reading in UTC.
vdm-history	Selected, historical VPN-related statistics.
vlan-db	VLAN database configuration (switches only).
xsm-session	Status of the current XSM session and related subscriptions. (This field is not shown in the example above.)

Related Commands

Command	Description
clear xsm	Clears XSM client sessions.
show xsm status	Displays information and status about clients subscribed to the XSM server.
xsm	Enables XSM client access to the router.
xsm privilege configuration level	Enables configuration privilege level to subscribe to XRDs.
xsm privilege monitor level	Enables monitor privilege level to subscribe to XRDs.

show zone security

To display zone security information, use the **show zone security**command in user EXEC or privileged EXEC mode.

show zone security [*security-zone-name*]

Syntax Description

security-zone-name	(Optional) The security zone name.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.4(24)T	This command was introduced in a release earlier than Cisco IOS Release 12.4(24)T.
Cisco IOS 2.1 XE	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

Use this command to display zone security information.

Examples

The following is sample output from the **show zone security**command. The fields are self-explanatory.

```
Router# show zone security
zone self
Description: System defined zone
```

show zone-pair security

To display the source zone, destination zone, and policy attached to the zone-pair, use the **show zone-pair security** command in privileged EXEC mode. To disable the display, use the **no** form of this command.

show zone-pair security [**source** *source-zone-name*] [**destination** *destination-zone-name*]
no show zone-pair security [**source** *source-zone-name*] [**destination** *destination-zone-name*]

Syntax Description

source *source-zone-name*	(Optional) Name of the source zone.
destination *destination-zone-name*	(Optional) Name of the destination zone.

Command Default

If you do not specify a source or destination zone, the system displays all the zone-pairs for the source, destination, and the associated policy.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.4(6)T	This command was introduced.

Examples

The following example displays the source zone, destination zone, and policy attached to the zone-pair:

```
Router# show zone-pair security source z1 destination z2
zone-pair name zp
  Source-Zone z1  Destination-Zone z2
  service-policy p1
```

The table below describes the significant fields shown in the display.

Table 220: show zone-pair security Field Descriptions

Field	Description
zone-pair name	Name of the zone-pair.
Source-Zone	Name of the source zone.
Destination-Zone	Name of the destination zone.
service-policy	Name of the service policy.

shutdown (firewall)

To shut down a group manually, use the **shutdown**command in redundancy application group configuration mode. To enable a redundancy group, use the **no** form of this command.

shutdown
no shutdown

Syntax Description

This command has no arguments or keywords.

Command Default

The group is active.

Command Modes

Redundancy application group configuration (config-red-app-grp)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Usage Guidelines

When a group is shut down, it does not participate in the role negotiation. The group remains in the shutdown state until you execute the **no shutdown**command.

Examples

The following example shows how to shut down a group named group1:

```
Router# configure terminal
Router(config)# redundancy
Router(config-red)# application redundancy
Router(config-red-app)# group 1
Router(config-red-app-grp)# shutdown
```

Related Commands

Command	Description
application redundancy	Enters redundancy application configuration mode.
group(firewall)	Enters redundancy application group configuration mode.
name	Configures the redundancy group with a name.
preempt	Enables preemption on the redundancy group.

shutdown (cs-server)

To allow a certificate server to be disabled without removing the configuration, use the **shutdown**command in certificate server configuration mode. To reenable the certificate server, use the **no** form of this command.

shutdown
no shutdown

Syntax Description

This command has no arguments or keywords.

Command Default

no shutdown

Command Modes

Certificate server configuration (cs-server)

Command History

Release	Modification
12.3(4)T	This command was introduced.

Usage Guidelines

You must configure the **crypto pki server** command with the name of the certificate server in order to enter certificate server configuration mode and configure this command.

You should issue the **no shutdown** command only after you have completely configured your certificate server.

The **shutdown** command disables the certificate server. If you prefer to disable simple certificate enrollment protocol (SCEP) but still want the certificate server for manual certificate enrollment, use the **no ip http server** command.

Examples

To ensure that the specified URL is working correctly, configure the **database url** command before you issue the **no shutdown** command on the certificate server for the first time. If the URL is broken, you will see output as follows:

```
Router(config)# crypto pki server mycs
Router(cs-server)# database url ftp://myftpserver
Router(cs-server)# no shutdown
% Once you start the server, you can no longer change some of
% the configuration.
Are you sure you want to do this? [yes/no]: yes

Translating "myftpserver"
% Failed to generate CA certificate - 0xFFFFFFFF
% The Certificate Server has been disabled.
```

Related Commands

Command	Description
auto-rollover	Enables the automated CA certificate rollover functionality.
cdp-url	Specifies a CDP to be used in certificates that are issued by the certificate server.

Command	Description
crl (cs-server)	Specifies the CRL PKI CS.
crypto pki server	Enables a CS and enters certificate server configuration mode, or immediately generates shadow CA credentials
database archive	Specifies the CA certificate and CA key archive format--and the password--to encrypt this CA certificate and CA key archive file.
database level	Controls what type of data is stored in the certificate enrollment database.
database url	Specifies the location where database entries for the CS is stored or published.
database username	Specifies the requirement of a username or password to be issued when accessing the primary database location.
default (cs-server)	Resets the value of the CS configuration command to its default.
grant auto rollover	Enables automatic granting of certificate reenrollment requests for a Cisco IOS subordinate CA server or RA mode CA.
grant auto trustpoint	Specifies the CA trustpoint of another vendor from which the Cisco IOS certificate server automatically grants certificate enrollment requests.
grant none	Specifies all certificate requests to be rejected.
grant ra-auto	Specifies that all enrollment requests from an RA be granted automatically.
hash (cs-server)	Specifies the cryptographic hash function the Cisco IOS certificate server uses to sign certificates issued by the CA.

Command	Description
issuer-name	Specifies the DN as the CA issuer name for the CS.
lifetime (cs-server)	Specifies the lifetime of the CA or a certificate.
mode ra	Enters the PKI server into RA certificate server mode.
mode sub-cs	Enters the PKI server into sub-certificate server mode
redundancy (cs-server)	Specifies that the active CS is synchronized to the standby CS.
serial-number (cs-server)	Specifies whether the router serial number should be included in the certificate request.
show (cs-server)	Displays the PKI CS configuration.

single-connection

To enable all TACACS packets to be sent to the same server using a single TCP connection, use the **single-connection**command in TACACS+ server configuration mode. To disable this feature, use the **no** form of this command.

single-connection
no single-connection

Syntax Description

This command has no arguments or keywords.

Command Default

TACACS packets are not sent on a single TCP connection.

Command Modes

TACACS+ server configuration (config-server-tacacs)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.

Usage Guidelines

Use the **single-connection** command to multiplex all TACACS packets to the same server over a single TCP connection.

Examples

The following example shows how to multiplex all TACACS packets over a single TCP connection to the TACACS server:

```
Router (config)# tacacs server server1
Router(config-server-tacacs)# single-connection
```

Related Commands

Command	Description
tacacs server	Configures the TACACS+ server for IPv6 or IPv4 and enters config server tacacs mode.

signature

To specify a signature for which the command-line interface (CLI) user tunings will be changed, use the **signature** command in signature-definition-signature (config-sigdef-sig) configuration mode. To remove the CLI user tunings and revert to the default values, use the **no** version of this command.

signature *signature-id* [*subsignature-id*]
no signature *signature-id* [*subsignature-id*]

Syntax Description

signature-id subsignature-id	Signature number. If a subsignature is not specified, the default is 0. For example, if signature 1105 is specified without a subsignature, the router will interpret the signature as 1105:0.

Command Default

Default signature parameters cannot be changed.

Command Modes

Signature-definition-signature configuration (config-sigdef-sig)

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Use the **signature** command to specify a signature whose CLI user tunings are to be customized. Thereafter, you can begin to specify which signature parameters (user tunings) are to be changed.

Examples

The following example shows how to modify signature 5081/0 to "produce alert" and "reset tcp connection":

```
Router(config)# ip ips signature-definition
Router(config-sigdef-sig)# signature 5081 0
Router(config-sigdef-action)# engine
Router(config-sigdef-action-engine)# event-action produce-alert reset-tcp-connection
Router(config-sigdef-action-engine)# ^Z
Do you want to accept these changes:[confirmm]y
```

Related Commands

Command	Description
ip ips signature-definition	Enters signature-definition-signature configuration mode, which allows you to define a signature for CLI user tunings.

slave (IKEv2 cluster)

To define settings for subordinate gateways in an Internet Key Exchange Version 2 (IKEv2) cluster, use the **slave** command in IKEv2 cluster configuration mode. To restore the default settings, use the **no** form of this command.

slave {**hello** *milliseconds* | **max-session** *number* | **priority** *number* | **update** *milliseconds*}
no slave {**hello** | **max-session** | **priority** | **update**}

Syntax Description

hello *milliseconds*	Specifies the hello interval, in milliseconds, for a subordinate gateway. The range is from 100 to 30000. The default is 1000.
max-session *number*	Specifies the maximum number of security associations (SA) allowed on a subordinate gateway. The range is from 1 to 100000. **Note** This keyword is mandatory.
priority *number*	Specifies the priority of the subordinate gateway. The range is from 1 to 100. The default is 100.
update *milliseconds*	Specifies the interval, in milliseconds, between two update messages for a subordinate gateway. The range is from 100 to 60000. The default is 3000.

Command Default

The default subordinate settings are used.

Command Modes

IKEv2 cluster configuration (config-ikev2-cluster)

Command History

Release	Modification
15.2(4)M	This command was introduced.

Usage Guidelines

You must enable the **crypto ikev2 cluster** command before enabling the **slave** command.

Examples

The following example shows how to set the priority setting to 90 for the IKEv2 subordinate gateway:

```
Device(config)# crypto ikev2 cluster
Device(config-ikev2-cluster)# slave priority 90
```

Related Commands

Command	Description
crypto ikev2 cluster	Defines an IKEv2 cluster policy in an HSRP cluster.

smart-tunnel list

To configure the smart tunnel list and enable it within a policy group, use the **smart-tunnel list** command in WebVPN context configuration mode or WebVPN group policy configuration mode. To disable the smart tunnel configuration, use the **no** form of this command.

smart-tunnel list *name*
no smart-tunnel list

Syntax Description

name	Smart tunnel list name.

Command Default

No smart tunnel list is created and enabled.

Command Modes

WebVPN context configuration mode (config-webvpn-context)
WebVPN group policy configuration mode (config-webvpn-group)

Command History

Release	Modification
15.1(3)T	This command was introduced.

Usage Guidelines

Before a smart tunnel list can be enabled within a group policy, it must be created. Applications that are to be directed to the smart tunnel then must be specified within the list. This list must later be applied to the group policy.

Note To remove a smart tunnel list, first use the **no smart-tunnel list** command in WebVPN group policy configuration mode, and then use the **no smart-tunnel list**command in WebVPN context configuration mode.

Examples

The following example shows how to create a smart tunnel list named "st1" and configure the applications for smart tunneling:

```
Router(config)# webvpn context sslgw
Router(config-webvpn-context)# smart-tunnel list st1
Router(config-webvpn-smart-tunnel)# appl ie ieexplore.exe windows
Router(config-webvpn-smart-tunnel)# appl telnet telnet.exe windows
```

The following example shows how to enable the smart tunnel list "st1" within a group policy:

```
Router(config)# webvpn context sslgw
Router(config-webvpn-context)# policy group new
Router(config-webvpn-group)# smart-tunnel list st1
```

Related Commands

Command	Description
webvpn context	Configures the SSL VPN context.

Command	Description
app (webvpn)	Configures applications to access smart tunnel.

smartcard-removal-disconnect

To terminate a session on removing the smart card, use the **smarcard-removal-disconnect** command in IKEv2 authorization policy configuration mode. To disable session termination, use the **no** form of this command.

smartcard-removal-disconnect

Syntax Description

This command has no arguments or keywords

Command Default

The session is not terminated.

Command Modes

IKEv2 authorization policy configuration (config-ikev2-author-policy)

Command History

Release	Modification
15.2(1)T	This command was introduced.

Usage Guidelines

Before using this command, you must first configure the **crypto ikev2 authorization policy** command. The parameter set by this command is sent to the client via the nonstandard Cisco unity configuration attribute. This command specifies that the client should terminate the session on removing the smart card.

Examples

The following example show how to configure the smartcard-removal-disconnect command:

```
Router(config)# crypto ikev2 authorization policy policy1
Router(config-ikev2-profile)# smartcard-removal-disconnect
```

Related Commands

Command	Description
crypto ikev2 authorization policy	Specifies an IKEv2 authorization policy.

snmp-server enable traps gdoi

To enable Group Domain of Interpretation (GDOI) Simple Network Management Protocol (SNMP) notifications for Cisco Group Encrypted Transport VPN (GET VPN), use the **snmp-server enable traps gdoi** command in global configuration mode. To disable GDOI SNMP notifications, use the **no** form of this command.

snmp-server enable traps
gdoi [*notification-type*]
no snmp-server enable traps
gdoi [*notification-type*]

Syntax Description

notification-type	(Optional) Specifies the particular SNMP notifications to be enabled. If you use the command without keywords, all GDOI notifications are enabled. You can specify any combination of the following types in any order: • **gm-incomplete-cfg**—A group member (GM) sent an error notification because of a missing configuration. • **gm-re-register**—A GM began the reregistration process with a key server (KS.) • **gm-registration-complete**—A GM completed registration to a KS. • **gm-rekey-fail**—A GM sent an error notification because it cannot process and install a rekey. • **gm-rekey-rcvd**—A rekey message was received by a GM. • **gm-start-registration**—A GM first sent a registration request to a KS. • **ks-new-registration**—A KS first received a registration request from a GM. • **ks-no-rsa-keys**—An error notification was received from a KS because of missing RSA keys. • **ks-reg-complete**—A GM completed registration to a KS. • **ks-rekey-pushed**—A rekey message was sent by the KS.

Command Default

No GDOI SNMP notifications are enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(1)T	This command was introduced.
Cisco IOS XE Release 3.8S	This command was integrated into Cisco IOS XE Release 3.8S.

Usage Guidelines

This command configures notifications for RFC 3547, *The Group Domain of Interpretation*; it supports only the objects related to the GDOI MIB IETF standard.

The GDOI MIB consists of objects and notifications that include information about GDOI groups, GM and KS peers, and the policies that are created or downloaded. Only “get” operations are supported by the GDOI MIB.

The command configures two kinds of notifications—those generated by the KS and those generated by each GM.

For more information about GDOI MIB support for GET VPN, see the *Cisco Group Encrypted Transport VPN Configuration Guide.*.

For a complete description of the notification types and additional MIB functions, refer to the CISCO-GDOI-MIB.my file.

Examples

The following example shows how to enable GDOI MIB notifications for when a GM begins the reregistration process with a KS and when a GM completes registration to a KS:

```
Device(config)# snmp-server enable traps gdoi gm-re-register gm-registration-complete
```

The following example shows how to enable the GDOI MIB notification for when a GM sends an error notification because it cannot process and install a rekey:

```
Device(config)# snmp-server enable traps gdoi gm-rekey-fail
```

The following example shows how to enable GDOI MIB notifications for when a KS first receives a registration request from a GM and a group member completes registration to the KS:

```
Device(config)# snmp-server enable traps gdoi ks-new-registration ks-reg-complete
```

The following example shows how to enable the GDOI MIB notification for when an error is received from the KS because of missing RSA keys:

```
Device(config)# snmp-server enable traps gdoi ks-no-rsa-keys
```

Related Commands

Command	Description
snmp-server community	Specifies the community access string to define the relationship between the SNMP manager and the SNMP agent to permit access to SNMP.
snmp-server host	Specifies the recipient (host) of an SNMP notification operation.

snmp-server enable traps ipsec

To enable the router to send IP Security (IPSec) Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps ipsec**command in global configuration mode. To disable IPSec SNMP notifications, use the **no**form of this command.

snmp-server enable traps ipsec [{**cryptomap** [{**add** | **delete** | **attach** | **detach**}] | **tunnel** [{**start** | **stop**}] | **too-many-sas**}]
no snmp-server enable traps ipsec [{**cryptomap** [{**add** | **delete** | **attach** | **detach**}] | **tunnel** [{**start** | **stop**}] | **too-many-sas**}]

Syntax Description

cryptomap add	(Optional) Notifications for cipsCryptomapAdded { cipsMIBNotifications 3 } events are generated, as defined in the CISCO-IPSEC-MIB. These notifications are generated when a new cryptomap is added to the specified cryptomap set.
cryptomap delete	(Optional) Notifications for cipsCryptomapDeleted { cipsMIBNotifications 4 } events are generated, as defined in the CISCO-IPSEC-MIB. These notifications are generated when a cryptomap is removed from the specified cryptomap set.
cryptomap attach	(Optional) Notifications for cipsCryptomapSetAttached { cipsMIBNotifications 5 } events are generated, as defined in the CISCO-IPSEC-MIB. These notifications are generated when a cryptomap set is attached to an active interface of the managed entity.
cryptomap detach	(Optional) Notifications for cipsCryptomapSetDetached { cipsMIBNotifications 6 } events are generated, as defined in the CISCO-IPSEC-MIB. These notifications are generated when a cryptomap set is detached from an interface to which it was previously bound.
tunnel start	(Optional) Notifications for cipSecTunnelStart { cipSecMIBNotifications 7 } events are generated, as defined in the CISCO-IPSEC-FLOW-MONITOR-MIB. These notifications are generated when an IPsec Phase-2 Tunnel becomes active.
tunnel stop	(Optional) Notifications for cipSecTunnelStop { cipSecMIBNotifications 8 } events are generated, as defined in the CISCO-IPSEC-FLOW-MONITOR-MIB. These notifications are generated when an IPsec Phase-2 Tunnel becomes inactive.
too-many-sas	(Optional) Notifications for cipsTooManySAs { cipsMIBNotifications 7 } events are generated, as defined in the CISCO-IPSEC-MIB.my. These notifications are generated when an attempt to make a new security association (SA) is made but there is insufficient memory on the device.

Command Default

SNMP notifications are disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.

Release	Modification
12.1(11b)E	This command was integrated into Cisco IOS Release 12.1(11b)E.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both traps and inform requests.

A cryptomap is a table that maps an IPSec Phase-2 tunnel to the corresponding IPSec Policy element.

For a complete description of the notification types and additional MIB functions, refer to the CISCO-IP-SEC.my and CISCO-IPSEC-FLOW-MONITOR-MIB.my files, available on Cisco.com through:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

The **snmp-server enable traps ipsec** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send SNMP notifications, you must configure at least one **snmp-server host** command.

Examples

In the following example, the router is configured to send IPSec MIB inform notifications to the host nms.cisco.com using the community string named "public":

```
snmp-server enable traps ipsec
snmp-server host nms.cisco.com informs public ipsec
```

Related Commands

Command	Description
snmp-server enable traps isakmps	Controls the sending of (ISAKMP) SNMP notifications
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server trap-source	Specifies the interface that an SNMP trap should originate from.

snmp-server enable traps isakmp

To enable the router to send IP Security (IPSec) Internet Security Association and Key Exchange Protocol (ISAKMP) Simple Network Management Protocol (SNMP) notifications, use the **snmp-server enable traps isakmp**command in global configuration mode. To disable ISAKMP IPSec SNMP notifications, use the **no**form of this command.

snmp-server enable traps isakmp [{**policy** {**add** | **delete**} | **tunnel** {**start** | **stop**}}]
no snmp-server enable traps isakmp [{**policy** {**add** | **delete**} | **tunnel** {**start** | **stop**}}]

Syntax Description

policy add	(Optional) Notifcations for cipsIsakmpPolicyAdded { cipsMIBNotifications 1 } events are generated, as defined in the CISCO-IPSEC-MIB. These notifications are generated when a new ISAKMP policy element is defined on the managed entity. The context of the event includes the updated number of ISAKMP policy elements currently available.
policy delete	(Optional) Notifcations for cipsIsakmpPolicyDeleted { cipsMIBNotifications 2 } events are generated, as defined in the CISCO-IPSEC-MIB. These notifications are generated when an existing ISAKMP policy element is deleted on the managed entity. The context of the event includes the updated number of ISAKMP policy elements currently available.
tunnel start	(Optional) Notifications for cikeTunnelStart { cipSecMIBNotifications 1 } events are generated, as defined by in the CISCO-IPSEC-FLOW-MONITOR-MIB.my. These notifications are generated when an IPsec Phase-1 IKE Tunnel becomes active.
tunnel stop	(Optional) Notifications for cikeTunnelStop { cipSecMIBNotifications 2 } events are generated, as defined by in the CISCO-IPSEC-FLOW-MONITOR-MIB.my. These notifications are generated when an IPsec Phase-1 IKE Tunnel becomes inactive.

Command Default

SNMP notifications are disabled by default.

If no keywords are specified, all available ISAKMP traps are enabled (or disabled if the **no** form is used).

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.1(11b)E	This command was integrated into Cisco IOS Release 12.1(11b)E
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

SNMP notifications can be sent as traps or inform requests. This command enables both ISAKMP trap and inform requests.

For a complete description of these notifications and additional MIB functions, refer to the CISCO-IPSEC-MIB.myand CISCO-IPSEC-FLOW-MONITOR-MIB.my files, available on Cisco.com through:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

The **snmp-server enable traps isakmp** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send SNMP notifications, you must configure at least one **snmp-server host** command.

Examples

In the following example, the router is configured to send IPSec MIB inform notifications to the host nms.cisco.com using the community string named "public":

```
snmp-server enable traps isakmp
snmp-server host nms.cisco.com informs public ipsec
```

Related Commands

Command	Description
snmp-server host	Specifies the recipient of an SNMP notification operation.
snmp-server trap-source	Specifies the interface that an SNMP trap should originate from.

snmp-server enable traps nhrp

To enable Simple Network Management Protocol (SNMP) notifications for the Next Hop Resolution Protocol (NHRP), use the **snmp-server enable traps nhrp** command in global configuration mode. To disable SNMP NHRP notifications, use the **no** form of this command.

snmp-server enable traps nhrp [{**nhc** [{**down** | **up**}] | **nhp** [{**down** | **up**}] | **nhs** [{**down** | **up**}] | **quota-exceeded**}]
no snmp-server enable traps nhrp [{**nhc** [{**down** | **up**}] | **nhp** [{**down** | **up**}] | **nhs** [{**down** | **up**}] | **quota-exceeded**}]

Syntax Description

nhc	(Optional) Enables Next Hop Client (NHC) notifications.
down	(Optional) Enables notifications for when the client, peer, or server interface is declared 'down'.
up	(Optional) Enables notifications for when the client, peer, or server interface is declared 'up'.
nhp	(Optional) Enables Next Hop Peer (NHP) notifications.
nhs	(Optional) Enables Next Hop Server (NHS) notifications.
quota-exceeded	(Optional) Enables notifications for when the rate limit set on NHRP packets is exceeded on the interface.

Command Default

No notifications (traps) are enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

By default all notifications (traps) are disabled. You must explicitly enable any notifications that you need in your system. After you enable traps in your system, you can use the **snmp-server host traps** command to control which traps are sent to a particular trap receiver.

The **snmp-server host traps nhrp** command enables the default NHRP traps only (it does not enable all NHRP traps). The default traps include the NHS, NHC, and quota-exceeded traps.

Examples

The following example shows how to enable the default NHRP traps, and how to send these NHRP traps to the notification receiver with the IP address 192.40.3.130 using the community string public:

```
Router(config)# snmp-server enable traps nhrp
Router(config)# snmp-server host 192.40.3.130 traps version 2c public nhrp
```

The following example shows how to disable NHC traps and enable rate limit traps:

```
Router(config)# no snmp-server enable traps nhrp nhc
Router(config)# snmp-server enable traps nhrp quota-exceeded
```

Related Commands

Command	Description
debug snmp mib nhrp	Displays messages about the SNMP NHRP MIB.
snmp-server host	Specifies the recipient of an SNMP notification operation.

snmp trap ip verify drop-rate

To configure the router to send a Simple Network Management Protocol (SNMP) notification when the Unicast Reverse Path Forwarding (RPF) drop rate exceeds the configured threshold, use the **snmp trap ip verify drop-rate**command in interface configuration mode. To disable SNMP notification, use the **no** form of this command.

snmp trap ip verify drop-rate
no snmp trap ip verify drop-rate

Syntax Description

This command has no arguments or keywords.

Command Default

No SNMP notifications are sent.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(31)SB2	This command was introduced.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
12.2(33)SXI2	This command was integrated into Cisco IOS Release 12.2(33)SXI2.

Usage Guidelines

This command enables cipUrpfIfDropRateNotify notification. This notification is sent when the Unicast RPF drop rate exceeds the threshold.

Examples

The following example shows how to configure SNMP notification for the Unicast RPF drop rate on Ethernet interface 3/0:

```
Router> enable
Router# configure terminal
Router(config)# interface ethernet 3/0
Router(config-if)# snmp trap ip verify drop-rate
```

Related Commands

Command	Description
ip verify drop-rate compute window	Configures the interval of time over which the Unicast RPF drop count used in the drop rate computation is collected.
ip verify unicast notification threshold	Configures the Unicast RPF drop count threshold which, when exceeded, triggers a notification.

source

To sequentially number the source address, use the **source** command in IKEv2 FlexVPN client profile configuration mode. To remove the sequence, use the **no** form of this command.

source *sequence interface* **track** *track-number*
no source *sequence*

Syntax Description

sequence	Assigns a sequence number.
interface	Interface type and number.
track *track-number*	Tracks the source address with a track number.

Command Default

The track status is always up.

Command Modes

IKEv2 FlexVPN client profile configuration (config-ikev2-flexvpn)

Command History

Release	Modification
15.2(1)T	This command was introduced.
Cisco IOS XE Release 3.7S	This command was integrated into Cisco IOS XE Release 3.7S.

Usage Guidelines

Before you enable this command, you must configure the **crypto ikev2 client flexvpn** command.

The source address is the one with the lowest sequence number for which track object is in the UP state only if the source IP address is available in the tunnel VRF of the tunnel interface. If a session is UP for a source, the source is said to be a "Current active source".

Note Any changes to this command terminates the active session.

Examples

The following example shows how to define a static peer:

```
Router(config)# crypto ikev2 client flexvpn client1
Router(config-ikev2-flexvpn)# source 1 Ethernet 0/1 track 11
```

Related Commands

Command	Description
crypto ikev2 client flexvpn	Defines an IKEv2 FlexVPN client profile.

source interface

To specify the address of an interface to be used as the source address for all outgoing TCP connections associated with a trustpoint, use the **source interface** command in ca-trustpoint configuration mode. To disable the interface that was specified, use the **no** form of this command.

source interface *interface-name*
no source interface *interface-name*

Syntax Description

interface-name	Interface address to be used as the source address for all outgoing TCP connections associated with a trustpoint.

Command Default

If this command is not specified, the address of the outgoing interface is used.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.

Usage Guidelines

This command must be used following the **crypto ca trustpoint** command. If this command is used and the address of the outgoing interface is specified, the router uses the specified address (or address of the specified interface) as the source address for any datagrams that are sent to the certification authority (CA) server or Lightweight Directory Access Protocol (LDAP) server during authentication, enrollment, and if appropriate, when obtaining certificate revocation lists (CRLs).

Examples

In the following example, the router is located in a branch office. The router uses IP Security (IPSec) to communicate with the main office. Ethernet 1 is the "outside" interface that connects to the Internet Service Provider (ISP). Ethernet 0 is the interface connected to the LAN of the branch office. To access the CA server located in the main office the router needs to send its IP datagrams out interface Ethernet 1 (address 10.2.2.205) using the IPSec tunnel. Address 10.2.2.205 is assigned by the ISP. Address 10.2.2.205 is not a part of the branch office or main office.

The CA cannot access any address outside the company because of a firewall. The CA sees a message coming from 10.2.2.205 and cannot respond (that is, it does not know that the router is located in a branch office at address 10.1.1.1, which it is able to reach).

Adding the **source interface** command tells the router to use address 10.1.1.1 as the source address of the IP datagram that it sends to the CA. The CA is able to respond to 10.1.1.1.

This scenario is configured using the **source interface** command and the interface addresses as described above.

```
crypto ca trustpoint ms-ca
 enrollment url http://yourname:80/certsrv/mscep/mscep.dll
 source interface ethernet0
!
```

```
interface ethernet 0
 description inside interface
 ip address 10.1.1.1 255.255.255.0
!
interface ethernet 1
 description outside interface
 ip address 10.2.2.205 255.255.255.0
 crypto map main-office
```

Related Commands

Command	Description
crypto ca trustpoint	Declares the CA that your router should use.

source interface (ca-trustpool)

To specify the source interface to be used for certificate revocation list (CRL) retrieval, online certificate status protocol (OCSP) status, or the downloading of a certificate authority (CA) certificate bundle for the public key infrastructure (PKI) trustpool, use the **source interface** command in ca-trustpool configuration mode. To disable the interface that was specified, use the **no** form of this command.

source interface *name number*
no source interface *name number*

Syntax Description

interface-name	Interface type used as the source address for the PKI trustpool.
interface	Interface number or slot and port of this interface.

Command Default

No source interface is specified.

Command Modes

Ca-trustpool configuration (ca-trustpool)

Command History

Release	Modification
15.2(2)T	This command was introduced.
15.1(1)SY	This command was integrated into Cisco IOS 15.1(1)SY.

Usage Guidelines

Before you can configure this command, you must enable the **crypto pki trustpool policy** command, which enters ca-trustpool configuration mode.

Examples

```
Router(config)# crypto pki trustpool policy
Router(ca-trustpool)# source interface tunnel 1
```

Related Commands

Command	Description
cabundle url	Configures the URL from which the PKI trustpool CA bundle is downloaded.
chain-validation	Enables chain validation from the peer's certificate to the root CA certificate in the PKI trustpool.
crl	Specifes the CRL query and cache options for the PKI trustpool.
crypto pki trustpool import	Manually imports (downloads) the CA certificate bundle into the PKI trustpool to update or replace the existing CA bundle.

Command	Description
crypto pki trustpool policy	Configures PKI trustpool policy parameters.
default	Resets the value of a ca-trustpool configuration command to its default.
match	Enables the use of certificate maps for the PKI trustpool.
ocsp	Specifies OCSP settings for the PKI trustpool.
revocation-check	Disables revocation checking when the PKI trustpool policy is being used.
show	Displays the PKI trustpool policy of the router in ca-trustpool configuration mode.
show crypto pki trustpool	Displays the PKI trustpool certificates of the router and optionally shows the PKI trustpool policy.
source interface	Specifies the source interface to be used for CRL retrieval, OCSP status, or the downloading of a CA certificate bundle for the PKI trustpool.
storage	Specifies a file system location where PKI trustpool certificates are stored on the router.
vrf	Specifies the VRF instance to be used for CRL retrieval.

source interface (Diameter peer)

To configure the interface to be used for the Diameter peer connection, use the **source interface** command in Diameter peer configuration mode. To disable the interface configuration, use the **no** form of this command.

source interface interface
no source interface interface

Syntax Description

interface	Source address and port that initiate the TCP connection to the peer.

Command Default

No source interface is defined.

Command Modes

Diameter peer configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

The Diameter client uses the configured source address and port to initiate a TCP connection to the Diameter peer.

Examples

The following example shows how to configure a source address and port on the Diameter client:

```
Router (config-dia-peer)# source interface
 interface_01
```

Related Commands

Command	Description
diameter peer	Configures a Diameter peer and enters Diameter peer configuration submode.
show diameter peer	Displays the Diameter peer configuration.

source-interface (URL parameter-map)

To specify the interface whose IP address will be used as the source IP address while making a TCP connection to the URL filter server, use the **source-interface** command in URL parameter-map configuration mode. To stop using the IP address of the specified interface, use the **no** form of this command.

source-interface *interface-name*
no source-interface *interface-name*

Syntax Description

interface-name	Name of the interface.

Command Default

None

Command Modes

URL parameter-map configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

When you are creating or modifying a URL parameter map, you can enter the **source-interface** subcommand after you enter the **parameter-map type urlfilter** command.

Examples

The following example specifies that the IP address of Ethernet0 will be used as the source IP address while making a TCP connection to the URL filter server:

```
parameter-map type urlfilter u1
 source-interface ethernet0
```

Related Commands

Command	Description
parameter-map type urlfilter	Creates or modifies a parameter map for URL filtering parameters

source (parameter-map)

To configure the source for Cloud Web Security content scan redirection, use the **source** command in parameter-map type inspect configuration mode. To disable the source for content scan redirection, use the **no** form of this command.

source {**address ipv4** *address* | **interface** *type number*}
no source address ipv4 *address*

Syntax Description

address	Specifies the source address.
ipv4 *address*	Specifies the IPv4 address of the source.
interface	Specifies the interface.
type	Interface type. For more information, use the question mark (?) online help function.
number	Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.

Command Default

A source for content scan redirection is not configured.

Command Modes

Parameter-map type inspect configuration (config-profile)

Command History

Release	Modification
15.2(1)T1	This command was introduced.

Usage Guidelines

The **source** command configures an interface or an IP address as the source from which packets to Cloud Web Security will originate from the device. The IP address that is configured in this command must be the IP addresses that is associated with the interface on which **cws out** command is configured.

Examples

The following example shows how to configure a source for content scan redirection:

```
Device(config)# parameter-map type cws global
Device(config-profile)# source address ipv4 10.1.1.1
```

Related Commands

Command	Description
cws out	Enables Cloud Web Security content scanning on an egress interface.
parameter-map type inspect cws global	Configures a global Cloud Web Security parameter map and enters parameter-map type inspect configuration mode.

split-dns

To specify a domain name that must be tunneled or resolved to the private network, use the **split-dns** command in Internet Security Association Key Management Protocol (ISAKMP) group configuration mode or IKEv2 authorization policy configuration mode. To remove a domain name, use the **no** form of this command.

split-dns *domain-name*
no split-dns *domain-name*

Syntax Description

domain-name	Name of the Domain Name System (DNS) domain that must be tunneled or resolved to the private network.

Command Default

All domain names are resolved via the public DNS server.

Command Modes

ISAKMP group configuration (config-isakmp-group)

IKEv2 authorization policy configuration (config-ikev2-author-policy)

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS 12.2SX family of releases. Support in a specific 12.2SX release is dependent on your feature set, platform, and platform hardware.

Usage Guidelines

If you configure the **split-dns** command, the split-dns attribute will be added to the policy group. The attribute will include the list of domain names that you configured. All other names will be resolved via the public DNS server.

You must enable the **crypto isakmp client configuration group** or **crypto ikev2 authorization policy** command, which specifies group policy information that needs to be defined or changed, before enabling the **split-dns** command.

Note If you have to configure more than one domain name, you have to add a **split-dns** command line for each.

Examples

The following example shows that the domain names "green.com" and "acme.org" will be added to the policy group:

```
Router (config)# crypto isakmp client configuration group cisco
Router (config-isakmp-group)# key cisco
Router (config-isakmp-group)# dns 10.2.2.2 10.2.2.3
Router (config-isakmp-group)# wins 10.6.6.6
Router (config-isakmp-group)# domain cisco.com
Router (config-isakmp-group)# pool green
Router (config-isakmp-group)# acl 199
```

```
Router (config-isakmp-group)# split-dns green.com
Router (config-isakmp-group)# split-dns acme.org
```

Related Commands

Command	Description
acl	Configures split tunneling.
crypto ikev2 authorization policy	Specifies an IKEv2 authorization policy.
crypto isakmp client configuration group	Specifies group policy information that needs to be defined or changed.

ssh

To start an encrypted session with a remote networking device, use the **ssh** command in user EXEC or privileged EXEC mode.

ssh [{**-v** {**1** | **2**} | **-c** {**aes128-ctr** | **aes192-ctr** | **aes256-ctr** | **aes128-cbc** | **3des** | **aes192-cbc** | **aes256-cbc**} | **-l** *user-id* | **-l** *user-id***:***vrf-name number ip-address ip-address* | **-l** *user-id***:***rotary number ip-address* | **-m** {**hmac-md5-128** | **hmac-md5-96** | **hmac-sha1-160** | **hmac-sha1-96**} | **-o** **numberofpasswordprompts** *n* | **-p** *port-num*}] {*ip-addr* | *hostname* [{**command** | **-vrf**}]

Syntax Description

-v	(Optional) Specifies the version of Secure Shell (SSH) to use to connect to the server. • **1**--Connects using SSH Version 1. • **2**--Connects using SSH Version 2.
-c {aes128-ctr | aes192-ctr | aes256-ctr | aes128-cbc | 3des | aes192-cbc | aes256-cbc}	(Optional) Specifies the crypto algorithms Data Encryption Standard (DES), Triple DES (3DES), or Advanced Encryption Standard (AES) to use for encrypting data. AES algorithms are **aes128-ctr**, **aes192-ctr**, **aes256-ctr**, **aes128-cbc**, **aes192-cbc**, and **aes256-cbc**. • To use SSH Version 1, you must have an encryption image running on the device. Cisco software images that include encryption have the designators “k8” (DES) or “k9” (3DES). • SSH Version 2 supports only the following crypto algorithms: **aes128-ctr**, **aes192-ctr**, **aes256-ctr**, **aes128-cbc**, **aes192-cbc**, **aes256-cbc**, and **3des**. SSH Version 2 is supported only in 3DES images. • If you do not specify the **-c** keyword, during negotiation the remote networking device sends all the supported crypto algorithms. • If you configure the**-c** keyword and the server does not support the argument that you have shown (**des**, **3des**, **aes128-ctr**, **aes192-ctr**, **aes256-ctr**, **aes128-cbc**, **aes192-cbc**, or **aes256-cbc**), the remote networking device closes the connection.
-l *user-id*	(Optional) Specifies the user ID to use when logging in on the remote networking device running the SSH server. If no user ID is specified, the default is the current user ID.

-l *user-id* **:** *vrf-namenumber ip-address*	(Optional) Specifies the user ID when configuring reverse SSH by including port information in the *user-id* field. • **:** --Signifies that a VRF name, number, and terminal IP address will follow the user ID. • *vrf-name* --User-specific VRF. • *number* --Terminal or auxiliary line number. • *ip-address* --IP address of the terminal server. **Note** The *user-id* argument and **:** *number ip-address* delimiter and arguments must be used if you are configuring reverse SSH by including port information in the *user-id* field (a method that is easier than the longer method of listing each terminal or auxiliary line on a separate command configuration line).The VRF name allows SSH to establish sessions with hosts whose addresses are in a VRF instance.
-l *user-id* **:rotary** *number ip-address*	(Optional) Specifies that the terminal lines are to be grouped under the rotary group for reverse SSH. • **:rotary** --Signifies that a rotary group number and terminal IP address will follow. • *number* --Terminal or auxiliary line number. • *ip-address* --IP address of the terminal server. **Note** The *user-id* argument and the **:rotary** *number ip-address* delimiter and arguments must be used if you are configuring reverse SSH by including rotary information in the *user-id* field (a process that is easier than the longer process of listing each terminal or auxiliary line on a separate command configuration line).
-m {**hmac-md5-128** | **hmac-md5-96** | **hmac-sha1-160** | **hmac-sha1-96**}	(Optional) Specifies a Hashed Message Authentication Code (HMAC) algorithm. • SSH Version 1 does not support HMACs. • If you do not specify the **-m** keyword, the remote device sends all the supported HMAC algorithms during negotiation. If you specify the **-m** keyword and the server does not support the algorithm that you have shown (**hmac-md5-128**, **hmac-md5-96**, **hmac-sha1-160**, and **hmac-sha1-96**), the remote device closes the connection.
-o numberofpasswordprompts *n*	(Optional) Specifies the number of password prompts that the software generates before ending the session. The SSH server may also apply a limit to the number of attempts. If the limit set by the server is less than the value specified by the **-o numberofpasswordprompts** keyword, the limit set by the server takes precedence. The default is 3 attempts, which is also the Cisco IOS SSH server default. The range of values is from 1 to 5.

-p *port-num*	(Optional) Indicates the desired port number for the remote host. The default port number is 22.
ip-addr | *hostname*	Specifies the IPv4 or IPv6 address or hostname of the remote networking device.
command	(Optional) Specifies the Cisco IOS command that you want to run on the remote networking device. If the remote host is not running Cisco IOS software, this may be any command recognized by the remote host. If the command includes spaces, you must enclose the command in quotation marks.
-vrf	(Optional) Adds VRF awareness to SSH client-side functionality. The VRF instance name in the client is provided with the IP address to look up the correct routing table and establish a connection.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.2(8)T	This command was modified. Support for IPv6 addresses was added.
12.0(21)ST	This command was modified. IPv6 address support was integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This command was modified. IPv6 address support was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was modified. IPv6 address support was integrated into Cisco IOS Release 12.2(14)S.
12.2(17a)SX	This command was integrated into Cisco IOS Release 12.2(17a)SX.
12.3(7)T	This command was modified to include Secure Shell Version 2 support. The **-c** keyword was expanded to include support for the following cryptic algorithms: aes128-cbc, aes192-cbc, and aes256-cbc. The **-m** keyword was added, with the following algorithms: hmac-md5, hmac-md5-96, hmac-sha1, and hmac-sha1-96. The **-v**keyword and **1** and **2** arguments were added.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.3(11)T	The **-l** *userid***:***number ip-address and* **-l** *userid***:rotary** *number ip-address* keyword and argument options were added.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.3(7)JA	This command was integrated into Cisco IOS Release 12.3(7)JA.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Release	Modification
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	The **-l** *userid***:***vrfname number ip-address* keyword and argument options were added
Cisco IOS XE Release 2.4	This command was integrated into Cisco IOS XE Release 2.4.
15.3(2)S	This command was modified. SSH version 2 supports counter-based AES encryption for 128-, 192-, and 256-bit key length.
Cisco IOS XE Release 3.9S	This command was modified. SSH version 2 supports counter-based AES encryption for 128-, 192-, and 256-bit key length.
15.2(2)SA2	This command was implemented on the Cisco ME 2600X Series Ethernet Access Switches.

Usage Guidelines

The **ssh** command enables a Cisco device to make a secure, encrypted connection to another Cisco device running an SSH Version 1 or Version 2 server. This connection provides functionality that is similar to that of an outbound Telnet connection except that the connection is encrypted. With authentication and encryption, the SSH client allows for a secure communication over an insecure network.

Note SSH Version 1 is supported on DES (56-bit) and 3DES (168-bit) data encryption software images only. In DES software images, DES is the only encryption algorithm available. In 3DES software images, both DES and 3DES encryption algorithms are available.

- SSH Version 2 supports only the following crypto algorithms: aes128-ctr, aes192-ctr, aes256-ctr, aes128-cbc, aes192-cbc, and aes256-cbc. SSH Version 2 is supported only in 3DES images.
- SSH Version 1 does not support HMAC algorithms.

Examples

The following example illustrates the initiation of a secure session between the local device and the remote host HQhost to run the **show users** command. The result of the **show users** command is a list of valid users who are logged in to HQhost. The remote host will prompt for the adminHQ password to authenticate the user adminHQ. If the authentication step is successful, the remote host will return the result of the **show users** command to the local device and will then close the session.

```
Device# ssh -l adminHQ HQhost "show users"
```

The following example illustrates the initiation of a secure session between the local device and the edge device HQedge to run the **show ip route** command. In this example, the edge device prompts for the adminHQ password to authenticate the user. If the authentication step is successful, the edge device will return the result of the **show ip route** command to the local device.

```
Device#ssh -l adminHQ HQedge "show ip route"
```

The following example shows the SSH client using 3DES to initiate a secure remote command connection with the HQedge device. The SSH server running on HQedge authenticates the session

for the admin7 user on the HQedge device using standard authentication methods. The HQedge device must have SSH enabled for authentication to work.

```
Device# ssh -l admin7 -c 3des -o numberofpasswordprompts 5 HQedge
```

The following example shows a secure session between the local device and a remote IPv6 device with the address 2001:DB8:0000:FFFF:FFFF:FFFF:FFFF:FFFF to run the **show running-config** command. In this example, the remote IPv6 device prompts for the adminHQ password to authenticate the user. If the authentication step is successful, the remote IPv6 device will return the result of the **show running-config** command to the local device and will then close the session.

```
Device# ssh -l adminHQ 2001:DB8:0000:FFFF:FFFF:FFFF:FFFF:FFFF "show running-config"
```

The following example shows an SSH Version 2 session using the crypto algorithm aes256-ctr and an HMAC of hmac-sha1-96. The user ID is user2 and the IP address is 10.76.82.24.

```
Device# ssh -v 2 -c aes256-ctr -m hmac-sha1-96 -l user2 10.76.82.24
```

The following example shows how to configure reverse SSH on the SSH client:

```
Device# ssh -l lab:1 device.example.com
```

The following command shows how to connect reverse SSH to the first free line in the rotary group:

```
Device# ssh -l lab:rotary1 device.example.com
```

Related Commands

Command	Description
ip ssh	Configures SSH server control parameters on the device.
show ip route	Displays the contents of the routing table.
show ip ssh	Displays the version and configuration data for SSH.
show running-config	Displays the contents of the running configuration file.
show ssh	Displays the status of SSH server connections.
show users	Displays information about the active lines on a device.

ssid (local RADIUS server group)

To assign up to 20 service set identifiers (SSIDs) to a user group, use the **ssid**command in local RADIUS server group configuration mode. To instruct the access point (AP) to not check if the client has come in on a list of specified SSIDs, use the **no** form of this command.

ssid *ssid-number*
no ssid *ssid-number*

Syntax Description

ssid-number	SSID number of user group members.

Command Default

No default behavior or values

Command Modes

Local RADIUS server group configuration

Command History

Release	Modification
12.2(11)JA	This command was introduced on Cisco Aironet Access Point 1100 and Cisco Aironet Access Point 1200.
12.3(11)T	This command was implemented on the following platforms: Cisco 2600XM, Cisco 2691, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3700, and Cisco 3800 series routers.

Usage Guidelines

You can enter up to 20 SSIDs to limit users to those SSIDs.

Examples

The following example shows that the SSID "green" has been added to the local user group:

```
ssid green
```

Related Commands

Command	Description
block count	Configures the parameters for locking out members of a group to help protect against unauthorized attacks.
clear radius local-server	Clears the statistics display or unblocks a user.
debug radius local-server	Displays the debug information for the local server.
group	Enters user group configuration mode and configures shared setting for a user group.
nas	Adds an access point or router to the list of devices that use the local authentication server.
radius-server host	Specifies the remote RADIUS server host.

Command	Description
radius-server local	Enables the access point or router to be a local authentication server and enters into configuration mode for the authenticator.
reauthentication time	Specifies the time (in seconds) after which access points or wireless-aware routers must reauthenticate the members of a group.
show radius local-server statistics	Displays statistics for a local network access server.
user	Authorizes a user to authenticate using the local authentication server.
vlan	Specifies a VLAN to be used by members of a user group.

ssl encryption

To specify the encryption algorithm that the Secure Sockets Layer (SSL) protocol uses for SSL Virtual Private Network (SSL VPN) connections, use the **ssl encryption**command in webvpn gateway configuration mode. To remove an algorithm from the SSL VPN gateway, use the **no** form of this command.

ssl encryption [**3des-sha1**] [**aes-sha1**] [**rc4-md5**]
no ssl encryption

Syntax Description

3des-sha1	(Optional) Configures the 3 DES-SHA1 encryption algorithm.
aes-sha1	(Optional) Configures the AES-SHA1 encryption algorithm.
rc4-md5	(Optional) Configures the RC4-MD5 encryption algorithm.

Command Default

All algorithms are available in the order shown above.

Command Modes

Webvpn gateway configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

The SSL VPN provides remote-access connectivity from almost any Internet-enabled location using only a Web browser and its native SSL encryption. Configuring this command allows you to restrict the encryption algorithms that SSL uses in Cisco IOS software. The ordering of the algorithms specifies the preference. If you specify this command after you have specified an algorithm, the previous setting is overridden.

Examples

The following example configures the gateway to use, in order, the 3DES-SHA1, AES-SHA1, or RC4-MD5 encryption algorithms for SSL connections:

```
Router(config)# webvpn gateway SSL_GATEWAY

Router(config-webvpn-gateway)#
ssl encryption rc4-md5

Router(config-webvpn-gateway)#
```

Related Commands

Command	Description
webvpn gateway	Defines a SSL VPN gateway and enters webvpn gateway configuration mode.

ssl-proxy module allowed-vlan

To add the VLANs allowed over the trunk to the Secure Socket Layer (SSL) Services Module, enter the **ssl-proxy module allowed-vlan** command in global configuration mode. To remove the SSL Services Module from the specified VLAN, use the **no** form of this command.

ssl-proxy module *mod* **allowed-vlan** *vlan-id*
no ssl-proxy module *mod* **allowed-vlan** *vlan-id*

Syntax Description

mod	Module number.
vlan-id	VLAN number; valid values are from 1 to 4094.

Command Default

This command has no default settings.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXD	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is supported on Cisco 7600 series routers that are configured with a Wireless LAN Services Module (WLSM) only.

One of the allowed VLANs must be the administrative VLAN.

To verify the configuration, enter the **show spanning-tree vlan** command.

To display the spanning-tree state for the specified VLAN, enter the **show ssl-proxy module state** command.

Examples

This example shows how to add an SSL Services Module installed in slot 6 to a specific VLAN:

```
Router (config)# ssl-proxy module 6 allowed-vlan 100
Router (config)#
```

This example shows how to remove the SSL Services Module from the specified VLAN:

```
Router (config)# no ssl-proxy module 6 allowed-vlan 100
Router (config)#
```

Related Commands

Command	Description
show ssl-proxy module state	Displays the spanning-tree state for the specified VLAN.

ssl truspoint

To configure the certificate trustpoint on a SSL VPN gateway, use the **ssl trustpoint**command in webvpn gateway configuration mode. To remove the trustpoint association, use the **no** form of this command.

ssl trustpoint *name*
no ssl trustpoint

Syntax Description

name	Name of the trust point.

Command Default

This command has no default behavior or values.

Command Modes

SSLVPN gateway configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

You can configure a persistent self-signed certificate or an external CA server to generate a valid trustpoint.

Examples

The following example configures a trustpoint named CA_CERT:

```
Router(config)#
webvpn gateway SSL_GATEWAY

Router(config-webvpn-gateway)#
ssl trustpoint CA_CERT
```

Related Commands

Command	Description
webvpn gateway	Defines a SSL VPN gateway and enters webvpn gateway configuration mode.

sslvpn use-pd

To enable the PD (platform dependent) solution for SSL VPN on Cisco Cloud Services Router 1000V Series, use the **sslvpn use-pd** command in global configuration mode. To disable the PD solution and enable the default PI solution, use the **no** form of this command

sslvpn use-pd
no sslvpn use-pd

Syntax Description

This command has no keywords or arguments.

Command Default

The PI (platform independent) solution is enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
IOS XE Everest 16.6.1	This command wsa introduced.

Usage Guidelines

The PD solution is used to increase the scale and throughput of SSL VPN.

Example

This example shows how to enable the PD solution:

```
Device(config) #platform sslvpn use-pd
Enable SSLVPN use pd solution will take effect after reboot!
```

sso-server

To create a Single SignOn (SSO) server name under a Secure Sockets Layer Virtual Private Network (SSL VPN) context and to enter webvpn sso server configuration mode--and to attach an SSO server to a policy group--use the **sso-server** command in webvpn sso server configuration and group policy configuration modes, respectively. To remove an SSO server name, use the **no** form of this command.

sso-server *name*
no sso-server *name*

Syntax Description

name	Name of the SSO server.

Command Default

A SSO server is not created or attached to a policy group.

Command Modes

Webvpn sso server configuration
Group policy configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

The SSO server name is configured under the SSL VPN context in webvpn context configuration mode. All SSO server-related parameters, such as web agent URL and policy server secret key, are configured under the SSO server name. The SSO server name is attached to the policy group in webvpn group policy configuration mode.

Examples

The following example shows that the SSO server "test-sso-server" is created under the SSL VPN context and attached to a policy group named "ONE":

```
webvpn context context1
 sso-server "test-sso-server"
  web-agent-url "http://webagent.example.com"
  secret-key "12345"
  retries 3
  timeout 15
 policy group ONE
  sso-server "test-sso-server"
```

Related Commands

Command	Description
policy group	Enters webvpn group policy configuration mode to configure a policy group.
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

standby-group

To specify a Hot Standby Router Protocol (HSRP) group to be used by a cluster, use the **standby-group** command in IKEv2 cluster configuration mode. To remove a HSRP group, use the **no** form of this command.

standby-group *group-name*
no standby-group

Syntax Description

group-name	HSRP group name.

Command Default

The HSRP group is not specified.

Command Modes

IKEv2 cluster configuration (config-ikev2-cluster)

Command History

Release	Modification
15.2(4)M	This command was introduced.

Usage Guidelines

You must enable the **crypto ikev2 cluster** command before enabling the **standby-group** command.

You must specify the same name that you specified in the *group-name* argument of the **standby name** command.

Examples

The following example shows how to set the HSRP group to group1:

```
Device(config)# crypto ikev2 cluster
Device(config-ikev2-cluster)# standby-group group1
```

Related Commands

Command	Description
crypto ikev2 cluster	Defines an IKEv2 cluster policy in an HSRP cluster.
standby name	Specifies the name of the HSRP standby group.

status

To enter the signature-definition-status configuration mode, which allows you to change the enabled or retired status of an individual signature, use the **status**command in signature-definition-action configuration mode. To return to the default action, use the **no** form of this command.

status

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Signature-definition-action configuration (config-sigdef-action)

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Before issuing the **status** command, you must specify at least one signature via the **signature** command.

Examples

The following example shows how to change the status of signature 9000:0 to enabled:

```
Router(config)# ip ips signature-definition
Router(config-sigdef-sig)# signature 9000 0
Router(config-sigdef-action)# status
Router(config-sigdef-status)# enabled true
```

Related Commands

Command	Description
signature	Specifies a signature for which the CLI user tunings will be changed.

strict-http

To allow HTTP messages to pass through the firewall or to reset the TCP connection when HTTP noncompliant traffic is detected, use the **strict-http**command in appfw-policy-http configuration mode. To disable configured settings, use the **no** form of this command.

strict-http action {**reset** | **allow**} [**alarm**]
no strict-http action {**reset** | **allow**} [**alarm**]

Syntax Description

action	HTTP messages are subject to the specified action (**reset** or **allow**).
reset	Sends a TCP reset notification to the client or server if the HTTP message fails the mode inspection.
allow	Forwards the packet through the firewall.
alarm	(Optional) Generates system logging (syslog) messages for the given action.

Command Default

If this command is not enabled, all traffic will be allowed through the firewall.

Command Modes

appfw-policy-http
configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Examples

The following example shows how to define the HTTP application firewall policy "mypolicy." This policy includes all supported HTTP policy rules. After the policy is defined, it is applied to the inspection rule "firewall," which will inspect all HTTP traffic entering the FastEthernet0/0 interface.

```
! Define the HTTP policy.
appfw policy-name mypolicy
 application http
  strict-http action allow alarm
  content-length maximum 1 action allow alarm
  content-type-verification match-req-rsp action allow alarm
  max-header-length request 1 response 1 action allow alarm
  max-uri-length 1 action allow alarm
  port-misuse default action allow alarm
  request-method rfc default action allow alarm
  request-method extension default action allow alarm
  transfer-encoding type default action allow alarm
!
!
! Apply the policy to an inspection rule.
ip inspect name firewall appfw mypolicy
ip inspect name firewall http
!
!
! Apply the inspection rule to all HTTP traffic entering the FastEthernet0/0 interface.
interface FastEthernet0/0
```

```
 ip inspect firewall in
!
!
```

storage

To specify a file system location where public key infrastructure (PKI) trustpool certificates are stored on the router, use the **storage** command in CA-trustpool configuration mode. To remove the file system location that was specified, use the **no** form of this command.

storage *location*
no storage *location*

Syntax Description

location	The file system location where the PKI trustpool certificates are stored. The types of file system locations are specified in the "Usage Guidelines" section.

Command Default

The storage location is not configured.

Command Modes

CA-trustpool configuration mode (ca-trustpool)

Command History

Release	Modification
15.2(2)T	This command was introduced.
15.1(1)SY	This command was integrated into Cisco IOS 15.1(1)SY.

Usage Guidelines

Before you can configure this command, you must enable the **crypto pki trustpool policy** command, which enters ca-trustpool configuration mode.

Previously stored certificates cannot be moved with this command.

The *location* argument specifies the file system storage location. The table below lists the available file system locations:

Table 221: File System Locations

File System	Description
disk0:	Stores the PKI trustpool in the disc0 file system.
disk1:	Stores the PKI trustpool in the disc1 file system.
nvram:	Stores the PKI trustpool in the NVRAM file system.
unix:	Stores the PKI trustpool in the the UNIX file system.
file-system-name =	The named file system that is stored in the PKI trustpool.

Examples

```
Router(config)# crypto pki trustpool policy
Router(ca-trustpool)# storage disk0:crca2048.crl
```

Related Commands

Command	Description
cabundle url	Configures the URL from which the PKI trustpool CA bundle is downloaded.
chain-validation	Enables chain validation from the peer's certificate to the root CA certificate in the PKI trustpool.
crl	Specifes the certificate revocation list (CRL) query and cache options for the PKI trustpool.
crypto pki trustpool import	Manually imports (downloads) the CA certificate bundle into the PKI trustpool to update or replace the existing CA bundle.
crypto pki trustpool policy	Configures PKI trustpool policy parameters.
default	Resets the value of a ca-trustpool configuration command to its default.
match	Enables the use of certificate maps for the PKI trustpool.
ocsp	Specifies OCSP settings for the PKI trustpool.
revocation-check	Disables revocation checking when the PKI trustpool policy is being used.
show	Displays the PKI trustpool policy of the router in ca-trustpool configuration mode.
show crypto pki trustpool	Displays the PKI trustpool certificates of the router and optionally shows the PKI trustpool policy.
source interface	Specifies the source interface to be used for CRL retrieval, OCSP status, or the downloading of a CA certificate bundle for the PKI trustpool.
vrf	Specifies the VRF instance to be used for CRL retrieval.

subject-alt-name

To specify the trustpoint certificate name in the Subject Alternative Name (subjectAltName) field in the X.509 certificate, which is contained in the trustpoint certificate, use the **subject-alt-name**in ca-trustpoint configuration mode. To remove this configuration, use the **no** form of this command.

subject-alt-name *name*
no subject-alt-name *name*

Syntax Description

name	Specifies the trustpoint certificate name.

Command Default

The Subject Alternative Name field is not included in the X.509 certificate.

Command Modes

Ca-trustpoint (ca-trustpoint)

Command History

Release	Modification
15.1(3)T	This command was introduced.

Usage Guidelines

The **subject-alt-name**command is used to create a self-signed trustpoint certificate for the router that contains the trustpoint name in the Subject Alternative Name (subjectAltName) field. This Subject Alternative Name can be used only when the trustpoint enrollment option is specified for self-signed enrollment in the trustpoint policy.

Note The Subject Alternative Name field in the X.509 certificate is defined in RFC 2511.

Examples

The following example shows how to create a self-signed trustpoint certificate for the router that contains the trustpoint name in the Subject Alternative Name (subjectAltName) field:

```
Router> enable
Router# configure terminal
Router(config)# crypto pki trustpoint TESTCA
Router(ca-trustpoint)# enrollment selfsigned
Router(ca-trustpoint)# subject-alt-name TESTCA
Router
(ca-trustpoint)#
exit
Router(config)# cypto pki enroll
TESTCA
% Include the router serial number in the subject name? [yes/no]: no
% Include an IP address in the subject name? [no]:
Generate Self Signed Router Certificate? [yes/no]: yes
Router Self Signed Certificate successfully created
Router(config)# exit
```

The following certificate is created:

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 2 (0x2)
        Signature Algorithm: md5WithRSAEncryption
        Issuer: CN=TESTCA/unstructuredName=r1.cisco.com
        Validity
            Not Before: Mar 22 20:26:20 2010 GMT
            Not After : Jan  1 00:00:00 2020 GMT
        Subject: CN=TESTCA/unstructuredName=r1.cisco.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (512 bit)
                Modulus (512 bit):
                    00:8d:71:2e:3b:eb:a2:e2:f3:44:d9:bc:a9:85:88:
                    f4:a9:bd:c9:7f:f0:69:f5:e7:75:8f:00:f2:8e:3e:
                    2f:ca:5e:c5:08:43:95:8c:a2:6a:ae:ce:a0:ae:82:
                    61:61:ff:4e:8c:8f:89:d1:56:d8:35:34:b7:95:93:
                    1a:72:03:71:fb
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints: critical
            CA:TRUE
            X509v3 Subject Alternative Name:
            DNS:TESTCA
            X509v3 Authority Key Identifier:
            keyid:F9:A4:95:87:5F:A4:CA:7D:65:FA:BE:38:20:55:18:F9:4C:6C:D5:F3
            X509v3 Subject Key Identifier:
            F9:A4:95:87:5F:A4:CA:7D:65:FA:BE:38:20:55:18:F9:4C:6C:D5:F3
    Signature Algorithm: md5WithRSAEncryption
        6d:92:e7:a8:a5:1a:5a:ef:13:58:02:1b:79:17:93:41:37:c9:
        2d:9f:1a:a3:f5:3a:73:05:cd:d1:02:84:43:7e:e0:84:07:46:
        55:f9:45:59:51:ba:25:48:6f:d8:e1:0d:35:44:07:5c:16:17:
        35:45:99:e2:80:6e:53:e5:35:76
-----BEGIN CERTIFICATE-----
MIIBszCCAV2gAwIBAgIBAjANBgkqhkiG9w0BAQQFADAuMQ8wDQYDVQQDEwZURVNU
Q0ExGzAZBgkqhkiG9w0BCQIWDHIxLmNpc2NvLmNvbTAeFw0xMDAzMjIyMDI2MjBa
Fw0yMDAxMDEwMDAwMDBaMC4xDzANBgNVBAMTBlRFU1RDQTEbMBkGCSqGSIb3DQEJ
AhYMcjEuY2lzY28uY29tMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAI1xLjvrouLz
RNm8qYWI9Km9yX/wafXndY8A8o4+L8pexQhDlYyiaq7OoK6CYWH/ToyPidFW2DU0
t5WTGnIDcfsCAwEAAaNmMGQwDwYDVR0TAQH/BAUwAwEB/zARBgNVHREECjAIggZU
RVNUQ0EwHwYDVR0jBBgwFoAU+aSVh1+kyn1l+r44IFUY+Uxs1fMwHQYDVR0OBBYE
FPmklYdfpMp9Zfq+OCBVGPlMbNXzMA0GCSqGSIb3DQEBBAUAA0EAbZLnqKUaWu8T
WAIbeReTQTfJLZ8ao/U6cwXN0QKEQ37ghAdGVflFWVG6JUhv2OENNUQHXBYXNUWZ
4oBuU+U1dg==
-----END CERTIFICATE-----
```

Related Commands

Command	Description
cypto pki enroll	Requests the certificates for the router from the trustpoint.
crypto pki trustpoint	Creates a trustpoint and enters ca-trustpoint configuration mode.
enrollment selfsigned	Specifies self-signed enrollment for a trustpoint.

subject-name

To specify the subject name in the certificate request, use the **subject-name** command in ca-trustpoint configuration mode. To clear any subject name from the configuration, use the **no** form of this command.

subject-name [*x.500-name*]
nosubject-name [*x.500-name*]

Syntax Description

x.500-name	(Optional) Specifies the subject name used in the certificate request.

Command Default

If the *x-500-name* argument is not specified, the fully qualified domain name (FQDN), which is the default subject name, will be used.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.4(24)T	Support for IPv6 Secure Neighbor Discovery (SeND) was added.

Usage Guidelines

Before you can issue the subject-name command, you must enable the **crypto ca trustpoint**command, which declares the certification authority (CA) that your router should use and enters ca-trustpoint configuration mode.

The subject-name command is an attribute that can be set for autoenrollment; thus, issuing this command prevents you from being prompted for a subject name during enrollment.

Examples

The following example shows how to specify the subject name for the "frog" certificate:

```
c
rypto ca trustpoint frog
 enrollment url http://frog.phoobin.com/
 subject-name OU=Spiral Dept., O=tiedye.com
 ip-address ethernet-0
 auto-enroll regenerate
 password revokme
```

Related Commands

Command	Description
crypto ca trustpoint	Declares the CA that your router should use.

subnet-acl

Note Effective with Cisco IOS Release 15.2(2)T, the **subnet-acl** command is replaced by the **route set** command. See the **route set** command for more information.

To configure split tunneling, use the **subnet-acl** command in IKEv2 authorization policy configuration mode. To remove this command from your configuration and restore the default value, use the **no** form of this command.

[{**ipv6**}] **subnet-acl** {*acl-numberacl-name*}
no [{**ipv6**}] **subnet-acl**

Syntax Description

ipv6	(Optional) Specifies an IPv6 attribute. To specify an IPv4 attribute, execute the command without this keyword.
acl-number	Access list number. The range is 100 to 199.
acl-name	Access list name.

Command Default

Split tunneling is disabled.

Command Modes

IKEv2 authorization policy configuration (config-ikev2-author-policy)

Command History

Release	Modification
15.1(3)T	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.
15.2(1)T	This command was modified. The **ipv6** keyword was added.
15.2(2)T	This command was replaced by the **route set** command.

Usage Guidelines

Use the **subnet-acl** command to specify that the groups of ACLs represent protected subnets for split tunneling. Split tunneling is the ability to have a secure tunnel to the central site and simultaneous clear text tunnels to the Internet.

You must enable the **crypto ikev2 authorization policy** command, which specifies local group policy group authorization parameters that have to be defined or changed, before enabling the **subnet-acl** command.

Examples

The following example shows how to apply split tunneling for the group name "cisco." In this example, all traffic sourced from the client and destined to the subnet 192.168.1.0 will be sent through the VPN tunnel.

```
crypto ikev2 client configuration group cisco
 key cisco
```

```
 dns 10.2.2.2 10.3.2.3
 pool dog
 subnet-acl 199
!
access-list 199 permit ip 192.168.1.0 0.0.0.255 any
```

Related Commands

Command	Description
crypto ikev2 authorization policy	Specifies an IKEv2 authorization policy.

subscriber access pppoe unique-key circuit-id

To specify a unique circuit ID tag for a PPP over Ethernet (PPPoE) user session to be tapped on the router, use the **subscriber access pppoe unique-key circuit-id**command in global configuration mode. To restore the default value, use the **no** form of this command.

subscriber access pppoe unique-key circuit-id
no subscriber access pppoe unique-key circuit-id

Syntax Description

This command has no arguments or keywords.

Command Default

A unique circuit ID tag for PPPoE user session is not specified.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Release 2.6	This command was introduced.

Usage Guidelines

In Cisco IOS XE Release 2.6, a user session is tapped based on the unique PPPoE circuit ID tag. This circuit ID tag serves as a unique parameter for the PPPoE user session on the device. The tapped user session is provisioned through SNMP, and user session data packets and RADIUS authentication data packets are tapped. This command is used in conjunction with the Lawful Intercept feature.

Related Commands

Command	Description
show idmgr session key	Verifies the user session information in the ID Manager (IDMGR) database by specifying the unique circuit ID tag using the **circuit-id** keyword and *circuit-id* argument.

subscriber service

To enable per-subscriber services, use the **subscriber service** command in global configuration mode. To disable per-subscriber services, use the **no** form of this command.

subscriber service {**accounting interim-interval** *minutes* | **coa-rfc-compliant** | **ignore** | **multiple-accept** | **password** | **police** | **session-accounting** | **shaper** | **target-atm-vc** | **vc-ignore-cos**}
no subscriber service {**accounting interim-interval** *minutes* | **coa-rfc-compliant** | **ignore** | **multiple-accept** | **password** | **police** | **session-accounting** | **shaper** | **target-atm-vc** | **vc-ignore-cos**}

Syntax Description

accounting interim-interval *minutes*	Enables the generation of interim service accounting records at periodic intervals for subscribers. The *minutes* argument indicates the number of periodic intervals to send accounting update records from 1 to 71582 minutes.
coa-rfc-compliant	Sends RFC 3576 compliant change of authorization (CoA) NAK messages.
ignore	Ignores any of per-subscriber services.
multiple-accept	Allows multiple services on access-accept.
password	Password to use when downloading services.
police	Quality of service (QoS) RADIUS service police command.
session-accounting	Enables the inclusion of activated services in a session accounting start message.
shaper	QoS RADIUS service shaper command.
target-atm-vc	Enables the QoS service on the target ATM virtual circuit (VC).
vc-ignore-cos	Ignores the set Layer 2 class of service (set-cos) value on the target ATM VC.

Command Default

Service accounting is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Release 12.2(31)ZV1	This command was introduced for session accounting and was implemented on the Cisco 10000 series router for the PRE3.
Cisco IOS XE Release 2.4	This command was integrated into Cisco IOS XE Release 2.4.

Usage Guidelines

The **subscriber service session-accounting** command enables the router to include all activated services in a single accounting Session-Start message for a session.

RADIUS can activate a service using the RADIUS Access-Accept message. When RADIUS activates a service on the router after the router sends the accounting Session-Start message, the router generates an accounting session update that includes all activated services.

When a session stops, all currently active services are included in the accounting session stop record.

The **subscriber service accounting interim-interval**command enables the router to generate interim service accounting records at periodic intervals for subscribers. RADIUS Attribute 85 in the user service profile always takes precedence over the configured interim-interval value. RADIUS Attribute 85 must be in the user service profile. See the RADIUS Attributes Overview and RADIUS IETF Attributes feature document for more information.

Note If RADIUS Attribute 85 is not in the user service profile, then the interim-interval value is used for service interim accounting records. The interim-interval value is configured by either using the **aaa accounting update** command in global configuration mode or the **action-type** command in accounting method list configuration mode. See the Configuring Accounting feature document for more information.

Examples

The following example enables per-service accounting:

```
Router(config)# subscriber service session-accounting
```

Related Commands

Command	Description
bandwidth account	Enables class-based fair queuing and ATM overhead accounting.
shape account	Shapes traffic to the indicated bit rate and enables ATM overhead accounting.

svc address-pool

To configure a pool of IP addresses to be assigned to end users in a policy group, use the **svc address-pool** command in webvpn group policy configuration mode. To remove the address pool from the policy group configuration, use the **no** form of this command.

svc address-pool *name* **netmask** *ip-netmask*
no svc address-pool

Syntax Description

name	Name of the address pool that is configured using the **ip local pool** command.
netmask *ip-netmask*	Specifies the IP netmask that is applied to the address pool.

Command Default

IP address pools are not assigned to end users.

Command Modes

Webvpn group policy configuration (config-webvpn-group)

Command History

Release	Modification
12.4(6)T	This command was introduced.
15.1(1)T	This command was modified. The **netmask** keyword and *ip-netmask* argument were added.
15.1(4)M3	This command was modified. The **netmask** keyword and *ip-netmask* argument were made mandatory.

Usage Guidelines

Before configuring the **svc address-pool** command, use the **ip local pool** command to define the address pool. The standard configuration assumes that the IP addresses in the pool are reachable from a directly connected network.

Configuring Address Pools for Networks That Are Not Directly Connected

If you need to configure an address pool for IP addresses from a network that is not directly connected, perform the following steps:

1. Create a local loopback interface and configure it with an IP address and subnet mask from the address pool.
2. Configure the address pool with the **ip local pool** command. The range of addresses must fall under the subnet mask configured in Step 1.
3. Configure the **svc address-pool** command with the address pool name configured in Step 2.

See the “Examples” section for an example of how to configure a pool of IP addresses to assign to end users in a policy group.

Note The Switched Virtual Circuits (SVC) software or the Secure Sockets Layer VPN (SSL VPN) client is the predecessor of the Cisco AnyConnect VPN Client software.

Examples

Directly Connected Network

The following example shows how to configure the 192.168.1/24 network as an address pool:

```
Router(config)# ip local pool ADDRESSES 192.168.1.1 192.168.1.254

Router(config)# webvpn context context1

Router(config-webvpn-context)# policy group ONE

Router(config-webvpn-group)# svc address-pool ADDRESSES netmask 255.255.255.0
Router(config-webvpn-group)# end
```

Indirectly Connected Network

The following example shows how to configure the 172.16.1/24 network as an address pool. Because the network is not directly connected, a local loopback is configured.

```
Router(config)# interface loopback 0

Router(config-if)# ip address 172.16.1.128 255.255.255.0

Router(config-if)# no shutdown
Router(config-if)# exit

Router(config)# ip local pool ADDRESSES 172.16.1.1 172.16.1.254

Router(config)# webvpn context context1

Router(config-webvpn-context)# policy group ONE

Router(config-webvpn-group)# svc address-pool ADDRESSES
 netmask 255.255.255.0
```

Related Commands

Command	Description
ip local pool	Configures a local pool of IP addresses to be used when a remote peer connects to a point-to-point interface.
policy group	Enters webvpn group policy configuration mode to configure a policy group.
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

svc default-domain

To configure the Cisco AnyConnect VPN Client domain for a policy group, use the **svc default-domain** command in webvpn group policy configuration mode. To remove the domain from the policy group configuration, use the **no** form of this command.

svc default-domain *name*
no svc default-domain

Syntax Description

name	Name of the domain.

Command Default

Cisco AnyConnect VPN Client domain is not configured.

Command Modes

Webvpn group policy configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

Note SVC software, or Secure Sockets Layer Virtual Private Network (SSL VPN) Client, is the predecessor of Cisco AnyConnect VPN Client software.

Examples

The following example configures cisco.com as the default domain:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# svc default-domain cisco.com
```

Related Commands

Command	Description
policy group	Enters webvpn group policy configuration mode to configure a policy group.
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

svc dns-server

To configure Domain Name System (DNS) servers for policy group end users, use the **svc dns-server** command in webvpn group policy configuration mode. To remove a DNS server from the policy group configuration, use the **no** form of this command.

svc dns-server {**primary** | **secondary**} *ip-address*
no svc dns-server {**primary** | **secondary**}

Syntax Description

primary | **secondary**	Configures the primary or secondary DNS server.
ip-address	An IPv4 address is entered to identify the server.

Command Default

DNS servers are not configured.

Command Modes

Webvpn group policy configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

Note SVC software, or Secure Sockets Layer Virtual Private Network (SSL VPN) Client, is the predecessor of Cisco AnyConnect VPN Client software.

Examples

The following example configures primary and secondary DNS servers for the policy group:

```
Router(config)# webvpn context context1

Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# svc dns-server primary 192.168.3.1

Router(config-webvpn-group)# svc dns-server secondary 192.168.4.1
```

Related Commands

Command	Description
policy group	Enters webvpn group policy configuration mode to configure a policy group.
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

svc dpd-interval

To configure the dead peer detection (DPD) timer value for the gateway or client, use the **svc dpd-interval**command in webvpn group policy configuration mode. To remove a DPD timer value from the policy group configuration, use the **no** form of this command.

svc dpd-interval {**client** | **gateway**} *seconds*
no svc dpd-interval {**client** | **gateway**}

Syntax Description

client | **gateway**	Specifies the client or gateway.
seconds	Sets the time interval, in seconds, for the DPD timer. A number from 0 through 3600 is entered.

Command Default

The DPD timer is reset every time a packet is received over the Secure Sockets Layer Virtual Private Network (SSL VPN) tunnel from the gateway or end user.

Command Modes

Webvpn group policy configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

Note SVC software, or Secure Sockets Layer Virtual Private Network (SSL VPN) Client, is the predecessor of Cisco AnyConnect VPN Client software.

Examples

The following example sets the DPD timer to 30 seconds for a SSL VPN gateway and to 5 minutes for end users (remote PC or device):

```
Router(config)# webvpn context context1

Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# svc dpd-interval gateway 30
Router(config-webvpn-group)# svc dpd-interval client 300
Router(config-webvpn-group)#
```

Related Commands

Command	Description
policy group	Enters webvpn group policy configuration mode to configure a policy group.
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

svc dtls

To enable Datagram Transport Layer Security (DTLS) support on the Cisco IOS Secure Socket Layer Virtual Private Network (SSL VPN), use the **svc dtls** command in WebVPN group policy configuration mode. To disable the configuration, use the **no** form of this command.

svc dtls
no svc dtls

Syntax Description

This command has no arguments or keywords.

Command Default

DTLS is enabled by default on the Cisco ISR G2 series routers (3900, 2900, 1900, 890, and 880) and is disabled on other routers.

Command Modes

WebVPN group policy configuration (config-webvpn-group)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The DTLS Support for IOS SSL VPN feature enables DTLS as a transport protocol for the traffic tunneled through SSL VPN. The DTLS Support for IOS SSL VPN feature is enabled by default on the Cisco IOS SSL VPN. You can use the **no svc dtls** command to disable DTLS support on the SSL VPN.

Examples

The following example shows how to disable DTLS support on the Cisco IOS SSL VPN gateway:

```
Router# configure terminal
Router(config)# webvpn context context1
Router(config-webvpn-context)# policy group group1
Router(config-webvpn-group)# no svc dtls
```

Related Commands

Command	Description
dtls port	Configures a DTLS port.

svc homepage

To configure the URL of the web page that is displayed upon successful user login, use the **svc homepage**command in webvpn group policy configuration mode. To remove the URL from the policy group configuration, use the **no** form of this command.

svc homepage *string*
no svc homepage

Syntax Description

string	The *string* argument is entered as an HTTP URL. The URL can be up to 255 characters in length.

Command Default

URL of the home page is not configured.

Command Modes

Webvpn group policy configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

Note SVC software, or Secure Sockets Layer Virtual Private Network (SSL VPN) Client, is the predecessor of Cisco AnyConnect VPN Client software.

Examples

The following example configures www.cisco.com as the Cisco AnyConnect VPN Client home page:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# svc homepage www.cisco.com
```

Related Commands

Command	Description
policy group	Enters webvpn group policy configuration mode to configure a policy group.
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

svc keepalive

To specify the Secure Socket Layer Virtual Private Network Client (SVC) keepalive value, use the **svc keepalive**command in webvpn group policy configuration mode. To return the **svc keepalive** command to its default, use the **no** form of this command.

svc keepalive seconds
no svc keepalive

Syntax Description

seconds	Specifies an SVC keepalive value from 0 to 600 seconds.

Command Default

The SVC is enabled to send keepalive messages by default with a frequency of 30 seconds.

Command Modes

Webvpn group policy configuration (config-webvpn-group)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

You can adjust the frequency of keepalive messages to ensure that an SVC connection through a proxy, IOS firewall, or Network Address Translation (NAT) device remains active, even if the device limits the time that the connection can be idle. Adjusting the frequency also ensures that the SVC does not disconnect and reconnect when the remote user is not actively running a socket-based application, such as Microsoft Outlook or Microsoft Internet Explorer.

If the **svc keepalive** command is configured with a value of **0** seconds, then the keepalive function is disabled.

Note SVC is the predecessor of Cisco AnyConnect VPN Client software.

Examples

In the following example, the security appliance is configured to enable the SVC to send keepalive messages with a frequency of 300 seconds (5 minutes), for the existing group-policy group "ONE":

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# svc keepalive 300
```

Related Commands

Command	Description
policy group	Enters webvpn group policy configuration mode to configure a policy group.
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

svc keep-client-installed

To configure the end user to keep Cisco AnyConnect VPN Client software installed when the SSL VPN connection is not enabled, use the **svc keep-client-installed**command in webvpn group policy configuration mode. To remove the software installation requirement from the policy group configuration, use the **no** form of this command.

svc keep-client-installed
no svc keep-client-installed

Syntax Description

This command has no keywords or arguments.

Command Default

No default behavior or values.

Command Modes

Webvpn group policy configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

The configuration of this command removes the overhead of pushing the Cisco AnyConnect VPN Client software to the end user on each connection attempt.

Note SVC, or Secure Sockets Layer Virtual Private Network (SSL VPN) Client, is the predecessor of Cisco AnyConnect VPN Client software.

Examples

The following example configures end users to keep Cisco AnyConnect VPN Client software installed:

```
Router(config)# webvpn context context1

Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# svc keep-client-installed
```

Related Commands

Command	Description
policy group	Enters webvpn group policy configuration mode to configure a policy group.
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

svc module

To configure Start Before Logon (SBL) functionality support for a Cisco IOS Secure Sockets Layer Virtual Private Network (SSL VPN) headend, use the **svc module** command in webvpn group policy configuration mode. To disable the configuration, use the **no** form of this command.

svc module *module-name*
no svc module

Syntax Description

module-name	Anyconnect module name.

Command Default

The SBL functionality is disabled by default.

Command Modes

Webvpn group policy configuration (config-webvpn-group)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Usage Guidelines

The SBL functionality connects the client PC to the enterprise network even before the users log in to the PC. This functionality allows the administrator to run the logon scripts even if the user is not connected to the enterprise network.

Use the **svc module** command to configure the SBL functionality support for the Cisco IOS SSL VPN headend. This command sets the module in the WebVPN cookie for the AnyConnect client, and thereby helps in downloading the SBL components to the client from the SSL VPN headend.

Examples

The following example shows how to configure the vpn1 AnyConnect module to Cisco IOS SSL VPN headend:

```
Router# configure terminal
Router(config)# webvpn context context1
Router(config-webvpn-context)# policy group group1
Router(config-webvpn-group)# svc module vpn1
```

Related Commands

Command	Description
policy group	Enters webvpn group policy configuration mode to configure a policy group.

svc msie-proxy

To configure Microsoft Internet Explorer (MSIE) browser proxy settings for policy group end users, use the **svc msie-proxy**command in webvpn group policy configuration mode. To remove a MSIE proxy setting from the policy group configuration, use the **no** form of this command.

svc msie-proxy {**server** *host* | **exception** *host* | **option** {**auto** | **bypass-local** | **none**}}
no svc msie-proxy {**server** *host* | **exception** *host* | **option** {**auto** | **bypass-local** | **none**}}

Syntax Description

server *host*	Specifies a MSIE proxy server for policy group end users. The *host* argument specifies the location of the MSIE server. The *host* argument is configured as an IPv4 address or fully qualified domain name, followed by a colon and port number.
exception *host*	Configures the browser not to send traffic for a single Domain Name System (DNS) hostname or IP address through the proxy.
option auto	Configures the browser to automatically detect proxy settings.
option bypass-local	Configures the browser to bypass proxy settings that are configured on the remote user.
option none	Configures the browser to use no proxy settings.

Command Default

MSIE browser proxy settings are not configured for policy group end users.

Command Modes

Webvpn group policy configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

The configuration of this command is applied to end users that use a MSIE browser. The configuration of this command has no effect on any other browser type.

Note SVC, or Secure Sockets Layer Virtual Private Network (SSL VPN) Client, is the predecessor of Cisco AnyConnect VPN Client software.

Examples

The following example configures automatic detection of MSIE proxy settings and configures proxy exceptions for traffic from www.example.com and the 10.20.20.1 host:

```
Router(config)# webvpn context context1

Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# svc msie-proxy option auto
Router(config-webvpn-group)# svc msie-proxy exception www.example.com
Router(config-webvpn-group)# svc msie-proxy exception 10.20.20.1
```

The following example configures a connection to an MSIE proxy server through a fully qualified domain name (FQDN) and a port number:

```
Router(config)# webvpn context context1

Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# svc msie-proxy server www.example.com:80
```

The following example configures a connection to an MSIE proxy server through an IP address and port number:

```
Router(config)# webvpn context context1

Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# svc msie-proxy server 10.10.10.1:80
```

Related Commands

Command	Description
policy group	Enters webvpn group policy configuration mode to configure a policy group.
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

svc msie-proxy server

To specify a Microsoft Internet Explorer (MSIE) proxy server for policy group end users, use the **svc msie-proxy server**command in SSLVPN group policy configuration mode. To remove the proxy server from the policy group configuration, use the **no** form of this command.

svc msie-proxy server *host*
no svc msie-proxy server

Syntax Description

host	Specifies the location of the MSIE server. The host argument is configured as an IPv4 address or fully qualified domain name, followed by a colon and port number.

Command Default

No default behavior or values.

Command Modes

SSLVPN group policy configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Examples

The following example configures a connection to an MSIE proxy server through a fully qualified domain name and a port number:

```
Router(config)# webvpn context SSLVPN

Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# svc msie-proxy server www.cisco.com:80
Router(config-webvpn-group)#
```

The following example configures a connection to an MSIE proxy server through an IP address and port number:

```
Router(config)# webvpn context SSLVPN

Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# svc msie-proxy server 10.10.10.1:80
Router(config-webvpn-group)#
```

Related Commands

Command	Description
policy group	Enters SSLVPN group policy configuration mode to configure a group policy.
webvpn context	Enters SSLVPN configuration mode to configure the WebVPN context.

svc mtu

To configure the MTU size for a policy group at the client end, use the **svc mtu** command in webvpn group policy configuration mode. To set the MTU size to its default, use the **no** form of this command.

svc mtu *size*
no svc mtu

Syntax Description

size	Size of MTU, in bytes. Range: 576 to 1406. Default:1406

Command Default

The default MTU size is 1406.

Command Modes

Webvpn group policy configuration (config-webvpn-group)

Command History

Release	Modification
12.4(24)T	This command was introduced.

Usage Guidelines

The maximum size of prefragmented packets that is supported by the adapter is only 1406 bytes. Sending packets larger than 1406 bytes could cause potential problems; as a result, there is a size restriction.

Examples

The following example configures the MTU size to 778 bytes:

```
Device(config)# webvpn context context1
Device(config-webvpn-context)# policy group ONE
Device(config-webvpn-group)# svc mtu 778
```

Related Commands

Command	Description
policy group	Enters webvpn group policy configuration mode to configure a policy group.
webvpn context	Enters webvpn context configuration mode to configure an SSL VPN context.

svc rekey

To configure the time and method that a tunnel key is refreshed for policy group end users, use the **svc rekey**command in webvpn group policy configuration mode. To remove the tunnel key configuration from the policy group configuration, use the **no** form of this command.

svc rekey {**method** {**new-tunnel** | **ssl**} | **time** *seconds*}
no svc rekey {**method** {**new-tunnel** | **ssl**} | **time** *seconds*}

Syntax Description

method new-tunnel	Refreshes the tunnel key by creating a new tunnel connection to the end user.
method ssl	Refreshes the tunnel key by renegotiating the Secure Sockets Layer (SSL) session.
time *seconds*	Configures the time interval, in seconds, at which the tunnel key is refreshed. A number from 0 through 43200 seconds is entered.

Command Default

Time and method are not configured.

Command Modes

Webvpn group policy configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

Note SVC, or Secure Sockets Layer Virtual Private Network (SSL VPN) Client, is the predecessor of Cisco AnyConnect VPN Client software.

Examples

The following example configures the tunnel key to be refreshed by initiating a new tunnel connection once an hour:

```
Router(config)# webvpn context context1

Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# svc rekey method new-tunnel
Router(config-webvpn-group)# svc rekey time 3600
```

Related Commands

Command	Description
policy group	Enters webvpn group policy configuration mode to configure a policy group.
webvpn context	Enters webvpn configuration mode to configure the SSL VPN context.

svc split

To enable split tunneling for Cisco AnyConnect VPN Client tunnel clients, use the **svc split**command in webvpn group policy configuration mode. To remove the split tunneling configuration from the policy group configuration, use the **no** form of this command.

svc split {**include** | **exclude** [**local-lans**]} {*ip-address mask* | **acl** {*access-list-numberaccess-list-name*}}
no svc split {**include** | **exclude** [**local-lans**]} {*ip-address mask* | **acl**}

Syntax Description

include	Specifies the traffic to be sent over Secure Sockets Layer Virtual Private Network (SSL VPN) tunnel. Traffic from the specified IP address and mask is resolved through the Cisco AnyConnect VPN Client tunnel.
exclude	Specifies the traffic not to be sent over SSL VPN tunnel. Traffic from the specified IP address and mask is not resolved through the Cisco AnyConnect VPN Client tunnel.
local-lans	Specifies the traffic for local LANs not to be sent over SSL VPN tunnel.
ip-address mask	Destination network prefix.
acl	Specifies access-list identifier for classifying the tunnel traffic.
access-list-number	Standard IP access-list number. Range is from 1 to 99.
access-list-name	Access-list name.

Command Default

Split tunneling is not enabled for Cisco AnyConnect VPN Client tunnel clients.

Command Modes

WebVPN group policy configuration (config-webvpn-group)

Command History

Release	Modification
12.4(6)T	This command was introduced.
15.1(1)T	This command was modified. The **acl** keyword and the *access-list* and *access-list-name* arguments were added.

Usage Guidelines

Split tunnel support allows you to configure a policy that permits specific traffic to be carried outside the Cisco AnyConnect VPN Client tunnel. Traffic is either included (resolved in tunnel) or excluded (resolved through the Internet service provider [ISP] or WAN connection). Tunnel resolution configuration is mutually exclusive. An IP address cannot be both included and excluded at the same time. Entering the **local-lans** keyword permits the remote user to access resources on a local LAN, such as a network printer.

Note Switched Virtual Circuits (SVC), or the Secure Sockets Layer Virtual Private Network (SSL VPN) client, is the predecessor of Cisco AnyConnect VPN Client software.

Examples

The following example shows how to configure a list of IP addresses to be resolved over the tunnel (included) and a list to be resolved outside of the tunnel (excluded):

```
Router(config-webvpn-group)# svc split exclude 192.168.1.0 255.255.255.0

Router(config-webvpn-group)# svc split include 172.16.1.0 255.255.255.0
```

Related Commands

Command	Description
policy group	Enters WebVPN group policy configuration mode to configure a policy group.
webvpn context	Enters WebVPN configuration mode to configure the SSL VPN context.

svc split dns

To configure the Secure Sockets Layers Virtual Private Network (SSL VPN) gateway to resolve the specified fully qualified Domain Name System (DNS) names through the Cisco AnyConnect VPN Client tunnel, use the **svc split dns**command in webvpn group policy configuration mode. To remove the split DNS statement from the policy group configuration, use the **no** form of this command.

svc split dns *name*
no svc split dns *name*

Syntax Description

dns *name*	The *name* argument is entered as a fully qualified DNS name.

Command Default

The SSL VPN gateway is not configured to resolve the specified fully qualified DNS names through the Cisco AnyConnect VPN Client tunnel.

Command Modes

Webvpn group policy configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

Entering this command configures the SSL VPN gateway to resolve the specified DNS suffixes (domains) through the tunnel. The gateway automatically incudes the default domain into the list of domains that are resolved through the tunnel. Up to 10 DNS statements can be configured.

Note SVC, or Secure Sockets Layer Virtual Private Network (SSL VPN) Client, is the predecessor of Cisco AnyConnect VPN Client software.

Examples

The following example configures primary and secondary DNS servers for the policy group:

```
Router(config)# webvpn context context1

Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# svc split dns cisco.com
Router(config-webvpn-group)# svc split dns my.company.net
```

Related Commands

Command	Description
policy group	Enters webvpn group policy configuration mode to configure a policy group.
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

svc wins-server

To configure Windows Internet Name Service (WINS) servers for policy group end users, use the **svc wins-server**command in webvpn group policy configuration mode. To remove a WINS server from the policy group configuration, use the **no** form of this command.

svc wins-server {**primary** | **secondary**} *ip-address*
no svc dns-server {**primary** | **secondary**}

Syntax Description

primary | **secondary**	Configures the primary or secondary WINS server.
ip-address	An IPv4 address is entered to identify the server.

Command Default

WINS servers are not configured for policy group end users.

Command Modes

Webvpn group policy configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

Note SVC, or Secure Sockets Layer Virtual Private Network (SSL VPN) Client, is the predecessor of Cisco AnyConnect VPN Client software.

Examples

The following example configures primary and secondary WINS servers for the policy group:

```
Router(config)# webvpn context context1

Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# svc wins-server primary 172.31.1.1

Router(config-webvpn-group)# svc wins-server secondary 172.31.2.1
```

Related Commands

Command	Description
policy group	Enters webvpn group policy configuration mode to configure a policy group.
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

switchport port-security

To enable port security on an interface, use the **switchport port-security** command in interface configuration mode. To disable port security, use the **no** form of this command.

switchport port-security
no switchport port-security

Syntax Description

This command has no keywords or arguments.

Command Default

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(18)SXE	This command was changed as follows on the Supervisor Engine 720: • With Release 12.2(18)SXE and later releases, port security is supported on nonnegotiating trunks. • With Release 12.2(18)SXE and later releases, port security is supported on IEEE 802.1Q tunnel ports.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Follow these guidelines when configuring port security:

- With Release 12.2(18)SXE and later releases, port security is supported on nonnegotiating trunks.
- With Release 12.2(18)SXE and later releases, port security is supported on IEEE 802.1Q tunnel ports.
- Port security does not support Switch Port Analyzer (SPAN) destination ports.
- Port security does not support EtherChannel port-channel interfaces.
- With Cisco IOS Release 12.2(33)SXH and later releases, you can configure port security and 802.1X port-based authentication on the same port. With releases earlier than Cisco IOS Release 12.2(33)SXH:
  - If you try to enable 802.1X port-based authentication on a secure port, an error message appears and 802.1X port-based authentication is not enabled on the port.
  - If you try to enable port security on a port configured for 802.1X port-based authentication, an error message appears and port security is not enabled on the port.

Examples

This example shows how to enable port security:

```
Device(config-if)# switchport port-security
```

This example shows how to disable port security:

```
Device(config-if)# no switchport port-security
```

Related Commands

Command	Description
show port-security	Displays information about the port-security setting.

switchport port-security aging

To configure the port security aging , use the **switchport** port-security aging time command in interface configuration mode . To disable aging, use the **no** form of this command.

switchport port-security aging {**time** *time* | **type** {**absolute** | **inactivity**}}
no switchport port-security aging

Syntax Description

time *time*	Sets the duration for which all addresses are secured; valid values are from 1 to 1440 minutes.
type	Specifies the type of aging.
absolute	Specifies absolute aging; see the "Usage Guidelines" section for more information.
inactivity	Specifies that the timer starts to run only when there is no traffic; see the "Usage Guidelines" section for more information.

Command Default

The defaults are as follows:

- Disabled.
- If enabled, t he defaults are as follows:
  - *time* is 0.
  - **type** is **absolute**

Command Modes

Interface configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(18)SXE	This command was changed as follows on the Supervisor Engine 720: • With Release 12.2(18)SXE and later releases, port security is supported on trunks. • With Release 12.2(18)SXE and later releases, port security is supported on 802.1Q tunnel ports. • The **type**, **absolute**, and **inactivity** keywords were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Follow these guidelines when configuring port security:

- With Release 12.2(18)SXE and later releases, port security is supported on trunks. With releases earlier than Release 12.2(18)SXE, port security is not supported on trunks.

- With Release 12.2(18)SXE and later releases, port security is supported on 802.1Q tunnel ports. With releases earlier than Release 12.2(18)SXE, port security is not supported on 802.1Q tunnel ports.

You can apply one of two types of aging for automatically learned addresses on a secure port:

- Absolute aging times out the MAC address after the age-time has been exceeded, regardless of the traffic pattern. This default is for any secured port, and the age-time is set to 0.
- Inactivity aging times out the MAC address only after the age_time of inactivity from the corresponding host has been exceeded.

Examples

This example shows how to set the aging time as 2 hours:

```
Router(config-if)# switchport port-security aging time 120
```

This example shows how to set the aging time as 2 minutes:

```
Router(config-if)# switchport port-security aging time 2
```

This example shows how to set the aging type on a port to absolute aging:

```
Router(config-if) switchport port-security aging type absolute
```

This example shows how to set the aging type on a port to inactivity aging:

```
Router(config-if) switchport port-security aging type
 inactivity
```

Related Commands

Command	Description
show port-security	Displays information about the port-security setting.

switchport port-security mac-address

To add a MAC address to the list of secure MAC addresses, use the **switchport port-security mac-address** command. To remove a MAC address from the list of secure MAC addresses, use the **no** form of this command.

switchport port-security mac-address {*mac-addr* | **sticky** [*mac-addr*] [{**vlan** *vlan* [**voice**]*vlan-list*}]}
no switchport port-security mac-address {*mac-addr* | **sticky** [*mac-addr*] [{**vlan** *vlan* [**voice**]*vlan-list*}]}

Syntax Description

mac-addr	MAC addresses for the interface; valid values are from 1 to 1024.
sticky	Configures the dynamic MAC addresses as sticky on an interface.
vlan *vlan* | *vlan-list*	(Optional) Specifies a VLAN or range of VLANs; see the "Usage Guidelines" section for additional information.

Command Default

MAC-addresses are not classified as secured.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(18)SXE	This command was changed as follows on the Supervisor Engine 720: • With Release 12.2(18)SXE and later releases, port security is supported on trunks. • With Release 12.2(18)SXE and later releases, port security is supported on 802.1Q tunnel ports. • The **vlan** *vlan* | *vlan-list*keyword and arguments were added. • The **sticky** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

If you configure fewer secure MAC addresses than the maximum number of secure MAC addresses on all interfaces, the remaining MAC addresses are dynamically learned.

To clear multiple MAC addresses, you must enter the **no** form of this command once for each MAC address to be cleared.

The *vlan-list* argument is visible only if the port has been configured and is operational as a trunk. Enter the **switchport mode trunk** command and then enter the **switchport nonegotiate** command.

The **sticky** keyword configures the dynamic MAC addresses as sticky on an interface. Sticky MAC addresses configure the static Layer 2 entry to stay sticky to a particular interface. This feature can prevent MAC moves or prevent the entry from being learned on a different interface.

You can configure the sticky feature even when the port security feature is not enabled on the interface. It becomes operational once port security is enabled on the interface.

Note You can enter the **switchport port-security mac-address sticky** command only if sticky is enabled on the interface.

When port security is enabled, disabling the sticky feature causes all configured and learned sticky addresses to be deleted from the configuration and converted into dynamic secure addresses.

When port security is disabled, disabling the sticky feature causes all configured and learned sticky addresses to be deleted from the configuration.

For trunk ports, if you enter the **no switchport port-security mac-address sticky** command, a search is conducted for the MAC address in the native VLAN. An error message is displayed if the MAC address is not found in the native VLAN. You must specify the VLAN in the **no** form of the **switchport port-security mac-address sticky** command to remove the MAC address.

For voice ports, you must specify the **vlan voice** keywords in the **no** form of the command.

Examples

This example shows how to configure a secure MAC address:

```
Router(config-if)# switchport port-security mac-address 1000.2000.3000
```

This example shows how to delete a secure MAC address from the address table:

```
Router(config-if)# no switchport port-security mac-address 1000.2000.3000
```

This example shows how to enable the sticky feature on an interface:

```
Router(config-if)# switchport port-security mac-address sticky
```

This example shows how to disable the sticky feature on an interface:

```
Router(config-if)# no switchport port-security mac-address sticky
```

This example shows how to make a specific MAC address as a sticky address:

```
Router(config-if)# switchport port-security mac-address sticky 0000.0000.0001
```

This example shows how to delete a specific sticky address:

```
Router(config-if)# no switchport port-security mac-address sticky 0000.0000.0001
```

This example shows how to delete all sticky and static addresses that are configured on an interface:

```
Router(config-if)# no switchport port-security mac-address
```

The following example shows how to configure a VLAN in the voice port:

```
Router(config-if)# switch port-security mac-address 0.0.1 vlan voice
```

To remove the MAC address 0.0.1 from the voice port, use the following command:

```
Router(config-if)# no switchport port-security mac-address 0.0.1 vlan voice
```

Related Commands

Command	Description
clear port-security	Deletes configured secure MAC addresses and sticky MAC addresses from the MAC address table.
show port-security	Displays information about the port-security setting.
switchport mode trunk	Configures the port as a trunk member.
switchport nonegotiate	Configures the LAN port into permanent trunking mode.

switchport port-security maximum

To set the maximum number of secure MAC addresses on a port, use the **switchport port-security maximum**command in interface configuration mode. To return to the default settings, use the **no** form of this command.

switchport port-security maximum *maximum* [{**vlan** *vlanvlan-list*}]
no switchport port-security maximum

Syntax Description

maximum	M aximum number of secure MAC addresses for the interface; valid values are from 1 to 4097.
vlan *vlan* | *vlan-list*	(Optional) Specifies a VLAN or range of VLANs; see the "Usage Guidelines" section for additional information.

Command Default

This command has no default setings .

Command Modes

Interface configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to the Release 12.2(17d)SXB.
12.2(18)SXE	This command was changed as follows on the Supervisor Engine 720 only: • The maximum number of secure MAC addresses was changed from 1024 to 4097. • The **vlan** *vlan* | *vlan-list*keyword and arguments were added. • With Release 12.2(18)SXE and later releases, port security is supported on trunks. • With Release 12.2(18)SXE and later releases, port security is supported on 802.1Q tunnel ports.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

If you enter this command more than once, subsequent use of this command overrides the previous value of *maximum*. If the new *maximum*argument is larger than the current number of the secured addresses on this port, there is no effect except to increase the value of the *maximum*.

If the new *maximum* is smaller than the old *maximum* and there are more secure addresses on the old *maximum*, the command is rejected.

If you configure fewer secure MAC addresses than the maximum number of secure MAC addresses on the port, the remaining MAC addresses are dynamically learned.

Once the maximum number of secure MAC addresses for the port is reached, no more addresses are learned on that port even if the per-VLAN port maximum is different from the aggregate maximum number.

You can override the maximum number of secure MAC addresses for the port for a specific VLAN or VLANs by entering the **switchport port-security maximum** *maximum* **vlan** *vlan* | *vlan-list*command.

The *vlan-list* argument allows you to enter ranges, commas, and delimited entries such as 1,7,9-15,17.

The *vlan-list* argument is visible only if the port has been configured and is operational as a trunk. Enter the **switchport mode trunk** command and then enter the **switchport nonegotiate** command.

Examples

This example shows how to set the maximum number of secure MAC addresses that are allowed on this port:

```
Router(config-if)# switchport port-security maximum 5
```

This command shows how to override the maximum set for a specific VLAN:

```
Router(config-if)# switchport port-security maximum 3 vlan 102
```

Related Commands

Command	Description
show port-security	Display information about the port-security setting.
switchport nonegotiate	Configures the LAN port into permanent trunking mode.

switchport port-security violation

To set the action to be taken when a security violation is detected, use the **switchport port-security violation** command in interface configuration mode. To return to the default settings, use the **no** form of this command.

switchport port-security violation {**shutdown** | **restrict** | **protect**}
no switchport port-security violation {**shutdown** | **restrict** | **protect**}

Syntax Description

shutdown	Shuts down the port if there is a security violation.
restrict	Drops all the packets from the insecure hosts at the port-security process level and increments the security-violation count.
protect	Drops all the packets from the insecure hosts at the port-security process level but does not increment the security-violation count.

Command Default

The port security violation is shutdown.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(18)SXE	This command was changed as follows on the Supervisor Engine 720: • With Release 12.2(18)SXE and later releases, port security is supported on trunks. • With Release 12.2(18)SXE and later releases, port security is supported on 802.1Q tunnel ports.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(14)SXH	**Platform port-security disable traps** was introduced as part of protect violation mode.

Usage Guidelines

When a security violation is detected, one of the following actions occurs:

- Protect--When the number of port-secure MAC addresses reaches the maximum limit that is allowed on the port, the packets with unknown source addresses are dropped until you remove a sufficient number of secure MAC addresses. Platform port-security disable traps is configurable only when the violation mode is set to **protect**. When this option is configured, drop entries will not be installed into hardware for violating addresses, thus allowing traffic to continue to flow to violating address from legitimate ports. To protect switch CPU against overload when this option is enabled, we recommend that you configure the port-security rate-limiter to 2000 packets per second with a burst rate of 10.

Note This feature also permits traffic to legitimate ports from insecure MAC addresses.

- Restrict--A port-security violation restricts data and causes the security-violation counter to increment.
- Shutdown--The interface is error disabled when a security violation occurs.

Note When a secure port is in the error-disabled state, you can bring it out of this state by entering the **errdisable recovery cause psecure-violation** global configuration command or you can manually reenable it by entering the **shutdown** and **no shutdown** commands in interface-configuration mode.

Examples

This example shows how to set the action to be taken when a security violation is detected:

```
Router(config-if)# switchport port-security violation restrict
```

This example allows the traffic to a secured MAC address on one port to flow even in the presence of violations on other ports while in protect mode.

```
Router(config-if)# switchport port-security violation protect
Router(config-if)# platform port-security disable traps
```

Related Commands

Command	Description
show port-security	Displays information about the port-security setting.
errdisable recovery cause psecure-violation (global configuration)	Removes a secure port from an error-disabled state.
platform port-security disable traps	Modifies the behavior of protect violation mode.

tacacs-server administration through title-color

tacacs server

To configure the TACACS+ server for IPv6 or IPv4 and enter TACACS+ server configuration mode, use the **tacacs server**command in global configuration mode. To remove the configuration, use the **no** form of this command.

tacacs server *name*
no tacacs server

Syntax Description

name	Name of the private TACACS+ server host.

Command Default

No TACACS+ server is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.

Usage Guidelines

The **tacacs server** command configures the TACACS server using the *name* argument and enters TACACS+ server configuration mode. The configuration is applied once you have finished configuration and exited TACACS+ server configuration mode.

Examples

The following example shows how to configure the TACACS server using the name server1 and enter TACACS+ server configuration mode to perform further configuration:

```
Router(config)# tacacs server server1
Router(config-server-tacacs)#
```

Related Commands

Command	Description
address ipv6 (TACACS+)	Configures the IPv6 address of the TACACS+ server.
key (TACACS+)	Configures the per-server encryption key on the TACACS+ server.
port (TACACS+)	Specifies the TCP port to be used for TACACS+ connections.
send-nat-address (TACACS+)	Sends a client's post-NAT address to the TACACS+ server.
single-connection **(TACACS+)**	Enables all TACACS packets to be sent to the same server using a single TCP connection.
timeout **(TACACS+)**	Configures the time to wait for a reply from the specified TACACS server.

tacacs-server administration

To enable the handling of administrative messages by the TACACS+ daemon, use the **tacacs-server administration** command in global configuration mode. To disable the handling of administrative messages by the TACACS+ daemon, use the **no** form of this command.

tacacs-server administration
no tacacs-server administration

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration

Command History

Release	Modification
Prior to 12.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example shows that the TACACS+ daemon is enabled to handle administrative messages:

```
tacacs-server administration
```

tacacs-server directed-request

To send only a username to a specified server when a direct request is issued, use the **tacacs-server directed-request**command in global configuration mode. To send the entire string to the TACACS+ server, use the **no** form of this command.

tacacs-server directed-request [**restricted**] [**no-truncate**]
no tacacs-server directed-request

Syntax Description

restricted	(Optional) Restrict queries to directed request servers only.
no-truncate	(Optional) Do not truncate the @hostname from the username.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
11.1	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command sends only the portion of the username before the "@" symbol to the host specified after the "@" symbol. In other words, with the directed-request feature enabled, you can direct a request to any of the configured servers, and only the username is sent to the specified server.

Disabling **tacacs-server directed-request** causes the whole string, both before and after the "@" symbol, to be sent to the default TACACS+ server. When the directed-request feature is disabled, the router queries the list of servers, starting with the first one in the list, sending the whole string, and accepting the first response that it gets from the server. The **tacacs-server directed-request** command is useful for sites that have developed their own TACACS+ server software that parses the whole string and makes decisions based on it.

With **tacacs-server directed-request** enabled, only configured TACACS+ servers can be specified by the user after the "@" symbol. If the host name specified by the user does not match the IP address of a TACACS+ server configured by the administrator, the user input is rejected.

Use **no tacacs-server directed-request** to disable the ability of the user to choose between configured TACACS+ servers and to cause the entire string to be passed to the default server.

Examples

The following example disables **tacacs-server directed-request** so that the entire user input is passed to the default TACACS+ server:

```
no tacacs-server directed-request
```

tacacs-server dns-alias-lookup

To enable IP Domain Name System (DNS) alias lookup for TACACS+ servers, use the command in global configuration mode. To disable IP DNS alias lookup, use the **no** form of this command.

tacacs-server dns-alias-lookup
no tacacs-server dns-alias-lookup

Syntax Description

This command has no arguments or keywords.

Command Default

IP DNS alias lookup is disabled.

Command Modes

global configuration

Command History

Release	Modification
Prior to 12.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example shows that IP DNS alias lookup has been enabled:

```
tacacs-server dns-alias-lookup
```

tacacs-server domain-stripping

To configure a network access server (NAS) to strip suffixes, or to strip both suffixes and prefixes from the username before forwarding the username to the remote TACACS+ server, use the **tacacs-server domain-stripping** command in global configuration mode. To disable a stripping configuration, use the no form of this command.

tacacs-server domain-stripping [{[**right-to-left**] [**prefix-delimiter** *character* [*character2 . . . character7*]] [**delimiter** *character* [*character2 . . . character7*]] | **strip-suffix** *suffix*}] [**vrf** *vrf-name*]
no tacacs-server domain-stripping [{[**right-to-left**] [**prefix-delimiter** *character* [*character2 . . . character7*]] [**delimiter** *character* [*character2 . . . character7*]] | **strip-suffix** *suffix*}] [**vrf** *vrf-name*]

Syntax Description

right-to-left	(Optional) Specifies that the NAS will apply the stripping configuration at the first delimiter found when parsing the full username from right to left. The default is for the NAS to apply the stripping configuration at the first delimiter found when parsing the full username from left to right.
prefix-delimiter *character* [*character2...character7*]	(Optional) Enables prefix stripping and specifies the character or characters that will be recognized as a prefix delimiter. Valid values for the *character* argument are @, /, $, %, \, #, and -. Multiple characters can be entered without intervening spaces. Up to seven characters can be defined as prefix delimiters, which is the maximum number of valid characters. If a \ is entered as the final or only value for the *character* argument, it must be entered as \\. No prefix delimiter is defined by default.
delimiter *character* [*character2...character7*]	(Optional) Specifies the character or characters that will be recognized as a suffix delimiter. Valid values for the *character* argument are @, /, $, %, \, #, and -. Multiple characters can be entered without intervening spaces. Up to seven characters can be defined as suffix delimiters, which is the maximum number of valid characters. If a \ is entered as the final or only value for the *character* argument, it must be entered as \\. The default suffix delimiter is the @ character.
strip-suffix *suffix*	(Optional) Specifies a suffix to strip from the username.
vrf *vrf-name*	(Optional) Restricts the domain stripping configuration to a Virtual Private Network (VPN) routing and forwarding (VRF) instance. The *vrf-name*argument specifies the name of a VRF.

Command Default

Stripping is disabled. The full username is sent to the TACACS+ server.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(4)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
XE 2.5	This command was integrated into Cisco IOS Release XE 2.5.

Usage Guidelines

Use the **tacacs-server domain-stripping** command to configure the NAS to strip the domain from a username before forwarding the username to the TACACS+ server. If the full username is user1@cisco.com, enabling the **tacacs-server domain-stripping** command results in the username "user1" being forwarded to the TACACS+ server.

Use the **right-to-left**keyword to specify that the username should be parsed for a delimiter from right to left, rather than from left to right. This allows strings with two instances of a delimiter to strip the username at either delimiter. For example, if the username is user@cisco.com@cisco.net, the suffix could be stripped in two ways. The default direction (left to right) would result in the username "user" being forwarded to the TACACS+ server. Configuring the **right-to-left**keyword would result in the username "user@cisco.com" being forwarded to the TACACS+ server.

Use the **prefix-delimiter** keyword to enable prefix stripping and to specify the character or characters that will be recognized as a prefix delimiter. The first configured character that is parsed will be used as the prefix delimiter, and any characters before that delimiter will be stripped.

Use the **delimiter** keyword to specify the character or characters that will be recognized as a suffix delimiter. The first configured character that is parsed will be used as the suffix delimiter, and any characters after that delimiter will be stripped.

Use **strip-suffix** *suffix*to specify a particular suffix to strip from usernames. For example, configuring the **tacacs-server domain-stripping strip-suffix cisco.net**command would result in the username user@cisco.net being stripped, while the username user@cisco.com will not be stripped. You may configure multiple suffixes for stripping by issuing multiple instances of the **tacacs-server domain-stripping** command. The default suffix delimiter is the @ character.

Note Issuing the **tacacs-server domain-stripping strip-suffix** *suffix* command disables the capacity to strip suffixes from all domains. Both the suffix delimiter and the suffix must match for the suffix to be stripped from the full username. The default suffix delimiter of @ will be used if you do not specify a different suffix delimiter or set of suffix delimiters using the **delimiter**keyword.

Note Issuing the **no tacacs-server host** command reconfigures the TACACS server host information. You can view the contents of the current running configuration file using the **show running-config** command.

To apply a domain-stripping configuration only to a specified VRF, use the **vrf** *vrf-name* option.

The interactions between the different types of domain stripping configurations are as follows:

- You may configure only one instance of the **tacacs-server domain-stripping**[**right-to-left**] [**prefix-delimiter** *character* [*character2...character7*]] [**delimiter** *character* [*character2...character7*]]command.
- You may configure multiple instances of the **tacacs-server domain-stripping**[**right-to-left**] [**prefix-delimiter** *character* [*character2...character7*]] [**delimiter** *character* [*character2...character7*]] [**vrf** *vrf-name*]command with unique values for **vrf** *vrf-name*.
- You may configure multiple instances of the **tacacs-server domain-stripping strip-suffix** *suffix*[**vrf** *per-vrf*]command to specify multiple suffixes to be stripped as part of a global or per-VRF ruleset.

- Issuing any version of the **tacacs-server domain-stripping**command automatically enables suffix stripping using the default delimiter character @ for that ruleset, unless a different delimiter or set of delimiters is specified.
- Configuring a per-suffix stripping rule disables generic suffix stripping for that ruleset. Only suffixes that match the configured suffix or suffixes will be stripped from usernames.

Examples

The following example shows how to configure the router to parse the username from right to left and set the valid suffix delimiter characters as @, \, and $. If the full username is cisco/user@cisco.com$cisco.net, the username "cisco/user@cisco.com" will be forwarded to the TACACS+ server because the $ character is the first valid delimiter encountered by the NAS when parsing the username from right to left.

```
tacacs-server domain-stripping right-to-left delimiter @\$
```

The following example shows how to configure the router to strip the domain name from usernames only for users associated with the VRF instance named abc. The default suffix delimiter @ will be used for generic suffix stripping.

```
tacacs-server domain-stripping vrf abc
```

The following example shows how to enable prefix stripping using the character / as the prefix delimiter. The default suffix delimiter character @ will be used for generic suffix stripping. If the full username is cisco/user@cisco.com, the username "user" will be forwarded to the TACACS+ server.

```
tacacs-server domain-stripping prefix-delimiter /
```

The following example shows how to enable prefix stripping, specify the character / as the prefix delimiter, and specify the character # as the suffix delimiter. If the full username is cisco/user@cisco.com#cisco.net, the username "user@cisco.com" will be forwarded to the TACACS+ server.

```
tacacs-server domain-stripping prefix-delimiter / delimiter #
```

The following example shows how to enable prefix stripping, configure the character / as the prefix delimiter, configure the characters $, @, and # as suffix delimiters, and configure per-suffix stripping of the suffix cisco.com. If the full username is cisco/user@cisco.com, the username "user" will be forwarded to the TACACS+ server. If the full username is cisco/user@cisco.com#cisco.com, the username "user@cisco.com" will be forwarded.

```
tacacs-server domain-stripping prefix-delimiter / delimiter $@#
tacacs-server domain-stripping strip-suffix cisco.com
```

The following example shows how to configure the router to parse the username from right to left and enable suffix stripping for usernames with the suffix cisco.com. If the full username is cisco/user@cisco.net@cisco.com, the username "cisco/user@cisco.net" will be forwarded to the TACACS+ server. If the full username is cisco/user@cisco.com@cisco.net, the full username will be forwarded.

```
tacacs-server domain-stripping right-to-left
tacacs-server domain-stripping strip-suffix cisco.com
```

The following example shows how to configure a set of global stripping rules that will strip the suffix cisco.com using the delimiter @, and a different set of stripping rules for usernames associated with the VRF named myvrf:

```
tacacs-server domain-stripping strip-suffix cisco.com
!
tacacs-server domain-stripping prefix-delimiter # vrf myvrf
tacacs-server domain-stripping strip-suffix cisco.net vrf myvrf
```

Related Commands

Command	Description
aaa new-model	Enables the AAA access control model.
ip vrf	Defines a VRF instance and enters VRF configuration mode.
radius-server domain-stripping	Configures a router to strip a prefix or suffix from the username before forwarding the username to the RADIUS server.

tacacs-server host

To specify a TACACS+ host, use the **tacacs-server host** command in global configuration mode. To delete the specified name or address, use the **no** form of this command.

tacacs-server host {*hostname host-ip-address*} [**key** *string*] [[**nat**] [**port** [{*integer*}]] [**single-connection**] [**timeout** [{*integer*}]]]
no tacacs-server host {*hostname host-ip-address*}

Syntax Description

hostname	Name of the host.
host-ip-address	IP address of the host.
key	(Optional) Specifies an authentication and encryption key. This must match the key used by the TACACS+ daemon. Specifying this key overrides the key set by the global command **tacacs-server key** for this server only.
string	(Optional) Character string specifying authentication and encryption key. The *string* can be **0** (specifies that an unencrypted key follows), **6** (specifies that an advanced encryption scheme [AES] encrypted key follows), **7** (specifies that a hidden key follows), or a line specifying the unencrypted (clear-text) server key.
nat	(Optional) Port Network Address Translation (NAT) address of the client is sent to the TACACS+ server.
port	(Optional) Specifies a TACACS+ server port number. This option overrides the default, which is port 49.
integer	(Optional) Port number of the server. Valid port numbers range from 1 through 65535.
single-connection	(Optional) Maintains a single open connection between the router and the TACACS+ server.
timeout	(Optional) Specifies a timeout value. This overrides the global timeout value set with the **tacacs-server timeout** command for this server only.
integer	(Optional) Integer value, in seconds, of the timeout interval. The value is from 1 through 1000.

Command Default

No TACACS+ host is specified.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.
12.1(11), 12.2(6)	This command was modified. The **nat** keyword was added.

Release	Modification
12.2(8)T	This command was modified. The **nat** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.4(1)T	This command was modified. The **6** keyword was added.

Usage Guidelines

You can use multiple **tacacs-server host** commands to specify additional hosts. The Cisco IOS software searches for hosts in the order in which you specify them. Use the **port**, **timeout**, **key**, **single-connection**, and **nat** keywords only when running a AAA/TACACS+ server.

Because some of the parameters of the **tacacs-server host** command override global settings made by the **tacacs-server timeout** and **tacacs-server key** commands, you can use this command to enhance security on your network by uniquely configuring individual routers.

The **single-connection** keyword specifies a single connection (only valid with CiscoSecure Release 1.0.1 or later). Rather than have the router open and close a TCP connection to the server each time it must communicate, the single-connection option maintains a single open connection between the router and the server. The single connection is more efficient because it allows the server to handle a higher number of TACACS operations.

Use the **password encryption aes** command to configure type 6 AES encrypted keys.

Examples

The following example shows how to specify a TACACS+ host named Sea_Change:

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# tacacs-server host Sea_Change
```

The following example shows how to specify that, for authentication, authorization, and accounting (AAA) confirmation, the router consults the TACACS+ server host named Sea_Cure on port number 51. The timeout value for requests on this connection is three seconds; the encryption key is a_secret.

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# tacacs-server host Sea_Cure port 51 timeout 3 key a_secret
```

Related Commands

Command	Description
aaa accounting	Enables AAA accounting of requested services for billing or security.
aaa authentication	Specifies or enables AAA authentication.
aaa authorization	Sets parameters that restrict user access to a network.
password encryption aes	Enables a type 6 encrypted preshared key.

Command	Description
ppp	Starts an asynchronous connection using PPP.
slip	Starts a serial connection to a remote host using SLIP.
tacacs-server key	Sets the authentication encryption key used for all TACACS+ communications between the access server and the TACACS+ daemon.

tacacs-server key

To set the authentication encryption key used for all TACACS+ communications between the access server and the TACACS+ daemon, use the **tacacs-server key** command in global configuration mode. To disable the key, use the **no** form of this command.

tacacs-server key {**0** *string* | **6** *string* | **7** *string string*}
no tacacs-server key {**0** *string* | **6** *string* | **7** *string string*}

Syntax Description

0 *string*	Specifies that an unencrypted key follows. • *string*—The unencrypted (clear text) shared key.
6 *string*	Specifies that an advanced encryption scheme (AES) encrypted key follows. • *string*—The advanced encryption scheme [AES] encrypted key.
7 *string*	Specifies that a hidden key follows. • *string*—The hidden shared key.
string	The unencrypted (clear text) shared key.

Command Default

This authentication encryption key is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.1	This command was introduced.
12.3(2)T	This command was modified. The **0** *string* and **7** *string* keywords and argument pairs were added.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2(33)SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.4(1)T	This command was modified. The **6** keyword was added.

Usage Guidelines

After enabling authentication, authorization, and accounting (AAA) with the**aaa new-model** command, you must set the authentication and encryption key using the **tacacs-server key** command.

The key entered must match the key used on the TACACS+ daemon. All leading spaces are ignored; spaces within and at the end of the key are not. If you use spaces in your key, do not enclose the key in quotation marks unless the quotation marks themselves are part of the key.

The use of special characters in the key are supported in Cisco IOS Release 12.2.58-SE1(ED) and later releases. If you use the ` character in the key in earlier releases, it generates an error.

Use the **password encryption aes** command to configure type 6 AES encrypted keys.

Examples

The following example shows how to set the authentication and encryption key to cisco123:

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# tacacs-server key cisco123
```

Related Commands

Command	Description
aaa new-model	Enables the AAA access control model.
password encryption aes	Enables a type 6 encrypted preshared key.
tacacs-server host	Specifies a TACACS+ host.

tacacs-server packet

To specify the maximum size of TACACS+ packets, use the **tacacs-server packet**command in global configuration mode. To disable, use the **no** form of this command.

tacacs-server packet maxsize *size*
no tacacs-server packet maxsize

Syntax Description

maxsize *size*	Specifies maximum TACACS+ packet size. The range is from 10240 to 65536.

Command Default

The default maximum size for a TACAC+ packet is 65536.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0	This command was introduced in a release earlier than Cisco IOS Release 12.0
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example shows how to set the the maximum TACACS+ packet size to 10240:

```
tacacs-server packet maxsize 10240
```

tacacs-server timeout

To set the interval for which the TACACS server waits for a server host to reply, use the **tacacs-server timeout** command in global configuration mode. To restore the default timeout interval, use the **no** form of this command.

tacacs-server timeout *seconds*
no tacacs-server timeout

Syntax Description

seconds	Timeout interval, in seconds. The range is from 1 to 1000. The default is 5.

Command Default

The default timeout interval for which the server waits for the server host to reply is 5 seconds.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **tacacs-server timeout**command to set the interval for which the server waits for a server host to reply. A TCP connection between the server and the host times out during higher loads. Therefore, to delay TCP timeouts, change the timeout interval to 30 seconds. You can also configure the **tacacs-server host** command with the **single-connection** keyword to delay TCP timeouts.

Examples

The following example shows how to set the timeout interval to 20 seconds:

```
Router# configure terminal
Router(config)# tacacs-server timeout 20
```

Related Commands

Command	Description
tacacs-server host	Specifies a TACACS+ host.

tag cts sgt

To enable Cisco TrustSec (CTS) SGT inline tagging in a GDOI group IPsec SA, use the **tag cts sgt** command in GDOI SA IPsec configuration mode.

tag cts sgt

Syntax Description

This command has no arguments or keywords.

Command Modes

GDOI SA IPsec configuration (gdoi-sa-ipsec)

Command History

Release	Modification
15.3(2)T	This command was introduced.
Cisco IOS XE Release 3.9S	This command was integrated into Cisco IOS XE Release 3.9S.

Usage Guidelines

CTS maintains classification of each packet by tagging packets on ingress to the CTS network, so that they can be properly identified for applying security and other policy criteria along the data path.

You use this command on a key server (KS) or primary KS.

Because GET VPN is a technology that is based on groups, all devices in the same group (including the KS, cooperative KSs, and GMs) must support CTS SGT inline tagging before the group's KS can enable the feature. If you want to enable the feature for a group, you must ensure that all devices in the group are running compatible versions of the GET VPN software by using the **show crypto gdoi feature cts-sgt** command on the KS or primary KS.

If incompatible devices exist in the group when you use this command, the following message appears:

```
WARNING for group GET-SGT: some devices cannot support SGT inline tagging. Rekey can cause
 traffic disruption and GM registration failures. Please check 'show crypto gdoi feature
sgt'.
Are you sure you want to proceed ? [yes/no]:
```

After you use this command, you must use the **crypto gdoi ks rekey** command on the KS or primary KS to trigger a rekey.

Examples

The following example shows how to configure CTS SGT inline tagging in an IPsec SA for a KS serving a single GDOI group:

```
Device> enable
Device# configure terminal
Device(config)# ip access-list extended ACL-SGT
Device(config-ext-nacl)# permit ip any any
Device(config-ext-nacl)# exit
Device(config)# crypto gdoi group GET-SGT
Device(config-gdoi-group)# identity number 1
Device(config-gdoi-group)# server local
Device(gdoi-local-server)# sa ipsec 1
Device(gdoi-sa-ipsec)# tag cts sgt
Device(gdoi-sa-ipsec)# profile gdoi-p2
Device(gdoi-sa-ipsec)# match address ipv4 ACL-SGT
```

```
Device(gdoi-sa-ipsec)# replay time window-size 100
Device(gdoi-sa-ipsec)# end
```

Related Commands

Command	Description
crypto gdoi ks rekey	Triggers a rekey of group members in a GET VPN network.
show crypto gdoi feature cts-sgt	Displays whether each device in the GET VPN network supports CTS SGT inline tagging, and displays the version of GET VPN software running on each device.

target-value

To define the target value rating for a host, use the **target-value**command in configuration rule configuration mode. To change the target value rating or revert to the default value, use the **no** form of this command.

target-value{**mission-critical** | **high** | **medium** | **low**}**target-address** *ip-address* [{*/nn* | **to***ip-address*}]
no target-value{**mission-critical** | **high** | **medium** | **low**}**target-address** *ip-address* [{*/nn* | **to***ip-address*}]

Syntax Description

mission-critical | **high** | **medium** | **low**	Rates how important the system is to the network.
target-address *ip-address* [*/ nn* | **to** *ip-address*	A host, which can consist of a single IP address or a range of IP addresses.

Command Default

medium

Command Modes

Configuration rule configuration (config-rul)

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Use the **target-value**command to set the target value rating, which allows users to develop security policies that can be more strict for some resources than others. The security policy is applied to a table of hosts that are protected by Cisco IOS Intrusion Prevention System (IPS). A host can be a single IP address or a range of IP addresses with an associated target value rating.

Note Changes to the target value rating is not shown in the run time config because the changes are recorded in the seap-delta.xml file, which can be located via the **ip ips config location**command.

Examples

The following example shows how to change the target value to low for the host 192.168.0.1:

```
configure terminal
ip ips event-action-rules
 target-value low target-address 192.168.0.1
```

tcp finwait-time

To specify how long a TCP session will be managed after the Cisco IOS firewall detects a FIN-exchange, use the **tcp finwait-time** command in parameter-map type inspect configuration mode. To disable this function, use the **no** form of this command.

tcp finwait-time *seconds* [{**ageout-time** *seconds*}]
no tcp finwait-time

Syntax Description

seconds	Amount of time, in seconds, that a TCP session will be managed after the firewall detects a FIN-exchange. The default is 5. Valid values are from 1 to 2147483.
ageout-time *seconds*	(Optional) Specifies the aggressive aging time for TCP packets. Valid values are from 1 to 2147483.

Command Default

The default management time is 5 seconds.

Command Modes

Parameter-map type inspect configuration (config-profile)

Command History

Release	Modification
12.4(6)T	This command was introduced.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
Cisco IOS XE Release 3.4S	This command was modified. The **ageout-time** *seconds* keyword and argument pair was added.

Usage Guidelines

In a TCP connection, the client and the server terminate their end of the connection by sending a finish (FIN) message. The time the client and the server wait for their FIN message to be acknowledged by the other side before closing the sequence during a TCP connection is called the finwait-time. The timeout that you set for the finwait-time is referred to as the finwait timeout.

When the software detects a valid TCP packet that is the first in a session, it establishes state information for the new session.

Use the **tcp finwait-time** command to define how long TCP session state information will be maintained after the firewall detects a FIN-exchange for the session. The FIN-exchange occurs when the TCP session is ready to close. The global value specified for the timeout applies to all TCP sessions.

When you configure an inspect parameter map, you can enter the **tcp finwait-time** command only after you enter the **parameter-map type inspect** command.

For detailed information about creating a parameter map, see the **parameter-map type inspect** command.

Examples

The following example show how to change the finwait timeout to 20 seconds:

```
parameter-map type inspect eng_network_profile
 tcp finwait-time 20
```

The following example show how to change the finwait idle timeout to 40 seconds:

```
parameter-map type inspect eng_network_profile
 tcp finwait-time 20 ageout-time 40
```

Related Commands

Command	Description
ip inspect tcp finwait-time	Defines how long a TCP session will still be managed after the firewall detects a FIN-exchange.
max-incomplete aggressive-aging	Configures aggressive aging of half-opened firewall sessions.
parameter-map type inspect	Configures an inspect parameter map for connecting thresholds, timeouts, and other parameters pertaining to the **inspect** action.

tcp half-close reset

To specify whether the TCP reset (RST) segment should be sent when a half-close session is cleared, use the **tcp half-close reset** command in parameter-map type inspect configuration mode. To specify that the TCP RST segment should not be sent when a half-close session is cleared, use the **no** form of this command.

tcp half-close reset {**off** | **on**}
no tcp half-close reset {**off** | **on**}

Syntax Description

off	Disables TCP half-close RST segment transmission.
on	Enables on TCP half-close RST segment transmission.

Command Default

The TCP reset segment is sent when a half-close session is cleared.

Command Modes

Parameter-map type inspect configuration (config-profile)

Command History

Release	Modification
Cisco IOS XE Release 3.8S	This command was introduced.

Usage Guidelines

TCP provides the ability for one end of a connection to terminate its output while still receiving data from the other end of the connection. This TCP state is called the half-close state. A session enters the half-close state when it receives the first TCP finish (FIN) segment and starts a timer. If another segment is received before the session timeout occurs, then the timer is restarted.

You can set the timeout value for a half-close session by using the **tcp synwait-time** command. The default timeout value is 30 seconds.

When you configure an inspect type parameter map, you can enter the **tcp half-close reset** command after you enter the **parameter-map type inspect** command.

If you configure the **tcp half-close reset on** command, the TCP RST segment is sent to both ends of the half-close session when half-close session is cleared. If you configure the **tcp half-close reset off** command, the TCP RST segment is not transmitted when the session is cleared.

Examples

The following example shows how to configure TCP half-close RST segment transmission:

```
Device(config)# parameter-map type inspect pmap
Device(config-profile)# tcp half-close reset on
```

Related Commands

Command	Description
parameter-map type inspect	Configures an inspect parameter map for connecting thresholds, timeouts, and other parameters pertaining to the **inspect** action.
tcp synwait-time	Specifies how long the software will wait for a TCP session to reach the established state before dropping the session.

tcp half-open reset

To specify whether the TCP reset (RST) segment should be sent when a half-open session is cleared, use the **tcp half-open reset** command in parameter-map type inspect configuration mode. To specify that the TCP RST segment should not be sent when a half-open session is cleared, use the **no** form of this command.

tcp half-open reset {**off** | **on**}
no tcp half-open reset {**off** | **on**}

Syntax Description

off	Disables TCP half-open RST segment transmission.
on	Enables TCP half-open RST segment transmission.

Command Default

The TCP reset segment is sent when a half-open session is cleared.

Command Modes

Parameter-map type inspect configuration (config-profile)

Command History

Release	Modification
Cisco IOS XE Release 3.8S	This command was introduced.

Usage Guidelines

A half-open session is an unestablished session that is initiated by a TCP synchronization (SYN) segment but has an incomplete three-way handshake. A timer is started as soon as the incomplete three-way handshake occurs.

Note You can set the timeout value for a half-open session by using the **tcp synwait-time** command. The default timeout value is 30 seconds.

When you configure an inspect type parameter map, you can enter the **tcp half-open reset** command after you enter the **parameter-map type inspect** command.

If you configure the **tcp half-open reset on** command, the TCP RST segment is sent to both ends of the half-open session when the half-open session is cleared. If you configure the **tcp half-open reset off** command, the TCP RST segment is not transmitted when the session is cleared.

Examples

The following example shows how to configure TCP half-open RST segment transmission:

```
Device(config)# parameter-map type inspect pmap
Device(config-profile)# tcp half-open reset on
```

Related Commands

Command	Description
parameter-map type inspect	Configures an inspect parameter map for connecting thresholds, timeouts, and other parameters pertaining to the **inspect** action.
tcp synwait-time	Specifies how long the software will wait for a TCP session to reach the established state before dropping the session.

tcp idle-time

To configure the amount of time a TCP session will still be managed while there is no activity, use the **tcp idle-time** command in parameter-map type inspect configuration mode. To disable this function, use the **no** form of this command.

tcp idle-time *seconds* [{**ageout-time** *seconds*}]
no tcp idle-time

Syntax Description

seconds	Amount of time, in seconds, during which a TCP session will still be managed while there is no activity. The default is 3600 seconds (1 hour). Valid values are from 1 to 2147483.
ageout-time *seconds*	(Optional) Specifies the aggressive aging time for TCP packets. Valid values are from 1 to 2147483.

Command Default

The default time is 3600 seconds.

Command Modes

Parameter-map type inspect configuration (config-profile)

Command History

Release	Modification
12.4(6)T	This command was introduced.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
Cisco IOS XE Release 3.4S	This command was modified. The **ageout-time** *seconds* keyword and argument pair was added.

Usage Guidelines

When you configure an inspect parameter map, you can enter the **tcp idle-time** command after you enter the **parameter-map type inspect** command.

When the software detects a valid TCP packet that is the first in a session, the software establishes state information for the new session.

If the software detects no packets for the session for a time period defined by the TCP idle timeout, the software will not manage state information for the session.

The value specified for this timeout applies to all TCP sessions.

For detailed information about creating a parameter map, see the **parameter-map type inspect** command.

Examples

The following example shows how to set the TCP timeout to 90 seconds:

```
parameter-map type inspect eng-network-profile
 tcp idle-time 90
```

The following example shows how to set the TCP ageout time to 70 seconds:

```
parameter-map type inspect eng-network-profile
 tcp idle-time 90 ageout-time 70
```

Related Commands

Command	Description
ip inspect tcp idle-time	Specifies the TCP idle timeout (the length of time during which a TCP session will still be managed while there is no activity).
max-incomplete aggressive-aging	Configures aggressive aging of half-opened firewall sessions.
parameter-map type inspect	Configures an inspect parameter map for connecting thresholds, timeouts, and other parameters pertaining to the **inspect** action.

tcp idle reset

To specify whether the TCP reset (RST) segment should be sent when an idle session is cleared, use the **tcp idle reset** command in parameter-map type inspect configuration mode. To specify that the TCP RST segment should not be sent when an idle session is cleared, use the **no** form of this command.

tcp idle reset {**off** | **on**}
no tcp idle reset {**off** | **on**}

Syntax Description

off	Disables TCP idle session RST segment transmission.
on	Enables TCP idle session RST segment transmission.

Command Default

The TCP RST segment is sent when an idle session is cleared.

Command Modes

Parameter-map type inspect configuration (config-profile)

Command History

Release	Modification
Cisco IOS XE Release 3.8S	This command was introduced.

Usage Guidelines

An idle session is a TCP session that is active between two devices even when no data is transmitted by either device for a prolonged period of time.

Note You can set the timeout value for an idle session by using the **tcp idle-time** command . The default timeout value for idle sessions is 3600 seconds.

When an idle TCP session is cleared, the TCP RST segment is sent and the session is reset if the TCP reset segment control is configured on the session.

When you configure an inspect type parameter map, you can enter the **tcp idle reset** command after you enter the **parameter-map type inspect** command.

If you configure the **tcp idle reset on** command, the TCP RST segment is sent to both ends of the idle session when the session is cleared. If you configure the **tcp idle reset off** command, the TCP RST segment is not transmitted when the session is cleared.

Examples

The following example shows how to send a TCP RST segment when an idle session is cleared:

```
Device(config)# parameter-map type inspect pmap
Device(config-profile)# tcp idle reset on
```

Related Commands

Command	Description
parameter-map type inspect	Configures an inspect parameter map for connecting thresholds, timeouts, and other parameters pertaining to the **inspect** action.

Command	Description
tcp idle-time	Configures the timeout for TCP sessions.

tcp max-incomplete

To specify threshold and blocking time values for TCP host-specific denial-of-service (DoS) detection and prevention, use the **tcp max-incomplete** command in parameter-map type inspect configuration mode. To reset the threshold and blocking time to the default values, use the **no** form of this command.

tcp max-incomplete host *threshold* [**block-time** *minutes*]
no tcp max-incomplete

Syntax Description

host *threshold*	Number of half-open TCP sessions with the same host destination address that can simultaneously exist before the software starts deleting half-open sessions to the host. The range is from 1 to 2147483647. The default is unlimited.
block-time *minutes*	(Optional) Amount of time, in minutes, the software prevents connections to the host. The default is 0.

Command Default

The thresholds is unlimited, and the blocking time value is 0.

Command Modes

Parameter-map type inspect configuration (config-profile)

Command History

Release	Modification
12.4(6)T	This command was introduced.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.

Usage Guidelines

When you are configuring an inspect type parameter map, you can enter the **tcp max-incomplete** command after you enter the **parameter-map type inspect** command.

After the specified threshold is exceeded, the router drops packets.

Half-open means that the session has not reached the established state.An unusually high number of half-open sessions with the same destination host address could indicate that a DoS attack is being launched against the host.

When the number of half-open sessions with the same destination host address rises above a threshold (the host threshold number), the software deletes half-open sessions according to one of the following methods.

- If the **block-time** *minutes* timeout is 0 (the default):

The software deletes the oldest existing half-open session for the host for every new connection request to the host. This ensures that the number of half-open sessions to a given host never exceeds the threshold.

- If the **block-time** *minutes* timeout is greater than 0:

The software deletes all existing half-open sessions for the host and then blocks all new connection requests to the host. The software continues to block all new connection requests until the block-time expires.

The software also sends syslog messages whenever the specified threshold is exceeded and when blocking of connection initiations to a host starts or ends.

The global values specified for the threshold and blocking time apply to all TCP connections that Cisco IOS stateful packet inspection inspects.

For more detailed information about creating a parameter map, see the **parameter-map type inspect** command.

Examples

The following example shows how to specifiy a maximum of 100 half-open sessions and a block time of 10 minutes. If a single host receives 400 half-open sessions, subsequent connections after 100 will be dropped. If a host receives 50 connections and another host receives 50 connections, no packets are dropped.

```
parameter-map type inspect eng-network-profile
 tcp max-incomplete host 100 block-time 10
```

Related Commands

Command	Description
ip inspect tcp max-incomplete host	Specifies threshold and blocking time values for TCP host-specific DoS detection and prevention.
max-incomplete aggressive-aging	Configures aggressive aging of half-open firewall sessions.
parameter-map type inspect	Configures an inspect parameter map for connecting thresholds, timeouts, and other parameters pertaining to the **inspect** action.

tcp reassembly

To change the default parameters for Out-of-Order (OoO) queue processing of TCP sessions, use the **tcp reassembly** command in parameter-map type configuration mode. To revert to the default parameters, use the **no** form of this command.

tcp reassembly {**alarm** {**on** | **off**} | **queue length** *queue-length* | **timeout** *seconds*}
no tcp reassembly {**alarm** {**on** | **off**} | **queue length** *queue-length* | **timeout** *seconds*}

Syntax Description

alarm {**on** | **off**}	Enables or disables the alert message configuration for OoO packets. The default is off.
queue length *queue-length*	Specifies the length of OoO queues. The range is from 0 to 1024. The default is 16.
timeout *seconds*	Specifies the timeout for OoO queues in seconds. The range is from 1 to 3600. The default is 5.

Command Default

Alert messages are disabled, the default OoO queue length is 16, and the default timeout for OoO queues is 5 seconds.

Command Modes

Parameter-map type configuration mode (config-profile)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

If the TCP queue length is set to 0, the TCP OoO packet buffering and reassembly is disabled.

If the TCP alarm is enabled, a syslog message is generated when an OoO packet is dropped.

Examples

The following example shows how to configure parameters for OoO queue processing of TCP sessions:

```
Device# configure terminal
Device(config)# parameter-map type ooo global
Device(config-profile)# tcp reassembly alarm on
Device(config-profile)# tcp reassembly queue length 89
```

Related Commands

parameter-map type ooo global	Configures an OoO global parameter map for all firewall policies.
show parameter-map type ooo global	Displays OoO global parameter-map information.
tcp reassembly memory limit	Specifies the limit of the OoO queue size for TCP sessions.

tcp reassembly memory limit

To specify the limit of the out-of-order (OOO) queue size for TCP sessions, use the **tcp reassembly memory limit** command in parameter map type OOO global configuration mode. To disable the configuration, use the **no** form of this command.

tcp reassembly memory limit *queue-size*
no tcp reassembly memory limit

Syntax Description

queue-size	Queue size, in kilobytes (KB). The range is from 1 to 4194303.

Command Default

The default OOO queue size is 1024 KB.

Command Modes

Parameter map type OOO global configuration (config-profile)

Command History

Release	Modification
15.0(1)M	This command was introduced.
15.1(3)T	This command was modified. The maximum limit value for the *queue-size*argument was changed from 4294967295 to 4194303.

Usage Guidelines

You must use the **tcp reassembly memory limit** command to specify the limit of the OOO queue size for TCP sessions when the deep packet inspection feature is configured on the router.

Examples

The following example shows how to specify 200 KB as the OOO queue size for TCP sessions:

```
Router(config)# parameter-map type ooo global
Router(config-profile)# tcp reassembly memory limit
 200
```

Related Commands

Command	Description
tcp reassembly queue length	Specifies the length of the OOO queue parameters.
tcp reassembly timeout	Specifies the timeout for the OOO TCP queues.
tcp reassembly alarm	Specifies the alert message configuration for the TCP sessions.

tcp syn-flood limit

To configure a limit to the number of TCP half-open sessions before triggering synchronization (SYN) cookie processing for new SYN packets, use the **tcp syn-flood limit**command in profile configuration mode. To disable the configuration, use the **no** form of this command.

tcp syn-flood limit *maximum-session-limit*
no tcp syn-flood limit *maximum-session-limit*

Syntax Description

maximum-session-limit	Maximum number of sessions. Valid values are from 1 to 4294967295.

Command Default

No limit to the number of TCP half-open sessions are set.

Command Modes

Profile configuration (config-profile)

Command History

Release	Modification
Cisco IOS XE Release 3.3S	This command was introduced.

Usage Guidelines

A TCP half-open session is a session that has not reached the established state.

In a VRF-aware firewall, you can configure a limit to the number of TCP half-open sessions for each VRF. At both the global level and at the VPN Routing and Forwarding (VRF) level, when the configured TCP SYN flood limit is reached, the TCP SYN cookie verifies the source of the half-open sessions before creating more sessions.

You must configure the **parameter-map type inspect-vrf** or the **parameter-map type inspect global**command before you can configure the **tcp syn-flood limit** command.

Examples

The following example shows how to limit the number of TCP half-open sessions to 500 at an inspect-VRF parameter map level:

```
Router(config)# parameter-map type inspect-vrf
Router(config-profile)# tcp syn-flood limit 500
Router(config-profile)# end
```

The following example shows how to limit the number of TCP half-open sessions to 300 at a global parameter map level:

```
Router(config)# parameter-map type global
Router(config-profile)# tcp syn-flood limit 300
Router(config-profile)# end
```

Related Commands

Command	Description
parameter-map type global	Configures a global parameter map and enters profile configuration mode.

Command	Description
parameter-map type inspect-vrf	Configures a parameter map of type inspect VRF and enters profile configuration mode.

tcp syn-flood rate per-destination

To configure a TCP synchronization (SYN) flood rate limit for each destination address, use the **tcp syn-flood rate per-destination** command in profile configuration mode. To disable TCP SYN flood packets, use the **no** form of this command.

tcp syn-flood rate per-destination *maximum-packet-rate*
no tcp syn-flood rate per-destination *maximum-packet-rate*

Syntax Description

maximum-packet-rate	Maximum rate of TCP SYN packets. Valid values are from 1 to 1000000000.

Command Default

No TCP SYN-flood packets are configured.

Command Modes

Profile configuration (config-profile)

Command History

Release	Modification
Cisco IOS XE Release 3.3S	This command was introduced.

Usage Guidelines

When the configured maximum packet rate is reached, the TCP SYN cookie protection is triggered.

You must configure the **parameter-map type inspect-zone** or the **parameter-map type global**command before you can configure the **tcp syn-flood rate per-destination** command.

Examples

The following example shows how to configure the TCP SYN-flood packet rate of 500 at an inspect-zone parameter map level:

```
Router(config)# parameter-map type inspect-zone
Router(config-profile)# tcp syn-flood rate per-destination 500
Router(config-profile)# end
```

The following example shows how to configure the TCP SYN-flood packet rate of 300 at a global parameter map level:

```
Router(config)# parameter-map type global
Router(config-profile)# tcp syn-flood rate per-destination 300
Router(config-profile)# end
```

Related Commands

Command	Description
parameter-map type global	Configures a global parameter map and enters profile configuration mode.
parameter-map type inspect-zone	Configures a parameter map of type inspect zone and enters profile configuration mode.

tcp synwait-time

To specify how long the software will wait for a TCP session to reach the established state before dropping the session, use the **tcp synwait-time** command in parameter-map type inspect configuration mode. To disable this function, use the **no** form of this command.

tcp synwait-time *seconds* [{**ageout-time** *seconds*}]
no tcp synwait-time

Syntax Description

seconds	Time, in seconds, that the system will wait for a TCP session to reach the established state before dropping the session. The default is 30. Valid values are from 1 to 2147483.
ageout-time *seconds*	(Optional) Specifies the aggressive aging time for TCP packets. Valid values are from 1 to 2147483.

Command Default

The default TCP synchronization (SYN) wait time is 30 seconds.

Command Modes

Parameter-map type inspect configuration (config-profile)

Command History

Release	Modification
12.4(6)T	This command was introduced.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
Cisco IOS XE Release 3.4S	This command was modified. The **ageout-time** *seconds* keyword and argument pair was added.

Usage Guidelines

You must configure the **parameter-map type inspect** command before you can configure the **tcp synwait-time** command.

Examples

The following example shows how to specify that the TCP session will be dropped if the TCP session does not reach the established state in 3 seconds:

```
parameter-map type inspect eng-network-profile
 tcp synwait-time 3
```

The following example shows how to specify the aging out time after which the TCP session will be dropped:

```
parameter-map type inspect eng-network-profile
 tcp synwait-time 3 ageout-time 20
```

Related Commands

Command	Description
max-incomplete aggressive-aging	Configures aggressive aging of half-opened firewall sessions.

Command	Description
parameter-map type inspect	Configures an inspect parameter map for connecting thresholds, timeouts, and other parameters pertaining to the **inspect** action.

tcp window-scale-enforcement loose

To disable the checking of the TCP window-scale option in a Zone-Based Policy Firewall, use the **tcp window-scale-enforcement loose** command in parameter-map type inspect configuration mode. To return to the command default, use the **no** form of this command.

tcp window-scale-enforcement loose
no tcp window-scale-enforcement loose

Syntax Description

This command has no arguments or keywords.

Command Default

A strict window-scale option check is enabled on the firewall.

Command Modes

Parameter-map type inspect configuration (config-profile)

Command History

Release	Modification
12.4(20)T	This command was introduced.
Cisco IOS XE Release 3.10S	This command was integrated into Cisco IOS XE Release 3.10S

Usage Guidelines

The window-scale extension expands the definition of the TCP window to 32 bits and then uses a scale factor to carry this 32-bit value in the 16-bit Window field of the TCP header. The firewall enforces the strict checking of the TCP window scale option. See RFC 1323 for more information on this function.

Sometimes server uses a non-RFC compliant TCP/IP protocol stack. In this case, the intiator does not offer the window-scale option, but the responder has the option enabled with a window-scale factor that is not zero.

Network administrators who experience issues with a noncompliant server may not have control over the server to which they need to connect. Disabling the firewall to connect to a noncompliant server is not desirable and may fail if each endpoint cannot agree on the window-scaling factor to use for its respective receive window.

Use the **tcp window-scale-enforcement loose** command in parameter-map type inspect configuration mode to allow noncompliant window scale negotiation and to ensure the window-scale option works without the firewall being disabled to access the noncompliant servers. This command is used by the firewall, which provides a unidirectional firewall policy between groups of interfaces known as zones.

Examples

The following example shows how to disable the window scale option check in the Zone-Based Firewall parameter map for a TCP packet that has an invalid window scale option:

```
Device> enable
Device# configure terminal
Device(config)# parameter-map type inspect pmap-fw
Device(config-profile)# tcp window-scale-enforcement loose
```

Related Commands

Command	Description
parameter-map type inspect	Configures an inspect parameter map for connecting thresholds, timeouts, and other parameters pertaining to the **inspect** action.
tcp synwait-time	Specifies how long the software will wait for a TCP session to reach the established state before dropping the session.

telnet

To log in to a host that supports Telnet, use the **telnet** command in user EXEC or privileged EXEC mode.

telnet *host* [*port*] [*keyword*]

Syntax Description

host	A hostname or an IP address.
port	(Optional) A decimal TCP port number, or port name; the default is the Telnet router port (decimal 23) on the host.
keyword	(Optional) One of the keywords listed in the table below.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.0(21)ST	The **/ipv4** and **/ipv6** keywords were added.
12.1	The **/quiet** keyword was added.
12.2(2)T	The **/ipv4** and **/ipv6** keywords were added.
12.0(22)S	This command was integrated into Cisco IOS Release 12.0(22)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

The table below lists the optional **telnet** command keywords.

Table 222: telnet Keyword Options

Option	Description
/debug	Enables Telnet debugging mode.

Option	Description
/encrypt kerberos	Enables an encrypted Telnet session. This keyword is available only if you have the Kerberized Telnet subsystem. If you authenticate using Kerberos Credentials, the use of this keyword initiates an encryption negotiation with the remote server. If the encryption negotiation fails, the Telnet connection will be reset. If the encryption negotiation is successful, the Telnet connection will be established, and the Telnet session will continue in encrypted mode (all Telnet traffic for the session will be encrypted).
/ipv4	Specifies version 4 of the IP protocol. If a version of the IP protocol is not specified in a network that supports both the IPv4 and IPv6 protocol stacks, IPv6 is attempted first and is followed by IPv4.
/ipv6	Specifies version 6 of the IP protocol. If a version of the IP protocol is not specified in a network that supports both the IPv4 and IPv6 protocol stacks, IPv6 is attempted first and is followed by IPv4.
/line	Enables Telnet line mode. In this mode, the Cisco IOS software sends no data to the host until you press the **Enter** key. You can edit the line using the standard Cisco IOS software command-editing characters. The **/line** keyword is a local switch; the remote router is not notified of the mode change.
/noecho	Disables local echo.
/quiet	Prevents onscreen display of all messages from the Cisco IOS software.
/route: *path*	Specifies loose source routing. The *path* argument is a list of hostnames or IP addresses that specify network nodes and ends with the final destination.
/source-interface	Specifies the source interface.
/stream	Turns on *stream* processing, which enables a raw TCP stream with no Telnet control sequences. A stream connection does not process Telnet options and can be appropriate for connections to ports running UNIX-to-UNIX Copy Program (UUCP) and other non-Telnet protocols.
port-number	Port number.
bgp	Border Gateway Protocol.
chargen	Character generator.
cmd *rcmd*	Remote commands.
daytime	Daytime.
discard	Discard.
domain	Domain Name Service.
echo	Echo.
exec	EXEC.

Option	Description
finger	Finger.
ftp	File Transfer Protocol.
ftp-data	FTP data connections (used infrequently).
gopher	Gopher.
hostname	Hostname server.
ident	Ident Protocol.
irc	Internet Relay Chat.
klogin	Kerberos login.
kshell	Kerberos shell.
login	Login (rlogin).
lpd	Printer service.
nntp	Network News Transport Protocol.
pim-auto-rp	Protocol Independent Multicast (PIM) auto-rendezvous point (RP).
node	Connect to a specific Local-Area Transport (LAT) node.
pop2	Post Office Protocol v2.
pop3	Post Office Protocol v3.
port	Destination local-area transport (LAT) port name.
smtp	Simple Mail Transfer Protocol.
sunrpc	Sun Remote Procedure Call.
syslog	Syslog.
tacacs	Specifies TACACS security.
talk	Talk (517).
telnet	Telnet (23).
time	Time (37).
uucp	UNIX-to-UNIX Copy Program (540).
whois	Nickname (43).
www	World Wide Web (HTTP, 80).

With the Cisco IOS implementation of TCP/IP, you are not required to enter the **connect** or **telnet** command to establish a terminal connection. You can enter only the learned hostname--as long as the following conditions are met:

- The hostname is different from a command word for the router.
- The preferred transport protocol is set to **telnet**.

To display a list of the available hosts, use the **show hosts** command. To display the status of all TCP connections, use the **show tcp** command.

The Cisco IOS software assigns a logical name to each connection, and several commands use these names to identify connections. The logical name is the same as the hostname, unless that name is already in use, or you change the connection name with the **name-connection** EXEC command. If the name is already in use, the Cisco IOS software assigns a null name to the connection.

The Telnet software supports special Telnet commands in the form of Telnet sequences that map generic terminal control functions to operating system-specific functions. To issue a special Telnet command, enter the escape sequence and then a command character. The default escape sequence is Ctrl-^ (press and hold the Ctrl and Shift keys and the 6 key). You can enter the command character as you hold down Ctrl or with Ctrl released; you can use either uppercase or lowercase letters. The table below lists the special Telnet escape sequences.

Table 223: Special Telnet Escape Sequences

Escape Sequence[2]	Purpose
Ctrl-^ b	Break
Ctrl-^ c	Interrupt Process (IP and IPv6)
Ctrl-^ h	Erase Character (EC)
Ctrl-^ o	Abort Output (AO)
Ctrl-^ t	Are You There? (AYT)
Ctrl-^ u	Erase Line (EL)

[2] The caret (^) symbol refers to Shift-6 on your keyboard.

At any time during an active Telnet session, you can list the Telnet commands by pressing the escape sequence keys followed by a question mark at the system prompt: **Ctrl-^ ?**

A sample of this list follows. In this sample output, the first caret (^) symbol represents the Ctrl key, and the second caret represents Shift-6 on your keyboard:

```
router> ^^?
[Special telnet escape help]
^^B  sends telnet BREAK
^^C  sends telnet IP
^^H  sends telnet EC
^^O  sends telnet AO
^^T  sends telnet AYT
^^U  sends telnet EL
```

You can have several concurrent Telnet sessions open and switch among them. To open a subsequent session, first suspend the current connection by pressing the escape sequence (Ctrl-Shift-6 then x [Ctrl^x] by default) to return to the system command prompt. Then open a new connection with the **telnet** command.

To terminate an active Telnet session, enter any of the following commands at the prompt of the device to which you are connecting:

- **close**
- **disconnect**
- **exit**
- **logout**
- **quit**

Examples

The following example establishes an encrypted Telnet session from a router to a remote host named host1:

```
router>

telnet host1 /encrypt kerberos
```

The following example routes packets from the source system host1 to example.com, then to 10.1.0.11, and finally back to *host1* :

```
router>
telnet host1 /route:example.com 10.1.0.11 host1
```

The following example connects to a host with the logical name host1:

```
router>
host1
```

The following example suppresses all onscreen messages from the Cisco IOS software during login and logout:

```
router>

telnet host2 /quiet
```

The following example shows the limited messages displayed when connection is made using the optional **/quiet** keyword:

```
login:User2
Password:
         Welcome to OpenVMS VAX version V6.1 on node CRAW
     Last interactive login on Tuesday, 15-DEC-1998 11:01
     Last non-interactive login on Sunday,  3-JAN-1999 22:32
Server3)logout
    User2        logged out at  16-FEB-2000 09:38:27.85
```

Related Commands

Command	Description
connect	Logs in to a host that supports Telnet, rlogin, or LAT.
kerberos clients mandatory	Causes the **rsh**, **rcp**, **rlogin**, and **telnet** commands to fail if they cannot negotiate the Kerberos Protocol with the remote server.
name connection	Assigns a logical name to a connection.
rlogin	Logs in to a UNIX host using rlogin.
show hosts	Displays the default domain name, the style of name lookup service, a list of name server hosts, and the cached list of hostnames and addresses.
show tcp	Displays the status of TCP connections.

template (identity policy)

To specify a virtual template from which commands may be cloned, use the **template** command in identity policy configuration mode. To disable the virtual template, use the **no** form of this command.

template {**virtual-template** *template-number*}
notemplate {**virtual-template** *template-number*}

Syntax Description

virtual-template	Specifies the virtual template interface that will serve as the configuration clone source for the virtual interface that is dynamically created for authenticated users.
template-number	Template interface number. The value ranges from 1 through 200.

Command Default

A virtual template from which commands may be cloned is not specified.

Command Modes

Identity policy configuration (config-identity-policy)

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

The **identity policy**command must be entered in global configuration mode before the **template** command can be used.

Examples

The following example shows that an identity policy and a template have been specified:

```
Router (config)# identity policy mypolicy
Router (config-identity-policy)# template virtual-template 1
```

Related Commands

Command	Description
identity policy	Creates an identity policy.

template (identity profile)

To specify a virtual template from which commands may be cloned, use the **template** command in identity profile configuration mode. To disable the virtual template, use the **no** form of this command.

template *virtual-template*
no template *virtual-template*

Syntax Description

virtual-template	Specifies the virtual template interface that will serve as the configuration clone source for the virtual interface that is dynamically created for authenticated users.

Command Default

A virtual template from which commands may be cloned is not specified.

Command Modes

Identity profile configuration

Command History

Release	Modification
12.3(2)XA	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines

The **identity profile command and default**keyword must be entered in global configuration mode before the **template** command can be used.

Examples

The following example shows that a default identity profile and a template have been specified:

```
Router (config)# identity profile default
Router (config-identity-prof)# template virtualtemplate1
```

Related Commands

Command	Description
description	Enters an identity profile description.
device	Statically authorizes or rejects individual devices.
identity profile	Creates an identity profile.

template config

To specify a remote URL for a Cisco IOS command-line interface (CLI) configuration template, use the **template config** command in tti-registrar configuration mode. To remove the template from the configuration and use the default configuration template, use the **no** form of this command.

template config *url* [**post**]
no template config *url*

Syntax Description

url	One of the keywords in the table below.
post	(Optional) Specifies that the registrar will issue an HTTP POST to the external management system. The HTTP POST will include information about the device such as the device name, the current Cisco IOS version, and the current configuration in order for the external management system to return a Cisco IOS configuration more specific to the device. **Note** Common Gateway Interface (CGI) scripts must be issued with the **post** keyword.

Command Default

A default template will be used.

Command Modes

tti-registrar configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.4(6)T	The **post** keyword was added.

Usage Guidelines

Use the **template config** command to specify a URL in which to retrieve the template that will be sent from the Secure Device Provisioning (SDP) registrar to the SDP petitioner during the Trusted Transitive Introduction (TTI) exchange.

If neither a configuration template nor the **post** keyword is specified, the default configuration template is used. The default configuration template contains the following commands:

```
!
$t
!
$c
!
! end
END_CONFIG
;
```

The variable "$t" will be expanded to include a Cisco IOS public key infrastructure (PKI) trustpoint that is configured for autoenrollment with the certificate server of the registrar. The variable "$c" will be expanded into the correct certificate chain for the certificate server of the registrar.

If an external template is specified, it must include the "$t" and "$c" variables to enable the petitioner device to obtain a certificate. The **end** command must be specified. If you want to specify details about the trustpoint, you can specify a template as follows:

```
!
crypto ca trustpoint $t
 enrollment url http://<registrar fqdn>
 rsakeypair $k $s
 auto-enroll 70
!
$c
end
```

Where $t comes from "trustpoint" configured under the petitioner, $k comes from "rsakeypair" under the trustpoint:

```
! $l will be replaced by 'mytp.'
crypto provisioning petitioner
  trustpoint mytp
! $k will be replaced by 'mykey.'
crypto ca trustpoint mytp
rsakeypair mykey
!
```

Note The template configuration location may include a variable "$n", which is expanded to the name of the introducer.

The table below lists the available options for the *url* argument.

Table 224: URL Keywords for the CLI Template

Keyword	Description
cns:	Retrieves from the Cisco Networking Services (CNS) configuration engine.
flash:	Retrieves from flash memory.
ftp:	Retrieves from the FTP network server.
http:	Retrieves from a HTTP server (also called a web server).
https:	Retrieves from a Secure HTTP (HTTPS) server.
null:	Retrieves from the file system.
nvram:	Retrieves from the NVRAM of the router.
rcp:	Retrieves from a remote copy (rcp) protocol network server.
scp:	Retrieves from a network server that supports Secure Shell (SSH).
system:	Retrieves from system memory, which includes the running configuration.
tftp:	Retrieves from a TFTP network server.

Keyword	Description
webflash:	Retrieves from the file system.
xmodem:	Retrieves from a network machine that uses the Xmodem protocol.

Expanded SDP CGI Template Support

Expanded SDP CGI template support allows you to specify a bootstrap configuration based on the client type, model, Cisco IOS version, and current configuration. Specifying a boot strap configuration is accomplished by the TTI registrar forwarding the device information to the external management system when requesting a bootstrap configuration.

The **template config** command with the **post** keyword supports expanded SDP CGI templates by allowing the SDP registrar to send the additional information about the device configuration to an external management system by issuing an HTTP POST or an HTTPS POST. Without the use of the **post** keyword, the SDP registrar requests information only from the management system based on the device name.

Note In order to use the expanded SDP CGI support, the registrar must be running Cisco IOS Release 12.4(6)T or a later release, the **template config** command must be issued with the **post** keyword, and the *url* argument must include either the HTTP or HTTPS protocol. No other protocol (for example, FTP) is supported for the expanded CGI template functionality.

The additional information sent to the external management system with the issuance of an HTTP POST from the SDP registrar to the external management system is shown in the table below.

Table 225: AV Pairs Sent During HTTP Post to External Management System

AV Pair	Description
TTIFixSubjectName	AAA_AT_TTI_SUBJECTNAME (sent only if the realm authentication user is not the root user on the registrar)
TTIIosRunningConfig	Output of **show running-config brief**
TTIKeyHash	Digest calculated over the device public key
TTIPrivilege	AAA_AT_TTI_PRIVILEGE--"admin" is sent if the user is an administrator; "user" is sent if the user is not an administrator (sent only if the realm authentication user is an administrator and the information is available from the authentication, authorization, and accounting [AAA] server)
TTISignature	Digest calculated over all attribute-value (AV) pairs except UserDeviceName and TTISignCert
TTISignCert	Device current certificate (sent only if the device currently has a certificate)
TTITemplateVar	AAA_AT_TTI_IOSCONFIG(1-9) (sent only if the realm authentication user is not the root user on the registrar)
TTIUserName	Device name as entered by the administrative introducer (sent only if the realm authentication user is an administrator)

AV Pair	Description
TTIVersion	TTI version of the registrar

Examples

The following example shows how to specify the HTTP URL "http://pki1-36a.cisco.com:80" for the Cisco IOS CLI configuration template, which is sent from the SDP registrar to the external management system during the TTI exchange:

```
crypto provisioning registrar
 pki-server cs1
 template config
http://pki1-36a.cisco.com:80
```

The following example shows how to specify that the SDP registrar will send additional device information to the external management system to retrieve a more specific bootstrap configuration file:

```
crypto provisioning registrar
 pki-server cs1
 template config http://myserver/cgi-bin/mycgi post
```

Related Commands

Command	Description
authentication list (tti-registrar)	Authenticates the introducer in an SDP operation.
authorization list (tti-registrar)	Specifies the appropriate authorized fields for both the certificate subject name and the list of template variables to be expanded into the Cisco IOS CLI snippet that is sent back to the petitioner in an SDP operation.
template username	Establishes a template username and password to access the configuration template on the file system.

template file

To specify the source template file location on the registrar and the destination template file location on the petitioner, use the **template file** command in tti-registrar configuration mode.

template file *sourceURL destinationURL*

Syntax Description

sourceURL	Specifies the source URL on the registrar for the template file using one of the keywords in .
destinationURL	Specifies the destination URL on the petitioner for template file using one of the keywords in .

Command Default

None

Command Modes

tti-registrar configuration (tti-registrar)

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 3.6	This command was integrated into Cisco IOS XE Release 3.6.

Usage Guidelines

Use the **template file** command to specify the location where a template file will be retrieved from and copied to during the Trusted Transitive Introduction (TTI) exchange. There may be up to nine template files transferred, each with a different source and destination location. A destination URL could also be a token on the petitioner, such as usbtoken0:.

The file content is expanded on the registrar. The destination URL and file content are expanded on the petitioner.

Table 226: Source and Destination URL Keywords

Keyword	Description
archive:	Retrieves from the archive location.
cns:	Retrieves from the Cisco Networking Services (CNS) configuration engine.
disk0:	Retrieves from disk0.
disk1:	Retrieves from disk1.
flash:	Retrieves from flash memory.
ftp:	Retrieves from the FTP network server.
http:	Retrieves from a HTTP server.
https:	Retrieves from a Secure HTTP (HTTPS) server.

Keyword	Description
null:	Retrieves from the file system.
nvram:	Retrieves from the NVRAM of the router.
rcp:	Retrieves from a remote copy (rcp) protocol network server.
scp:	Retrieves from a network server that supports Secure Shell (SSH).
system:	Retrieves from system memory, which includes the running configuration.
tar:	Retrieves from a compressed file in tar format.
tftp:	Retrieves from a TFTP network server.
tmpsys:	Retrieves from a temporary system location.
unix:	Retrieves from the UNIX system location.
usbtoken:	Retrieves from the USB token.

Examples

The following example shows how to specify where the source template file is located and where the template file will be copied to on the petitioner:

```
crypto provisioning registrar
  pki-server cs1
  template file http://myserver/file1 usbtoken0://file1
  template file http://myserver/file2 flash://file2
```

Related Commands

Command	Description
binary file	Specifies the binary file location on the registrar and the destination binary file location on the petitioner.
crypto provisioning registrar	Configures a device to become an SDP registrar and enter tti-registrar configuration mode.

template http admin-introduction

To use a custom administrator introduction template rather than the default template, issue the **template http admin-introduction** command in tti-registrar configuration mode.

template http admin-introduction *URL*

Syntax Description

URL	Location of the custom administrator introduction template.

Command Default

If this command is not issued, the default template will be used.

Command Modes

tti-registrar configuration

Command History

Release	Modification
12.4(4)T	This command was introduced.

Usage Guidelines

You may want to use a custom administrator introduction template rather than a default template because the device name can be prefilled on the web page for the user. Without this command, the welcome page must be the first page requested by the user.

Examples

The following example shows how to direct the registrar to use the administrator introduction page template located at tftp://walnut.cisco.com/admin-introducer.html:

```
template http admin-introduction tftp://walnut.cisco.com/admin-introducer.html
```

Related Commands

Command	Description
template http completion	Uses a custom completion template rather than the default template.
template http error	Uses a custom error template rather than the default template.
template http introduction	Uses a custom introduction template rather than the default template.
template http start	Directs the TTI registrar to use the custom start page template.
template http welcome	Uses a custom welcome template rather than the default template.

template http completion

To use a custom completion template rather than the default template, issue the **template http completion** command in tti-registrar configuration mode.

template http completion *URL*

Syntax Description

URL	Location of the custom completion template.

Command Default

If this command is not issued, the default template will be used.

Command Modes

tti-registrar configuration

Command History

Release	Modification
12.4(4)T	This command was introduced.

Usage Guidelines

Custom templates allow for additional information specific to the deployment to be displayed on the web pages. The easy way to define a custom template is to modify the default template.

Examples

The following example shows how to direct the registrar to use the completion page template located at specified location:

```
template http completion tftp://walnut.cisco.com/completion.html
```

Related Commands

Command	Description
template http admin-introduction	Uses a custom admin-introduction template rather than the default template.
template http error	Uses a custom error template rather than the default template.
template http introduction	Uses a custom introduction template rather than the default template.
template http start	Directs the TTI registrar to use the custom start page template.
template http welcome	Uses a custom welcome template rather than the default template.

template http error

To use a custom error template rather than the default template, issue the **template http error** command in tti-registrar configuration mode.

template http error *URL*

Syntax Description

URL	Location of the custom error template.

Command Default

If this command is not issued, the default template will be used.

Command Modes

tti-registrar configuration

Command History

Release	Modification
12.4(4)T	This command was introduced.

Usage Guidelines

Custom templates allow for additional information specific to the deployment to be displayed on the web pages. The easy way to define a custom template is to modify the default template.

Examples

The following example shows how to direct the registrar to use the error page template located at specified location:

```
template http error tftp://walnut.cisco.com/error.html
```

Related Commands

Command	Description
template http admin-introduction	Uses a custom admin-introduction template rather than the default template.
template http completion	Uses a custom completion template rather than the default template.
template http introduction	Uses a custom introduction template rather than the default template.
template http start	Directs the TTI registrar to use the custom start page template.
template http welcome	Uses a custom welcome template rather than the default template.

template http introduction

To use a custom introduction template rather than the default template, issue the **template http introduction** command in tti-registrar configuration mode.

template http introduction *URL*

Syntax Description

URL	Location of the custom introduction template.

Command Default

If this command is not issued, the default template will be used.

Command Modes

tti-registrar configuration

Command History

Release	Modification
12.4(4)T	This command was introduced.

Usage Guidelines

From a custom introduction page, the completion URL of the petitioner may be prefilled on the page for the user.

Examples

The following example shows how to direct the registrar to use the customer introduction template located at specified location:

```
template http introduction tftp://walnut.cisco.com/introduction.html
```

Related Commands

Command	Description
template http admin-introduction	Uses a custom admin-introduction template rather than the default template.
template http completion	Uses a custom completion template rather than the default template.
template http start	Directs the TTI registrar to use the custom start page template.
template http welcome	Uses a custom welcome template rather than the default template.

template http start

To direct the Trusted Transitive Introduction (TTI) registrar to use the custom start page template, issue the **template http start** command in tti-registrar configuration mode.

template http start *URL*

Syntax Description

URL	Location of the start page template.

Command Default

If this command is not issued, the welcome page will be the initial communication between the introducer and the petitioner.

Command Modes

tti-registrar configuration

Command History

Release	Modification
12.4(4)T	This command was introduced.

Usage Guidelines

Use the **template http start**command to display the start page on the registrar and make that page the starting point of the TTI transaction. From the start page, the registrar can direct the user to the welcome page on the petitioner.

Examples

The following example shows how to direct the registrar to use the start page template located at the specified location:

```
template http start tftp://walnut.cisco.com/start.html
```

Related Commands

Command	Description
template http admin-introduction	Uses a custom admin-introduction template rather than the default template.
template http completion	Uses a custom completion template rather than the default template.
template http introduction	Uses a custom introduction template rather than the default template.
template http welcome	Uses a custom welcome template rather than the default template.

template http welcome

To use a custom welcome template rather than the default template, issue the **template http welcome** command in tti-registrar configuration mode.

template http welcome *URL*

Syntax Description

URL	Location of the custom welcome template.

Command Default

If this command is not issued, the default template will be used.

Command Modes

tti-registrar configuration

Command History

Release	Modification
12.4(4)T	This command was introduced.

Usage Guidelines

From a custom welcome page, the introduction URL of the registrar may be prefilled on the page for the user.

Examples

The following example shows how to direct the registrar to use the welcome page template located at specified location:

```
template http welcome tftp://walnut.cisco.com/welcome.html
```

Related Commands

Command	Description
template http admin-introduction	Uses a custom admin-introduction template rather than the default template.
template http completion	Uses a custom completion template rather than the default template.
template http introduction	Uses a custom introduction template rather than the default template.
template http start	Directs the TTI registrar to use the custom start page template.

template location

To specify the location of the template that the SDP Registrar should use while responding to a request received through the URL profile, use the **template location**command in tti-registrar configuration mode. To remove this configuration, use the **no** form of this command.

template location *location*
no template location *location*

Syntax Description

location	Specifies the template location for the SDP Registrar.

Command Default

No template *location* is associated with the SDP Registrar.

Command Modes

Tti-registrar configuration mode (tti-registrar)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **template location**command is required in the SDP registrar configuration, which is used to deploy Apple iPhones on a corporate network.

Examples

The following example configures the SDP registrar to run HTTPS in order to deploy Apple iPhones on a corporate network from global configuration mode:

```
Router(config)# crypto provisioning registrar
Router(tti-registrar)# url-profile start START
Router(tti-registrar)# url-profile intro INTRO
Router(tti-registrar)# match url /sdp/intro
Router(tti-registrar)# match authentication trustpoint apple-tp
Router(tti-registrar)# match certificate cat 10
Router(tti-registrar)# mime-type application/x-apple-aspen-config
Router(tti-registrar)# template location flash:intro.mobileconfig
Router(tti-registrar)# template variable p iphone-vpn
```

Related Commands

Command	Description
crypto provisioning registrar	Configures a device to become a registrar for the SDP exchange and enters tti-registrar configuration mode.
url-profile	Specifies a URL profile that configures the SDP registrar to run HTTPS in order to deploy Apple iPhones on a corporate network.
match authentication trustpoint	Enters the trustpoint name that should be used to authenticate the peer's certificate.
match certificate	Enters the name of the certificate map used to authorize the peer's certificate.

Command	Description
match url	Specifies the URL to be associated with the URL profile.
mime-type	Specifies the MIME type that the SDP registrar should use to respond to a request received through the URL profile.
template location	Specifies the location of the template that the SDP Registrar should use while responding to a request received through the URL profile.
template variable p	Specifies the value that goes into the OU field of the subject name in the certificate to be issued.

template username

To establish a template username in which to access the file system, use the **template username** command in tti-registrar configuration mode.

template username *name*

Syntax Description

name	Template username.

Command Default

A template username is not established.

Command Modes

tti-registrar configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

Use the **template username**command to create a username-based authentication system that allows you to access the configuration template, which is sent from the Secure Device Provisioning (SDP) registrar to the SDP petitioner during the Trusted Transitive Introduction (TTI) exchange.

Examples

The following example shows how to create the username "mycs" to access the configuration template for the TTI exchange:

```
crypto wui tti registrar
 pki-server cs1
 template username mycs
```

Related Commands

Command	Description
crypto wui tti registrar	Configures a device to become an SDP registrar and enters tti-registrar configuration mode.
template config	Specifies a remote URL for a Cisco IOS CLI configuration template.

template variable p

To specify the value that goes into the Organizational Unit (OU) field of the subject name in the trustpoint certificate to be issued by the SDP Registrar, use the **template variable**command in tti-registrar configuration mode. To remove this configuration, use the **no** form of this command.

template variable p *value*
no template variable p *value*

Syntax Description

value	Specifies the OU field value.

Command Default

No OU field value is associated with the trustpoint certificate.

Command Modes

Tti-registrar configuration mode (tti-registrar)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **template variable p**command can be specified optionally in the SDP registrar configuration.

Examples

The following example configures the SDP registrar to run HTTPS in order to deploy Apple iPhones on a corporate network from global configuration mode:

```
Router(config)# crypto provisioning registrar
Router(tti-registrar)# url-profile start START
Router(tti-registrar)# url-profile intro INTRO
Router(tti-registrar)# match url /sdp/intro
Router(tti-registrar)# match authentication trustpoint apple-tp
Router(tti-registrar)# match certificate cat 10
Router(tti-registrar)# mime-type application/x-apple-aspen-config
Router(tti-registrar)# template location flash:intro.mobileconfig
Router(tti-registrar)# template variable p iphone-vpn
```

Related Commands

Command	Description
crypto provisioning registrar	Configures a device to become a registrar for the SDP exchange and enters tti-registrar configuration mode.
url-profile	Specifies a URL profile that configures the SDP registrar to run HTTPS in order to deploy Apple iPhones on a corporate network.
match authentication trustpoint	Enters the trustpoint name that should be used to authenticate the peer's certificate.
match certificate	Enters the name of the certificate map used to authorize the peer's certificate.

Command	Description
match url	Specifies the URL to be associated with the URL profile.
mime-type	Specifies the MIME type that the SDP registrar should use to respond to a request received through the URL profile.
template location	Specifies the location of the template that the SDP Registrar should use while responding to a request received through the URL profile.

test aaa group

To associate a dialed number identification service (DNIS) or calling line identification (CLID) user profile with the record that is sent to the RADIUS server or to manually test load-balancing server status, use the **test aaa group** command in privileged EXEC mode.

DNIS and CLID User Profile
test aaa group {*group-name* | **radius**} *username password* **new-code** [**profile** *profile-name*]

RADIUS Server Load Balancing Manual Testing
test aaa group *group-name* [**server** *ip-address*] [**auth-port** *port-number*] [**acct-port** *port-number*] *username password* **new-code** [**count** *requests*] [**rate** *requests-per-second*] [**blocked** {**yes** | **no**}]

Syntax Description

group-name	Subset of RADIUS servers that are used, as defined by the server group group-name.
radius	Uses RADIUS servers for authentication.
username	Name for the test user. **Caution** If you use this command to manually test RADIUS load-balancing server state, it is recommended that a test user, one that is not defined on the RADIUS server, be used to protect against security issues that may arise if the test user is not correctly configured.
password	Password.
new-code	Code path through the new code, which supports a CLID or DNIS user profile association with a RADIUS server.
profile *profile-name*	(Optional) Identifies the user profile specified in the aaa user profile command. To associate a user profile with the RADIUS server, you must identify the user profile name.
server *ip-address*	(Optional) For RADIUS server load balancing, specifies to which server in the server group the test packets will be sent.
auth-port	(Optional) User Datagram Protocol (UDP) destination port for authentication requests.
port-number	(Optional) Port number for authentication requests; the host is not used for authentication if set to 0. If unspecified, the port number defaults to 1646.
acct-port	(Optional) UDP destination port for accounting requests.
port-number	(Optional) Port number for accounting requests; the host is not used for accounting if set to 0. If unspecified, the port number defaults to 1646.
count *requests*	(Optional) Number of authentication and accounting requests that are to be sent to the server for each port. Range: 1 to 50000. Default: 1.

rate *requests-per-second*	(Optional) Number of requests per second that are to be sent to the server. Range: 1 to 1000. Default: 10.
blocked {**yes** | **no**}	(Optional) Specifies whether the request is sent in blocking or nonblocking mode. If the **blocked** keyword is not used and one request is sent, the default is **yes**; if more than one request is sent, the default is **no**.

Command Default

DNIS or CLID attribute values are not sent to the RADIUS server.

RADIUS Server Load Balancing Manual Testing

RADIUS server load-balancing server status manual testing does not occur.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(4)T	This command was introduced.
12.2(28)SB	The following keywords and arguments were added for configuring RADIUS load balancing manual testing functionality: **server** *ip-address*, **auth-port** *port-number*, **acct-port** *port-number*, **count** *request*, **rate** *requests-per-second*, **blocked**.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.2(31)ZV1	This command was enhanced to show user attributes returned from RADIUS authentication when authentication is successful.
Cisco IOS XE Release 2.4	This command was integrated into Cisco IOS XE Release 2.4.

Usage Guidelines

The **test aaa group** command can be used to

- Associate a DNIS or CLID named user profile with the record that is sent to the RADIUS server, which can then access DNIS or CLID information when the server receives a RADIUS record.
- Verify RADIUS load-balancing server status.

Note The **test aaa group**command does not work with TACACS+.

Examples

The following example shows how to configure a dnis = dnisvalue user profile named prfl1 and associate it with a **test aaa group**command:

```
aaa user profile prfl1
  aaa attribute dnis
  aaa attribute dnis dnisvalue
  no aaa attribute clid
! Attribute not found.
```

```
  aaa attribute clid clidvalue
  no aaa attribute clid
  exit
!
! Associate the dnis user profile with the test aaa group command.
test aaa group radius user1 pass new-code profile prfl1
```

The following example shows the response from a load-balanced RADIUS server that is alive when the username "test" does not match a user profile. The server is verified alive when it issues an Access-Reject response to a AAA packet generated by the **test aaa group** command.

```
Router# test aaa group SG1 test lab new-code

00:06:07: RADIUS/ENCODE(00000000):Orig. component type = INVALID
00:06:07: RADIUS/ENCODE(00000000): dropping service type, "radius-server attribute 6
on-for-login-auth" is off
00:06:07: RADIUS(00000000): Config NAS IP: 192.0.2.4
00:06:07: RADIUS(00000000): sending
00:06:07: RADIUS/ENCODE: Best Local IP-Address 192.0.2.141 for Radius-Server 192.0.2.176
00:06:07: RADIUS(00000000): Send Access-Request to 192.0.2.176:1645 id 1645/1, len 50
00:06:07: RADIUS:  authenticator CA DB F4 9B 7B 66 C8 A9 - D1 99 4E 8E A4 46 99 B4
00:06:07: RADIUS:  User-Password       [2]   18  *
00:06:07: RADIUS:  User-Name           [1]   6   "test"
00:06:07: RADIUS:  NAS-IP-Address      [4]   6   192.0.2.141
00:06:07: RADIUS: Received from id 1645/1 192.0.2.176:1645, Access-Reject, len 44
00:06:07: RADIUS:  authenticator 2F 69 84 3E F0 4E F1 62 - AB B8 75 5B 38 82 49 C3
00:06:07: RADIUS:  Reply-Message       [18]  24
00:06:07: RADIUS:   41 75 74 68 65 6E 74 69 63 61 74 69 6F 6E 20 66  [Authentication ]
00:06:07: RADIUS:   61 69 6C 75 72 65                               [failure]
00:06:07: RADIUS(00000000): Received from id 1645/1
00:06:07: RADIUS/DECODE: Reply-Message fragments, 22, total 22 bytes
```

Cisco 10000 Series Router

The following example shows the user attribute list that the RADIUS server returns when you issue the test aaa command and authentication is successful:

```
Router# test aaa group radius viral viral new-code blocked no
AAA/SG/TEST: Sending 1 Access-Requests @ 10/sec, 0 Accounting-Requests @ 10/sec
CLI-1#
AAA/SG/TEST: Testing Status
AAA/SG/TEST:      Authen Requests to Send    : 1
AAA/SG/TEST:      Authen Requests Processed  : 1
AAA/SG/TEST:      Authen Requests Sent       : 1
AAA/SG/TEST:      Authen Requests Replied    : 1
AAA/SG/TEST:      Authen Requests Successful : 1
AAA/SG/TEST:      Authen Requests Failed     : 0
AAA/SG/TEST:      Authen Requests Error      : 0
AAA/SG/TEST:      Authen Response Received   : 1
AAA/SG/TEST:      Authen No Response Received: 0
AAA/SG/TEST: Testing Status
AAA/SG/TEST:      Account Requests to Send    : 0
AAA/SG/TEST:      Account Requests Processed  : 0
AAA/SG/TEST:      Account Requests Sent       : 0
AAA/SG/TEST:      Account Requests Replied    : 0
AAA/SG/TEST:      Account Requests Successful : 0
AAA/SG/TEST:      Account Requests Failed     : 0
AAA/SG/TEST:      Account Requests Error      : 0
AAA/SG/TEST:      Account Response Received   : 0
AAA/SG/TEST:      Account No Response Received: 0
```

```
USER ATTRIBUTES
username              "Username:viral"
nas-ip-address        3.1.1.1
interface             "210"
service-type          1 [Login]
Framed-Protocol       3 [ARAP]
ssg-account-info      "S20.5.0.2"
ssg-command-code      0B 4C 32 54 50 53 55 52 46
Router
```

Related Commands

Command	Description
aaa attribute	Adds DNIS or CLID attribute values to a user profile.
aaa user profile	Creates a AAA user profile.
load-balance	Enables RADIUS server load-balancing for RADIUS-named server groups.
radius-server host	Enables RADIUS automated testing for load balancing.
radius-server load-balance	Enables RADIUS server load-balancing for the global RADIUS server group.

test crypto self-test

To test the crypto configuration to see if it passes or fails, use the **test crypto self-test**command in privileged or user EXEC mode.

test crypto self-test

Syntax Description

This command has no arguments or keywords.

Command Default

Privileged EXEC (#)

User EXEC (>)

Command History

Release	Modification
12.2XN	This command was introduced.

Usage Guidelines

As a result of the test, a new SELF_TEST_RESULT system log is generated. If the crypto test fails, a SELF_TEST_FAILURE system log is generated.

Examples

The following example displays the output of the **test crypto self-test**command:

```
Router# test crypto self-test
*Apr 23 01:48:49.678: %CRYPTO-6-SELF_TEST_RESULT: Self test info: (Self test ac)
*Apr 23 01:48:49.822: %CRYPTO-6-SELF_TEST_RESULT: Self test info: (DH self test)
*Apr 23 01:48:49.954: %CRYPTO-6-SELF_TEST_RESULT: Self test info: (Software Cry)
*Apr 23 01:48:50.054: %CRYPTO-6-SELF_TEST_RESULT: Self test info: (Software che)
*Apr 23 01:48:50.154: %CRYPTO-6-SELF_TEST_RESULT: Self test info: (DES encrypti)
Router#
*Apr 23 01:48:50.254: %CRYPTO-6-SELF_TEST_RESULT: Self test info: (3DES encrypt)
*Apr 23 01:48:50.354: %CRYPTO-6-SELF_TEST_RESULT: Self test info: (SHA hashing )
*Apr 23 01:48:50.454: %CRYPTO-6-SELF_TEST_RESULT: Self test info: (Random KAT t)
*Apr 23 01:48:50.674: %CRYPTO-6-SELF_TEST_RESULT: Self test info: (AES encrypti)
*Apr 23 01:48:50.774: %CRYPTO-6-SELF_TEST_RESULT: Self test info: (HMAC-SHA    )
Router#
*Apr 23 01:48:50.874: %CRYPTO-6-SELF_TEST_RESULT: Self test info: (SHA256 hashi)
*Apr 23 01:48:50.974: %CRYPTO-6-SELF_TEST_RESULT: Self test info: (SHA512 hashi)
*Apr 23 01:48:50.974: %CRYPTO-6-SELF_TEST_RESULT: Self test info: (ALL TESTS PA)
```

test cws

To test the Cloud Web Security configuration, use the **test cws** command in privileged EXEC mode.

test cws {**off-tower-check** | **on-tower-check** | **telemetry now**}

Syntax Description

off-tower-check	Disables Cloud Web Security server validation.
on-tower-check	Enables Cloud Web Security server validation.
telemetry now	Immediately sends telemetry and exceptions data to the Cloud Web Security server.

Command Default

Telemetry and exceptions data are sent at configured intervals.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.4(2)T	This command was introduced. This command replaces the **test content-scan** command.

Usage Guidelines

Note This command is used by the Technical Assistance Center to troubleshoot issues.

Telemetry is an automated communications process in which measurements are made and data that is collected at remote sites is transmitted to receiving equipment for monitoring.

The device on which the Cloud Web Security is configured is monitored, and data is generated periodically. Because most of these devices do not have a lot memory or secondary storage, the generated data is exported and stored in the Cloud Web Security server. The device connects to a URL hosted by the Cloud Web Security server by using the HTTP POST method to periodically send telemetry data.

Because the Cloud Web Security server does not have information about all web traffic, a connector (a persistent, out-of-band secure channel between the device and the Cloud Web Security server) periodically sends all exception rules to the server. The connector makes a POST request and pushes all exception rules to a URL. This URL is separate from the telemetry URL.

Examples

The following example shows how to immediately send telemetry and exceptions data to the Cloud Web Security server:

```
Device# test cws telemetry now
```

Related Commands

Command	Description
out-of-band telemetry	Enables Cloud Web Security out-of-band telemetry and content-scan exception rules.

Command	Description
parameter-map type cws	Configures a global Cloud Web Security parameter map and enters parameter-map type inspect configuration mode.

test urlf cache snapshot

To save the contents of the URL filtering cache to a file, use the **test urlf cache snapshot** command in privileged EXEC mode.

test urlf cache snapshot *file-name*

Syntax Description

file-name	The name of the Cisco IOS file in which the contents of the URL filtering cache are saved. Use the Cisco IOS file system naming conventions.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

To save the contents of the URL filtering cache to a file, use the **test urlf cache snapshot** command in privileged EXEC mode.

Examples

The following example shows how to save the contents of the URL filtering cache to a flash memory file system in the file trend-cache-snapshot:

```
Router# test urlf cache snapshot flash:trend-cache-snapshot
```

text-color

Note Effective with Cisco IOS Release 12.4(6)T, the **text-color**command is not available in Cisco IOS software.

To set the color of the text on the title bars of a Secure Sockets Layer Virtual Private Network (SSLVPN), use the **text-color** command in Web VPN configuration mode. To revert to the default color, use the **no** form of this command.

text-color [{**black** | **white**}]
no text-color [{**black** | **white**}]

Syntax Description

black	(Optional) Color of the text is black. This is the default value
white	(Optional) Color of the text is white.

Command Default

Color of the text is black.

Command Modes

Web VPN configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(6)T	This command was removed.

Usage Guidelines

This command is limited to only two values to limit the number of icons that are on the toolbar.

Examples

The following example shows that the text color will be white:

```
text-color white
```

Related Commands

Command	Description
webvpn	Enters Web VPN configuration mode.

threat-detection basic-threat

To configure basic threat detection for a zone, use the **threat-detection basic-threat** command in parameter-map type inspect configuration mode. To disable basic threat detection, use the **no** form of this command.

threat-detection basic-threat
no threat-detection basic-threat

Syntax Description

This command has no arguments or keywords.

Command Default

Threat detection is not enabled.

Command Modes

Parameter-map type inspect configuration (config-profile)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.

Usage Guidelines

You must configure the **parameter-map type inspect-zone** command before you can configure threat detection.

Threat detection refers to the ability of a security device to detect and take action against possible threats, anomalies, or attacks. Basic threat detection monitors the rate of predefined events per zone. Once the rate of a certain type of event exceeds the event rate monitoring limit, an alert is sent if the **alert on** command is configured.

Note You cannot associate a default zone to a zone parameter map. As a result, the Event Rate Monitoring feature is not configured as part of the default zone.

After you enable logging for a zone, a log message is logged for each threat detected.

Examples

The following example shows how to configure basic threat detection:

```
Router(config)# parameter-map type inspect-zone pmap-zone
Router(config-profile)# threat-detection basic-threat
Router(config-profile)# end
```

Related Commands

Command	Description
alert on	Turns on or off console display of Cisco IOS stateful packet inspection alert messages.
parameter-map type inspect-zone	Configures an inspect zone-type parameter map and enters parameter-map type inspect configuration mode.

Command	Description
show policy-firewall stats zone	Displays policy firewall statistics at a zone level.
threat-detection rate	Configures the threat detection rate for a zone.

threat-detection rate

To configure the threat detection rate for an event type, use the **threat-detection rate** command in parameter-map type inspect configuration mode. To disable basic threat detection, use the **no** form of this command.

threat-detection rate {**fw-drop** | **inspect-drop** | **syn-attack**} **average-time-frame** *seconds* **average-threshold** *packets-per-second* **burst-threshold** *packets-per-second*
no threat-detection rate {**fw-drop** | **inspect-drop** | **syn-attack**}

Syntax Description

fw-drop	Configures the threat detection rate for firewall drop events.
inspect-drop	Configures the threat detection rate for firewall inspection-based drop events.
syn-attack	Configures the threat detection rate for SYN attack events.
average-time-frame *seconds*	Configures the average time frame for threat detection, in seconds. Valid values are from 600 to 3600.
average-threshold *packet-per-second*	Configures the average threat detection threshold, in packets per second. Valid values are from 1 to 4294967295.
burst-threshold *packets-per-second*	Configures the burst threshold for threat detection, in packets per second. Valid values are from 1 to 1000000000.

Command Default

Threat detection rate is enabled by default.

Command Modes

Parameter-map type inspect configuration (config-profile)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.

Usage Guidelines

You must configure the **parameter-map type inspect-zone** command before you can configure the threat detection rate.

You must configure the **threat-detection basic-threat** command before you can configure the **threat-detection rate** command that configures the event rate monitoring rate limit.

Threat detection refers to the ability of a security device to detect possible threats, anomalies, or attacks and to take action against them.

Note Because you cannot associate a default zone to a zone parameter map, the Event Rate Monitoring feature is not configured as part of the default zone.

When you enable logging for a zone, a log message is logged for each threat detected.

Examples

The following example shows how to configure the threat detection rate for inspection-based drop events for a zone:

```
Router(config)# parameter-map type inspect-zone pmap-zone
Router(config-profile)# threat-detection rate inspect-drop average-time-frame 200
average-threshold 30 burst-threshold 40
Router(config-profile)# end
```

Related Commands

Command	Description
parameter-map type inspect-zone	Configures an inspect zone-type parameter map and enters parameter-map type inspect configuration mode.
show policy-firewall stats zone	Displays policy firewall statistics at a zone level.
threat-detection basic-threat	Configures basic threat detection for a zone.

throttle

To configure server group throttling of access (authentication and authorization) and accounting records that are sent to the RADIUS server, use the **throttle**command in server group configuration mode. To disable server group throttling of access (authentication and authorization) and accounting records that are sent to the RADIUS server, use the **no** form of this command.

throttle [**accounting** *threshold*] [**access** *threshold* [**access-timeout** *number-of-timeouts*]]
no throttle [**accounting** *threshold*] [**access** *threshold* [**access-timeout** *number-of-timeouts*]]

Syntax Description

accounting *threshold*	Configures the specified server group threshold value for accounting requests sent to a RADIUS server. The range is 0 through 65536. The default value is 0 (throttling disabled).
access *threshold*	Configures the specified server group threshold value for access requests sent to a RADIUS server. The range is 0 through 65536. The default value is 0 (throttling disabled).
access-timeout *number-of-timeouts*	(Optional) Specifies the number of consecutive access timeouts that are allowed before the access request from the specified server group is dropped. The range is 1 through 10. The default value is 3.

Command Default

Throttling is disabled.

Command Modes

Server-group configuration (config-sg-radius)

Command History

Release	Modification
12.2(33)SRC	This command was introduced.
12.2(33)SB	This command was implemented on the Cisco 10,000 series routers.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use this command to configure server group throttling of access (authentication and authorization) and accounting records that are sent to the RADIUS server. Server group configurations are used to enable or disable throttling for a particular server group and to specify the threshold value for that server group.

Examples

The following examples shows how to configure server group throttling of access (authentication and authorization) and accounting records that are sent to the RADIUS server.

The following example shows how to limit the number of accounting requests sent to server-group-A to 100:

```
Router> enable
Router# configure terminal
Router(config)# aaa group server radius server-group-A
Router(config-sg-radius)# throttle accounting 100
```

The following example shows how to limit the number of access requests packets sent to server-group-A to 200 and sets the number of timeouts allowed per transactions to 2:

```
Router> enable
Router# configure terminal
Router(config)# aaa group server radius server-group-A
Router(config-sg-radius)# throttle access 200 access-timeout 2
```

The following example shows how to throttle both accounting and access request packets for server-group-A:

```
Router> enable
Router# configure terminal
Router(config)# aaa group server radius server-group-A
Router(config-sg-radius)# throttle accounting 100 access 200
```

Related Commands

Command	Description
radius-server host	Specifies a RADIUS server host.
radius-server key	Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon.
radius-server retransmit	Specifies the number of times the Cisco IOS software searches the list of RADIUS server hosts before giving up.
radius-server throttle	Configures global throttling of access (authentication and authorization) and accounting records that are sent to the RADIUS server.
radius-server timeout	Specifies the number of seconds a router waits for a server host to reply before timing out.
show radius statistics	Displays the RADIUS statistics for accounting and authentication packets.

timeout (application firewall application-configuration)

To specify the elapsed length of time before an inactive connection is torn down, use the **timeout** command in the appropriate configuration mode. To return to the default value, use the **no** form of this command.

timeout *seconds*
no timeout *seconds*

Syntax Description

seconds	Idle timeout value. Available range: 5 to 43200 (12 hours).

Command Default

If this command is not issued, the default value specified via the **ip inspect tcp idle-time**command will be used.

Command Modes

cfg-appfw-policy-http
configuration

cfg-appfw-policy-aim configuration

cfg-appfw-policy-ymsgr configuration

cfg-appfw-policy-msnmsgr configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(4)T	Support for the inspection of instant messenger applications was introduced.

Usage Guidelines

The **timeout** command overrides the global TCP idle timeout value for HTTP traffic or for traffic of a specified instant messenger application (AOL, Yahoo, or MSN).

Before you can issue the **timeout** command, you must enable protocol inspection via the **application** command, which allows you to specify whether you want to inspect HTTP traffic or instant messenger application traffic. The **application** command puts the router in appfw-policy-*protocol*configuration mode, where "*protocol*" is dependent upon the specified protocol.

Examples

The following example shows how to define the HTTP application firewall policy "mypolicy." This policy includes all supported HTTP policy rules. After the policy is defined, it is applied to the inspection rule "firewall," which will inspect all HTTP traffic entering the FastEthernet0/0 interface.

```
! Define the HTTP policy.
appfw policy-name mypolicy
 application http
  strict-http action allow alarm
  content-length maximum 1 action allow alarm
  content-type-verification match-req-rsp action allow alarm
```

```
  max-header-length request 1 response 1 action allow alarm
  max-uri-length 1 action allow alarm
  port-misuse default action allow alarm
  request-method rfc default action allow alarm
  request-method extension default action allow alarm
  transfer-encoding type default action allow alarm
  timeout 60
!
!
! Apply the policy to an inspection rule.
ip inspect name firewall appfw mypolicy
ip inspect name firewall http
!
!
! Apply the inspection rule to all HTTP traffic entering the FastEthernet0/0 interface.
interface FastEthernet0/0
 ip inspect firewall in
!
!
```

Related Commands

Command	Description
ip inspect tcp idle-time	Specifies the TCP idle timeout (the length of time a TCP session will be managed while there is no activity).

timeout (config-radius-server)

To specify the time interval (in seconds) that the router waits for the RADIUS server to reply before retransmitting, use the **timeout** command in RADIUS server configuration mode. To restore the default value, use the **no** form of this command.

timeout *seconds*
no timeout

Syntax Description

seconds	Specifies the timeout interval, in seconds. The range is from 1 to 1000. The default is 5.

Command Default

The default timeout interval is 5 seconds.

Command Modes

RADIUS server configuration (config-radius-server)

Command History

Release	Modification
15.2(2)T	This command was introduced.

Usage Guidelines

Use the **timeout** command to set the number of seconds a router waits for a server host to reply before timing out.

If the RADIUS server is only a few hops from the router, it is recommended that you configure the RADIUS server timeout to 15 seconds.

Examples

The following example shows how to set the interval timer to 10 seconds:

```
Device(config)# aaa new-model
Device(config)# radius server myserver
Device(config-radius-server)# address ipv4 192.0.2.2
Device(config-radius-server)# timeout 10
```

Related Commands

Command	Description
aaa new-model	Enables the AAA access control model.
address ipv4	Configures the IPv4 address for the RADIUS server accounting and authentication parameters.
radius server	Specifies the name for the RADIUS server configuration and enters RADIUS server configuration mode.

timeout (GTP)

To configure timeout values for General Packet Radio Service (GPRS) Tunneling Protocol (GTP), use the **timeout** command in parameter-map type inspect configuration mode. To remove the configured timeout values, use the **no** form of this command.

timeout {**pdp-context** | **request-queue**}*time*
no timeout {**pdp-context** | **request-queue**}

Syntax Description

pdp-context *time*	Configures the timeout, in minutes, for inactive Packet Data Protocol (PDP) contexts. Valid values are from 1 to 35791. The default is 30.
request-queue *time*	Configures the timeout, in seconds, for inactive request queues. Valid values are from 0 to 2147483. The default is 60.

Command Default

Timeout values are not configured for GTP.

Command Modes

Parameter-map type inspect configuration mode (config-profile)

Command History

Release	Modification
Cisco IOS XE Release 3.7S	This command was introduced.

Usage Guidelines

When you configure the **timeout pdp-context** command, inactive PDP request queues are dropped based on the timeout value. Similarly, when you configure **timeout request-queue** command, GTP requests that are queued to wait for a response are dropped based on the timeout value.

Examples

The following example shows how to configure a timeout of 3000 minutes for inactive PDP contexts:

```
Device(config)# parameter-map type inspect-global gtp
Device(config-profile)# timeout pdp-context 3000
Device(config-profile)#
```

Related Commands

Command	Description
parameter-map type inspect-global	Configures a global parameter map and enters parameter-map type inspect configuration mode.

timeout (parameter-map)

To configure the time interval for content scanning, use the **timeout** command in parameter-map type inspect configuration. To disable the time interval for content scanning, use the **no** form of this command.

timeout {**server** *seconds* | **session-inactivity** *seconds*}
no timeout {**server** *seconds* | **session-inactivity** *seconds*}

Syntax Description

server	Specifies the server keepalive time in seconds.
seconds	Timeout in seconds. Valid values are from 5 to 43200. The default is 300.
session-inactivity	Specifies the session inactivity time in seconds.
seconds	Timeout in seconds. Valid values are from 5 to 43200. The default is 3600.

Command Default

The time interval for content scanning is not configured.

Command Modes

Parameter-map type inspect configuration (config-profile)

Command History

Release	Modification
15.2(1)T1	This command was introduced.

Usage Guidelines

The **timeout** command configures the timeout to check the availability of the Cloud Web Security servers and to determine the active tower. The primary tower is tried first and if it fails, the secondary tower is chosen as the active. The secondary tower falls back to the primary tower, if the primary is detected to be active for three consecutive timeouts. The session inactivity timer is used to remove the sessions that are inactive for the configured duration.

Examples

The following example shows how to configure the server timeout:

```
Device(config)# parameter-map type content-scan global
Device(config-profile)# timeout server 3450
```

Related Commands

Command	Description
parameter-map type cws global	Configures a global Cloud Web Security parameter map and enters parameter-map type inspect configuration mode.

timeout (policy group)

To configure the length of time that an end user session can remain idle or the total length of time that the session can remain connected, use the **timeout** command in webvpn group policy configuration mode. To configure timeout timers to default values, use the **no** form of this command.

timeout {**idle** *seconds* | **session** *seconds*}
no timeout {**idle** | **session**}

Syntax Description

idle *seconds*	Configures the length time that an end user connection can remain idle.
session *seconds*	Configures the total length of time that an end user can maintain a single connection.

Command Default

The following default values are used if this command is not configured or if the **no** form is entered:

idle 2100 **session** 43200

Command Modes

Webvpn group policy configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

This command is used to configure the idle or session timer value. The idle timer sets the length of time that a session will remain connected when the end user generates no activity. The session timer sets the total length of time that a session will remain connected, with or without activity. Upon expiration of either timer, the end user connection is closed. The user must login or reauthenticate to access the Secure Sockets Layer Virtual Private Network (SSL VPN).

Note The idle timer is not the same as the dead peer timer. The dead peer timer is reset when any packet type is received over the Cisco AnyConnect VPN Client tunnel. The idle timer is reset only when the end user generates activity.

Examples

The following example sets the idle timer to 30 minutes and session timer to 10 hours:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# policy group ONE

Router(config-webvpn-group)# timeout idle 1800

Router(config-webvpn-group)# timeout session 36000
```

Related Commands

Command	Description
policy group	Enters webvpn group policy configuration mode to configure a policy group.

Command	Description
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

timeout (TACACS+)

To configure the time to wait for a reply from the specified TACACS server, use the **timeout**command in TACACS+ server configuration mode. To return to the command default, use the **no** form of this command.

timeout *seconds*
no timeout *seconds*

Syntax Description

seconds	(Optional) Amount of time, in seconds.

Command Default

Time to wait is 5 seconds.

Command Modes

TACACS+ server configuration (config-server-tacacs)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.

Usage Guidelines

Use the **timeout** command to set the time, in seconds, to wait for a reply from the TACACS server. If the **timeout** command is configured, the specified number of seconds overrides the default time of 5 seconds.

Examples

The following example shows how to configure the wait time to 10 seconds:

```
Router(config)# tacacs server server1
Router(config-server-tacacs)# timeout 10
```

Related Commands

Command	Description
tacacs server	Configures the TACACS+ server for IPv6 or IPv4 and enters TACACS server configuration mode.

timeout file download

To specify how often the consent webpage should be downloaded from the file server, use the **timeout file download** command in parameter-map-type consent configuration mode. To remove the configured download time, use the **no** form of this command with the configured time.

timeout file download *minutes*
no timeout file download *minutes*

Syntax Description

minutes	The time, in minutes, that specifies how often the consent webpage should be downloaded from the file server. Available range: 1 to 525600.

Command Default

The consent webpage is not downloaded from the file server.

Command Modes

Parameter-map-type consent (config-profile)

Command History

Release	Modification
12.4(15)T	This command was introduced.

Usage Guidelines

Using the **timeout file download**command ensures that the consent file has the most current parameter map defintions.

Examples

In the following example, the file "consent_page.html" will be downloaded from the file server every 35791 minutes:

```
parameter-map type consent consent_parameter_map
 copy tftp://192.168.104.136/consent_page.html flash:consent_page.html
 authorize accept identity consent_identity_policy
 timeout file download 35791
 file flash:consent_page.html
 logging enabled
 exit
!
parameter-map type consent default
 copy tftp://192.168.104.136/consent_page.html flash:consent_page.html
 authorize accept identity test_identity_policy
 timeout file download 35791
 file flash:consent_page.html
 logging enabled
 exit
!
```

timeout login response

To specify how long the system will wait for login input (such as username and password) before timing out, use the **timeout login response**command in line configuration mode. To set the timeout value to 30 seconds (which is the default timeout value), use the **no**form of this command.

timeout login response *seconds*
no timeout login response *seconds*

Syntax Description

seconds	Integer that determines the number of seconds the system will wait for login input before timing out. Available settings are from 1 to 300 seconds. The default value is 30 seconds.

Command Default

The default login timeout value is 30 seconds.

Command Modes

Line configuration

Command History

Release	Modification
11.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example changes the login timeout value to 60 seconds:

```
line 10
 timeout login response 60
```

timeout retransmit

To set an interval for a router to wait for a reply from the Lightweight Directory Access Protocol (LDAP) server before it times out, use the **timeout retransmit**command in LDAP server configuration. To restore the default, use the **no** form of this command.

timeout retransmit *seconds*
no timeout retransmit *seconds*

Syntax Description

seconds	The timeout interval, in seconds. The range is from 1 to 65535. The default is 30.

Command Default

The default timeout interval value is 30 seconds.

Command Modes

LDAP server configuration (config-ldap-server)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Usage Guidelines

The recommended value to configure the LDAP server to timeout is 30 seconds.

Examples

The following example shows how to set an interval timer of 20 seconds for the LDAP server:

```
Router(config)# ldap server server1
Router(config-ldap-server)# timeout retransmit 20
```

Related Commands

Command	Description
ipv4(ldap)	Creates an IPv4 address within an LDAP server address pool.
ldap server	Defines an LDAP server and enters LDAP server configuration mode.
transport port (**ldap**)	Configures the transport protocol for establishing a connection with the LDAP server.

timer (Diameter peer)

To configure the Diameter Credit Control Application (DCCA) for peer-to-peer communication, use the **timer** command in Diameter peer configuration mode. To disable the configured protocol, use the **no** form of this command.

timer {**connection** | **transaction** | **watchdog**} **value**
no timer {**connection** | **transaction** | **watchdog**} **value**

Syntax Description

connection	Maximum interval, in seconds, for the Gateway General Packet RadioService (GPRS) Support Node (GGSN) to attempt reconnection to a Diameter peer after after being disconnected because of a transport failure. The range is from 1 to 1000. The default is 30. A value of 0 configures the GGSN not to attempt reconnection.
transaction	Maximum interval, in seconds, the GGSN waits for a Diameter peer to respond before trying another peer. The range is from 1 to 1000. The default is 30.
watchdog	Maximum interval, in seconds, the GGSN waits for a Diameter peer response to a watchdog packet. The range is from 1 to 1000. The default is 30. **Note** When the watchdog timer expires, a device watchdog request (DWR) is sent to the Diameter peer and the watchdog timer is reset. If a device watchdog answer (DWA) is not received before the next expiration of the watchdog timer, a transport failure to the Diameter peer has occurred.
value	The valid range, in seconds, from 1 to 1000. The default is 30.

Command Default

The default for each timer is 30 seconds.

Command Modes

Diameter peer configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.

Usage Guidelines

When configuring timers, the value for the transaction timer should be larger than the transmission-timeout value, and, on the Serving GPRS Support Node (SGSN), the values configured for the number of GPRS Tunneling Protocol (GTP) N3 requests and T3 retransmissions must be larger than the sum of all possible server timers (RADIUS, Diameter Credit Control Application (DCCA), and Cisco Content Services Gateway (CSG)). Specifically, the SGSN N3*T3 must be greater than 2 x RADIUS timeout + *N* x DCCA timeout + CSG timeout where:

- The factor *2* is for both authentication and accounting.
- *The value N* is for the number of Diameter servers configured in the server group.

Examples

The following example shows how to configure the Diameter base protocol timers for a Diameter peer:

```
Router (config-dia-peer)# timer connection
 20
Router (config-dia-peer)# timer watchdog
 25
```

Related Commands

Command	Description
diameter peer	Configures a Diameter peer and enters Diameter peer configuration sub-mode.
diameter peer timer	Configures the Diameter base protocol timers globally.

timer reauthentication (config-if-cts-dot1x)

To set the reauthentication timer period to be used if the authentication server does not specify a period, use the **timer reauthentication** command in CTS dot1x interface configuration mode. Use the **no** form of the command to disable the timer.

timer reauthentication *seconds*
no timer reauthentication *seconds*

Syntax Description

seconds	Specifies the reauthentication timer period in seconds.

Command Default

86400 seconds.

Command Modes

CTS dot1x interface configuration (config-if-cts-dot1x)

Command History

Release	Modification
12.2(33) SXI	This command was introduced on the Catalyst 6500 series switches.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

When the reauthentication timer expires, the device reauthenticates to the CTS network (NDAC).

Examples

The following example sets the reauthentication timer to 44 seconds:

```
Router(config-if-cts-dot1x)# timer reauthentication 44
```

Related Commands

Command	Description
cts dot1x	Enables Network Device Admission Control (NDAC) and configure NDAC authentication parameters.
propagate sgt (config-if-cts-dot1x)	Enables Security Group Tag (SGT) propagation on a Cisco TrustSec (CTS) 802.1X interface.
sap mode-list (config-if-cts-dot1x)	Configures CTS Security Association Protocol (SAP) authentication.
show cts interface	Displays CTS interface status and configurations.
show dot1x interface	Displays IEEE 802.1x configurations and statistics.

timers delay

To configure the time that a redundancy group takes to delay role negotiations that start after a fault occurs or the system is reloaded, use the **timers delay**command in redundancy application group configuration mode. To disable the timer, use the **no** form of this command.

timers delay *seconds* [**reload** *seconds*]
no timers delay *seconds* [**reload** *seconds*]

Syntax Description

seconds	Delay value. The range is from 0 to 10000. The default is 10.
reload	(Optional) Specifies the redundancy group reload timer.
seconds	(Optional) Reload timer value in seconds. The range is from 0 to 10000. The default is 120.

Command Default

The default is 10 seconds for timer delay and 120 seconds for reload delay.

Command Modes

Redundancy application group configuration (config-red-app-grp)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Examples

The following example shows how to set the timer delay value and reload value for a redundancy group named group 1:

```
Router# configure terminal
Router(config)# redundancy

Router(config-red)# application redundancy
Router(config-red-app)# group 1
Router(config-red-app-grp)# timers delay 100 reload 400
```

Related Commands

Command	Description
application redundancy	Enters redundancy application configuration mode.
authentication	Configures clear text authentication and MD5 authentication for a redundancy group.
control	Configures the control interface type and number for a redundancy group.
data	Configures the data interface type and number for a redundancy group.
group(firewall)	Enters redundancy application group configuration mode.
name	Configures the redundancy group with a name.

Command	Description
preempt	Enables preemption on the redundancy group.
protocol	Defines a protocol instance in a redundancy group.
redundancy rii	Configures the RII for the redundancy group.

timers hellotime

To configure timers for hellotime and holdtime messages for a redundancy group, use the **timers hellotime**command in redundancy application protocol configuration mode. To disable the timers in the redundancy group, use the **no** form of this command.

timers hellotime [**msec**] *seconds* **holdtime** [**msec**] *seconds*
no timers hellotime [**msec**] *seconds* **holdtime** [**msec**] *seconds*

Syntax Description

msec	(Optional) Specifies the interval, in milliseconds, for hello messages.
seconds	Interval time, in seconds, for hello messages. The range is from 1 to 254.
holdtime	Specifies the hold timer.
msec	Specifies the interval, in milliseconds, for hold time messages.
seconds	Interval time, in milliseconds, for hold time messages. The range is from 6 to 255.

Command Default

The default value for the hellotime interval is 3 seconds and for the holdtime interval is 10 seconds.

Command Modes

Redundancy application protocol configuration (config-red-app-prtc)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Usage Guidelines

The hello time is an interval in which hello messages are sent. The holdtime is the time before the active or the standby device is declared to be in down state. Use the **msec** keyword to configure the timers in milliseconds.

Note If you allocate a large amount of memory to the log buffer (e.g. 1 GB), then the CPU and memory utilization of the router increases. This issue is compounded if small intervals are set for the hellotime and the holdtime. If you want to allocate a large amount of memory to the log buffer, we recommend that you accept the default values for the hellotime and holdtime. For the same reason, we also recommend that you do not use the **preempt** command.

Examples

The following example shows how to configure the hellotime and holdtime messages:

```
Router# configure terminal
Router(config)# redundancy
Router(config-red)# application redundancy
Router(config-red-app)# protocol 1
Router(config-red-app-prtcl)# timers hellotime 100 holdtime 100
```

Related Commands

Command	Description
application redundancy	Enters redundancy application configuration mode.
authentication	Configures clear text authentication and MD5 authentication for a redundancy group.
group(firewall)	Enters redundancy application group configuration mode.
name	Configures the redundancy group with a name.
preempt	Enables preemption on the redundancy group.
protocol	Defines a protocol instance in a redundancy group.

title

To configure the HTML title string that is shown in the browser title and on the title bar of a Secure Sockets Layer Virtual Private Network (SSL VPN), use the **title** command in webvpn context configuration mode. To revert to the default text string, use the **no** form of this command.

title [*title-string*]
no title [*title-string*]

Syntax Description

title-string	(Optional) Title string, up to 255 characters in length, that is displayed in the browser of the user. The string value may contain 7-bit ASCII characters, HTML tags, and escape sequences.

Command Default

If this command is not configured or if the **no** form is entered, the following text is displayed:

"WebVPN Service"

Command Modes

Webvpn context configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

The optional form of the **title** command is entered to configure a custom text string. If this command is issued without entering a text string, a title will not be displayed in the browser window. If the **no** form of this command is used, the default title string "WebVPN Service" is displayed.

Examples

The following example configures "Secure Access: Unauthorized users prohibited" as the title string:

```
Router(config)#
webvpn context context1
Router(config-webvpn-context)# title "Secure Access: Unauthorized users prohibited"
Router(config-webvpn-context)#
```

Related Commands

Command	Description
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

title-color

To specify the color of the title bars on the login and portal pages of a Secure Sockets Layer Virtual Private Network (SSL VPN), use the **title-color** command in webvpn context configuration mode. To remove the color, use the **no** form of this command.

title-color *color*
no title-color *color*

Syntax Description

color	The value for the *color* argument is entered as a comma-separated red, green, blue (RGB) value, an HTML color value (beginning with a"#"), or the name of the color that is recognized in HTML (no spaces between words or characters). The value is limited to 32 characters. The value is parsed to ensure that it matches one of the following formats (using Perl regex notation): • \#/x{6} • \d{1,3},\d{1,3},\d{1,3} (and each number is from 1 to 255) • \w+ The default is purple.

Command Default

The color purple is used if this command is not configured or if the **no** form is entered.

Command Modes

Webvpn context configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(6)T	Support for the SSL VPN enhancements feature was added.

Usage Guidelines

Configuring a new color overrides the color the preexisting color.

Examples

The following examples show the three command forms that can be used to configure the title color:

```
Router(config-webvpn-context)# title-color darkseagreen

Router(config-webvpn-context)# title-color #8FBC8F

Router(config-webvpn-context)# title-color 143,188,143
```

Related Commands

Command	Description
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

traffic-export through zone security

- zone security, on page 1294

track(firewall)

To configure the redundancy group tracking, use the **track**command in redundancy application group configuration mode. To remove the redundancy group tracking, use the **no** form of this command.

track *object-number* {**decrement** *value* | **shutdown**}
no track *object-number* {**decrement** *value* | **shutdown**}

Syntax Description

object-number	ID of the event type.
decrement *value*	Specifies the value that the priority will be decremented. The range is from 1 to 255.
shutdown	Shuts down a redundancy group if the tracked object goes down instead of changing the priority.

Command Default

Objects and decrement priority per object are not tracked.

Command Modes

Redundancy application group configuration (config-red-app-grp)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Usage Guidelines

The redundancy group can track an object and decrease the priority value per object. Multiple objects can be tracked by the redundancy group to influence the priority appropriately. You can shut down a redundancy group if the tracked object goes down instead of changing the priority.

Examples

The following example shows how to track the redundancy group named group1 and assign a decrement value:

```
Router# configure terminal
Router(config)# redundancy

Router(config-red)# application redundancy
Router(config-red-app)# group 1
Router(config-red-app-grp)# track 200 decrement 50
```

Related Commands

Command	Description
application redundancy	Enters redundancy application configuration mode.
authentication	Configures clear text authentication and MD5 authentication for a redundancy group.
control	Configures the control interface type and number for a redundancy group.
data	Configures the data interface type and number for a redundancy group.

Command	Description
group(firewall)	Enters redundancy application group configuration mode.
name	Configures the redundancy group with a name.
preempt	Enables preemption on the redundancy group.
protocol	Defines a protocol instance in a redundancy group.
redundancy rii	Configures the RII for the redundancy group.

tracking

To override the default tracking policy on a port, use the **tracking**command in Neighbor Discovery (ND) inspection policy configuration mode.

tracking {**enable** [**reachable-lifetime** {*value* | **infinite**}] | **disable** [**stale-lifetime** {*value* | **infinite**}]}

Syntax Description

enable	Tracking is enabled.
reachable-lifetime	(Optional) The maximum amount of time a reachable entry is considered to be directly or indirectly reachable without proof of reachability. • The **reachable-lifetime** keyword can be used only with the **enable** keyword. • Use of the **reachable-lifetime** keyword overrides the global reachable lifetime configured by the **ipv6 neighbor binding reachable-lifetime** command.
value	Lifetime value, in seconds. The range is from 1 to 86400, and the default is 300.
infinite	Keeps an entry in a reachable or stale state for an infinite amount of time.
disable	Disables tracking.
stale-lifetime	(Optional) Keeps the time entry in a stale state, which overwrites the global stale-lifetime configuration. • The stale lifetime is 86,400 seconds. • The **stale-lifetime** keyword can be used only with the **disable** keyword. • Use of the **stale-lifetime** keyword overrides the global stale lifetime configured by the **ipv6 neighbor binding stale-lifetime** command.

Command Default

The time entry is kept in a reachable state.

Command Modes

ND inspection policy configuration (config-nd-inspection)

Command History

Release	Modification
12.2(50)SY	This command was introduced.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S.

Usage Guidelines

The **tracking** command overrides the default tracking policy set by the **ipv6 neighbor tracking** command on the port on which this policy applies. This function is useful on trusted ports where, for example, you may not want to track entries but want an entry to stay in the binding table to prevent it from being stolen.

The **reachable-lifetime** keyword is the maximum time an entry will be considered reachable without proof of reachability, either directly through tracking or indirectly through ND inspection. After the **reachable-lifetime** value is reached, the entry is moved to stale. Use of the **reachable-lifetime** keyword with the **tracking** command overrides the global reachable lifetime configured by the **ipv6 neighbor binding reachable-lifetime** command.

The **stale-lifetime** keyword is the maximum time an entry is kept in the table before it is deleted or the entry is proven to be reachable, either directly or indirectly. Use of the **stale-lifetime** keyword with the **tracking** command overrides the global stale lifetime configured by the **ipv6 neighbor binding stale-lifetime** command.

Examples

The following example defines an ND policy name as policy1, places the router in ND inspection policy configuration mode, and configures an entry to stay in the binding table for an infinite length of time on a trusted port:

```
Router(config)# ipv6 nd inspection policy policy1
Router(config-nd-inspection)# tracking disable stale-lifetime infinite
```

Related Commands

Command	Description
ipv6 nd inspection policy	Defines the ND inspection policy name and enters ND inspection policy configuration mode.
ipv6 nd raguard policy	Defines the RA guard policy name and enters RA guard policy configuration mode.
ipv6 neighbor binding	Changes the defaults of neighbor binding entries in a binding table.
ipv6 neighbor tracking	Enables tracking of entries in the binding table.

traffic-export

To control the operation of IP traffic capture mode in IP traffic export, use the **traffic-export** command in privileged EXEC mode.

traffic-export interface *type number* {**start** | **stop** | **clear** | **copy** *memory-device*}

Syntax Description

type number	Type and number of the interface over which the packets being captured travel.
start	Initiates a packet capture sequence.
stop	Halts a packet capture sequence.
clear	Clears the packet capture buffer.
copy	Copies the contents of the packet capture buffer to an external device.
memory-device	External memory device to which captured packets are transmitted. Options are *flash:*, *tftp:*, or *usbflash0:*.

Command Default

This command has no defaults.

Command Modes

Privileged EXEC.

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Use the **traffic-export** command to control the operation of IP traffic capture mode in IP traffic export. The operator uses CLI commands to start or stop capture of packets flowing across a monitored interface, to copy the captured packets to an external memory device, or to clear the internal buffer which holds the captured packets.

Examples

The following example illustrates the use of the **traffic-export** command to initiate the capture of packets on interface FastEthernet 0/0.

```
Router# traffic-export interface fastethernet 0/0 start
%RITE-5-CAPTURE_START: Started IP traffic capture for interface FastEthernet0/0
router#
```

The following example illustrates the use of the **traffic-export** command to halt the packet capture sequence on interface FastEthernet 0/0.

```
Router# traffic-export interface fastethernet 0/0 stop
%RITE-5-CAPTURE_STOP: Stopped IP traffic capture for interface FastEthernet0/0
router#
```

The following example illustrates the use of the **traffic-export** command to copy the contents of the packet capture buffer to an external memory device. The example of the interactive dialog identifies the external memory device and the remote host in which it resides.

```
Router# traffic-export interface fastethernet0/0 copy tftp:

Address or name of remote host []? 172.18.207.15

Capture buffer filename []? atmcapture

Copying capture buffer to tftp://172.18.207.15/atmcapture !!
router#
```

The following example illustrates the use of the **traffic-export** command to clear the packet capture buffer that is in local memory.

```
Router# traffic-export interface fastethernet 0/0 clear
%RITE-5-CAPTURE_CLEAR: Cleared IP traffic capture buffer for interface FastEthernet0/0
router#
```

Related Commands

Command	Description
ip traffic-export apply profile	Applies an IP traffic export or IP traffic capture profile to a specific interface.
ip traffic-export profile	Creates an IP traffic export or IP traffic capture profile on an ingress interface.

transfer-encoding type

To permit or deny HTTP traffic according to the specified transfer-encoding of the message, use the **transfer-encoding type**command in appfw-policy-http configuration mode. To disable this inspection parameter, use the **no** form of this command.

transfer-encoding type {**chunked** | **compress** | **deflate** | **gzip** | **identity** | **default**} **action** {**reset** | **allow**} [**alarm**]
no transfer-encoding type {**chunked** | **compress** | **deflate** | **gzip** | **identity** | **default**} **action** {**reset** | **allow**} [**alarm**]

Syntax Description

chunked	Encoding format (specified in RFC 2616, *Hypertext Transfer Protocol--HTTP/1*) in which the body of the message is transferred in a series of chunks; each chunk contains its own size indicator.
compress	Encoding format produced by the UNIX "compress" utility.
deflate	"ZLIB" format defined in RFC 1950, *ZLIB Compressed Data Format Specification version 3.3* , combined with the "deflate" compression mechanism described in RFC 1951, *DEFLATE Compressed Data Format Specification version 1.3* .
gzip	Encoding format produced by the "gzip" (GNU zip) program.
identity	Default encoding, which indicates that no encoding has been performed.
default	All of the transfer encoding types.
action	Encoding types outside of the specified type are subject to the specified action (**reset** or **allow**).
reset	Sends a TCP reset notification to the client or server if the HTTP message fails the mode inspection.
allow	Forwards the packet through the firewall.
alarm	(Optional) Generates system logging (syslog) messages for the given action.

Command Default

If a given type is not specified, all transfer-encoding types are supported with the reset alarm action.

Command Modes

appfw-policy-http configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

Only encoding types specified by the **transfer-encoding-type**command are allowed through the firewall.

Examples

The following example shows how to define the HTTP application firewall policy "mypolicy." This policy includes all supported HTTP policy rules. After the policy is defined, it is applied to the inspection rule "firewall," which will inspect all HTTP traffic entering the FastEthernet0/0 interface.

```
! Define the HTTP policy.
appfw policy-name mypolicy
 application http
  strict-http action allow alarm
  content-length maximum 1 action allow alarm
  content-type-verification match-req-rsp action allow alarm
  max-header-length request 1 response 1 action allow alarm
  max-uri-length 1 action allow alarm
  port-misuse default action allow alarm
  request-method rfc default action allow alarm
  request-method extension default action allow alarm
  transfer-encoding type default action allow alarm
!
!
! Apply the policy to an inspection rule.
ip inspect name firewall appfw mypolicy
ip inspect name firewall http
!
!
! Apply the inspection rule to all HTTP traffic entering the FastEthernet0/0 interface.
interface FastEthernet0/0
 ip inspect firewall in
!
!
```

transport port

To configure the transport protocol for establishing a connection with the Diameter peer, use the **transport port**command in Diameter peer configuration mode. To block all sessions that are bound to the peer from using the connection, use the no form of this command.

transport tcp port port-number
no transport tcp port port-number

Syntax Description

tcp	Currently, TCP is the only supported transport protocol for establishing the connection with the Diameter peer.
port-number	Character string identifying the peer connection port.

Command Default

TCP is the default transport protocol.

Command Modes

Diameter peer configuration

Command History

Release	Modification
12.4(9)T	This command was introduced .

Examples

The following example configures TCP as the transport protocol and port 4100 as the peer connection port:

```
Router (config-dia-peer)# transport tcp port
 4100
```

Related Commands

Command	Description
diameter peer	Defines a Diameter peer and enters Diameter peer configuration mode.

transport port (ldap)

To configure the transport protocol for establishing a connection with the Lightweight Directory Access Protocol (LDAP) server, use the **transport port** command in LDAP server configuration mode. To delete all sessions that are bound to the server from using the connection, use the **no** form of this command.

transport port *port-number*
no transport port *port-number*

Syntax Description

port-number	Server connection port number. Valid port numbers range from 1 to 65535. The default is 389.

Command Default

The default port number is 389.

Command Modes

LDAP server configuration (config-ldap-server)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Examples

The following example shows how to configure the transport protocol and port 200 as the peer connection port:

```
Router(config)# ldap server server1
Router(config-ldap-server)# transport port 200
```

Related Commands

Command	Description
ipv4 (ldap)	Creates an IPv4 address within an LDAP server address pool.
ldap server	Defines an LDAP server and enters LDAP server configuration mode.

trm register

To allow the user to manually register the platform with the Trend Router Provisioning Server (TRPS), use the **trm register**command in privileged EXEC mode.

trm register [**force**]

Syntax Description

force	Sends a new registration request to TRPS.

Command Default

This command is not enabled.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(15)XZ	This command was introduced.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
15.1(2)T	This command was modified. The **force**keyword was added.

Usage Guidelines

Use the **trm register** command to enable manual registration of the platform with the TRPS. If you do not use this command, the system sends a registration request to the TRPS every minute after boot-up until the registration is successful.

Examples

The following is sample output from the **trm register**command:

```
Router# trm register
Processing registration request.
Please run 'show ip trm subscription" status to get more info
```

trustpoint (tti-petitioner)

To specify the trustpoint that is to be associated with the Trusted Transitive Introduction (TTI) exchange between the Secure Device Provisioning (SDP) petitioner and the SDP registrar, use the **trustpoint**command in tti-petitioner configuration mode. To change the specified trustpoint or use the default trustpoint, use the **no** form of this command.

trustpoint *trustpoint-label*
no trustpoint *trustpoint-label*

Syntax Description

trustpoint-label	Name of trustpoint.

Command Default

If a trustpoint is not specified, a default trustpoint called "tti" is generated.

Command Modes

tti-petitioner configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.

Usage Guidelines

Use the **trustpoint** command in tti-petitioner configuration mode to associate a trustpoint with the SDP petitioner.

Examples

The following example shows how specify the trustpoint "mytrust":

```
crypto wui tti petitioner
 trustpoint mytrust
```

After the SDP exchange is complete, the petitioner will automatically enroll with the registrar and obtain a certificate. The following sample output from the **show running-config** command shows an automatically generated configuration which generates the default trustpoint "tti":

```
crypto pki trustpoint tti
 enrollment url http://pki1-36a.cisco.com:80
 revocation-check crl
 rsakeypair tti 1024
 auto-enroll 70
```

Related Commands

Command	Description
crypto ca trustpoint	Declares the CA that your router should use.
crypto wui tti petitioner	Configures a device to become an SDP petitioner and enters tti-petitioner configuration mode.

trustpoint signing

To specify the trustpoint and associated certificate to be used when signing all introduction data during the Secure Device Provisioning (SDP) exchange, use the **trustpoint signing**command in tti-petitioner configuration mode. To change the specified trustpoint or use the default trustpoint, use the **no** form of this command.

trustpoint signing *trustpoint-label*
no trustpoint signing *trustpoint-label*

Syntax Description

trustpoint-label	Name of trustpoint.

Command Default

If a trustpoint is not specified, any existing device certificate is used. If none is available, a self-signed certificate is generated.

Command Modes

tti-petitioner configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

Use the **trustpoint** signing command in tti-petitioner configuration mode to associate a specific trustpoint with the petitioner for signing its certificate.

Examples

The following example shows how to specify the trustpoint mytrust:

```
crypto provisioning petitioner
 trustpoint signing mytrust
```

After the SDP exchange is complete, the petitioner automatically enrolls with the registrar and obtains a certificate. The following sample output from the **show running-config** command shows an automatically generated configuration with the default trustpoint tti:

```
crypto pki trustpoint tti
 enrollment url http://pki1-36a.cisco.com:80
 revocation-check crl
 rsakeypair tti 1024
 auto-enroll 70
```

Related Commands

Command	Description
crypto ca trustpoint	Declares the CA that your router should use.
crypto provisioning petitioner	Configures a device to become an SDP petitioner and enters tti-petitioner configuration mode.
trustpoint (tti-petitioner)	Specifies the trustpoint associated with the SDP exchange between the petitioner and the registrar.

trusted-port (IPv6 NDP Inspection Policy)

To configure a port to become a trusted port, use the **trusted-port** command in Neighbor Discovery Protocol (NDP) inspection policy configuration mode . To disable this function, use the **no** form of this command.

trusted-port
no trusted-port

Syntax Description

This command has no arguments or keywords.

Command Default

No ports are trusted.

Command Modes

NDP inspection policy configuration
(config-nd-inspection)

Command History

Release	Modification
12.2(50)SY	This command was introduced.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S.

Usage Guidelines

When the **trusted-port** command is enabled, limited or no verification is performed when messages are received on ports that have this policy. However, to protect against address spoofing, messages are analyzed so that the binding information that they carry can be used to maintain the binding table. Bindings discovered from these ports will be considered more trustworthy than bindings received from ports that are not configured to be trusted.

Use the **trusted-port** command after enabling NDP inspection policy configuration mode using the **ipv6 nd inspection policy** command.

Examples

The following example defines an NDP policy name as policy1, places the router in NDP inspection policy configuration mode, and configures the port to be trusted:

```
Router(config)# ipv6 nd inspection policy policy1
Router(config-nd-inspection)# trusted-port
```

Related Commands

Command	Description
ipv6 nd inspection policy	Defines the NDP inspection policy name and enters NDP inspection policy configuration mode.

trusted-port (IPv6 RA Guard Policy)

To configure a port to become a trusted port, use the **trusted-port**command in router advertisement (RA) guard policy configuration . To disable this function, use the **no** form of this command.

trusted-port
no trusted-port

Syntax Description

This command has no arguments or keywords.

Command Default

No ports are trusted.

Command Modes

RA guard policy configuration
(config-ra-guard)

Command History

Release	Modification
12.2(50)SY	This command was introduced.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
15.3(1)S	This command was integrated into Cisco IOS Release 15.3(1)S.

Usage Guidelines

When the **trusted-port** command is enabled, limited or no verification is performed when messages are received on ports that have this policy. However, the **device-role** command takes precedence over the **trusted-port** command; if the device role is configured as host, messages will be dropped regardless of **trusted-port** command configuration.

Examples

The following example defines an RA guard policy name as raguard1, places the router in RA guard policy configuration mode, and configures the port to be trusted:

```
Router(config)# ipv6 nd inspection policy policy1
Router(config-ra-guard)# trusted-port
```

Related Commands

Command	Description
ipv6 nd inspection policy	Defines the NDP inspection policy n ame and enters NDP inspection policy configuration mode.
ipv6 nd raguard policy	Defines the RA guard policy name and enter RA guard policy configuration mode.

tunnel-limit (GTP)

To specify the maximum number of General Packet Radio Service (GPRS) Tunneling Protocol (GTP) tunnels that can be configured, use the **tunnel-limit** command in parameter-map type inspect configuration mode. To return to the default tunnel limit, use the **no** form of this command.

tunnel-limit *max-tunnels*
no tunnel-limit

Syntax Description

max-tunnels	Number of GTP tunnels that can be configured. Valid values are from 1 to 4294967295. The default is 500.

Command Default

A tunnel limit of 500 is configured.

Command Modes

Parameter-map type inspect configuration (config-profile)

Command History

Release	Modification
Cisco IOS XE Release 3.7S	This command was introduced.

Examples

The following example shows how to limit the number of configured GTP tunnels to 23456:

```
Device(config)# parameter-map type inspect-global gtp
Device(config-profile)# tunnel-limit 23456
Device(config-profile)#
```

Related Commands

Command	Description
parameter-map type inspect-global	Configures a global parameter map and enters parameter-map type inspect configuration mode.

tunnel mode

To set the encapsulation mode for the tunnel interface, use the **tunnel mode** command in interface configuration mode. To restore the default mode, use the no form of this command.

tunnel mode {**aurp** | **auto** | **cayman** | **dvmrp** | **eon** | **gre** | **gre multipoint** | **gre ip** | **gre ipv6** | **ipip** [**decapsulate-any**] | **ipsec ipv4** | **iptalk** | **ipv6** | **ipsec ipv6** | **mpls** | **nos** | **rbscp**}
no tunnel mode

Syntax Description

aurp	Specifies AppleTalk Update-Based Routing Protocol.
auto	Enables auto tunneling mode.
cayman	Specifies Cayman TunnelTalk AppleTalk encapsulation.
dvmrp	Specifies Distance Vector Multicast Routing Protocol.
eon	Specifies EON compatible Connectionless Network Protocol (CLNS) tunnel.
gre	Specifies generic routing encapsulation (GRE) protocol. This is the default.
gre multipoint	Specifies Multipoint GRE (mGRE).
gre ip	Specifies GRE tunneling using IPv4 as the delivery protocol.
gre ipv6	Specifies GRE tunneling using IPv6 as the delivery protocol.
ipip	Specifies IP-over-IP encapsulation.
decapsulate-any	(Optional) Terminates any number of IP-in-IP tunnels at one tunnel interface. This tunnel will not carry any outbound traffic; however, any number of remote tunnel endpoints can use a tunnel configured this way as their destination.
ipsec ipv4	Specifies tunnel mode is IPsec, and the transport is IPv4.
iptalk	Specifies Apple IPTalk encapsulation.
ipv6	Specifies static tunnel interface configured to encapsulate IPv6 or IPv4 packets in IPv6.
ipsec ipv6	Specifies tunnel mode is IPsec, and the transport is IPv6.
mpls	Specifies Multiprotocol Label Switching (MPLS) encapsulation.
nos	Specifies KA9Q/NOS compatible IP over IP.
rbscp	Specifies Rate Based Satellite Control Protocol (RBSCP).

Command Default

The default is GRE tunneling.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
10.0	This command was introduced.
10.3	This command was modified. The **aurp**, **dvmrp**, and **ipip** keywords were added.
11.2	This command was modified. The optional **decapsulate-any** keywords were added.
12.2(13)T	This command was modified. The **gre multipoint** keywords were added.
12.3(7)T	This command was modified. The following keywords were added: • **gre ipv6** to support GRE tunneling using IPv6 as the delivery protocol. • **ipv6** to allow a static tunnel interface to be configured to encapsulate IPv6 or IPv4 packets in IPv6. • **rbscp** to support RBSCP.
12.3(14)T	This command was modified. The **ipsec ipv4** keywords were added.
12.2(18)SXE	This command was modified. The **gre multipoint** keywords were added.
12.2(30)S	This command was integrated into Cisco IOS Release 12.2(30)S.
12.2(25)SG	This command was integrated into Cisco IOS Release 12.2(25)SG.
12.4(4)T	This command was modified. The **ipsec ipv6** keywords were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 2.1	This command was implemented on the Cisco ASR 1000 Series Aggregation Services Routers.
15.4(2)T	This command was modified. The **auto** keyword was added.
15.4(2)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.
Cisco IOS XE Release 3.12S	This command was integrated into Cisco IOS XE Release 3.12S.

Usage Guidelines

Auto Tunneling

Auto tunneling mode eases the configuration and spares you about knowing the responder's details. It automatically applies the tunneling protocol (GRE or IPsec) and transport protocol (IPv4 or IPv6) on the virtual template as soon as the IKE profile creates the virtual access interface.

Cayman Tunneling

Designed by Cayman Systems, Cayman tunneling implements tunneling to enable Cisco devices to interoperate with Cayman GatorBoxes. With Cayman tunneling, you can establish tunnels between two devices or between a Cisco device and a GatorBox. When using Cayman tunneling, you must not configure the tunnel with an AppleTalk network address.

DVMRP

Use DVMRP when a device connects to an mrouted (multicast) device to run DVMRP over a tunnel. You must configure Protocol Independent Multicast (PIM) and an IP address on a DVMRP tunnel.

GRE with AppleTalk

GRE tunneling can be done between Cisco devices only. When using GRE tunneling for AppleTalk, you configure the tunnel with an AppleTalk network address. Using the AppleTalk network address, you can ping the other end of the tunnel to check the connection.

IPsec in IPv6 Transport

IPv6 IPsec encapsulation provides site-to-site IPsec protection of IPv6 unicast and multicast traffic. This feature allows IPv6 devices to work as a security gateway, establishes IPsec tunnels between another security gateway device, and provides crypto IPsec protection for traffic from an internal network when being transmitting across the public IPv6 Internet. IPv6 IPsec is very similar to the security gateway model using IPv4 IPsec protection.

Multipoint GRE

After enabling mGRE tunneling, you can enable the **tunnel protection** command, which allows you to associate the mGRE tunnel with an IPsec profile. Combining mGRE tunnels and IPsec encryption allows a single mGRE interface to support multiple IPsec tunnels, thereby simplifying the size and complexity of the configuration.

Note GRE tunnel keepalives configured using the **keepalive** command under a GRE interface are supported only on point-to-point GRE tunnels.

RBSCP

RBSCP tunneling is designed for wireless or long-distance delay links with high error rates, such as satellite links. Using tunnels, RBSCP can improve the performance of certain IP protocols, such as TCP and IPsec, over satellite links without breaking the end-to-end model.

Source and Destination Address

You cannot have two tunnels that use the same encapsulation mode with exactly the same source and destination address. The workaround is to create a loopback interface and source packets off of the loopback interface.

Examples

The following example shows how to enable auto tunneling mode:

```
Device(config)# interface tunnel 0
Device(config-if)# tunnel source ethernet 0
Device(config-if)# tunnel destination 10.108.164.19
Device(config-if)# tunnel mode auto
```

The following example shows how to enable Cayman tunneling:

```
Device(config)# interface tunnel 0
Device(config-if)# tunnel source ethernet 0
Device(config-if)# tunnel destination 10.108.164.19
Device(config-if)# tunnel mode cayman
```

The following example shows how to enable GRE tunneling:

```
Device(config)# interface tunnel 0
Device(config-if)# appletalk cable-range 4160-4160 4160.19
Device(config-if)# appletalk zone Engineering
Device(config-if)# tunnel source ethernet0
Device(config-if)# tunnel destination 10.108.164.19
Device(config-if)# tunnel mode gre
```

The following example shows how to configure a tunnel using IPsec encapsulation with IPv4 as the transport mechanism:

```
Device(config)# crypto ipsec profile PROF
Device(config)# set transform tset
Device(config)# interface Tunnel0
Device(config)# ip address 10.1.1.1 255.255.255.0
Device(config)# tunnel mode ipsec ipv4
Device(config)# tunnel source Loopback0
Device(config)# tunnel destination 172.16.1.1
Device(config-if)# tunnel protection ipsec profile PROF
```

The following example shows how to configure an IPv6 IPsec tunnel interface:

```
Device(config)# interface tunnel 0
Device(config-if)# ipv6 address 2001:0DB8:1111:2222::2/64
Device(config-if)# tunnel destination 10.0.0.1
Device(config-if)# tunnel source Ethernet 0/0
Device(config-if)# tunnel mode ipsec ipv6
Device(config-if)# tunnel protection ipsec profile profile1
```

The following example shows how to enable mGRE tunneling:

```
interface Tunnel0
 bandwidth 1000
 ip address 10.0.0.1 255.255.255.0
! Ensures longer packets are fragmented before they are encrypted; otherwise, the ! receiving
 router would have to do the reassembly.
 ip mtu 1416
! Turns off split horizon on the mGRE tunnel interface; otherwise, EIGRP will not ! advertise
 routes that are learned via the mGRE interface back out that interface.
 no ip split-horizon eigrp 1
 no ip next-hop-self eigrp 1
 delay 1000
! Sets IPSec peer address to Ethernet interface's public address.
 tunnel source Ethernet0
 tunnel mode gre multipoint
! The following line must match on all nodes that want to use this mGRE tunnel.
 tunnel key 100000
 tunnel protection ipsec profile vpnprof
```

The following example shows how to enable RBSCP tunneling:

```
Device(config)# interface tunnel 0
Device(config-if)# tunnel source ethernet 0
Device(config-if)# tunnel destination 10.108.164.19
Device(config-if)# tunnel mode rbscp
```

Related Commands

Command	Description
appletalk cable-range	Enables an extended AppleTalk network.

Command	Description
appletalk zone	Sets the zone name for the connected AppleTalk network.
tunnel destination	Specifies the destination for a tunnel interface.
tunnel protection	Associates a tunnel interface with an IPsec profile.
tunnel source	Sets the source address of a tunnel interface.

tunnel mode ipsec dual-overlay

To configure the tunnel mode as dual-overlay, use the **tunnel mode ipsec dual-overlay** command in interface configuration mode. To restore the default mode, use the no form of this command.

tunnel mode ipsec dual-overlay
no tunnel mode ipsec dual-overlay

Syntax Description

ipsec	Tunnel mode is IPsec.
dual-overlay	Specifies a dual-overlay tunnel.

Command Default

None.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
Cisco IOS XE Cupertino 17.9.1a	This command was introduced.

Usage Guidelines

Use the **tunnel mode ipsec dual-overlay** command to specify the encapsulation protocol for the tunnel. IPsec dual-overlay tunnel modes provides the capabilities to carry both IPv4 and IPv6 traffic using a single IPsec Security Association (SA) that is tunnelled over IPv4.

Examples

The following example shows how to configure the tunnel mode as dual-overlay:

```
Device(config)# interface tunnel 1
Device(config-if)# ipv6 enable
Device(config-if)# tunnel source ethernet 0/0
Device(config-if)# tunnel mode ipsec dual-overlay
Device(config-if)# tunnel destination 10.108.164.19 255.255.255.255.0
Device(config-if)# tunnel protection IPsec profile ipsecprof
```

Related Commands

Command	Description
tunnel protection	Associates a tunnel interface with an IPsec profile.
tunnel mode	Sets the encapsulation mode for the tunnel interface.

tunnel protection

To associate a tunnel interface with an IP Security (IPsec) profile, use the **tunnel protection** command in interface configuration mode. To disassociate a tunnel with an IPsec profile, use the **no** form of this command.

tunnel protection { ipsec profile *name* **[shared | { isakmp-profile | ikev2-profile }** *name* **] } | { timeout pending-connection** *<timeout>* **}**
no tunnel protection { ipsec profile *name* **[shared | { isakmp-profile | ikev2-profile }** *name* **] } | { timeout pending-connection** *<timeout>* **}**

Syntax Description

ipsec profile	Enables generic routing encapsulation (GRE) tunnel encryption via IPsec.
name	Name of the IPsec profile. This value must match the *name* specified in the **crypto ipsec profile** command.
shared	(Optional) Allows the tunnel protection IPsec Security Association Database (SADB) to share the same dynamic crypto map instead of creating a unique crypto map per tunnel interface.
isakmp-profile	Specifies the isakmp profile for the crypto connection.
ikev2-profile	Specifies the ikev2 profile for the crypto connection.
shared name	Name of the shared socket for the crypto connection.
timeout pending-connection *seconds*	Specifies the timeout to terminate pending connections. The default value is 300 seconds. The range is 60-3600

Command Default

Tunnel interfaces are not associated with IPsec profiles.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
XE 17.3.4	The **timeout pending-connection** keyword was introduced.
12.2(13)T	This command was introduced.
12.3(5)T	The shared keyword was added.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.4(5)	The **shared** keyword was changed so that if it is used with the **tunnel protection** command, the **tunnel source** command must specify an interface instead of an IP address.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.(33)SRA.
Cisco IOS XE Release 2.5	This command was modified. This command was integrated into Cisco IOS XE Release 2.5.

Release	Modification
15.4(2)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

Usage Guidelines

Use the **tunnel protection** command to specify that IPsec encryption will be performed after the GRE has been added to the tunnel packet. The **tunnel protection** command can be used with multipoint GRE (mGRE) and point-to-point GRE (p-pGRE) tunnels. With p-pGRE tunnels, the tunnel destination address will be used as the IPsec peer address. With mGRE tunnels, multiple IPsec peers are possible; the corresponding Next Hop Resolution Protocol (NHRP) mapping nonbroadcast multiaccess (NBMA) destination addresses will be used as the IPsec peer addresses.

The shared Keyword

If you want to configure two Dynamic Multipoint VPN (DMVPN) mGRE and IPsec tunnels on the same router with the same local endpoint (tunnel source) configuration, you *must* issue the **shared** keyword.

The dynamic crypto map that is created by the **tunnel protection** command is always different from a crypto map that is configured directly on the interface.

Unlike with the **tunnel protection** command, which specifies that IPsec encryption will be performed after GRE encapsulation, configuring a crypto map on a tunnel interface specifies that encryption will be performed before GRE encapsulation.

If the **shared** keyword is used, the **tunnel source** command must specify an interface instead of an IP address. Crypto sockets are not shared if the tunnel source is not specified as an interface.

Note GRE keepalive is supported only with crypto map. GRE tunnel keepalives (configured with the **keepalive** command under the GRE interface) are not supported in combination with the **tunnel protection** command.

The **tunnel mode** command must be configured before running the **tunnel protection** command. Changing the sequence by configuring this command followed by the **tunnel mode** command results in the tunnel not having connectivity.

Examples

The following example shows how to associate the IPsec profile “vpnprof” with an mGRE tunnel interface. In this example, the IPsec source peer address will be the IP address from Ethernet interface 0. There is a static NHRP mapping from IP address 10.0.0.3 to IP address 172.16.2.1, so for this NHRP mapping the IPsec destination peer address will be 172.16.2.1. The IPsec proxy will be as follows: **permit gre host ethernet0-ip-address host ip-address**. Other NHRP mappings (static or dynamic) will automatically create additional IPsec security associations (SAs) with the same source peer address and the destination peer address from the NHRP mapping. The IPsec proxy for these NHRP mappings will be as follows: **permit gre host** *ethernet0-ip-address* **host** *NHRP-mapping-NBMA-address*.

```
crypto ipsec profile vpnprof
 set transform-set trans2
!
interface Tunnel0
 bandwidth 1000
 ip address 10.0.0.1 255.255.255.0
! Ensures that longer packets are fragmented before they are encrypted; otherwise, the
! receiving router would have to do the reassembly.
```

```
 ip mtu 1416
 ip nhrp authentication donttell
 ip nhrp map multicast dynamic
 ip nhrp network-id 99
 ip nhrp holdtime 300
! Turns off split horizon on the mGRE tunnel interface; otherwise, EIGRP will not
! advertise routes that are learned via the mGRE interface back out that interface.
 no ip split-horizon eigrp 1
 no ip next-hop-self eigrp 1
 delay 1000
! Sets the IPSec peer address to the Ethernet interface's public address.
 tunnel source Ethernet0
 tunnel mode gre multipoint
! The following line must match on all nodes that want to use this mGRE tunnel.
 tunnel key 100000
 tunnel protection ipsec profile vpnprof
```

The following example shows how to associate the IPsec profile "vpnprof" with a p-pGRE tunnel interface. In this example, the IPsec source peer address will be the IP address from Ethernet interface 0. The IPsec destination peer address will be 172.16.1.10 (per the **tunnel destination address** command). The IPsec proxy will be as follows: **permit gre host** *ethernet0-ip-address* **host** *ip-address*.

```
interface Tunnel1
 ip address 10.0.1.1 255.255.255.252
! Ensures that longer packets are fragmented before they are encrypted; otherwise, the
! receiving router would have to do the reassembly.
 ip mtu 1420
 tunnel source Ethernet0
 tunnel destination 172.16.1.10
 tunnel protection ipsec profile vpnprof
```

In the following example, the crypto sockets are shared between the Tunnel0 and Tunnel1 interfaces because the **tunnel protection** command on both interfaces uses the same profile and is configured with the **shared** keyword. Both tunnels specify the tunnel source to be an Ethernet0/0 interface.

```
interface Tunnel0
ip address 10.255.253.3 255.255.255.0
no ip redirects
ip mtu 1436
ip nhrp authentication h1there
ip nhrp map 10.255.253.1 192.168.1.1
ip nhrp map multicast 192.168.1.1
ip nhrp network-id 253
ip nhrp holdtime 600
ip nhrp nhs 10.255.253.1
ip ospf message-digest-key 1 md5 wellikey
ip ospf network broadcast
ip ospf cost 35
ip ospf priority 0
no ip mroute-cache
tunnel source Ethernet0/0
tunnel mode gre multipoint
tunnel key 253
tunnel protection ipsec profile dmvpn-profile shared
interface Tunnel1
ip address 10.255.254.3 255.255.255.0
no ip redirects
ip mtu 1436
ip nhrp authentication h1there
ip nhrp map multicast 192.168.1.3
ip nhrp map 10.255.254.1 192.168.1.3
ip nhrp network-id 254
```

```
ip nhrp holdtime 600
ip nhrp nhs 10.255.254.1
ip ospf message-digest-key 1 md5 wellikey
ip ospf network broadcast
ip ospf priority 0
no ip mroute-cache
tunnel source Ethernet0/0
tunnel mode gre multipoint
tunnel key 254
tunnel protection ipsec profile dmvpn-profile shared
```

Related Commands

Command	Description
crypto ipsec profile	Defines the IPsec parameters that are to be used for IPsec encryption between two IPsec routers.
interface	Configures an interface type and enters interface configuration mode.
keepalive (tunnel interfaces)	Enables keepalive packets and specifies the number of times that the Cisco IOS software tries to send keepalive packets without a response before bringing the tunnel protocol down for a specific interface.
permit	Sets conditions for a named IP access list.
tunnel source	Sets the source address for a tunnel interface.

tunnel protection ipsec policy

To associate an ACL with a Static Virtual Tunnel Interface (SVTI), use the **tunnel protection ipsec policy** command in the interface configuration mode. To disassociate an ACL from an SVTI, use the **no** form of this command.

tunnel protection ipsec policy {**ipv4** | **ipv6**} *acl*
no tunnel protection ipsec policy {**ipv4** | **ipv6**} *acl*

Syntax Description

ipv4	Specifies that the traffic selector is of type IPv4.
ipv6	Specifies that the traffic selector is of type IPv6.
acl	Name or number identifying the ACL to be associated.

Command Default

By default, an ACL is not associated with an SVTI and a traffic selector of 'any any' is used.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
16.12.1	Command introduced.

Usage Guidelines

By default, an SVTI supports a single IPSec SA with 'any any' as the traffic selector. To create IPSec SAs for non-any-any proxies, define the non-any-any proxies in ACLs and associate the ACL with an SVTI using this command.

To disassociate an ACL from an SVTI use the **no** form of the command. When an ACL is disassociated from an SVTI, the SVTI resumes the default behavior of supporting a single IPSec SA with 'any any' as the traffic selector.

Example

The following example shows how to configure multi-SA support for an SVTI with an IPv4 traffic selector:

```
Device(conf)# interface Tunnel0
Device(config-if)# ip address 11.1.1.2 255.255.255.0
Device(config-if)# tunnel source Ethernet0/0
Device(config-if)# tunnel mode ipsec ipv4
Device(config-if)# tunnel destination 172.168.17.1
Device(config-if)# tunnel protection ipsec policy ipv4 ipsec_acl1
Device(config-if)# tunnel protection ipsec profile ipsec_prof


ip access-list extended ipsec_acl1
permit ip 30.0.0.0 0.0.0.255 40.0.0.0 0.0.0.255
permit ip 50.0.0.0 0.0.0.255 60.0.0.0 0.0.0.255
```

The following example shows how to configure multi-SA support for an SVTI with an IPv6 traffic selector:

```
Device(config)# interface Tunnel0
Device(config-if)# ipv6 address 400::10:1/112
Device(config-if)# tunnel destination 2003::8:2
Device(config-if)# tunnel source Ethernet 0/0
Device(config-if)# tunnel mode ipsec ipv6
Device(config-if)# tunnel protection ipsec policy ipv6 ipsec_acl2
Device(config-if)# tunnel protection ipsec profile ipsec_prof

ipv6 access-list ipsec_acl2
sequence 10 permit ipv6 host 2005::10:1 host 2005::11:1
sequence 20 permit ipv6 host 2005::15:1 host 2005::16:1
sequence 30 permit ipv6 host 2005::20:1 host 2005::21:1
```

type echo protocol ipIcmpEcho

Note Effective with Cisco IOS Release 12.4(4)T, 12.2(33)SRB, 12.2(33)SB, and 12.2(33)SXI, the **type echo protocol ipIcmpEcho**command is replaced by the **icmp-echo** command. See the **icmp- echo** command for more information.

To configure an IP Service Level Agreements (SLAs) Internet Control Message Protocol (ICMP) echo operation, use the **type echo protocol ipIcmpEcho**command in IP SLA monitor configuration mode.

type echo protocol ipIcmpEcho {*destination-ip-addressdestination-hostname*} [{**source-ipaddr** {*ip-addresshostname*} | **source-interface** *interface-name*}]

Syntax Description

destination-ip-address | *destination-hostname*	Destination IP address or hostname for the operation.
source-ipaddr {*ip-address* | *hostname*}	(Optional) Specifies the source IP address or hostname . When a source IP address or hostname is not specified, IP SLAs chooses the IP address nearest to the destination.
source-interface *interface-name*	(Optional) Specifies the source interface for the operation.

Command Default

No IP SLAs operation type is configured for the operation being configured.

Command Modes

IP SLA monitor configuration (config-sla-monitor)

Command History

Release	Modification
11.2	This command was introduced.
12.0(5)T	The following keyword and arguments were added: • **source-ipaddr** {*ip-address* | *hostname*
12.3(7)XR	The **source-interface** keyword and *interface-name* argument were added.
12.3(11)T	The **source-interface** keyword and *interface-name* argument were added.
12.4(4)T	This command was replaced by the **icmp-echo** command.
12.2(33)SRB	This command was replaced by the **icmp-echo** command.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SB	This command was replaced by the **icmp-echo** command.
12.2(33)SXI	This command was replaced by the **icmp-echo** command.

Usage Guidelines

The default request packet data size for an ICMP echo operation is 28 bytes. Use the **request-data-size** command to modify this value. This data size is the payload portion of the ICMP packet, which makes a 64-byte IP packet.

You must configure the type of IP SLAs operation (such as User Datagram Protocol [UDP] jitter or Internet Control Message Protocol [ICMP] echo) before you can configure any of the other parameters of the operation. To change the operation type of an existing IP SLAs operation, you must first delete the IP SLAs operation (using the **no ip sla monitor** global configuration command) and then reconfigure the operation with the new operation type.

Examples

In the following example, IP SLAs operation 10 is created and configured as an echo operation using the IP/ICMP protocol and the destination IP address 172.16.1.175.

```
ip sla monitor 10
 type echo protocol ipIcmpEcho 172.16.1.175
!
ip sla monitor schedule 10 start-time now
```

Related Commands

Command	Description
ip sla monitor	Begins configuration for an IP SLAs operation and enters IP SLA monitor configuration mode.

udp half-open

To configure timeout values for UDP half-opened sessions, use the **udp half-open** command in parameter-map type inspect configuration mode. To disable the timeout values for UDP half-opened sessions, use the **no** form of this command.

udp half-open idle-time *milliseconds* [{**ageout-time** *miliiseconds*}]
udp half-open idle-time

Syntax Description

idle-time	Specifies the idle timeout for UDP half-opened sessions going through the firewall.
milliseconds	Amount of time, in milliseconds, during which a UDP session will continue to be managed while there is no activity. Valid values are from 1 to 2147483.
ageout-time *milliseconds*	(Optional) Specifies the aggressive aging time for UDP half-opened sessions. Valid values are from 1 to 2147483.

Command Default

The timeout default is 30 seconds.

Command Modes

Parameter-map type inspect configuration (config-profile)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.

Usage Guidelines

You must configure the **parameter-map type inspect** command before you can configure the **udp half-open** command.

An UDP half-opened session is when only one UDP packet is detected in the UDP flow.

Examples

The following example shows how to configure the idle timeout and the aggressive aging time for UDP half-open sessions:

```
Router(config)# parameter-map type inspect pmap
Router(config-profile)# udp half-open idle-time 67800 ageout-time 67800
Router(config-profile)# end
```

Related Commands

Command	Description
parameter-map type inspect	Configures an inspect parameter map for connecting thresholds, timeouts, and other parameters pertaining to the inspect action.

udp idle-time

To configure the idle timeout for UDP sessions, use the **udp idle-time** command in parameter-map type inspect configuration mode. To disable the timeout, use the **no** form of this command.

udp idle-time *seconds* [{**ageout-time** *seconds*}]
no udp idle-time

Syntax Description

seconds	Amount of time, in seconds, during which a UDP session will continue to be managed while there is no activity. Valid values are from 1 to 2147483.
ageout-time *seconds*	(Optional) Specifies the aggressive aging time for UDP packets. Valid values are from 1 to 2147483.

Command Default

The timeout default is 30 seconds.

Command Modes

Parameter-map type inspect configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
Cisco IOS XE Release 3.4S	This command was modified. The **ageout-time** *seconds* keyword and argument pair was added.

Usage Guidelines

When you configure an inspect parameter map, you can enter the **udp idle-time** command after you enter the **parameter-map type inspect** command.

When the software detects a valid UDP packet, it establishes state information for a new UDP session. Because UDP is a connectionless service, there are no actual sessions, and the software examines the information in the packet and determines if the packet is similar to other UDP packets (for example, it has similar source or destination addresses and if the packet was detected soon after another similar UDP packet).

If the software detects no UDP packets for the UDP session for the period of time defined by the UDP idle timeout, the software will not continue to manage state information for the session.

For detailed information about creating a parameter map, see the **parameter-map type inspect** command.

Examples

The following example shows that there is no activity and the UDP session will continue to be managed for 75 seconds:

```
Router(config)# parameter-map type inspect eng-network-profile
Router(config-profile)# udp idle-time 75
Router(config-profile)# end
```

The following example shows how to configure the aging out time for UDP sessions:

```
Router(config)# parameter-map type inspect eng-network-profile
```

```
Router(config-profile)# udp idle-time 75 ageout-time 50
Router(config-profile)# end
```

Related Commands

Command	Description
ip inspect udp idle-time	Specifies the UDP idle timeout (the length of time for which a UDP session will still be managed while there is no activity).
parameter-map type inspect	Configures an inspect parameter map for connecting thresholds, timeouts, and other parameters pertaining to the **inspect** action.

unmatched-action

To define the action when the user request does not match the IP address or host site configuration, use the **unmatched-action** command in URL rewrite configuration mode. To disable the action, use the **no** form of this command.

unmatched-action [{**direct-access** | **redirect**}]
no unmatched-action [{**direct-access** | **redirect**}]

Syntax Description

direct-access	(Optional) Provides direct access to the URL and an information page stating that the user can access the URL directly.
redirect	(Optional) Provides the user with direct access to the URL, but the user does not receive the information page as with the **direct-access** keyword.

Command Default

Direct access to the URL

Command Modes

URL rewrite configuration (config-webvpn-url-rewrite)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Examples

The following example shows that the user has direct access to the URL:

```
Router (config)# webvpn context
Router (config-webvpn-context)# url rewrite
Router (config-webvpn-url-rewrite)# unmatched-action direct-access
```

Related Commands

Command	Description
host (webvpn url rewrite)	Selects the hostname of the site to be mangled on an SSL VPN gateway.
ip (webvpn url rewrite)	Configures the IP address of the site to be mangled on an SSL VPN gateway.

url (ips-auto-update)

To define a location in which to retrieve the Cisco IOS Intrusion Prevention System (IPS) signature configuration files, use the **url**command in IPS-auto-update configuration mode.

url *url*

Syntax Description

url	Location in which the router retrieves the latest signature files.

Command Default

The default value is defined in the signature definition XML.

Command Modes

IPS-auto-update configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Automatic signature updates allow users to override the existing IPS configuration and automatically keep signatures up to date on the basis of a preset time, which can be configured to a preferred setting.

Examples

In this example, the signature package file is pulled from the TFTP server at the start of every hour or every day, Sunday through Thursday. (Note that adjustments are made for months without 31 days and daylight savings time.)

```
Router# show ip ips auto-update

IPS Auto Update Configuration
URL : tftp://192.168.0.2/jdoe/ips-auto-update/IOS_reqSeq-dw.xml
Username : not configured
Password : not configured
Auto Update Intervals
  minutes (0-59) : 0
  hours (0-23) : 0-23
  days of month (1-31) : 1-31
  days of week: (0-6) : 1-5
```

Related Commands

Command	Description
ip ips auto-update	Enables automatic signature updates for Cisco IOS IPS.

url rewrite

To mangle selective URL requests on a Secure Socket Layer virtual private network (SSL VPN) gateway and enter URL rewrite mode, use the **url rewrite** command in webvpn context configuration mode. To disable selected URL requests, use the **no** form of this command.

url rewrite
no url rewrite

Syntax Description

This command has no arguments or keywords.

Command Default

All requests are mangled.

Command Modes

Webvpn context configuration (config-webvpn-context)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

Configuring the **url rewrite** command enters the url rewrite submode, in which selected IP addresses or hosts are defined for mangling.

Examples

The following example shows that selective URL mangling has been configured for IP address 10.1.1.0 255.255.0.0:

```
Router (config)# webvpn context
Router (config-webvpn-context)# url rewrite
Router (config-webvpn-url-rewrite)# ip 10.1.0.0 255.255.0.0
```

Related Commands

Command	Description
host (webvpn url rewrite)	Selects the name of the host site to be mangled on an SSL VPN gateway.
ip (webvpn url rewrite)	Configures the IP address of the site to be mangled on an SSL VPN gateway.
unmatched-action (webvpn url rewrite)	Defines the action when the user request does not match the IP address or host site configuration.

urlfilter

To enable Cisco IOS URL filtering, use the **urlfilter** command in policy-map-class configuration mode. To disable URL filtering, use the **no** form of this command.

urlfilter *parameter-map-name*
no urlfilter *parameter-map-name*

Syntax Description

parameter-map-name	Name of the parameter map for the URL filter.

Command Default

None

Command Modes

Policy-map-class configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

You can use this command only after entering the **policy-map type inspect**, **class type inspect**, and **parameter-map type inspect** commands.

Examples

The following example enables Cisco IOS firewall URL filtering:

```
policy-map type inspect p1
 class type inspect c1
  urlfilter param1
```

Related Commands

Command	Description
class type inspect	Specifies the traffic (class) on which an action is to be performed.
policy-map type inspect	Creates Level 3 and Level 4 inspect type policy maps.

url-list

To enter webvpn URL list configuration mode to configure a list of URLs to which a user has access on the portal page of a Secure Sockets Layer Virtual Private Network (SSL VPN) and to attach the URL list to a policy group, use the **url-list** command in webvpn context configuration and webvpn group policy configuration mode, respectively. To remove the URL list from the SSL VPN context configuration and from the policy group, use the **no** form of this command.

url-list *name*
no url-list *name*

Syntax Description

name	Name of the URL list. The list name can up to 64 characters in length.

Command Default

Webvpn URL list configuration mode is not entered, and a list of URLs to which a user has access on the portal page of a SSL VPN website is not configured. If the command is not used to attach a URL list to a policy group, then a URL list is not attached to a group policy.

Command Modes

Webvpn context configuration
Webvpn group policy configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Usage Guidelines

Entering this command places the router in SSL VPN URL list configuration mode. In this mode, the list of URLs is configured. A URL list can be configured under the SSL VPN context configuration and then separately for each individual policy group configuration. Individual URL list configurations must have unique names.

Examples

The following example creates a URL list:

```
Router(config)# webvpn context context1

Router(config-webvpn-context)# url-list ACCESS

Router(config-webvpn-url)# heading "Quick Links"

Router(config-webvpn-url)# url-text "Human Resources" url-value hr.mycompany.com

Router(config-webvpn-url)# url-text Engineering url-value eng.mycompany.com
Router(config-webvpn-url)# url-text "Sales and Marketing" products.mycompany.com
```

The following example attaches a URL list to a policy group configuration:

```
Router(config)# webvpn context context1

Router(config-webvpn-context)# url-list ACCESS

Router(config-webvpn-url)# heading "Quick Links"
```

```
Router(config-webvpn-url)# url-text "Human Resources" url-value hr.mycompany.com

Router(config-webvpn-url)# url-text Engineering url-value eng.mycompany.com
Router(config-webvpn-url)# url-text "Sales and Marketing" products.mycompany.com
Router(config-webvpn-url)# exit

Router(config-webvpn-context)# policy group ONE

Router(config-webvpn-group)# url-list ACCESS
```

Related Commands

Command	Description
heading	Configures the heading that is displayed above URLs listed on the portal page of a SSL VPN website.
policy group	Attaches a URL list to policy group configuration.
url-list	Enters webvpn URL list configuration mode to configure the list of URLs to which a user has access on the portal page of a SSL VPN website.
url-text	Adds an entry to a URL list.
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

url-profile

To specify a URL profile that configures the SDP registrar to run HTTPS, use the **url-profile**command in tti-registrar configuration mode. To remove this configuration, use the **no** form of this command.

url-profile {**start** *profile-name* | **intro** *profile-name*}
nourl-profile {**start** *profile-name* | **intro** *profile-name*}

Syntax Description

start	Indicates that a URL profile is to be associated with the Start SDP deployment phase of iPhone deployment.
intro	indicate that a URL profile is to be associated with the Introduction SDP deployment phase of iPhone deployment.
profile-name	Specifies the name of a unique URL profile.

Command Default

No URL profile is defined for the iPhone deployment.

Command Modes

Tti-registrar configuration mode (tti-registrar)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The SDP Registrar is enabled to run HTTPs. It is recommended that the **ip http secure-server** command is issued to enable the HTTPS web server. If a secure server is enabled, then the **ip http secure-trustpoint** command should also be issued. Disable standard HTTP server through the **no ip http server** command (if the standard server is enabled). The specified trustpoint is a registrar local trustpoint appropriate for HTTPS communication between the registrar and the iPhone's browser.

The **url-profile command can use the same or a different URL profile for**the Introduction and Start SDP deployment phases.

Examples

The following example configures the SDP registrar to run HTTPS in order to deploy Apple iPhones on a corporate network from global configuration mode:

```
Router(config)# crypto provisioning registrar
Router(tti-registrar)# url-profile start START
Router(tti-registrar)# url-profile intro INTRO
Router(tti-registrar)# match url /sdp/intro
Router(tti-registrar)# match authentication trustpoint apple-tp
Router(tti-registrar)# match certificate cat 10
Router(tti-registrar)# mime-type application/x-apple-aspen-config
Router(tti-registrar)# template location flash:intro.mobileconfig
Router(tti-registrar)# template variable p iphone-vpn
```

Related Commands

Command	Description
crypto provisioning registrar	Configures a device to become a registrar for the SDP exchange and enters tti-registrar configuration mode.
match url	Specifies the URL to be associated with the URL profile.
match authentication trustpoint	Enters the trustpoint name that should be used to authenticate the peer's certificate.
match certificate	Enters the name of the certificate map used to authorize the peer's certificate.
mime-type	Specifies the MIME type that the SDP registrar should use to respond to a request received through the URL profile.
template location	Specifies the location of the template that the SDP Registrar should use while responding to a request received through the URL profile.
template variable p	Specifies the value that goes into the OU field of the subject name in the certificate to be issued.

validate source-mac

To check the source media access control (MAC) address against the link-layer address, use the **validate source-mac**command in Neighbor Discovery (ND) inspection policy configuration mode .

validate source-mac
no validate source-mac

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled by default.

Command Modes

ND inspection policy configuration (config-nd-inspection)
RA guard policy configuration
(config-ra-guard)

Command History

Release	Modification
12.2(50)SY	This command was introduced.

Usage Guidelines

When the router receives an ND message that contains a link-layer address, the source MAC address is checked against the link-layer address. Use the **validate source-mac** command to drop the packet if the link-layer address and the MAC addresses are different from each other.

Examples

The following example enables the router to drop an ND message whose link-layer address does not match the MAC address:

```
Router(config)# ipv6 nd inspection policy policy1
Router(config-nd-inspection)# validate source-mac
```

Related Commands

Command	Description
ipv6 nd inspection policy	Defines the ND inspection policy n ame and enters ND inspection policy configuration mode.
ipv6 nd raguard policy	Defines the RA guard policy name and enter RA guard policy configuration mode.

url-text

To add an entry to a URL list, use the **url-text** command in webvpn URL list configuration mode. To remove the entry from a URL list, use the **no** form of this command.

url-text *name* **url-value** *url*
no url-text *name* **url-value** *url*

Syntax Description

name	Text label for the URL. The label must be inside quotation marks if it contains spaces.
url-value *url*	An HTTP URL.

Command Default

An entry is not added to a URL list.

Command Modes

Webvpn URL list configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.

Examples

The following example configures a heading for a URL list:

```
Router(config)# webvpn context context1

Router(config-webvpn-context)# url-list ACCESS
Router(config-webvpn-url)# heading "Quick Links"

Router(config-webvpn-url)# url-text "Human Resources" url-value hr.mycompany.com

Router(config-webvpn-url)# url-text Engineering url-value eng.mycompany.com
Router(config-webvpn-url)# url-text "Sales and Marketing" products.mycompany.com
```

Related Commands

Command	Description
url-list	Enters webvpn URL list configuration mode to configure the list of URLs to which a user has access on the portal page of a SSL VPN website.

usage

To specify the intended use for the certificate, use the **usage** command in ca-trustpoint configuration mode. To restore the default behavior, use the **no** form of this command.

usage *method1* [*method2* [*method3*]]
no usage *method1* [*method2* [*method3*]]

Syntax Description

method1 method2 method3]]	Intended use for the certificate; the available options are **ike**, **ssl-client**, and **ssl-server**. You must choose at least one method, and you may choose all three methods.

Command Default

ike

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

Before you can issue the usage command, you must enable the **crypto ca trustpoint**command, which declares the certification authority (CA) that your router should use and enters ca-trustpoint configuration mode.

This command may be used as a hint to set or clear key usage or other attributes in the certificate request.

Examples

The following example shows how to specify the certificate named "frog" for Internet Key Exchange (IKE):

```
crypto ca trustpoint frog
 enrollment url http://frog.phoobin.com/
 subject-name OU=Spiral Dept., O=tiedye.com
 ip-address ethernet-0
 usage ike
 auto-enroll regenerate
 password revokeme
 rsa-key frog 2048
```

Related Commands

Command	Description
crypto ca trustpoint	Declares the CA that your router should use.

user

To enter the names of users that are allowed to authenticate using the local authentication server, use the **user**command in local RADIUS server configuration mode. To remove the username and password from the local RADIUS server, use the **no** form of this command.

user *username* {**password** | **nthash**} *password* [{**group** *group-name* | **mac-auth-only**}]
no user *username* {**password** | **nthash**} **password** [{**group group-name** | **mac-auth-only**}]

Syntax Description

username	Name of the user that is allowed to authenticate using the local authentication server.
password	Indicates that the user password will be entered.
nthash	Indicates that the NT value of the password will be entered.
password	User password.
group *group-name*	(Optional) Name of group to which the user will be added.
mac-auth-only	(Optional) Specifies that the user is allowed to authenticate using only MAC authentication.

Command Default

If no group name is entered, the user is not assigned to a VLAN and is never required to reauthenticate.

Command Modes

Local RADIUS server configuration

Command History

Release	Modification
12.2(11)JA	This command was introduced on the Cisco Aironet Access Point 1100 and the Cisco Aironet Access Point 1200.
12.2(15)JA	This command was modified to support MAC address authentication on the local authenticator.
12.3(2)JA	This command was modified to support EAP-FAST authentication on the local authenticator.
12.3(11)T	This command was integrated into Cisco IOS Release 12.3(11)T and implemented on the following platforms: Cisco 2600XM, Cisco 2691, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3700, and Cisco 3800 series routers.

Usage Guidelines

This command is not supported on bridges.

If you do not know the user password, look up the NT value of the password in the authentication server database, and enter the NT hash as a hexadecimal string.

Examples

The following example shows that the user named "user1" has been allowed to authenticate using the local authentication server (using the password "userisok"). This user will be added to the group named "team1".

```
Router(config-radsrv)# user user1 password userisok group team1
```

The following example shows how to add a user to the list of clients allowed to authenticate using MAC-based authentication on the local authenticator.

```
AP(config-radsrv)# user 00074218d01b password 00074218d01b group cashiers
```

Related Commands

Command	Description
block count	Configures the parameters for locking out members of a group to help protect against unauthorized attacks.
clear radius local-server	Clears the statistics display or unblocks a user.
debug radius local-server	Displays the debug information for the local server.
group	Enters user group configuration mode and configures shared setting for a user group.
nas	Adds an access point or router to the list of devices that use the local authentication server.
radius-server host	Specifies the remote RADIUS server host.
radius-server local	Enables the access point or router to be a local authentication server and enters into configuration mode for the authenticator.
reauthentication time	Specifies the time (in seconds) after which access points or wireless-aware routers must reauthenticate the members of a group.
show radius local-server statistics	Displays statistics for a local network access server.
ssid	Specifies up to 20 SSIDs to be used by a user group.
vlan	Specifies a VLAN to be used by members of a user group.

user-group

To define a user group for dynamically authenticating and enforcing security policies on a per user basis, use the **user-group**command in identity policy configuration mode. To delete the user-group, use the **no** form of this command.

user-group *group-name*
no user-group *group-name*

Syntax Description

group-name	Name of the user-group.

Command Default

None

Command Modes

Identity policy configuration (config-identity policy)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

The **user-group** command is used if the Tag and Template method of user-group support is used. The Tag and Template method associates IP addresses with user-groups using locally defined policies. A tag is received from the access control server (ACS), and this tag matches a template (identity policy with defined user-group) on the network access device (NAD).

To use the **user-group** command, you must first enter identity policy configuration mode by using the **identity policy**command. The identity policy defines one or more user-groups, to which source IP addresses are associated.

Note Another method of user-group association is available. User-group support can be achieved by configuring the supplicant-group attribute on the ACS.

Examples

The following example creates the identity policy "auth_proxy_ip" and configures the user-group "auth_proxy_ug":

```
Router(config)# identity policy auth_proxy_ip
Router(config-identity-policy)# user-group auth_proxy_ug
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
identity policy	Creates an identity policy.

user-group (parameter-map)

To configure the user group associations for Cloud Web Security content scanning, use the **user-group** command in parameter-map type inspect configuration mode. To disable the user group association, use the **no** form of this command.

user-group {*group-name* [{**username**}] | **exclude** | **include**} *username*
no user-group {**name** [{**username**}] | **exclude** | **include**} *username*

Syntax Description

group-name	Name of the default user group.
username	(Optional) Specifies the default username.
exclude	Excludes the specified user group.
include	Includes the specified user group.
username	Username.

Command Default

A user group is not configured.

Command Modes

Parameter-map type inspect configuration (config-profile)

Command History

Release	Modification
15.2(1)T1	This command was introduced.

Usage Guidelines

Use the *group-name* argument to have the same content scanning policy for all users in a branch office. A prefix of LDAP:// is attached the *group-name* argument when this information is sent to Cloud Web Security to match the configured directory groups.

The **username** keyword is the global username that is sent to Cloud Web Security when there is no content scanning session specific to the configured username.

By default, all the configured user groups of a user are sent to Cloud Web Security. Use the **user-group** command to allow the administrator to filter the user groups sent to Cloud Web Security by configuring the **include** or the **exclude** keywords. When you configure the **include** keyword, only user groups that are in the include list are sent to Cloud Web Security. User groups in the exclude list are filtered from the list of user groups that is sent to Cloud Web Security. The default value for the include list is everything and the exclude list is empty. You can configure multiple instances of include and exclude user groups.

You can configure only one group on an interface. The static user group that is configured on the interface takes precedence over the group name configured in the Cloud Web Security parameter map.

Examples

The following example shows how to exclude a user group from being sent to Cloud Web Security:

```
Device(config)# parameter-map type cws global
Device(config-profile)# user-group exclude group1
```

Related Commands

Command	Description
parameter-map type cws global	Configures a global Cloud Web Security parameter map and enters parameter-map type inspect configuration mode.

user-group logging

To enable user-group syslogs, use the **user-group logging**command in global configuration mode. To disable user-group syslogs, use the **no** form of this command.

user-group logging [**group** *group-name*]
no user-group logging [**group** *group-name*]

Syntax Description

group	(Optional) Configures logging for a specific user group.
group-name	(Optional) Name of the user-group.

Command Default

None

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Examples

The following example enables syslogs for the user-group "auth_proxy_ug":

```
Router(config)# user-group logging group auth_proxy_ug
```

Related Commands

Command	Description
user-group	Creates a user-group for dynamically authenticating and enforcing security policies on a per user basis

username

To establish a username-based authentication system, use the **username** command in global configuration mode. To remove an established username-based authentication, use the **no** form of this command.

username *name* [**aaa attribute list** *aaa-list-name*]
username *name* [**access-class** *access-list-number*]
username *name* [**autocommand** *command*]
username *name* [**callback-dialstring** *telephone-number*]
username *name* [**callback-line** [**tty**] *line-number* [*ending-line-number*]]
username *name* [**callback-rotary** *rotary-group-number*]
username *name* [**dnis**]
username *name* [**mac**]
username *name* [**nocallback-verify**]
username *name* [**noescape**]
username *name* [**nohangup**]
username *name* [{**nopassword** | **password** *password* | **password** *encryption-type encrypted-password*}]
username *name* [**one-time** {**password** {**0** | **7***password*} | **secret** {**0** | **5***password*}}]
username *name* [**password** *secret*]
username *name* [**privilege** *level*]
username *name* [**secret** {**0** | **5***password*}]
username *name* [**user-maxlinks** *number*]
username [**lawful-intercept**] *name* [{**privilege** *privilege-level* | **view** *view-name*}] **password** *password*
no username *name*

Syntax Description

name	Hostname, server name, user ID, or command name. The *name* argument can be only one word. Blank spaces and quotation marks are not allowed.
aaa attribute list *aaa-list-name*	Uses the specified authentication, authorization, and accounting (AAA) method list.
access-class *access-list-number*	(Optional) Specifies an outgoing access list that overrides the access list specified in the **access-class** command available in line configuration mode. It is used for the duration of the user's session.
autocommand *command*	(Optional) Causes the specified command to be issued automatically after the user logs in. When the command is complete, the session is terminated. Because the command can be any length and can contain embedded spaces, commands using the **autocommand** keyword must be the last option on the line.
callback-dialstring *telephone-number*	(Optional) For asynchronous callback only: permits you to specify a telephone number to pass to the DCE device.
callback-line *line-number*	(Optional) For asynchronous callback only: relative number of the terminal line (or the first line in a contiguous group) on which you enable a specific username for callback. Numbering begins with zero.

ending-line-number	(Optional) Relative number of the last line in a contiguous group on which you want to enable a specific username for callback. If you omit the keyword (such as **tty**), then line-number and ending-line-number are absolute rather than relative line numbers.
tty	(Optional) For asynchronous callback only: standard asynchronous line.
callback-rotary *rotary-group-number*	(Optional) For asynchronous callback only: permits you to specify a rotary group number on which you want to enable a specific username for callback. The next available line in the rotary group is selected. Range: 1 to 100.
dnis	Does not require a password when obtained via Dialed Number Identification Service (DNIS).
mac	Allows a MAC address to be used as the username for MAC filtering done locally.
nocallback-verify	(Optional) Specifies that the authentication is not required for EXEC callback on the specified line.
noescape	(Optional) Prevents a user from using an escape character on the host to which that user is connected.
nohangup	(Optional) Prevents Cisco IOS software from disconnecting the user after an automatic command (set up with the **autocommand** keyword) has completed. Instead, the user gets another EXEC prompt.
nopassword	No password is required for this user to log in. This is usually the most useful keyword to use in combination with the **autocommand** keyword.
password	Specifies the password to access the *name* argument. A password must be from 1 to 25 characters, can contain embedded spaces, and must be the last option specified in the **username** command.
password	Password that a user enters.
encryption-type	Single-digit number that defines whether the text immediately following is encrypted and if so, what type of encryption is used. Defined encryption types are 0, which means that the text immediately following is not encrypted, and 7, which means that the text is encrypted using a Cisco-defined encryption algorithm.
encrypted-password	Encrypted password that a user enters.
one-time	Specifies that the username and password is valid for only one time. This configuration is used to prevent default credentials from remaining in user configurations.
0	Specifies that an unencrypted password or secret (depending on the configuration) follows.
7	Specifies that a hidden password follows.
5	Specifies that a hidden secret follows.

secret	Specifies a secret for the user.
secret	For Challenge Handshake Authentication Protocol (CHAP) authentication: specifies the secret for the local router or the remote device. The secret is encrypted when it is stored on the local router. The secret can consist of any string of up to 11 ASCII characters. There is no limit to the number of username and password combinations that can be specified, allowing any number of remote devices to be authenticated.
privilege *privilege-level*	(Optional) Sets the privilege level for the user. Range: 1 to 15.
user-maxlinks *number*	Maximum number of inbound links allowed for a user.
lawful-intercept	(Optional) Configures lawful intercept users on a Cisco device.
name	Hostname, server name, user ID, or command name. The *name* argument can be only one word. Blank spaces and quotation marks are not allowed.
view *view-name*	(Optional) For CLI view only: associates a CLI view name, which is specified with the **parser view** command, with the local AAA database.
password *password*	Password to access the CLI view.

Command Default

No username-based authentication system is established.

Command Modes

Global configuration (config)

Command History

Release	Modification
10.0	This command was introduced.
11.1	This command was modified. The following keywords and arguments were added: • **callback-dialstring** *telephone-number* • **callback-rotary** *rotary-group-number* • **callback-line** [**tty**] *line-number* [*ending-line-number* • **nocallback-verify**
12.3(7)T	This command was modified. The following keywords and arguments were added: • **lawful-intercept** • **view** • *view-name*

Release	Modification
12.2(33)SRB	This command was modified. The following keywords and arguments were integrated into Cisco IOS Release 12.2(33)SRB: • **lawful-intercept** • **view** • *view-name*
12.2(33)SB	This command was modified. The following keywords and arguments were integrated into Cisco IOS Release 12.2(33)SB: • **lawful-intercept** • **view** • *view-name*
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.
12.4	This command was modified. The following keywords were integrated into Cisco IOS Release 12.4: • **one-time** • **secret** • **0, 5, 7**
15.1(1)S	This command was modified. Support for the **nohangup** keyword was removed from Secure Shell (SSH).
Cisco IOS XE Release 3.2SE	This command was modified. The **mac** keyword was added.

Usage Guidelines

The **username** command provides username or password authentication, or both, for login purposes only.

Multiple **username** commands can be used to specify options for a single user.

Add a username entry for each remote system with which the local router communicates and from which it requires authentication. The remote device must have a username entry for the local router. This entry must have the same password as the local router’s entry for that remote device.

This command can be useful for defining usernames that get special treatment. For example, you can use this command to define an "info" username that does not require a password but connects the user to a general purpose information service.

The **username** command is required as part of the configuration for CHAP. Add a username entry for each remote system from which the local router requires authentication.

Note To enable the local router to respond to remote CHAP challenges, one **username** *name* entry must be the same as the **hostname** entry that has already been assigned to the other router.

- To avoid the situation of a privilege level 1 user entering into a higher privilege level, configure a per-user privilege level other than 1 (for example, 0 or 2 through 15).
- Per-user privilege levels override virtual terminal privilege levels.

In Cisco IOS Release 15.1(1)S and later releases, the **nohangup** keyword is not supported with SSH. If the **username** *user* **autocommand** *command-name* command is configured and SSH is used, the session disconnects after executing the configured command once. This behavior with SSH is opposite to the Telnet behavior, where Telnet continuously asks for authentication and keeps executing the command until the user exits Telnet manually.

CLI and Lawful Intercept Views

Both CLI views and lawful intercept views restrict access to specified commands and configuration information. A lawful intercept view allows a user to secure access to lawful intercept commands that are held within the TAP-MIB, which is a special set of Simple Network Management Protocol (SNMP) commands that stores information about calls and users.

Users who are specified via the **lawful-intercept** keyword are placed in the lawful-intercept view, by default, if no other privilege level or view name has been explicitly specified.

If no value is specified for the *secret* argument and the **debug serial-interface** command is enabled, an error is displayed when a link is established and the CHAP challenge is not implemented. The CHAP debugging information is available using the **debug ppp negotiation , debug serial-interface ,** and **debug serial-packet** commands. For more information about **debug** commands, refer to the *Cisco IOS Debug Command Reference* .

Examples

The following example shows how to implement a service similar to the UNIX **who** command, which can be entered at the login prompt and lists the current users of the router:

```
username who nopassword nohangup autocommand show users
```

The following example shows how to implement an information service that does not require a password to be used. The command takes the following form:

```
username info nopassword noescape autocommand telnet nic.ddn.mil
```

The following example shows how to implement an ID that works even if all the TACACS+ servers break. The command takes the following form:

```
username superuser password superpassword
```

The following example shows how to enable CHAP on interface serial 0 of "server_l." It also defines a password for a remote server named "server_r."

```
hostname server_l
username server_r password theirsystem
interface serial 0
 encapsulation ppp
 ppp authentication chap
```

The following is output from the **show running-config** command displaying the passwords that are encrypted:

```
hostname server_1
username server_r password 7 121F0A18
interface serial 0
 encapsulation ppp
 ppp authentication chap
```

In the following example, a privilege level 1 user is denied access to privilege levels higher than 1:

```
username user privilege 0 password 0 cisco
username user2 privilege 2 password 0 cisco
```

The following example shows how to remove the username-based authentication for user2:

```
no username user2
```

Related Commands

Command	Description
arap callback	Enables an ARA client to request a callback from an ARA client.
callback forced-wait	Forces the Cisco IOS software to wait before initiating a callback to a requesting client.
debug ppp negotiation	Displays PPP packets sent during PPP startup, where PPP options are negotiated.
debug serial-interface	Displays information about a serial connection failure.
debug serial-packet	Displays more detailed serial interface debugging information than you can obtain using **debug serial interface** command.
ppp callback (DDR)	Enables a dialer interface that is not a DTR interface to function either as a callback client that requests callback or as a callback server that accepts callback requests.
ppp callback (PPP client)	Enables a PPP client to dial into an asynchronous interface and request a callback.
show users	Displays information about the active lines on the router.

username (dot1x credentials)

To specify the username for an 802.1X credentials profile, use the **username** command in dot1x credentials configuration mode. To remove the username, use the **no** form of this command.

username *name*
no username

Syntax Description

name	Name of the credentials profile.

Command Default

A username is not specified.

Command Modes

Dot1x credentials configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

Before using this command, the **dot1x credentials** command must have been configured.

Examples

The following example shows which credentials profile should be used when configuring a supplicant:

```
dot1x credentials basic-user
 username router
 password secret
 description This credentials profile should be used for most configured ports
```

The credentials structure can be applied to an interface, along with the **dot1x pae supplicant** command and keyword, to enable supplicant functionality on that interface.

```
interface fastethernet 0/1
 dot1x credentials basic-user
 dot1x pae supplicant
```

Related Commands

Command	Description
dot1x credentials	Specifies an 802.1X credentials profile to be used.

username (ips-autoupdate)

To define a username and password in which to access signature files from the server, use the **username**command in IPS-auto-update configuration mode.

username *name* **password** *password*

Syntax Description

name	Username required to access the latest updated signature file package.
password *password*	Password required to access the latest updated signature file package.

Command Default

The default value is defined in the signature definition XML.

Command Modes

IPS-auto-update configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Automatic signature updates allow users to override the existing Intrusion Prevention System (IPS) configuration and automatically keep signatures up to date on the basis of a preset time, which can be configured to a preferred setting.

Use the **ip ips auto-update** command to enable Cisco IOS IPS to automatically update the signature file on the system. Thereafter, you can optionally issue the **username** command to specify a username and password to access signature files.

Examples

The following example shows how to configure automatic signature updates and issue the **show ip ips auto-update** command to verify the configuration:

```
Router# clock set ?
hh:mm:ss Current Time
Router# clock set 10:38:00 20 apr 2006
Router#
*Apr 20 17:38:00.000: %SYS-6-CLOCKUPDATE: System clock has been updated from 10:37:55 MST
Thu Apr 20 2006 to 10:38:00 MST Thu Apr 20 2006, configured from console by cisco on console.
Router(config)# ip ips auto-update
Router(config-ips-auto-update)# occur-at 0 0-23 1-31 1-5
Router(config-ips-auto-update)# $s-auto-update/IOS_reqSeq-dw.xml

Router(config-ips-auto-update)#^Z
Router#
*May 4 2006 15:50:28 MST: IPS Auto Update: setting update timer for next update: 0 hrs 10
min
*May 4 2006 15:50:28 MST: %SYS-5-CONFIG_I: Configured from console by cisco on console
Router#
Router# show ip ips auto-update

IPS Auto Update Configuration
URL : tftp://192.168.0.2/jdoe/ips-auto-update/IOS_reqSeq-dw.xml
Username : not configured
```

```
Password : not configured
Auto Update Intervals
  minutes (0-59) : 0
  hours (0-23) : 0-23
  days of month (1-31) : 1-31
  days of week: (0-6) : 1-5
```

Related Commands

Command	Description
ip ips auto-update	Enables automatic signature updates for Cisco IOS IPS.

username algorithm-type

To set the algorithm type to hash a user password configured using the **username secret** command, use the **username algorithm-type** command in global configuration mode.

username *name* **algorithm-type** {**md5** | **scrypt** | **sha256**}

Syntax Description

md5	Selects the message digest algorithm 5 (MD5) as the hashing algorithm.
scrypt	Selects scrypt as the hashing algorithm.
sha256	Selects Password-Based Key Derivation Function 2 (PBKDF2) with Secure Hash Algorithm, 26-bits (SHA-256) as the hashing algorithm.

Command Default

No algorithm type is established for the username-based authentication system.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.3(3)M	This command was introduced.
15.3(3)S	This command was integrated into the Cisco IOS Release 15.3(3)S.

Usage Guidelines

You must configure the password using the **username secret** command before hashing the password with the **username algorithm-type** command.

Use the **username algorithm-type** command to generate the following types of passwords:

Command keyword	Type of password
md5	Type 5
sha256	Type 8
scrypt	Type 9

Note Type 5, 8, and 9 passwords are not reversible.

If you configure type 8 or type 9 passwords and then downgrade to a release that does not support type 8 and type 9 passwords, you must configure the type 5 passwords before downgrading. If not, you are locked out of the device and a password recovery is required.

Note If you are using an external AAA server to manage privilege levels, you are not locked out of the device.

Examples

The following example shows how to generate a type 8 (PBKDF2 with SHA-256) or a type 9 (SCRYPT) password:

```
Device# configure terminal
Device(config)# enable algorithm-type sha256 secret cisco
Device(config)# enable algorithm-type scrypt secret cisco
Device(config)# end
Device# show running-config | inc username

enable secret 8 $8$dsYGNam3K1SIJO$7nv/35M/qr6t.dVc7UY9zrJDWRVqncHub1PE9UlMQFs
enable secret 9 $9$nhEmQVczB7dqsO$X.HsgL6x1il0RxkOSSvyQYwucySCt7qFm4v7pqCxkKM
```

Related Commands

Command	Description
enable algorithm-type	Sets the algorithm type to hash a user password configured using the **enable secret** command.
enable password	Sets a local password to control access to various privilege levels.
enable secret	Specifies an additional layer of security over the **enable password** command.
username	Establishes a username-based authentication system.

username secret

To encrypt a user password with irreversible encryption, use the **username secret** command in global configuration mode.

username *name* **secret** {**0** *password* | **5** *secret-string* | **4** *secret-string* | **8** *secret-string* | **9** *secret-string*}

Syntax Description

name	Username.
0	Specifies an unencrypted secret.
password	Clear-text password.
5 *secret-string*	message digest alogrithm5 (MD5) encrypted secret text string, which is stored as the encrypted user password.
4 *secret-string*	Secure Hash Algorithm, 26-bits (SHA-256) encrypted secret text string, which is stored as the encrypted user password. **Note** NOTE: Effective with CSCue95644, the **4** keyword is deprecated.
8 *secret-string*	Password-Based Key Derivation Function 2 (PBKDF2) with SHA-256 hashed secret text string, which is stored as the hashed user password.
9 *secret-string*	Scrypt hashed secret text string, which is stored as the hashed user password.

Command Default

No username-based authentication system is established.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(18)S	This command was introduced.
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Cisco IOS Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S. Algorithm types **0**, **4**, and **5** were added.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Release	Modification
15.3(3)M	This command was modified. • The **4** keyword was deprecated and support for type **8** and type **9** algorithms were added. • The warning message for the type **5** algorithm was removed. • The warning message for removal of support for the type **4** algorithm was added.
15.3(3)S	The command modifications were integrated into Cisco IOS Release 15.3(3)S.

Usage Guidelines

Use the **username secret** command to configure a username and MD5-encrypted user password. MD5 encryption is a strong encryption method that is not retrievable; thus, you cannot use MD5 encryption with protocols that require clear-text passwords, such as Challenge Handshake Authentication Protocol (CHAP).

The **username secret** command provides an additional layer of security over the username password. It also provides better security by encrypting the password using non reversible MD5 encryption and storing the encrypted text. The added layer of MD5 encryption is useful in environments in which the password crosses the network or is stored on a TFTP server.

Use MD5 as the encryption type if you paste into this command an encrypted password that you copied from a router configuration file.

Use this command to enable Enhanced Password Security for the specified, unretrievable username. This command enables MD5 encryption on the password. MD5 encryption is a strong encryption method. You cannot use MD5 encryption with protocols, such as CHAP, that require clear-text passwords.

This command can be useful for defining usernames that get special treatment. For example, you can use this command to define an “info” username that does not require a password but connects the user to a general-purpose information service.

With CSCue95644, you can use the **username secret** command to configure a username and hash the user password with MD5, PBKDF2 with SHA-256, or scrypt hashing algorithms.

Note If you use type 8 or type 9 passwords and then downgrade to an older version of Cisco IOS software that does not support type 8 and type 9 passwords, you must reconfigure the passwords to use type 5 hashing before downgrading. If not, you are locked out of the device and password recovery is required. If you are using an external AAA server to manage privilege levels, you are not locked out of the device.

The **username** command provides username or secret authentication for login purposes only. The *name* argument can be one word only. Spaces and quotation marks are not allowed. You can use multiple **username** commands to specify options for a single user.

Examples

The following example shows how to configure username “abc” and enable MD5 encryption on the clear-text password “xyz”:

```
username abc secret 0 xyz
```

The following example shows how to configure username “cde” and enter an MD5 encrypted text string that is stored as the username password:

```
username cde secret 5 $1$feb0$a104Qd9UZ./Ak00KTggPD0
```

The following example shows how to configure username “xyz” and enter an MD5 encrypted text string that is stored as the username password:

```
username xyz secret 5 $1$feb0$a104Qd9UZ./Ak00KTggPD0
```

The following example shows the sample warning message that is displayed when a user enters the **username secret 4** *encrypted-password* command:

```
Device# configure terminal
Device(config)# username demo secret 4 tnhtc92DXBhelxjYk8LWJrPV36S2i4ntXrpb4RFmfqY

WARNING: Command has been added to the configuration but Type 4 passwords have been
deprecated.
Migrate to a supported password type

Device(config)# end
Device# show running-config | inc username

username demo secret 4 tnhtc92DXBhelxjYk8LWJrPV36S2i4ntXrpb4RFmfqY
```

Related Commands

Command	Description
enable password	Sets a local password to control access to various privilege levels.
enable secret	Specifies an additional layer of security over the enable password command.
username	Establishes a username-based authentication system.
username algorithm-type	Sets the algorithm type to hash a user password configured using the **username secret** command.

user-profile location

To store user bookmarks in a directory on a device, use the **user-profile location** command in webvpn context configuration mode. To remove a directory that has been configured, use the **no** form of this command.

user-profile location device:*directory*
nouser-profile location device:*directory*

Syntax Description

device:	Storage location on a device. See the table below for a list of acceptable storage locations.
directory	Name of the directory.

Command Default

The default location is flash:/webvpn/<context-name>/.

Command Modes

Webvpn context configuration (config-webvpn-context)

Command History

Release	Modification
12.4(15)T	This command was introduced.

Usage Guidelines

The table below lists accept storage locations.

Table 227: Type of Storage Location

Type of Storage Location	Description
archive	Archived file system.
Bootflash	Bootflash memory.
disk0	On Disk 0.
disk1	On Disk 1.
Flash	Flash memory.
FTP	FTP network server.
HTTP	HTTP file server.
HTTPS	HTTP secure server.
null	Null destination for copies. You can copy a remote file to null to determine its size.
NVRAM	Storage location is in NVRAM.
PRAM	Phase-change memory (PRAM)--type of nonvolatile computer memory.
RCP	Remote copy protocol network server.

Type of Storage Location	Description
SCP	Secure Copy--A means of securely transferring computer files between a local and a remote host or between two remote hosts using the Secure Shell (SSH) protocol.
slot0	On Slot 0.
slot1	On Slot 1.
system	System memory, including the running configuration.
tmpsys	Temporary system in a file system.

Examples

The following example shows bookmarks are stored in flash on the directory webvpn/sslvpn_context/.

```
Router# webvpn context context1
Router# user-profile location flash:/webvpn/sslvpn_context/
```

Related Commands

Command	Description
webvpn context	Configures the SSL VPN context and enters webvpn context configuration mode.

variable

To define the next-hop variable in a mitigation parameter map for Transitory Messaging Services (TMS), use the **variable** command in parameter-map configuration mode. To remove the next-hop variable from the mitigation parameter map, use the **no** form of this command.

Note Effective with Cisco IOS Release 12.4(20)T, the **variable** command is not available in Cisco IOS software.

variable *name* {*number* | **ipv4** *ip-address* | **null0**}
no variable *name*

Syntax Description

name	Specifies the variable name.
number	Specifies the number associated with this variable from 0 to 4294967295.
ipv4*ip-address*	Sets the next hop action-variable type to a specific IP address.
null0	Sets the next hop to interface null 0 (null route).

Command Default

The next-hop variable in a mitigation parameter map for TMS is not defined.

Command Modes

Parameter-map configuration (config-profile)

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.4(15)XZ	This command was integrated into Cisco IOS Release 12.4(15)XZ.

Usage Guidelines

The **variable** command is configured to set the next-hop variable in a mitigation type parameter map. The next hop can be configured to route to a null 0 interface (null route) or route to a specific interface for collection and analysis.

Note If the next hop is defined in a threat file and as a variable by configuring this command, the next-hop value defined in the threat file will have precedence over the parameter map variable.

Examples

The following example configures a variable that routes all priority 5 traffic to the null0 interface:

```
Router(config)# class-map type control mitigation match-all MIT_CLASS_2
Router(config-cmap)# match primitive any
Router(config-cmap)# match priority 5
```

```
Router(config-cmap)# exit
Router(config)# parameter-map type mitigation MIT_PAR_2
Router(config-profile)# variable RTBH null0
Router(config-profile)# exit
Router(config)# policy-map type control mitigation MIT_POL_2

Router(config-pmap)# class MIT_CLASS_2
Router(config-pmap-c)# redirect route $RTBH
Router(config-pmap-c)# source parameter MIT_PAR_2
Router(config-pmap-c)# exit
Router(config-pmap)# exit
```

Related Commands

Command	Description
acl drop	Configures an ACL drop enforcement action in a TMS Rules Engine configuration.
class-map type control mitigation	Configures a mitigation type class map.
ignore (TMS)	Configures the TMS Rules Engine to ignore a mitigation enforcement action.
match primitive	Configures a primitive match in a mitigation type class map.
match priority	Configures the match priority level for a mitigation enforcement action.
parameter-map type mitigation	Configures a mitigation type parameter map.
policy-map type control tms	Configures a TMS type policy map.
redirect route	Configures a redirect enforcement action in a mitigation type policy map.
source parameter	Attaches a mitigation type parameter map to a policy-map class configuration.
tms-class	Associates an interface with an ACL drop enforcement action.

view

To add a normal command-line interface (CLI) view to a superview, use the **view** command in view configuration mode. To remove a CLI view from a superview, use the **no** form of this command.

view *view-name*
no view *view-name*

Syntax Description

view-name	CLI view that is to be added to the given superview.

Command Default

A superview will not contain any CLI views until this command is enabled.

Command Modes

View configuration (config-view)

Command History

Release	Modification
12.3(11)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
Cisco IO XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

Before you can use this command to add normal views to a superview, ensure that the following steps have been taken:

- A password has been configured for the superview (via the **secret 5** command).
- The normal views that are to be added to the superview are valid views in the system; that is, the views have been successfully created via the **parser view** command.

Examples

The following sample output from the **show running-config** command shows that "view_one" and "view_two" have been added to superview "su_view1," and "view_three" and "view_four" have been added to superview "su_view2":

```
!
parser view su_view1 superview
 secret 5 <encoded password>
 view view_one
 view view_two
!
parser view su_view2 superview
 secret 5 <encoded password>
 view view_three
 view view_four
!
```

Related Commands

Command	Description
parser view	Creates or changes a CLI view and enters view configuration mode.
secret 5	Associates a CLI view or a superview with a password.

virtual-template (IKEv2 profile)

To configure an Internet Key Exchange (IKEv2) profile with a virtual template to be used for cloning the virtual access interfaces, use the **virtual-template** command in IKEv2 profile configuration mode. To remove the virtual template from IKEv2 profile, use the **no** form of this command.

virtual-template *template-number* **mode auto**
no virtual-template *template-number*

Syntax Description

template-number	Identifying number of the virtual template that will be used to clone virtual access interfaces.
mode auto	Enables auto tunneling mode.

Command Default

A virtual template is not specified.

Command Modes

IKEv2 profile configuration (config-ikev2-profile)

Command History

Release	Modification
15.1(1)T	This command was introduced.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
15.4(2)T	This command was modified. The **mode auto** keywords were added.
Cisco IOS XE Release 3.12S	This command was integrated into Cisco IOS XE Release 3.12S.

Usage Guidelines

Use this command to specify the virtual template for cloning a virtual access interface.

Auto tunneling mode eases the configuration and spares you about knowing the responder's details. It automatically applies the tunneling protocol (GRE or IPsec) and transport protocol (IPv4 or IPv6) on the virtual template as soon as the IKE profile creates the virtual access interface.

Examples

The following example shows how virtual-template 1 is configured for profile1:

```
Device(config)# crypto ikev2 profile profile1
Device(config-ikev2-profile)# virtual-template 1
```

The following example shows how auto tunneling mode is configured for profile A:

```
Device(config)# crypto ikev2 profile profile A
Device(config-ikev2-profile)# virtual-template 1 mode auto
```

Related Commands

Command	Description
crypto ikev2 profile	Defines an IKEv2 profile.
show ikev2 profile	Displays the default or user-defined IKEv2 profile.

virtual-template (webvpn context)

To associate a virtual template with a Secure Socket Layer Virtual Private Network (SSL VPN) context, use the **virtual-template** command in webvpn context configuration mode. To disable the configuration, use the **no** form of this command.

virtual-template *template-number* [**tunnel**]
no virtual-template

Syntax Description

template-number	Number of the virtual template that will be used to clone virtual access interfaces. The range is from 1 to 1000.
tunnel	(Optional) Applies the virtual template for every full tunnel session.

Command Default

No virtual template is enabled.

Command Modes

Webvpn context configuration (config-webvpn-context)

Command History

Release	Modification
15.0(1)M	This command was introduced.
15.1(1)T	This command was modified. The **tunnel** keyword was added.

Usage Guidelines

You can configure the desired IP features in the virtual template and then use the **virtual-template** command to apply the configuration on a per-context or per-tunnel basis. The per-context configuration applies the IP features to all the users connecting to that WebVPN context and the per-tunnel configuration applies the IP features for each SSL VPN full tunnel established in the WebVPN context.

Examples

The following example shows how to associate a virtual template with an SSL VPN context:

```
Router# configure terminal
Router(config)# webvpn context context1
Router(config-webvpn-context)# virtual-template 1
```

Related Commands

Command	Description
inservice	Enables an SSL VPN context.
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

vlan (local RADIUS server group)

To specify a VLAN to be used by members of the user group, use the **vlan** command in local RADIUS server group configuration mode. To reset the parameter to the default value, use the **no** form of this command.

vlan *vlan*
no vlan *vlan*

Syntax Description

vlan	VLAN ID.

Command Default

No default behavior or values

Command Modes

Local RADIUS server group configuration

Command History

Release	Modification
12.2(11)JA	This command was introduced on Cisco Aironet Access Point 1100 and Cisco Aironet Access Point 1200.
12.3(11)T	This command was implemented on the following platforms: Cisco 2600XM, Cisco 2691, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3700, and Cisco 3800 series routers.

Usage Guidelines

The access point or router moves group members into the VLAN that you specify, overriding any other VLAN assignments. You can assign only one VLAN to a user group.

Examples

The following example shows that VLAN "225" *is* to be used by members of the user group:

```
vlan 225
```

Related Commands

Command	Description
block count	Configures the parameters for locking out members of a group to help protect against unauthorized attacks.
clear radius local-server	Clears the statistics display or unblocks a user.
debug radius local-server	Displays the debug information for the local server.
group	Enters user group configuration mode and configures shared setting for a user group.
nas	Adds an access point or router to the list of devices that use the local authentication server.
radius-server host	Specifies the remote RADIUS server host.

Command	Description
radius-server local	Enables the access point or router to be a local authentication server and enters into configuration mode for the authenticator.
reauthentication time	Specifies the time (in seconds) after which access points or wireless-aware routers must reauthenticate the members of a group.
show radius local-server statistics	Displays statistics for a local network access server.
ssid	Specifies up to 20 SSIDs to be used by a user group.
user	Authorizes a user to authenticate using the local authentication server.

vlan group

To create or modify a VLAN group, use the **vlan group** command in global configuration mode. To remove a VLAN list from the VLAN group, use the **no** form of this command.

vlan group *group-name* **vlan-list** *vlan-list*
no vlan group *group-name* **vlan-list** *vlan-list*

Syntax Description

group-name	VLAN group name.
vlan-list	VLAN list name. See the "Usage Guidelines" section for additional information about the *vlan-list*argument.

Command Default

This command has no default settings.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SXI1	This command was introduced.

Usage Guidelines

The VLAN group name may contain up to 32 characters and must begin with a letter.

The *vlan-list* argument can be a single VLAN ID, a list of VLAN IDs, or VLAN ID ranges (*vlan-id-vlan-id*). Multiple entries are separated by a hyphen (-) or a comma (,).

If the named VLAN group does not exist, the **vlan group** command creates the group and maps the specified VLAN list to the group. If the named VLAN group exists, the specified VLAN list is mapped to the group.

The **no** form of the **vlan group** command removes the specified VLAN list from the VLAN group. When you remove the last VLAN from the VLAN group, the VLAN group is deleted.

A maximum of 100 VLAN groups can be configured, and a maximum of 4094 VLANs can be mapped to a VLAN group.

Examples

This example shows how to map VLANs 7 through 9 and 11 to a VLAN group:

```
Router(config)# vlan group ganymede vlan-list 7-9,11
```

This example shows how to remove VLAN 7 from the VLAN group:

```
Router(config)# no vlan group ganymede vlan-list 7
```

Related Commands

Command	Description
show vlan group	Displays the VLANs mapped to VLAN groups.

vpdn aaa attribute

To enable reporting of network access server (NAS) authentication, authorization, and accounting (AAA) attributes related to a virtual private dialup network (VPDN) to the AAA server, use the **vpdn aaa attribute**command in global configuration mode. To disable reporting of AAA attributes related to VPDN, use the **no** form of this command.

vpdn aaa attribute {**nas-ip-address** {**vpdn-nas** | **vpdn-tunnel-client**} | **nas-port** {**physical-channel-id** | **vpdn-nas**}}
no vpdn aaa attribute {**nas-ip-address** {**vpdn-nas** | **vpdn-tunnel-client**} | **nas-port**}

Syntax Description

nas-ip-address vpdn-nas	Enables reporting of the VPDN NAS IP address to the AAA server.
nas-ip-address vpdn-tunnel-client	Enables reporting of the VPDN tunnel client IP address to the AAA server.
nas-port vpdn-nas	Enables reporting of the VPDN NAS port to the AAA server.
nas-port physical-channel-id	Enables reporting of the VPDN NAS port physical channel identifier to the AAA server.

Command Default

AAA attributes are not reported to the AAA server.

Command Modes

Global configuration

Command History

Release	Modification
11.3NA	This command was introduced.
11.3(8.1)T	This command was integrated into Cisco IOS Release 11.3(8.1)T.
12.1(5)T	This command was modified to support the PPP extended NAS-Port format.
12.2(13)T	The **physical-channel-id** keyword was added
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.4(24)T	The **vpdn-tunnel-client** keyword was added.
12.2(33)XND	The **vpdn-tunnel-client** keyword was added.
12.2(33)SRE	The **vpdn-tunnel-client** keyword was added.
Cisco IOS XE Release 2.5	The **vpdn-tunnel-client** keyword was added.

Usage Guidelines

This command can be used with RADIUS or TACACS+, and is applicable only on the VPDN tunnel server.

The PPP extended NAS-Port format enables the NAS-Port and NAS-Port-Type attributes to provide port details to a RADIUS server when one of the following protocols is configured:

- PPP over ATM
- PPP over Ethernet (PPPoE) over ATM
- PPPoE over 802.1Q VLANs

Before PPP extended NAS-Port format attributes can be reported to the RADIUS server, the **radius-server attribute nas-port format** command with the **d**keyword must be configured on both the tunnel server and the NAS, and the tunnel server and the NAS must both be Cisco routers.

When you configure the **vpdn aaa attribute nas-ip-address vpdn-nas** command, the L2TP network server (LNS) reports the IP address of the last multihop node for multihop over Layer 2 Forwarding (L2F). For multihop over Layer 2 Tunneling Protocol (L2TP), the IP address of the originating NAS is reported.

When you configure the **vpdn aaa attribute nas-ip-address vpdn-tunnel-client** command, the LNS reports the IP address of the last multihop node in the RADIUS NAS-IP-Address attribute for the L2TP multihop. This eases the migration for customers moving from L2F to L2TP.

Note Reporting of NAS AAA attributes related to a VPDN on a AAA server is not supported for Point-to-Point Tunneling Protocol (PPTP) sessions with multihop deployment.

Examples

The following example configures VPDN on a tunnel server and enables reporting of VPDN AAA attributes to the AAA server:

```
vpdn enable
vpdn-group 1
 accept-dialin
  protocol any
  virtual-template 1
!
 terminate-from hostname nas1
 local name ts1
!
vpdn aaa attribute nas-ip-address vpdn-nas
vpdn aaa attribute nas-port vpdn-nas
vpdn aaa attribute nas-port physical-channel-id
```

The following example configures the tunnel server for VPDN, enables AAA, configures a RADIUS AAA server, and enables reporting of PPP extended NAS-Port format values to the RADIUS server. PPP extended NAS-Port format must also be configured on the NAS for this configuration to be effective.

```
vpdn enable
vpdn-group L2TP-tunnel
 accept-dialin
  protocol l2tp
  virtual-template 1
!
 terminate-from hostname nas1
 local name ts1
```

```
!
aaa new-model
aaa authentication ppp default local group radius
aaa authorization network default local group radius
aaa accounting network default start-stop group radius
!
radius-server host 172.16.79.76 auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server attribute nas-port format d
radius-server key ts123
!
vpdn aaa attribute nas-port vpdn-nas
```

Related Commands

Command	Description
radius-server attribute nas-port format	Selects the NAS-Port format used for RADIUS accounting features.

vrf (ca-trustpoint)

To specify the VRF instance in the public key infrastructure (PKI) trustpoint to be used for enrollment, certificate revocation list (CRL) retrieval, and online certificate status protocol (OCSP) status, use the **vrf** command in ca-trustpoint configuration mode. To remove the VRF instance that was specified, use the **no** form of this command.

vrf *vrf-name*
no vrf *vrf-name*

Syntax Description

vrf *vrf-name*	Specifies the name of the VRF.

Command Default

No VRF is specified.

Command Modes

Ca-trustpoint configuration (ca-trustpoint)

Command History

Release	Modification
15.1T	This command was introduced.

Usage Guidelines

Before you can configure this command, you must enable the **crypto pki trustpoint** command with and the *trustpoint-name* argument, which enters ca-trustpoint configuration mode.

Examples

```
Router(config)# crypto pki trustpoint mytp
Router(ca-trustpoint)# vrf myvrf
```

Related Commands

Command	Description
crypto pki trustpoint	Declares the trustpoint and a given name and enters ca-trustpoint configuration mode.

vrf (ca-trustpool)

To specify the VRF instance in the public key infrastructure (PKI) trustpool to be used for enrolment, certificate revocation list (CRL) retrieval, and online certificate status protocol (OCSP) status, use the **vrf** command in ca-trustpool configuration mode. To remove the VRF instance that was specified, use the **no** form of this command.

vrf *vrf-name*
no vrf *vrf-name*

Syntax Description

vrf *vrf-name*	Specifies the name of the VRF.

Command Default

No VRF is specified.

Command Modes

Ca-trustpool configuration (ca-trustpool)

Command History

Release	Modification
15.2(2)T	This command was introduced.
15.1(1)SY	This command was integrated into Cisco IOS 15.1(1)SY.

Usage Guidelines

Before you can configure this command, you must enable the **crypto pki trustpool policy** command, which enters ca-trustpool configuration mode.

Examples

```
Router(config)# crypto pki trustpool policy
Router(ca-trustpool)# vrf myvrf
```

Related Commands

Command	Description
cabundle url	Configures the URL from which the PKI trustpool CA bundle is downloaded.
chain-validation	Enables chain validation from the peer's certificate to the root CA certificate in the PKI trustpool.
crypto pki trustpool import	Manually imports (downloads) the CA certificate bundle into the PKI trustpool to update or replace the existing CA bundle.
crypto pki trustpool policy	Configures PKI trustpool policy parameters.

Command	Description
default	Resets the value of a ca-trustpool configuration command to its default.
match	Enables the use of certificate maps for the PKI trustpool.
ocsp	Specifies OCSP settings for the PKI trustpool.
revocation-check	Disables revocation checking when the PKI trustpool policy is being used.
show	Displays the PKI trustpool policy of the router in ca-trustpool configuration mode.
show crypto pki trustpool	Displays the PKI trustpool certificates of the router and optionally shows the PKI trustpool policy.
source interface	Specifies the source interface to be used for CRL retrieval, OCSP status, or the downloading of a CA certificate bundle for the PKI trustpool.
storage	Specifies a file system location where PKI trustpool certificates are stored on the router.

vrf (isakmp profile)

To define the virtual routing and forwarding (VRF) value to which the IP Security (IPSec) tunnel will be mapped, use the **vrf**command in Internet Security Association Key Management (ISAKMP) profile configuration mode. To disable the VRF that was defined, use the **no** form of this command.

vrf *ivrf*
no vrf *ivrf*

Syntax Description

ivrf	VRF to which the IPSec tunnel will be mapped.

Command Default

The VRF will be the same as the front door VRF (FVRF).

Command Modes

ISAKMP
profile configuration (config-isa-prof)

Command History

Release	Modification
12.2(15)T	This command was introduced.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

Use this command to map IPSec tunnels that terminate on a global interface to a specific Virtual Private Network (VPN).

If traffic from the router to a certification authority (CA) (for authentication, enrollment, or for obtaining a certificate revocation list [CRL]) or to a Lightweight Directory Access Protocol (LDAP) server (for obtaining a CRL) needs to be routed via a VRF, the **vrf** command must be added to the trustpoint. Otherwise, such traffic will use the default routing table.

If a profile does not specify one or more trustpoints, all trustpoints in the router will be used to attempt to validate the certificate of the peer (Internet Key Exchange [IKE] main mode or signature authentication). If one or more trustpoints are specified, only those trustpoints will be used.

Examples

The following example shows that two IPSec tunnels to VPN 1 and VPN 2 are terminated:

```
crypto isakmp profile vpn1
 vrf vpn1
 keyring vpn1
 match identity address 172.16.1.1 255.255.255.255
crypto isakmp profile vpn2
 vrf vpn2
 keyring vpn2
 match identity address 10.1.1.1 255.255.255.255
crypto ipsec transform-set vpn1 esp-3des esp-sha-hmac
crypto ipsec transform-set vpn2 esp-3des esp-md5-hmac
```

```
!
crypto map crypmap 1 ipsec-isakmp
 set peer 172.16.1.1
 set transform-set vpn1
 set isakmp-profile vpn1
 match address 101
crypto map crypmap 3 ipsec-isakmp
 set peer 10.1.1.1
 set transform-set vpn2
 set isakmp-profile vpn2
 match address 102
!
!
interface Ethernet1/2
 ip address 172.26.1.1 255.255.255.0
 duplex half
 no keepalive
 no cdp enable
 crypto map crypmap
```

vrfname

To associate a Virtual Private Network (VPN) front-door routing and forwarding instance (FVRF) with a SSL VPN gateway, use the **vrfname** command in webvpn gateway configuration mode. To disassociate the FVRF from the SSL VPN gateway, use the **no** form of this command.

vrfname *name*
no vrfname *name*

Syntax Description

name	Name of the VRF.

Command Default

A VPN FVRF is not associated with a SSL VPN gateway.

Command Modes

Webvpn gateway (config-webvpn-gateway)

Command History

Release	Modification
12.4(15)T	This command was introduced.

Usage Guidelines

Only one FVRF can be associated with each SSL VPN context configuration.

Examples

The following example shows FVRF has been configured:

```
Router (config) ip vrf vrf_1
Router (config-vrf) end
Router (config) webvpn gateway mygateway
Router (config-webvpn-gateway) vrfname vrf_1
Router (cofig-webvpn-gateway) end
```

Related Commands

Command	Description
webvpn gateway	Enters webvpn gateway configuration mode to configure a SSL VPN gateway.

vrf-name

To associate a Virtual Private Network (VPN) routing and forwarding instance (VRF) with a SSL VPN context, use the **vrf-name** command in webvpn context configuration mode. To remove the VRF from the WebVPN context configuration, use the **no** form of this command.

vrf-name *name*
no vrf-name

Syntax Description

name	Name of the VRF.

Command Default

A VPN VRF is not associated with a SSL VPN context.

Command Modes

Webvpn context configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

The VRF is first defined in global configuration mode. Only one VRF can be associated with each SSL VPN context configuration.

Examples

The following example associates a VRF with a SSL VPN context:

```
Router (config)# ip vrf BLUE
Router (config-vrf)# rd 10.100.100.1
Router (config-vrf)# webvpn context context1
Router (config-webvpn-context)# vrf-name BLUE
```

Related Commands

Command	Description
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

vsa vendor-id

To define vendor-specific attributes (VSAs), use the **vsa vendor-id** command in server-group configuration mode. To remove the configuration from the list, use the **no** form of this command.

vsa vendor-id *vendor-id* **vendor-type** *vendor-type*
no vsa vendor-id *vendor-id* **vendor-type** *vendor-type*

Syntax Description

vendor-id	Vendor-specific ID. Valid values are from 0 to 65535.
vendor-type *vendor-type*	Specifies the sub-attribute type for the vendor ID.

Command Default

Vendor ID is not defined.

Command Modes

Server-group configuration (config-radius-attrl)

Command History

Release	Modification
Cisco IOS Release 12.2(33)SRA	This command was introduced.

Usage Guidelines

Vendor-specific ID 9 defines Cisco VSAs and 311 defines Microsoft VSAs. For more information about vendor-specific attributes, see the RADIUS Vendor-Specific Attributes and RADIUS Disconnect-Cause Attribute Values chapter.

Note In Cisco IOS Release 15.1(1)SY, the Microsoft VSAs was defined as 8; however, it was changed to 311 in Cisco IOS Release 15.1(1)SY2.

Examples

The following example shows how to define vendor-specific attributes:

```
Device(config)# aaa new-model
Device(config)# radius-server attribute list usage-only
Device(config-radius-attrl)# vsa vendor-id  311 vendor-type 11
Device(config-radius-attrl)# exit
```

Related Commands

Command	Description
aaa new-model	Enables the AAA access control model.
attribute (**server-group**)	Adds attributes to an accept or reject list.
radius-server host	Specifies a RADIUS server host.

web-agent-url

To configure the Netegrity agent URL to which Single SignOn (SSO) authentication requests will be dispatched, use the **web-agent-url** command in webvpn sso server configuration mode. To remove the Netegrity agent URL, use the **no** form of this command.

web-agent-url *url*
no web-agent-url *url*

Syntax Description

url	URL to which SSO authentication requests will be dispatched.

Command Default

Authentication requests will not be dispatched to a Netegrity agent URL.

Command Modes

Webvpn sso server configuration

Command History

Release	Modification
12.4(11)T	This command was introduced.

Usage Guidelines

Note A web agent URL and policy server secret key are required for a SSO server configuration. If they are not configured, a warning message is displayed. (See the warning message information in the Examples section below.)

Examples

The following example shows that SSO authentication requests will be dispatched to the URL http://www.example.com/webvpn/:

```
webvpn context context1
 sso-server test-sso-server
  web-agent-url http://www.example.com/webvpn/
```

Warning Message

If a web agent URL and policy server secret key are not configured, a message similar to the following is received:

```
Warning: must configure web agent URL for sso-server "example"
Warning: must configure SSO policy server secret key for sso-server "example"
Warning: invalid configuration. SSO for "example" being disabled
```

Related Commands

Command	Description
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

webvpn

Note Effective with Cisco IOS Release 12.4(6)T, the **webvpn**command is replaced by the **webvpn context** and **webvpn gateway** commands. See the these commands for more information.

To enter Web VPN configuration mode, use the **webvpn** command in global configuration mode. To remove all commands that were entered in Web VPN configuration mode, use the **no** form of this command.

webvpn
no webvpn

Syntax Description

This command has no arguments or keywords.

Command Default

Web VPN configuration mode is not entered.

Command Modes

Global configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(6)T	This command was replaced by the **webvpn context** and **webvpn gateway** commands.

Examples

The following example shows that Web VPN configuration mode has been entered:

```
Router (config)#
webvpn
Router (config-webvpn)#
```

Related Commands

Command	Description
webvpn enable	Enables WebVPN in the system.

webvpn-homepage

To specify the WebVPN home page URL, use the **webvpn-homepage** command in WebVPN group policy configuration mode. To disable the configuration, use the **no** form of this command.

webvpn-homepage *homepage-url* [**redirection-time** *seconds*]
no webvpn-homepage

Syntax Description

homepage-url	Home page URL.
redirection-time *seconds*	(Optional) Specifies the home page redirection time, in seconds. The range is from 0 to 15. The default value is 5.

Command Default

The default reditection time is 5 seconds.

Command Modes

WebVPN group policy configuration (config-webvpn-group)

Command History

Release	Modification
15.1(1)T	This command was introduced.

Usage Guidelines

You can use the **webvpn-homepage** command to specify the WebVPN home page URL and apply the WebVPN redirection time to a particular policy group users. This command helps you to customize and have your own portal page.

The portal page is not displayed if you configure the **webvpn-homepage** command and set the redirection time to 0. If the redirection time is greater than 0, then the portal page is displayed for the time the redirection time is configured and then redirects you to the home page.

If the configuration is not successful, an appropriate error message is displayed.

Examples

The following example shows how to specify the home page URL "http://192.0.2.0" with the redirection time of 12 seconds:

```
Router# configure terminal
Router(config)# webvpn context context1
Router(config-webvpn-context)# policy group policy1
Router(config-webvpn-group)# webvpn-homepage http://192.0.2.0 redirection-time 12
```

Related Commands

Command	Description
policy group	Enters WebVPN group policy configuration mode.
show webvpn policy group	Displays the context configuration associated with a policy group.
webvpn context	Enters WebVPN context configuration mode.

webvpn cef

To enable Secure Socket Layer virtual private network (SSL VPN) full-tunnel Cisco Express Forwarding (CEF) support, use the **webvpn cef** command in global configuration mode. To disable full-tunnel CEF support, use the **no** form of this command.

webvpn cef
no webvpn cef

Syntax Description

There are no arguments or keywords.

Command Default

This command is set by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

IP CEF must be turned on before this command can take effect.

Examples

The following example shows that full-tunnel CEF is being disabled:

```
Router (config)# no webvpn cef
```

Related Commands

Command	Description
ip cef	Enables CEF on the route processor card.

webvpn context

To enter webvpn context configuration mode to configure the Secure Sockets Layer Virtual Private Network (SSL VPN) context, use the **webvpn context**command in global configuration mode. To remove the SSL VPN configuration from the router configuration file, use the **no** form of this command.

webvpn context *name*
no webvpn context *name*

Syntax Description

name	Name of the SSL VPN context configuration.

Command Default

Webvpn context configuration mode is not entered, and a SSL VPN context is not configured.

Command Modes

Global configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

The SSL VPN context defines the central configuration of the SSL VPN. Entering the **webvpn context** command places the router in webvpn context configuration mode.

Note The **ssl authenticate verify all** command is enabled by default when a context configuration is created. The context cannot be removed from the router configuration while a SSL VPN gateway is in an enabled state (in service).

Examples

The following example configures and activates the SSL VPN context configuration:

```
Router(config)# webvpn context context1

Router(config-webvpn-context)# inservice
```

Related Commands

Command	Description
aaa authentication (WebVPN)	Configures AAA authentication for SSL VPN sessions.
csd enable	Enables CSD support for SSL VPN sessions.
default-group-policy	Specifies a default group policy for SSL VPN sessions.
gateway (WebVPN)	Specifies the gateway for SSL VPN sessions.
inservice	Enables a SSL VPN gateway or context process.

Command	Description
login-message	Configures a message for a user login text box on the login page.
logo	Configures a custom logo to be displayed on the login and portal pages of a SSL VPN website.
max-users (WebVPN)	Limits the number of connections to a SSL VPN that will be permitted
nbns-list	Enters webvpn NBNS list configuration mode to configure a NBNS server list for CIFS name resolution.
policy group	Enters a webvpn group policy configuration mode to configure a group policy.
port-forward	Enters webvpn port-forward list configuration mode to configure a port-forwarding list.
secondary-color	Configures the color of the secondary title bars on the login and portal pages of a SSL VPN website.
secondary-text-color	Configures the color of the text on the secondary bars of a SSL VPN website.
title	Configures the HTML title string that is shown in the browser title and on the title bar of a SSL VPN website.
title-color	Configures the color of the title bars on the login and portal pages of a SSL VPN website.
url-list	Enters webvpn URL list configuration mode to configure the list of URLs to which a user has access on the portal page of a SSL VPN website.
vrf-name	Associates a VRF with a SSL VPN context.

webvpn create template

To create templates for multilanguage support for messages initiated by the head-end in a Secure Socket Layer Virtual Private Network (SSL VPN), configure the **webvpn create template** command in user EXEC or privileged EXEC mode.

webvpn create template
{**browser-attribute** | **language** | **url-list**}
device:

Syntax Description

browser-attribute	Creates a template file named "battr_tpl.xml".
language	Creates a template file named "lang.js".
url-list	Creates a template file named "url_list_tpl.xml".
device **:**	Storage device on the system for the templates, such as flash: or disk0.

Command Default

Template files are not created.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.4(22)T	This command was introduced.

Usage Guidelines

After template files have been created, they can be copied to a PC for editing and then reimported to the storage device.

Examples

The following example shows that a browser-attribute template file is to be created in flash:

```
Router# webvpn create template browser-attribute flash:
```

The following example shows that the language file is to be created in flash:

```
Router# webvpn create template language flash:
```

The following example shows that a URL list template is to be created in flash:

```
Router# webvpn create template url-list flash:
```

Related Commands

Command	Description
browser-attribute import	Imports user-defined browser attributes into a webvpn context.
import	Imports a user-defined URL list into a webvpn context.

Command	Description
language	Specifies the language to be used in a webvpn context.
url-list	Enters webvpn URL list configuration mode to configure a list of URLs to which a user has access on the portal page of a SSL VPN and attaches the URL list to a policy group.

webvpn enable

Note Effective with Cisco IOS Release 12.4(6)T, the **webvpn enable**command is replaced by the **inservice**command. See the **inservice** command for more information.

To enable WebVPN in the system, use the **webvpn enable**command in global configuration mode. To disable WebVPN in the system, use the **no** form of this command.

webvpn enable [**gateway-addr** *ip-address*]
no webvpn enable [**gateway-addr** *ip-address*]

Syntax Description

gateway-addr	*ip-address*	(Optional) Enables WebVPN on only the IP address that is specified. If this keyword and argument are not configured, WebVPN is enabled globally on all IP addresses.

Command Default

WebVPN is disabled in the system.

Command Modes

Web VPN configuration

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(6)T	This command was replaced by the **inservice** command.

Usage Guidelines

This command initializes the required system data structures, initializes TCP sockets, and performs other startup tasks related to WebVPN.

Examples

The following example shows that WebVPN has been enabled in the system:

```
webvpn enable
```

Related Commands

Command	Description
webvpn	Enters Web VPN configuration mode.

webvpn gateway

To enter webvpn gateway configuration mode to configure a SSL VPN gateway, use the **webvpn gateway** command in global configuration mode. To remove the SSL VPN gateway from the router configuration file, use the **no** form of this command.

webvpn gateway *name*
no webvpn gateway *name*

Syntax Description

name	Name of the virtual gateway service.

Command Default

Webvpn gateway configuration mode is not entered, and a SSL VPN gateway is not configured.

Command Modes

Global configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.

Usage Guidelines

Entering the **webvpn gateway** command places the router in webvpn gateway configuration mode. Configuration settings specific to the SSL VPN gateway are entered in this configuration mode.

The SSL VPN gateway acts as a proxy for connections to protected resources. Protected resources are accessed through a secure encrypted connection between the gateway and a web-enabled browser on a remote device, such as a personal computer.

The gateway is configured using an IP address at which SSL VPN remote-user sessions terminate. The gateway is not active until the inservice command has been entered in SSL VPN gateway configuration mode. Only one gateway can be configured in a SSL VPN-enabled network.

Examples

The following example creates and enables a SSL VPN gateway process named SSL_GATEWAY:

```
Router(config)# webvpn gateway SSL_GATEWAY

Router(config-webvpn-gateway)# ip address 10.1.1.1 port 443
Router(config-webvpn-gateway)# ssl trustpoint SSLVPN

Router(config-webvpn-gateway)# http-redirect 80

Router(config-webvpn-gateway)# inservice
```

Related Commands

Command	Description
hostname (WebVPN)	Configures a SSL VPN hostname.
http-redirect	Configures HTTP traffic to be carried over HTTPS.
inservice	Enables a SSL VPN gateway or context process.

Command	Description
ip address (WebVPN)	Configures a proxy IP address on a SSL VPN gateway.
ssl encryption	Configures the specify the encryption algorithms that the SSL protocol will use for an SSL VPN.
ssl trustpoint	Configures the certificate trust point on a SSL VPN gateway.

webvpn import svc profile

To enable an AnyConnect profile to be imported from a router, use the **webvpn import svc profile** command in global configuration mode. To disable the configuration, use the **no** form of this command.

webvpn import svc profile *profile-name device-name*
no webvpn import svc profile *profile-name*

Syntax Description

profile-name	Name of the AnyConnect profile.
device-name	Device name and filename of the AnyConnect profile thats needs to be imported.

Command Default

AnyConnect profiles are not imported to the Cisco IOS headend.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

You can use the **webvpn import svc profile** command to import the AnyConnect profile to the Cisco IOS headend. In order to import the AnyConnect profile to the Cisco IOS headend, the administrator must download the AnyConnect profile from an AnyConnect client (this profile comes by default with AnyConnect), update the profile file to enable the AnyConnect support, and then import the modified profile into the Cisco IOS software.

Examples

The following example shows how to import the AnyConnect profile to the Cisco IOS headend:

```
Router> enable

Router# configure terminal
Router(config)# webvpn import svc profile profile1 disk0:filename
```

Related Commands

Command	Description
svc profile	Applies a particular AnyConnect profile to the webvpn gateway.

webvpn install

To install a Cisco Secure Desktop (CSD) or Cisco AnyConnect VPN Client package file to a Secure Socket Layer virtual private network (SSL VPN) gateway for distribution to end users, use the **webvpn install** command in global configuration mode. To remove a package file from the SSL VPN gateway, use the **no** form of this command.

webvpn install [{**csd** *location-name* | **svc** *location-name* [**sequence** *sequence-number*]}]
no webvpn install [{**csd** *location-name* | **svc** *location-name* [**sequence** *sequence-number*]}]

Syntax Description

csd *location-name*	(Optional) Installs the CSD client software package. The filename and path are entered.
svc *location-name*	(Optional) Installs the Cisco AnyConnect VPN Client software package. The filename and path are entered.
sequence *sequence-number*	(Optional) Allows for multiple packages to be installed to one gateway. If the **sequence**keyword and the *sequence-number*argument are not configured, a sequence number of 1 is applied to the package.

Command Default

Neither a CSD nor a Cisco AnyConnect VPN Client package file is installed to a WebVPN gateway.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.4(20)T	The **sequence** *sequence-number*keyword and argument were added.

Usage Guidelines

The installation packages must first be copied to a local file system, such as disk, flash or USB flash. The CSD and Cisco AnyConnect VPN Client software packages are pushed to end users as access is needed. The end user must have administrative privileges, and the Java Runtime Environment (JRE) for Windows version 1.4 or a later version must be installed before a CSD or Cisco AnyConnect VPN Client package can be installed.

Note Secure Sockets Layer Virtual Private Network (SSL VPN) Client (SVC) is the predecessor of Cisco AnyConnect VPN Client software.

If you have not entered the **sequence** keyword and the *sequence-number* argument and you want to install another package, you can remove the previous package (using the **no** form of the command) or you can provide another sequence number.

If you try to install a package with a sequence number that is being used, you will get an error message.

Examples

The following example shows how to install the Cisco AnyConnect VPN Client package to an SSL VPN gateway. The package is being copied to a flash file system.

```
Router(config)# webvpn install svc flash:/webvpn/svc.pkg

SSLVPN Package SSL-VPN-Client : installed successfully
```

The following example shows how to install the CSD package to an SSL VPN gateway. The package is being copied to a flash file system.

```
Router(config)# webvpn install csd flash:/securedesktop_3_1_0_9.pkg

SSLVPN Package Cisco-Secure-Desktop : installed successfully
```

The following example shows how to install Cisco AnyConnect VPN Client package to an SSL VPN gateway. The file is being copied to a USB file system.

```
Router(config)# webvpn install csd usbflash0:securedesktop-ios-3.1.1.45-k9.pkg
SSLVPN Package Cisco-Secure-Desktop : installed successfully
```

Related Commands

Command	Description
show webvpn install status	Displays the installation status of SVC or CSD client software packages.

webvpn sslvpn-vif nat

To enable Network Address Translation (NAT) on the WebVPN virtual interface, use the **webvpn sslvpn-vif nat**command in global configuration mode. To disable NAT on the WebVPN virtual interface, use the **no** form of this command.

webvpn sslvpn-vif nat {**enable** | **inside** | **outside**}
no webvpn sslvpn-vif nat {**enable** | **inside** | **outside**}

Syntax Description

enable	Enables address translation.
inside	Enables the inside interface for address translation.
outside	Enables the outside interface for address translation.

Command Default

NAT is disabled by default on the WebVPN virtual interface.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

Use the show running-config command to verify if NAT has been enabled.

Examples

The following example shows that NAT has been enabled on the WebVPN virtual interface:

```
Router(config)# webvpn sslvpn-vif nat enable
```

Related Commands

Command	Description
show running-config	Displays the contents of the current running configuration file.

whitelist (cws)

To configure allowed listing of traffic based on the access control list (ACL) and the HTTP header whose header matches the configured regular expression, use the **whitelist** command in Cloud Web Security allowed listing configuration mode. To disable allowed listing of traffic, use the **no** form of this command.

whitelist {**acl** {*acl-list extended-acl-list acl-name*} | [{**header** | {**host** | **user-agent**} | **user** | **user-group**}] **regex** *regex-host* | **notify-tower**}
no whitelist {**acl** {*acl-list extended-acl-list acl-name*} | [{**header** | {**host** | **user-agent**} | **user** | **user-group**}] **regex** *regex-host* | **notify-tower**}

Syntax Description

acl	Specifies the ACL. The IP addresses that are used are the pre-NAT IP addresses for matching the access control list.
acl-list	Access list to create allowed listing of content scanning traffic. Valid values are from 1 to 199.
extended-acl-list	Extended access list to allowed listing of content-scan traffic. Valid values are from 1300 to 2699.
acl-name	Access list name.
header	Specifies the allowed list using the HTTP header.
host	Specifies the allowed list using the host header field.
user-agent	Specifies the allowed list using the user agent header field.
user	Specifies the name of the user whose content appears in the allowed list.
user-group	Specifies the user-group whose content appears on the allowed list.
regex	Specifies the HTTP header host, user, and user group values as regular expression (regex).
regex-host	Name of the host regular expression.
notify-tower	Specifies the allowed list to notify Cloud Web Security.

Command Default

Allowed listing is not configured.

Command Modes

Cloud Web Security allowed listing configuration (config-cws-wl)

Command History

Release	Modification
15.3(3)M	This command was introduced.
15.4(2)T	This command was modified. The **notify-tower** keyword was removed.

Usage Guidelines

An approved list contains entities that are provided a particular privilege, service, mobility, access, or recognition. An approved list means to grant access. The web traffic that is on the allowed list is not sent for content scanning to Cloud Web Security.

The **header** keyword specifies the allowed listing attribute on the HTTP header that matches the configured regular expression.

The **notify-tower** keyword specifies whether ScanSafe needs to be notified about allowed listing.

Examples

The following example shows how to configure allowed listing based on the ACL for Cisco IOS Release 15.3(3)M:

```
Device(config)# content-scan whitelisting
Device(config-cws-wl)# whitelist acl 199
```

The following example shows how to configure whitelisting based on the ACL for Cisco IOS Release 15.4(2)T and later:

```
Device(config)# cws whitelisting
Device(config-cws-wl)# whitelist acl 199
```

Related Commands

Command	Description
content-scan whitelisting	Enables allowed listing of incoming traffic and enters Cloud Web Security allowed listing configuration mode.
cws whitelisting	Enables allowed listing of incoming traffic and enters Cloud Web Security allowed listing configuration mode.

wins

To specify the primary and secondary Windows Internet Naming Service (WINS) servers, use the **wins**command in ISAKMP group configuration mode or IKEv2 client group configuration mode. To remove this command from your configuration, use the **no** form of this command.

wins *primary-server* [*secondary-server*]
no wins *primary-server* [*secondary-server*]

Syntax Description

primary-server	Name of the primary WINS server.
secondary-server	(Optional) Name of the secondary WINS server.

Command Default

No primary or secondary WINS server is specified.

Command Modes

ISAKMP group configuration (config-isakmp-group)
IKEv2 client group configuration (config-ikev2-client-config-group)

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS 12.2SX family of releases. Support in a specific 12.2SX release is dependent on your feature set, platform, and platform hardware.
Cisco IOS XE Release 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.

Usage Guidelines

Use this command to specify the primary and secondary WINS server for the remote access client. You must enable the following commands before enabling the **wins** command:

- **crypto isakmp client configuration group** --**Specifies the group policy information that has to be defined or changed.**
- **crypto ikev2 authorization policy** --Specifies the local group policy authorization parameters.

Examples

The following example shows how to define a primary and secondary WINS server for the group "cisco":

```
crypto isakmp client configuration group cisco
  key cisco
  dns 10.2.2.2 10.3.2.3
  pool dog
  acl 199
  wins 10.1.1.2 10.1.1.3
```

Related Commands

Command	Description
acl	Configures split tunneling.
crypto ikev2 authorization policy	Specifies an IKEv2 client configuration group.
crypto isakmp client configuration group	Specifies the DNS domain to which a group belongs.

wlccp authentication-server client

To configure the list of servers to be used for 802.1X authentication, use the **wlccp authentication-server client** command in global configuration mode. To disable the server list, use the **no**form of this command.

wlccp authentication-server client {**any** | **eap** | **leap** | **mac**} *list*
no wlccp authentication-server client {**any** | **eap** | **leap** | **mac**} *list*

Syntax Description

any	Specifies client devices that use any authentication.
eap	Specifies client devices that use Extensible Authentication Protocol (EAP) authentication.
leap	Specifies client devices that use Light Extensible Authentication Protocol (LEAP) authentication.
mac	Specifies client devices that use MAC-based authentication.
list	List of client devices.

Command Default

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)JA	This command was introduced.
12.3(11)T	This command was implemented on the following platforms: Cisco 2600XM, Cisco 2691, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3700, and Cisco 3800 series routers.

Usage Guidelines

You can specify a list of client devices that use any type of authentication, or you can specify a list of client devices that use a certain type of authentication (such as EAP, LEAP, or MAC-based authentication).

Examples

The following example shows how to configure the server list for LEAP authentication for client devices:

```
Router (config)# wlccp authentication-server client leap leap-list1
```

Related Commands

Command	Description
debug wlccp packet	Displays packet traffic to and from the WDS router.
debug wlccp wds	Displays either WDS debug state or WDS statistics messages.
show wlccp wds	Shows information about access points and client devices on the WDS router.
wlccp authentication-server infrastructure	Configures the list of servers to be used for 802.1X authentication for the wireless infrastructure devices.

Command	Description
wlccp wds priority interface	Enables a wireless device such as an access point or a wireless-aware router to be a WDS candidate.

wlccp authentication-server infrastructure

To configure the list of servers to be used for 802.1X authentication for the wireless infrastructure devices, use the **wlccp authentication-server infrastructure** command in global configuration mode. To disable the server list, use the **no**form of this command.

wlccp authentication-server infrastructure *list*
no wlccp authentication-server infrastructure *list*

Syntax Description

list	List of servers to be used for 802.1X authentication for the wireless infrastructure devices, such as access points, repeaters, and wireless-aware routers.

Command Default

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)JA	This command was introduced on Cisco Aironet access points.
12.3(11)T	This command was implemented on the following platforms: Cisco 2600XM, Cisco 2691, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3700, and Cisco 3800 series routers.

Examples

This example shows how to configure the server list for 802.1X authentication for infrastructure devices participating in Cisco Centralized Key Management:

```
Router (config)# wlccp authentication-server infrastructure wlan-list1
```

Related Commands

Command	Description
debug wlccp packet	Displays packet traffic to and from the WDS router.
debug wlccp wds	Displays either WDS debug state or WDS statistics messages.
show wlccp wds	Shows information about access points and client devices on the WDS router.
wlccp authentication-server client	Configures the list of servers to be used for 802.1X authentication.
wlccp wds priority interface	Enables a wireless device such as an access point or a wireless-aware router to be a WDS candidate.

wlccp wds priority interface

To configure the router or access point to provide WDS, use the **wlccp wds priority interface**command in global configuration mode. To remove the WDS configuration from the router or access point, use the **no** form of the command .

wlccp wds priority *priority* **interface interface**
no wlccp wds priority *priority* **interface interface**

Syntax Description

priority	Priority of this WDS candidate. The valid range is from 1 to 255. The greater the priority value, the higher the priority.
interface	Interface on which the router sends out WDS advertisements. Supported interface types are as follows: • For access points--bvi • For wireless-aware routers--bvi, svi, Fast Ethernet, and Gigabit Ethernet.

Command Default

No default behavior or values

Command Modes

Global configuration

Command History

Release	Modification
12.2(11)JA	This command was introduced with support for Cisco Aironet access points.
12.3(11T	This command was implemented on the following platforms: Cisco 2600XM, Cisco 2691, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3700, and Cisco 3800 series routers.

Usage Guidelines

The WDS candidate with the highest priority becomes the active WDS device.

Examples

This example shows how to configure the priority for an access point as a candidate to provide WDS with priority 200:

```
Router (config)# wlccp wds priority 200 interface bvi 1
```

Related Commands

Command	Description
debug wlccp packet	Displays packet traffic to and from the WDS router.
debug wlccp wds	Displays either WDS debug state or WDS statistics messages.
show wlccp wds	Shows information about access points and client devices on the WDS router.
wlccp authentication-server client	Configures the list of servers to be used for 802.1X authentication.

Command	Description
wlccp authentication-server infrastructure	Configures the list of servers to be used for 802.1X authentication for the wireless infrastructure devices.

xauth userid mode

To specify how the Easy VPN client handles extended authentication (Xauth) requests, use the **xauth userid mode**command in Cisco IOS Easy VPN remote configuration mode. To remove the setting, use the **no** form of this command.

xauth userid mode {**http-intercept** | **interactive** | **local**}
no xauth userid mode {**http-intercept** | **interactive** | **local**}

Syntax Description

http-intercept	HTTP connections are intercepted from the user through the inside interface and the prompt.
interactive	To authenticate, the user must use the command-line interface (CLI) prompts on the console. Interactive is the default behavior.
local	The saved username or password is used in the configuration.

Command Default

If the command is not configured, the default behavior is interactive.

Command Modes

Cisco IOS Easy VPN remote configuration (config-crypto-ezvpn)

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS 12.2SX family of releases. Support in a specific 12.2SX release is dependent on your feature set, platform, and platform hardware.

Usage Guidelines

If you want to be prompted by the console, use the **interactive** keyword.

If you want to use a saved username or password, use the **local**keyword. If a local username or password is defined, the mode changes to that username or password.

Examples

The following example shows that HTTP connections will be intercepted from the user and that the user can authenticate using web-based activation:

```
crypto ipsec client ezvpn tunnel22
  connect manual
  group tunnel22 key 22tunnel
  mode client
  peer 192.168.0.1
  xauth userid mode http-intercept
!
!
interface Ethernet0
  ip address 10.4.23.15 255.0.0.0
  crypto ipsec client ezvpn tunnel22 inside !
interface Ethernet1
  ip address 192.168.0.13 255.255.255.128
```

```
  duplex auto
  crypto ipsec client ezvpn catch22
!
```

Related Commands

Command	Description
crypto ipsec client ezvpn	Creates a Cisco Easy VPN remote configuration.
debug crypto ipsec client ezvpn	Displays information about voice control messages that have been captured by the Voice DSP Control Message Logger.
debug ip auth-proxy ezvpn	Displays information related to proxy authentication behavior for web-based activation.
show crypto ipsec client ezvpn	Displays the Cisco Easy VPN Remote configuration.
show ip auth-proxy	Displays the authentication proxy entries or the running authentication proxy configuration.

xsm

To enable XML Subscription Manager (XSM) client access to the device, use the **xsm** command in global configuration mode. To disable XSM client access to the device, use the **no** form of this command.

xsm
no xsm

Syntax Description

This command has no arguments or keywords.

Command Default

XSM client access to the device is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1(6)E	This command was introduced.
12.2(9)YE	This command was integrated into Cisco IOS Release 12.2(9)YE.
12.2(9)YO1	This command was integrated into Cisco IOS Release 12.2(9)YO1.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command requires that the **ip http server** command is enabled. Enabling the **xsm** command also enables the **xsm vdm** and **xsm edm** commands. This command must be enabled for the XSM client (such as VPN Device Manager [VDM]) to operate.

Examples

In the following example, access by remote XSM clients to XSM data on the device is disabled:

```
Router# no xsm
```

Related Commands

Command	Description
ip http server	Enables a device to be reconfigured through the Cisco browser interface.
show xsm status	Displays information and status about clients subscribed to the XSM server.
show xsm xrd-list	Displays all XRDs for clients subscribed to the XSM server.
xsm dvdm	Grants access to switch operations.

Command	Description
xsm edm	Grants access to EDM monitoring and configuration data.
xsm vdm	Grants access to VPN-specific monitoring and configuration data.

xsm dvdm

To enable switch-specific configuration data (for example, configuring switch ports and VLANs) when running VPN Device Manager (VDM) on a switch, use the **xsm dvdm**command in global configuration mode. To disable switch-specific configuration data for VDM, use the **no** form of this command.

xsm dvdm
no xsm dvdm

Syntax Description

This command has no arguments or keywords.

Command Default

Access to switch-specific configuration data is enabled when XSM is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(9)YO1	This command was introduced.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.

Usage Guidelines

Access to switch-specific configuration data (dVDM) is enabled by default when XSM is enabled.

The **no xsm dvdm** command allows you to disable only switch-specific XSM data. Note however that disabling dVDM will prevent the VDM application from communicating properly with the device (switch). There is minimal performance impact associated with leaving dVDM enabled.

Examples

In the following example, access to switch-specific configuration data is disabled in XSM:

```
Router(config)# no xsm dvdm
```

Related Commands

Command	Description
xsm	Enables XSM client access to the router.
xsm edm	Grants access to EDM monitoring and configuration data.
xsm history vdm	Enables specific VPN statistics collection on the XSM server.
xsm vdm	Grants access to VPN-specific monitoring and configuration data.

xsm edm

To grant access to Embedded Device Manager (EDM) monitoring and configuration data, use the **xsm edm**command in global configuration mode. To cancel access to EDM monitoring and configuration data, use the **no** form of this command.

xsm edm
no xsm edm

Syntax Description

This command has no arguments or keywords.

Command Default

Access to EDM monitoring and configuration data is granted by default if XSM is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1(6)E	This command was introduced.
12.2(9)YE	This command was integrated into Cisco IOS Release 12.2(9)YE.
12.2(9)YO1	This command was integrated into Cisco IOS Release 12.2(9)YO1.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command exists to allow you to disable EDM using the **no xsm edm** form of the command. EDM is enabled by default when XSM is enabled.

EDM provides the following generic information to the VPN Device Manager (VDM):

- Relevant interfaces
- IP routing
- Access-list details
- Basic device health

Note that disabling EDM prevents XSM clients (such as VDM) from working properly and also disables the **xsm history edm**command. There is minimal performance impact associated with leaving EDM enabled.

Examples

In the following example, access to EDM data is disabled:

```
Router(config)# xsm
```

```
Router(config)# no xsm edm
```

Related Commands

Command	Description
xsm	Enables XSM client access to the router.
xsm dvdm	Grants access to switch operations.
xsm history edm	Enables statistics collection for the EDM on the XSM server.
xsm vdm	Grants access to VPN-specific monitoring and configuration data.

xsm history vdm

To enable specific VPN statistics collection on the XML Subscription Manager (XSM) server, use the **xsm history vdm** command in global configuration mode. To disable collection of specific selected VPN statistics on the XSM server, use the **no** form of this command.

xsm history vdm
no xsm history vdm

Syntax Description

This command has no arguments or keywords.

Command Default

VPN statistics collecting is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1(6)E	This command was introduced.
12.2(9)YE	This command was integrated into Cisco IOS Release 12.2(9)YE.
12.2(9)YO1	This command was integrated into Cisco IOS Release 12.2(9)YO1.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

With this command enabled, you can save up to five days of data. Historical information on items such as the number of active IKE tunnels, IPSec tunnels, total crypto throughput, and total throughput is gathered and made available, thus enabling XSM clients (such as VPN Device Manager [VDM]) to display charts and data. Use of this command consumes resources on the device. Disabling this command clears all your historical data. The XSM server does not save history data across reloads.

Examples

The following example shows how to enable specific VPN statistics collection on the XSM server:

```
Router(config)# xsm

Router(config)# xsm history vdm
```

Related Commands

Command	Description
xsm	Enables XSM client access to the router.

Command	Description
xsm history edm	Enables statistics collection for the EDM on the XSM server.
xsm vdm	Grants access to VPN-specific monitoring and configuration data.

xsm history edm

To enable statistics collection for the Embedded Device Manager (EDM) on the XML Subscription Manager (XSM) server, use the **xsm history edm**command in global configuration mode. To disable statistics collection for the EDM on the XSM server, use the **no** form of this command.

xsm history edm
no xsm history edm

Syntax Description

This command has no arguments or keywords.

Command Default

EDM statistics collection is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1(6)E	This command was introduced.
12.2(9)YE	This command was integrated into Cisco IOS Release 12.2(9)YE.
12.2(9)YO1	This command was integrated into Cisco IOS Release 12.2(9)YO1.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use this command to save up to five days of data. Historical information on items such as RAM and CPU utilization is gathered and made available, thus enabling XSM clients (such as VPN Device Manager [VDM]) to display charts and data. Use of this command consumes resources on the device. Disabling this command clears all your historical data, as the XSM server does not save this data between reloads.

Examples

In the following example, statistics collection for the EDM is enabled on the XSM server:

```
Router(config)# xsm

Router(config)# xsm history edm
```

Related Commands

Command	Description
xsm	Enables XSM client access to the router.
xsm edm	Grants access to EDM monitoring and configuration data.

Command	Description
xsm history vdm	Enables specific VPN statistics collection on the XSM server.

xsm privilege configuration level

To enable the XML Subscription Manager (XSM) configuration privilege level required to subscribe to XML Request Descriptors (XRDs), use the **xsm privilege configuration level** command in global configuration mode. To remove a previously configured XSM configuration privilege level, use the **no** form of this command.

xsm privilege configuration level *number*
no xsm privilege configuration level *number*

Syntax Description

number	Integer in the range from 1 to 15 that identifies the privilege level. The default is 15.

Command Default

The default level is 15.

Command Modes

Global configuration

Command History

Release	Modification
12.1(6)E	This command was introduced.
12.2(9)YE	This command was integrated into Cisco IOS Release 12.2(9)YE.
12.2(9)YO1	This command was integrated into Cisco IOS Release 12.2(9)YO1.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The privilege level for the **xsm privilege configuration level**command must be greater than or equal to the privilege level for the **xsm privilege monitor level** command. For example, if the **xsm privilege configuration 7**command is enabled, you need a minimum privilege level of 7 to subscribe to configuration XRDs. The higher the number the higher the privilege level. Trying to set a conflicting range of privilege settings will force the Cisco device to display the following message:

```
Attempt to set monitor privilege greater than configuration. Privilege denied.
```

You can check the XSM privilege level settings by using the **show xsm status** command. Use the **show xsm xrd-list** command to check which privilege level is required for each XRD.

Note The initial login set by your system administrator determines whether you have the necessary IOS privilege level for actually configuring the Cisco router. Ask your system administrator for more information about privilege levels.

Examples

The following example shows how to set a configuration privilege level of 15, and a monitor privilege level of 11 for subscription to XRDs. Users with a privilege level below 11 are denied access.

```
Router(config)# xsm privilege configuration level 15
Router(config)# xsm privilege monitor level 11
```

Related Commands

Command	Description
privilege	Configures IOS privilege parameters.
xsm privilege monitor level	Enables monitor privilege level to subscribe to XRDs.

xsm privilege monitor level

To enable the XML Subscription Manager (XSM) monitoring privilege level required to subscribe to XML Request Descriptors (XRDs), use the **xsm privilege monitor level** command in global configuration mode. To remove a previously configured XSM monitoring privilege level, use the **no** form of this command.

xsm privilege monitor level *number*
no xsm privilege monitor level *number*

Syntax Description

number	Integer in the range from 1 to 15 that identifies the privilege level. The default is 15.

Command History

The default is level 1.

Command Modes

Global configuration

Command History

Release	Modification
12.1(6)E	This command was introduced.
12.2(9)YE	This command was integrated into Cisco IOS Release 12.2(9)YE.
12.2(9)YO1	This command was integrated into Cisco IOS Release 12.2(9)YO1.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The privilege level for the **xsm privilege monitor level**command must be less than or equal to the privilege level for the **xsm privilege configuration level** command. For example, if the **xsm privilege monitor 7**command is enabled, you need a minimum privilege level of 7 to subscribe to monitor XRDs. The higher the number the higher the privilege level. Trying to set a conflicting range of privilege settings will force the Cisco device to display the following message:

```
Attempt to set monitor privilege greater than configuration. Privilege denied.
```

You can check the XSM privilege level settings by using the **show xsm status** command. Use the **show xsm xrd-list** command to check which privilege level is required for each XRD.

Note The initial login set by your system administrator determines whether you have the necessary IOS privilege level for actually configuring the Cisco router. Ask your system administrator for more information about privilege levels.

Examples

The following example shows how to set a configuration privilege level of 15 and a monitor privilege level of 11 for subscription to XRDs. Users with a privilege level below 11 are denied access.

```
Router(config)# xsm privilege configuration level 15
Router(config)# xsm privilege monitor level 11
```

Related Commands

Command	Description
privilege	Configures IOS privilege parameters.
xsm privilege configuration level	Enables configuration privilege level to subscribe to XRDs.

xsm vdm

To grant access to VPN-specific monitoring and configuration data for the VPN Device Manager (VDM), use the **xsm vdm**command in global configuration mode. To cancel access to VPN-specific monitoring and configuration data for VDM, use the **no** form of this command.

xsm vdm
no xsm vdm

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled (Access to VPN-specific monitoring and configuration data for the VDM is granted when XSM is enabled.)

Command Modes

Global configuration

Command History

Release	Modification
12.1(6)E	This command was introduced.
12.2(9)YE	This command was integrated into Cisco IOS Release 12.2(9)YE.
12.2(9)YO1	This command was integrated into Cisco IOS Release 12.2(9)YO1.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command enables access to the following VPN-specific information:

- IPSec
- IKE
- Tunneling
- Encryption
- Keys and certificates

If XSM is enabled, this command is enabled by default. Access to VPN-specific monitoring and configuration data within XSM can be disabled by using the **no** form of the command. However, disabling this command will prevent VDM from working properly and will also disable the **xsm history vdm**command. Leaving this command enabled has minimal performance impact.

Examples

In the following example, access to VPN-specific monitoring and configuration data is disabled:

```
Router(config)# xsm
```

```
Router(config)# no xsm dvm
```

Related Commands

Command	Description
xsm	Enables XSM client access to the router.
xsm dvdm	Grants access to switch operations.
xsm edm	Grants access to EDM monitoring and configuration data.
xsm history vdm	Enables specific VPN statistics collection on the XSM server.

zone-member security

To attach an interface to a security zone, use the **zone-member security** command in interface configuration mode. To detach the interface from a zone, use the **no** form of this command.

zone-member security *zone-name*
no zone-member security *zone-name*

Syntax Description

zone-name	Name of the security zone to which an interface is attached.

Command Default

None

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(6)T	This command was introduced.
Cisco IOS XE Release 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

The **zone-member security** command attaches an interface into a security zone. When an interface is in a security zone, all traffic to and from that interface (except traffic going to the router or initiated by the router) is dropped by default. To permit traffic through an interface that is a zone member, you must make that zone part of a zone-pair to which you apply a policy. If the policy permits traffic (via **inspect** or **pass** actions), traffic can flow through the interface.

Examples

The following example attaches interface GigabitEthernet 0/0/1 to zone z1:

```
Device(config)# interface gigabitethernet 0/0/1
 Device(config-if)# zone-member security z1
```

Related Commands

Command	Description
zone security	Creates a zone.

zone-mismatch drop

To validates the zone pair that is attached to an existing session, and allow traffic that matches the zone pair into the network, use the **zone-mismatch drop** command. To disable the configuration, use the **no** form of this command.

zone-mismatch drop
no zone-mismatch drop

Syntax Description

This command has no arguments or keywords.

Command Default

The traffic that do not belong to a zone pair are inspected by the zone-based firewall.

Command Modes

Parameter map type inspect (config-profile)

Command History

Release	Modification
Cisco IOS XE Release 3.15S	This command was introduced.
Cisco IOS 15.5(2)T	This command was implemented on Cisco IOS Release 15.5(2)T.

Usage Guidelines

The command allows you to validate the zone pair that is associated with an existing session, and allows traffic that matches the zone pair into the network. When you configure the command, the firewall drops all packets (IPv4 and IPv6) that match an existing session but whose zone pair does not match the zone through which these packets arrive or leave.

When you configure the**zone-mismatch drop** command under the **parameter-map type inspect-global** command, the zone mismatch handling configuration applies to the global firewall configuration. Traffic between all zones are inspected for zone-pair mismatch.

When you configure the**zone-mismatch drop** command under the **parameter-map type inspect** command the zone mismatch handling configuration is applied on a per-policy basis.

When you configure this command, the configuration is effective only for new sessions. For existing sessions, traffic is not dropped if the sessions do not belong to the same zone pair.

Examples

The following example shows how configure the **zone-mismatch drop** command:

```
Device# configure terminal
Device(config)# parameter-map type inspect pmap1
Device(config-profile)# zone-mismatch drop
Device(config-profile)# end
```

The following example shows how configure the zone mismatch handling configuration for the global firewall configuration:

```
Device# configure terminal
Device(config)# parameter-map type inspect-global
Device(config-profile)# zone-mismatch drop
Device(config-profile)# end
```

Related Commands

Command	Description
parameter-map type inspect *parameter-map-name*	Configures an inspect-type parameter map for connecting thresholds, timeouts, and other parameters pertaining to the inspect action.
parameter-map type inspect-global	Configures a global parameter map and enters parameter-map type inspect configuration mode.

zone pair security

To create a zone pair, use the **zone-pair security** command in global configuration mode. To delete a zone pair, use the **no** form of this command.

zone-pair security *zone-pair-name* **source** {*source-zone-name* | **self** | **default**} **destination** {*destination-zone-name* | **self** | **default**}
no zone-pair security *zone-pair-name* **source** {*source-zone-name* | **self** | **default**} **destination** {*destination-zone-name* | **self** | **default**}

Syntax Description

zone-pair-name	Name of the zone being attached to an interface.
source *source-zone-name*	Specifies the name of the router from which traffic is originating.
default	Specifies the name of the default security zone. Interfaces without configured zones belong to the default zone.
destination *destination-zone-name*	Specifies the name of the device to which traffic is bound.
self	Specifies the system-defined zone. Indicates whether traffic will be going to or from a device.

Command Default

A zone pair is not created.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(6)T	This command was introduced.
Cisco IOS XE Release 2.6S	This command was modified. The **default** keyword was added.
15.1(2)T	This command was modified. Support for IPv6 was added.
Cisco IOS XE Release 3.9S	This command was modified to define a zone pair and attach a service policy to the zone pair.

Usage Guidelines

This command creates a zone pair, which permits a unidirectional firewall policy between a pair of security zones. After you enter this command, you can enter the **service-policy type inspect** command.

If you created only one zone, you can use the system-defined default zone (self) as part of a zone pair. Such a zone pair and its associated policy applies to traffic directed to the router or generated by the router. It does not affect traffic through the router.

You can specify the **self** keyword for the source or destination, but not for both. You cannot modify or remove configuration from the self zone. You can specify the **default** keyword to include all the interfaces that are not configured with any other zones. However, the default zone needs to be defined before it can be used in a zone pair.

Examples

The following example shows how to create zones z1 and z2, identify them, and create a zone pair where z1 is the source and z2 is the destination:

```
zone security z1
 description finance department networks
zone security z2
 description engineering services network
zone-pair security zp source z1 destination z2
zone-pair security
```

The following example shows how to define zone pair z1-z2 and attach the service policy p1 to the zone pair:

```
zone-pair security zp source z1 destination z2
 service-policy type inspect p1
```

The following example shows how to define a zone pair z1 and z2 and attach the service policy gtp_l4p to the zone pair:

```
zone-pair security clt2srv1 source z1 destination z2
  service-policy type inspect gtp_l4p
interface GigabitEthernet0/0/0
ip address 172.168.0.1 255.255.255.0
zone-member security z1
interface GigabitEthernet0/0/2
ip address 172.168.0.1 255.255.255.0
zone-member security z2
```

The following example shows how the zone pair is configured between system-defined and default zones:

```
zone security default
class-map type inspect match-all tcp-traffic
   match protocol tcp
   match access-group 199
policy-map type inspect p1
   class type inspect tcp-traffic
zone-pair security self-default-zp source self destination default
   service-policy type inspect p1
```

Related Commands

Command	Description
zone-member security	Attaches an interface to a security zone.
zone-pair	Creates a zone pair.

zone security

To create a security zone, use the **zone security** command in global configuration mode. To delete a security zone, use the **no** form of this command.

zone security {*zone-name* | **default**}
no zone security {*zone-name* | **default**}

Syntax Description

zone-name	Name of the security zone. You can enter up to 256 alphanumeric characters.
default	Specifies the name of a default security zone. Interfaces that are not configured on any of the security zones belong to the default zone.

Command Default

There is a system-defined "self" zone.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(6)T	This command was introduced.
Cisco IOS XE Release 2.6	This command was modified. The **default** keyword was added.
15.1(2)T	Support for IPv6 was added.

Usage Guidelines

We recommend that you create at least two security zones so that you can create a zone pair. If you create only one zone, you can use the default system-defined self zone. The self zone cannot be used for traffic going through a router. You can specify the **default**keyword to include all the interfaces that are not configured with any other zones.

To configure an interface to be a member of a security zone, use the **zone-member security** command.

Examples

The following example shows how to create and describe zones x1 and z1:

```
zone security x1
 description testzonex
zone security z1
 description testzonez
```

The following example shows how to create a default zone:

```
zone security default
 description system level default zone
```

Related Commands

Command	Description
description (identify zone)	Contains a description of a zone.

Command	Description
zone-member security	Attaches an interface to a zone.
zone-pair security	Creates a zonepair.

INDEX

S