Cisco IOS Security Command Reference: Commands D to L

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

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

CONTENTS

database archive through dns

data

To configure the data interface type and number for a redundancy group, use the **data**command in redundancy application group configuration mode. To remove the configuration, use the **no** form of this command.

data *interface-type interface-number*

no data *interface-type interface-number*

Syntax Description

interface-type	Interface type.
interface-number	Interface number.

Command Default

No data interface is configured.

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

Use the **data** command to configure the data interface. The data interface can be the same physical interface as the control interface.

Examples

The following example shows how to configure the data Gigabit Ethernet interface for group1:

```
Router# configure terminal
Router(config)# redundancy
Router(config-red)# application redundancy
Router(config-red-app)# group 1
Router(config-red-app-grp)# data GigabitEthernet 0/0/0
```

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.

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.

database archive

To set the certification authority (CA) certificate and CA key archive format--and the password--to encrypt this CA certificate and CA key archive file, use the **database archive**command in certificate server configuration mode. To disable the auto-archive feature, use the **no** form of this command.

database archive {**pkcs12**| **pem**} [**password** *password*]

no database archive {**pkcs12**| **pem**} [**password** *password*]

Syntax Description

pkcs12	Export as a PKCS12 file. The default is PKCS12.
pem	Export as a privacy-enhanced mail (PEM) file.
password *password*	(Optional) Password to encrypt the CA certificate and CA key. The password must be at least eight characters. If a password is not specified, you will be prompted for the password after the **no shutdown** command has been issued for the first time. When the password is entered, it will be encrypted.

Command Default

The archive format is PKCS (that is, the CA certificate and CA key are exported into a PKCS12 file, and you are prompted for the password when the certificate server is turned on the first time).

Command Modes

Certificate server configuration (cs-server)

Command History

Release	Modification
12.3(11)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 configure the autoarchive format for the CA certificate and CA key. The archive can later be used to restore your certificate server.

If autoarchiving is not explicitly turned off when the certificate server is first enabled (using the **no shutdown** command), the CA certificate and CA key will be archived automatically, applying the following rule:

- The CA key must be (1) manually generated and marked “exportable” or (2) automatically generated by the certificate server (it will be marked nonexportable).

Note It is strongly recommended that if the password is included in the configuration to suppress the prompt after the **no shutdown** command, the password should be removed from the configuration after the archiving is finished.

Examples

The following example shows that certificate server autoarchiving has been enabled. The CA certificate and CA key format has been set to PEM, and the password has been set as cisco123.

```
Router (config)# crypto pki server myserver
Router (cs-server)# database archive pem password cisco123
```

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 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.

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

database level

To control what type of data is stored in the certificate enrollment database, use the **database level** command in certificate server configuration mode. To return to the default functionality, use the **no** form of this command.

database level {**minimal**| **names**| **complete**}

no database level {**minimal**| **names**| **complete**}

Syntax Description

minimal	Enough information is stored only to continue issuing new certificates without conflict. This is the default functionality.
names	The serial number and subject name of each certificate are stored in the database, providing enough information for the administrator to find and revoke and particular certificate, if necessary.
complete	Each issued certificate is written to the database. If this keyword is used, you should enable the **database url** command; see "Usage Guidelines" for more information.

Command Default

minimal

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.

The **database level** command is used to describe the database of certificates and certification authority (CA) states. After the user downgrades the database level, the old data stays the same and the new data is logged at the new level.

minimum Level

The *ca-label*.ser file is always available. It contains the previously issued certificate's serial number, which is always 1. If the .ser file is unavailable and the CA server has a self-signed certificate in the local configuration, the CA server will refuse to issue new certificates.

The file format is as follows:

```
last_serial =
serial-number
```

names Level

The *serial-number*.cnm file, which is written for each issued certificate, contains the “human readable decoded subject name” of the issued certificate and the “der encoded” values. This file can also include a certificate expiration date and the current status. (The **minimum** level files are also written out.)

The file format is as follows:

```
subjectname_der = <
base64 encoded der value>
subjectname_str = <
human readable decode subjectname>
expiration = <
expiration date>
status = valid | revoked
```

complete Level

The *serial-number* .cer file, which is written for each issued certificate, is the binary certificate without additional encoding. (The **minimum** and **names** level files are also written out.)

The **complete** level produces a large amount of information, so you may want to store all database entries on an external TFTP server via the **database url** command unless your router does one of the following:

- Issues only a small number of certificates
- Has a local file system that is designed to support a large number of write operations and has sufficient storage for the certificates that are being issued

Examples

The following example shows how configure a minimum database to be stored on the local system:

```
Router#(config) ip http server
Router#(config) crypto pki server myserver
Router#(cs-server) database level minimum
Router#(cs-server) database url nvram:
Router#(cs-server) issuer-name CN = ipsec_cs,L = Santa Cruz,C = US
```

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

Command	Description
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 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.

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

database url

To specify the location where database entries for the certificate server (CS) is stored or published, use the **database url**command in certificate server configuration mode. To return to the default location, use the **no** form of this command.

Storing Files to a Primary Location

database url *root-url*

Storing Critical CS Files to a Specific Location

database url [**cnm**| **crl**| **crt**| **p12**| **pem**| **ser**] *root-url* [**username** *username*] [**password** [*encrypt-type*] *password*]

no database url [**cnm**| **crl**| **crt**| **p12**| **pem**| **ser**] *root-url* [**username** *username*] [**password** [*encrypt-type*] *password*]

Publishing Noncritical CS Files to a Specific Location

database url {**cnm**| **crl**| **crt**} **publish** *root-url* [**username** *username*] [**password** [*encrypt-type*] *password*]

no database url {**cnm**| **crl**| **crt**} **publish** *root-url* [**username** *username*] [**password** [*encrypt-type*] *password*]

Syntax Description

root-url	Location where database entries will be written out. The URL can be any URL that is supported by the Cisco IOS file system (IFS).
cnm	(Optional) Specifies the certificate name and expiration file to be stored or published to a specific location.
crl	(Optional) Specifies the DER-encoded certificate revocation list to be stored or published to a specific location
crt	(Optional) Specifies the DER-encoded certificate files to be stored or published to a specific location.
p12	(Optional) Specifies the CS certificate and key archive file in PKCS12 format to be stored to a specific location.
pem	(Optional) Specifies the CS certificate and key archive file in privacy-enhanced mail format to be stored to a specific location.
ser	(Optional) Specifies the current serial number to be stored to a specific location.

publish	Specifies that the files will be made available to a published location.
username *username*	(Optional) When prompted, a username will be used to access a storage location.
password *password*	(Optional) When prompted, a password will be used to access a storage location.
encrypt-type	(Optional) Type of encryption to be used for the password. If no password type is specified the password is sent as clear text. • Default is 0; specifies that the password entered will be encrypted. • 7; specifies that the password entered is already encrypted.

Command Default

The default file storage location is flash.

No default file publish location is specified.

Command Modes

Certificate server configuration (cs-server)

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.4(4)T	This command was modified. The following keywords and arguments were added **cnm**, **crl**, **crt**, **p12**, **pem**, **ser**, **publish, username** *username* **,** *encrypt-type* and **password** *password*.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.(33)SRA.

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.

The **database url** command specifies a combined list of all the certificates that have been issued and the current command revocation list (CRL). The CRL is written to the certificate enrollment database with the name of the certificate server.

Note Although issuing the **database url** command is not required, it is recommended. Unless your router has a local file system that is designed for a large number of write operations and has sufficient storage for the certificates that are issued, you should issue this command.

Cisco IOS File System

The router uses any file system that is supported by your version of Cisco IOS software (such as TFTP, FTP, flash, and NVRAM) to send a certificate request and to receive the issued certificate. A user may wish to enable IFS certificate enrollment when his or her certification authority (CA) does not support Simple Certificate Enrollment Protocol (SCEP).

Specifying CS Storage and Publication Location by File Type

The CS allows the flexibility to store different critical file types to specific storage locations and publish non-critical files to the same or alternate locations. When choosing storage locations consider the file security needed and server performance. For instance, serial number files (.ser) and archive files (.p12 or .pem) might have greater security restrictions than the general certificates storage location (.crt) or the name file storage location (.cnm). Performance of your certificate server may be affected by the storage location(s) you choose, for example, reading from a network location would likely take more time than reading directly from a router’s local storage device.

Examples

The following example shows how to configure all database entries to be written out to a TFTP server:

```
Router#(config) ip http server
Router#(config) crypto pki server myserver
Router#(cs-server) database level complete
Router#(cs-server) database url tftp://mytftp
```

The following example shows the configuration of a primary storage location for critical files, a specific storage location for the critical file serial number file, the main CS database file, and a password protected file publication location for the CRL file:

```
Router(config)# crypto pki server mycs
Router(cs-server)# database url ftp://cs-db.company.com
!
% Server database url was changed. You need to move the
% existing database to the new location.
!
Router(cs-server)# database url ser nvram:
Router(cs-server)# database url crl publish ftp://crl.company.com username myname password
 mypassword
Router(cs-server)# end
```

The following show output displays the specified primary storage location and critical file storage locations specified:

```
Router# show
Sep  3 20:19:34.216: %SYS-5-CONFIG_I: Configured from console by user on console Router#
show crypto pki server

Certificate Server mycs:
     Status: disabled
     Server's configuration is unlocked  (enter "no shut" to lock it)
     Issuer name: CN=mycs
     CA cert fingerprint: -Not found-
     Granting mode is: manual
     Last certificate issued serial number: 0x0
     CA certificate expiration timer: 00:00:00 GMT Jan 1 1970
     CRL not present.
     Current primary storage dir: ftp://cs-db.company.com
     Current storage dir for .ser files: nvram:
     Database Level: Minimum - no cert data written to storage
Router#
```

The following show output displays all storage and publication locations. The serial number file (.ser) is stored in NVRAM. The CRL file will be published to ftp://crl.company.com with a username and password. All other critical files will be stored to the primary location, ftp://cs-db.company.com.

```
Router# show running-config
   section crypto pki server
   crypto pki server mycs shutdown database url ftp://cs-db.company.com
   database url crl publish ftp://crl.company.com username myname password 7
12141C0713181F13253920
   database url ser nvram:
```

Router#

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"
```

% There was a problem reading the file 'mycs.ser' from certificate storage.

% Please verify storage accessibility and enable the server again.

```
% 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.
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.

Command	Description
database level	Controls what type of data is stored in the certificate enrollment database.
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

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

database username

To require a username or password to be issued when accessing the primary database location, use the **database username** command in certificate server configuration mode. To return to the default value, use the **no** form of this command.

database username *username* [**password** [*encr-type*] *password*]

no database username *username* [**password** [*encr-type*] *password*]

Syntax Description

username	When prompted, a username will be used to access a storage location.
password *password*	(Optional) When prompted, a password will be used to access a storage location.
encr-type	(Optional) Type of encryption to be used for the password. If no password encryption type is specified, the password is sent as clear text. • Default is 0; specifies that the password entered will be encrypted. • 7; specifies the password entered is already encrypted.

Command Default

No username or password will be used to access the primary database storage location.

Command Modes

Certificate server configuration (cs-server)

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.4(4)T	The command name was changed from **database**(certificate server) to **database username**.

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.

All information stored in the remote database is public: there are no private keys stored in the database location. Using a password helps to protect against a potential attacker who can change the contents of the .ser or .crl file. If the contents of the files are changed, the certificate server may shut down, refusing to either issue new certificates or respond to Simple Certificate Enrollment Protocol (SCEP) requests until the files are restored.

It is good security practice to protect all information exchanges with the database server using IP Security (IPsec). To protect your information, use a remote database to obtain the appropriate certificates and setup the necessary IPsec connections to protect all future access to the database server.

Examples

The following example shows how to specify the username “mystorage” when the primary storage location is on an external TFTP server:

```
Router (config)# ip http server
Router (config)# crypto pki server myserver
Router (cs-server)# database level complete
Router (cs-server)# database url tftp://mytftp
Router (cs-server)#
database username mystorage
```

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.
default (cs-server)	Resets the value of the CS configuration command to its default.

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

deadtime (server-group configuration)

To configure deadtime within the context of RADIUS server groups, use the **deadtime**command in server group configuration mode. To set deadtime to 0, use the **no** form of this command.

deadtime *minutes*

no deadtime

Syntax Description

minutes	Length of time, in minutes, for which a RADIUS server is skipped over by transaction requests, up to a maximum of 1440 minutes (24 hours).

Command Default

Deadtime is set to 0.

Command Modes

Server-group configuration

Command History

Release	Modification
12.1(1)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 this command to configure the deadtime value of any RADIUS server group. The value of deadtime set in the server groups will override the server that is configured globally. If deadtime is omitted from the server group configuration, the value will be inherited from the master list. If the server group is not configured, the default value (0) will apply to all servers in the group.

When the RADIUS Server Is Marked As Dead

For Cisco IOS versions prior to 12.2(13.7)T, the RADIUS server will be marked as dead if a transaction is transmitted for the configured number of retransmits and a valid response is not received from the server within the configured timeout for any of the RADIUS packet transmissions.

For Cisco IOS versions 12.2(13.7)T and later, the RADIUS server will be marked as dead if both of the following conditions are met:

1. A valid response has not been received from the RADIUS server for any outstanding transaction for at least the timeout period that is used to determine whether to retransmit to that server, and

2 Across all transactions being sent to the RADIUS server, at least the requisite number of retransmits +1 (for the initial transmission) have been sent consecutively without receiving a valid response from the server with the requisite timeout.

Examples

The following example specifies a one-minute deadtime for RADIUS server group group1 once it has failed to respond to authentication requests:

```
aaa group server radius group1
 server 10.1.1.1 auth-port 1645 acct-port 1646
 server 10.2.2.2 auth-port 2000 acct-port 2001
 deadtime 1
```

Related Commands

Command	Description
radius-server deadtime	Sets the deadtime value globally.

def-domain

To specify the default domain for the client to use, use the **def-domain** command in IKEv2 authorization policy configuration mode. To disable, use the **no** form of this command.

def-domain *domain-name*

no def-domain *domain-name*

Syntax Description

domain-name	Domain name.

Command Default

The default domain is not specified.

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 the def-domain command, you must first configure the **crypto ikev2 authorization policy** command. This value set in this command is sent to the client via the nonstandard Cisco unity configuration attribute.

Examples

The following example show how to configure the **def-domain** command:

```
Router(config)# crypto ikev2 authorization policy policy1
Router(config-ikev2-profile)# def-domain cisco
```

Related Commands

Command	Description
crypto ikev2 authorization policy	Specifies an IKEv2 authorization policy group.

default (cs-server)

To reset the value of the certificate server (CS) configuration subcommand to its default, use the **default**command in ca-trustpoint configuration mode.

default *command-name*

Syntax Description

command-name	Certificate server configuration subcommand.

Command Default

No default behavior or values.

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.

Examples

The following example shows how to remove the **crl**commandfrom your configuration; the default of **crl** is off.

```
Router(cs-server)# default crl
```

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

Command	Description
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.
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.

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

default (ca-trustpoint)

To reset the value of a ca-trustpoint configuration subcommand to its default, use the **default**command in ca-trustpoint configuration mode.

default *command-name*

Syntax Description

command-name	Ca-trustpoint configuration subcommand.

Command Default

No default behavior or values.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.2(8)T	The command mode was changed from **default (ca-root)** to **default (ca-trustpoint)** to support the **crypto ca trustpoint** command and all related subcommands.
12.2(18)SXD	The **default (ca-root)** command was integrated into Cisco IOS Release 12.2(18)SXD.
12.2(33)SRA	The **default (ca-root)** command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Before you can configure this command, you must enable the **crypto ca trustpoint**command , which enters ca-trustpoint configuration mode.

Use this command to reset the value of a ca-trustpoint configuration mode subcommand to its default.

Note The **crypto ca trustpoint** command deprecates the **crypto ca identity** and **crypto ca trusted-root** commands and all related subcommands (all ca-identity and trusted-root configuration mode commands). If you enter a ca-identity or trusted-root subcommand, the configuration mode and command will be written back as ca-trustpoint.

Examples

The following example shows how to remove the **crl optional**commandfrom your configuration; the default of **crl optional** is off.

```
default crl optional
```

Related Commands

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

default (ca-trustpool)

To reset the value of a ca-trustpool configuration command to its default in the public key infrastructure (PKI) trustpool, use the **default** command in ca-trustpool configuration mode.

default *command-name*

Syntax Description

command-name	Ca-trustpool configuration subcommand with its applicable 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 Release 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)# default crl query
```

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.

Command	Description
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.
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.

default-group-policy

To associate a policy group with a SSL VPN context configuration, use the **default-group-policy** command in webvpn context configuration mode. To remove the policy group from the webvpn context configuration, use the **no** form of this command.

default-group-policy *name*

no default-group-policy

Syntax Description

name	Name of the policy configured with the **policy group** command.

Command Default

A policy group is not associated with a SSL VPN context configuration.

Command Modes

Webvpn context configuration

Command History

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

Usage Guidelines

The **policy group** command is first configured to define policy group configuration parameters. This command is configured to attach the policy group to the SSL VPN context when multiple policy groups are defined under the context. This policy will be used as the default unless an authentication, authorization, and accounting (AAA) server pushes an attribute that specifically requests another group policy.

Examples

The following example configures policy group ONE as the default policy group:

```
Router(config)# webvpn context context1

Router(config-webvpn-context)# policy-group ONE

Router(config-webvpn-group)# exit

Router(config-webvpn-context)# policy-group TWO
Router(config-webvpn-group)# exit

Router(config-webvpn-context)# default-group-policy ONE
```

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.

deny

To set conditions in a named IP access list or object group access control list (OGACL) that will deny packets, use the **deny** configuration command in the appropriate configuration mode. To remove a deny condition from an IP access list or OGACL, use the **no** form of this command.

deny *protocol* {*src-addr src-wildcard*| **object-group** *object-group-name*| **any**| **host** {*addr*| *name*}} {*dest-addr dest-wildcard*| **any**| **eq** *port*| **gt** *port*| **host** {*addr*| *name*}| **lt** *port*| **neq** *port*| **portgroup** *srcport-groupname*| **object-group** *dest-addr-groupname*| **range** *port*| [**dscp** *type*| **fragments**| **option** *option*| **precedence** *precedence*| **log**| **log-input**| **time-range** *time-range-name*| **tos** *tos*| **ttl** *ttl-value*]}

no deny *protocol* {*src-addr src-wildcard*| **object-group** *object-group-name*| **any**| **host** {*addr*| *name*}} {*dest-addr dest-wildcard*| **any**| **eq** *port*| **gt** *port*| **host** {*addr*| *name*}| **lt** *port*| **neq** *port*| **portgroup** *srcport-groupname*| **object-group** *dest-addr-groupname*| **range** *port*| [**dscp** *type*| **fragments**| **option** *option*| **precedence** *precedence*| **log**| **log-input**| **time-range** *time-range-name*| **tos** *tos*| **ttl** *ttl-value*]}

Syntax Description

protocol	Name or number of a protocol; valid values are **eigrp**, **gre**, **icmp**, **igmp**, **igrp**, **ip**, **ipinip**, **nos**, **ospf**, **tcp**, or **udp**, or an integer in the range 0 to 255 representing an IP protocol number. To match any Internet protocol (including Internet Control Message Protocol (ICMP), TCP, and User Datagram Protocol (UDP), use the keyword **ip**. See the “Usage Guidelines” section for additional qualifiers.
src-addr	Number of the source network or host from which the packet is being sent in a 32-bit quantity in four-part, dotted-decimal format.
src-wildcard	Wildcard bits to be applied to source network in four-part, dotted-decimal format. Place ones in the bit positions you want to ignore.
object-group *object-group-name*	Specifies the source or destination name of the object group.
any	Specifies any source or any destination host as an abbreviation for the *source-addr*or *destination-addr value*and the *source-wildcard* or *destination-wildcard* value of 0.0.0.0 255.255.255.255.
host *addr*	Specifies the source or destination address of a single host.
host *name*	Specifies the source or destination name of a single host.
tcp	Specifies the TCP protocol.

udp	Specifies the UDP protocol.
object-group *source-addr-group-name*	Specifies the source address group name.
destination-addr	Number of the network or host to which the packet is being sent in a 32-bit quantity in four-part, dotted-decimal format.
destination-wildcard	Wildcard bits to be applied to the destination in a 32-bit quantity in four-part, dotted-decimal format. Place ones in the bit positions you want to ignore.
eq *port*	Matches only packets on a given port number; see the "Usage Guidelines" section for valid values.
gt *port*	Matches only the packets with a greater port number; see the "Usage Guidelines" section for valid values.
lt *port*	Matches only the packets with a lower port number; see the "Usage Guidelines" section for valid values.
neq *port*	Matches only the packets that are not on a given port number; see the "Usage Guidelines" section for valid values.
portgroup *srcport-group-name*	Specifies the source port object group name.
object-group *dest-addr-group-name*	Specifies the destination address group name.
portgroup *destport-group-name*	Specifies the destination port object group name.
dscp *type*	(Optional) Matches the packets with the given Differentiated Services Code Point (DSCP) value; see the "Usage Guidelines" section for valid values.
fragments	(Optional) Applies the access list entry to noninitial fragments of packets; the fragment is either permitted or denied accordingly. For more details about the **fragments** keyword, see the "Access List Processing of Fragments" and "deny, on page 33" sections in the "Usage Guidelines" section.
option *option*	(Optional) Matches the packets with the given IP options value number; see the "Usage Guidelines" section for valid values.
precedence *precedence*	(Optional) Specifies the precedence filtering level for packets; valid values are a number from 0 to 7 or by a name. See the "Usage Guidelines" section for a list of valid names.

log	(Optional) Causes an informational logging message about the packet that matches the entry to be sent to the console. (The level of messages logged to the console is controlled by the **logging console** command.) The message for a standard list includes the access list number, whether the packet was permitted or denied, the source address, and the number of packets. The message for an extended list includes the access list number; whether the packet was permitted or denied; the protocol; whether the protocol was TCP, UDP, ICMP, or a number; and, if appropriate, the source and destination addresses and source and destination port numbers. For both standard and extended lists, the message is generated for the first packet that matches, and then at 5-minute intervals, including the number of packets permitted or denied in the prior 5-minute interval. The logging facility might drop some logging message packets if there are too many to be handled or if there is more than one logging message to be handled in 1 second. This behavior prevents the router from reloading because of too many logging packets. Therefore, the logging facility should not be used as a billing tool or an accurate source of the number of matches to an access list.
log-input	(Optional) Matches the log against this entry, including the input interface.
time-range *time-range-name*	(Optional) Specifies a time-range entry name.
tos *tos*	(Optional) Specifies the service filtering level for packets; valid values are a number from 0 to 15 or by a name as listed in the "Usage Guidelines" section of the **access-list**(IP extended) command.
option option	(Optional) Matches packets with the IP options value; see the "Usage Guidelines" section for the valid values.
fragments	(Optional) Applies the access list entry to noninitial fragments of packets; the fragment is either permitted or denied accordingly. For more details about the **fragments** keyword, see the deny, on page 33 and "deny, on page 33" sections in the "Usage Guidelines" section.

ttl *ttl-value*	(Optional) Matches packets with a given Time-to-live (ttl) value.

Command Default

There is no specific condition under which a packet is denied passing the access list.

Command Modes

Standard access-list configuration (config-std-nacl) Extended access-list configuration (config-ext-nacl)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

Use this command following the **ip access-list** command to specify conditions under which a packet cannot pass the access list.

The **portgroup** keyword appears only when you configure an extended ACL.

The *address* or *object-group-name* value is created using the **object-group** command.

The **object-group** *object-group-name*keyword and argument allow you to create logical groups of users (or servers), which you can use to define access policy using ACLs. For example, with one ACL entry you can permit the object group named engineering to access all engineering servers. Otherwise, you would need one ACL entry for every person in the engineering group.

If the operator is positioned after the *source-addr* and *source-wildcard* values, it must match the source port.

If the operator is positioned after the *destination-addr* and *destination-wildcard* values, it must match the destination port.

If you are entering the port number of a TCP or UDP port, you can enter the decimal number or name of a TCP or UDP port. A port number is a number from 0 to 65535. TCP and UDP port names are listed in the “Usage Guidelines” section of the **access-list**(IP extended) command. TCP port names can be used only when filtering TCP. UDP port names can be used only when filtering UDP.

The valid values for the **dscp** *type* keyword and argument are as follows:

- 0 to 63--Differentiated services code point value.
- **af11** --Match packets with AF11 dscp (001010).
- **af12** --Match packets with AF12 dscp (001100).
- **af13** --Match packets with AF13 dscp (001110).
- **af21** --Match packets with AF21 dscp (010010).
- **af22** --Match packets with AF22 dscp (010100).
- **af23** --Matches the patches with the AF23 dscp (010110).
- **af31** --Matches the patches with the AF31 dscp (011010).
- **af32** --Matches the patches with the AF32 dscp (011100).

- **af33** --Matches the patches with the AF33 dscp (011110).
- **af41** --Matches the patches with the AF41 dscp (100010).
- **af42** --Matches the patches with the AF42 dscp (100100).
- **af43** --Matches the patches with the AF43 dscp (100110).
- **cs1** --Matches the patches with the CS1 (precedence 1) dscp (001000).
- **cs2** --Matches the patches with the CS2 (precedence 2) dscp (010000).
- **cs3** --Matches the patches with the CS3 (precedence 3) dscp (011000).
- **cs4** --Matches the patches with the CS4 (precedence 4) dscp (100000).
- **cs5** --Matches the patches with the CS5 (precedence 5) dscp (101000).
- **cs6** --Matches the patches with the CS6 (precedence 6) dscp (110000).
- **cs7** --Matches the patches with the CS7 (precedence 7) dscp (111000).
- **default** --Matches the patches with the default dscp (000000).
- **ef** --Matches the patches with the EF dscp (101110).

The valid values for the **eq** *port* keyword and argument are as follows:

- 0 to 65535--Port number.
- **bgp** --Border Gateway Protocol (179).
- **chargen** --Character generator (19).
- **cmd** --Remote commands (rcmd, 514).
- **daytime** --Daytime (13).
- **discard** --Discard (9).
- **domain** --Domain Name Service (53).
- **echo** --Echo (7).
- **exec** --Exec (rsh, 512).
- **finger** --Finger (79).
- **ftp** --File Transfer Protocol (21).
- **ftp-data** --FTP data connections (20).
- **gopher** --Gopher (70).
- **hostname** --NIC hostname server (101).
- **ident** --Ident Protocol (113).
- **irc** --Internet Relay Chat (194).
- **klogin** --Kerberos login (543).
- **kshell** --Kerberos shell (544).
- **login** --Login (rlogin, 513).

- **lpd** --Printer service (515).
- **nntp** --Network News Transport Protocol (119).
- **pim-auto-rp** --PIM Auto-RP (496).
- **pop2** --Post Office Protocol v2 (109).
- **pop3** --Post Office Protocol v3 (110).
- **smtp** --Simple Mail Transport Protocol (25).
- **sunrpc** --Sun Remote Procedure Call (111).
- **syslog** --Syslog (514).
- **tacacs** --TAC Access Control System (49).
- **talk** --Talk (517).
- **telnet** --Telnet (23).
- **time** --Time (37).
- **uucp** --Unix-to-Unix Copy Program (540).
- **whois** --Nicname (43).
- **www** --World Wide Web (HTTP, 80).

The valid values for the **gt** *port* keyword and argument are as follows:

- 0-65535--Port number.
- **biff** --Biff (mail notification, comsat, 512).
- **bootpc** --Bootstrap Protocol (BOOTP) client (68).
- **bootps** --Bootstrap Protocol (BOOTP) server (67).
- **discard** --Discard (9).
- **dnsix** --DNSIX security protocol auditing (195).
- **domain** --Domain Name Service (DNS, 53).
- **echo** --Echo (7).
- **isakmp** --Internet Security Association and Key Management Protocol (500).
- **mobile-ip** --Mobile IP registration (434).
- **nameserver** --IEN116 name service (obsolete, 42).
- **netbios-dgm** --NetBios datagram service (138).
- **netbios-ns** --NetBios name service (137).
- **netbios-ss** --NetBios session service (139).
- **non500-isakmp** --Internet Security Association and Key Management Protocol (4500).
- **ntp** --Network Time Protocol (123).
- **pim-auto-rp** --PIM Auto-RP (496).

- **rip** --Routing Information Protocol (router, in.routed, 520).
- **snmp** --Simple Network Management Protocol (161).
- **snmptrap** --SNMP Traps (162).
- sunrpc--Sun Remote Procedure Call (111).
- **syslog** --System Logger (514).
- **tacacs** --TAC Access Control System (49).
- **talk** --Talk (517).
- **tftp** --Trivial File Transfer Protocol (69).
- **time** --Time (37).
- **who** --Who service (rwho, 513).
- **xdmcp** --X Display Manager Control Protocol (177).

The valid values for the **lt** *port* keyword and argument are as follows:

- 0-65535--Port number.
- **biff** --Biff (mail notification, comsat, 512).
- **bootpc** --Bootstrap Protocol (BOOTP) client (68).
- **bootps** --Bootstrap Protocol (BOOTP) server (67).
- **discard** --Discard (9).
- **dnsix** --DNSIX security protocol auditing (195).
- **domain** --Domain Name Service (DNS, 53).
- **echo** --Echo (7).
- **isakmp** --Internet Security Association and Key Management Protocol (500).
- **mobile-ip** --Mobile IP registration (434).
- **nameserver** --IEN116 name service (obsolete, 42).
- **netbios-dgm** --NetBios datagram service (138).
- **netbios-ns** --NetBios name service (137).
- **netbios-ss** --NetBios session service (139).
- **non500-isakmp** --Internet Security Association and Key Management Protocol (4500).
- **ntp** --Network Time Protocol (123).
- **pim-auto-rp** --PIM Auto-RP (496).
- **rip** --Routing Information Protocol (router, in.routed, 520).
- **snmp** --Simple Network Management Protocol (161).
- **snmptrap** --SNMP Traps (162).
- **sunrpc** --Sun Remote Procedure Call (111).

- **syslog** --System Logger (514).
- **tacacs** --TAC Access Control System (49).
- **talk** --Talk (517).
- **tftp** --Trivial File Transfer Protocol (69).
- **time** --Time (37).
- **who** --Who service (rwho, 513).
- **xdmcp** --X Display Manager Control Protocol (177).

The valid values for the **neg** *port* keyword and argument are as follows:

- 0 to 65535--Port number.
- **biff** --Biff (mail notification, comsat, 512).
- **bootpc** --Bootstrap Protocol (BOOTP) client (68).
- **bootps** --Bootstrap Protocol (BOOTP) server (67).
- **discard** --Discard (9).
- **dnsix** --DNSIX security protocol auditing (195).
- **domain** --Domain Name Service (DNS, 53).
- **echo** --Echo (7).
- **isakmp** --Internet Security Association and Key Management Protocol (500).
- **mobile-ip** --Mobile IP registration (434).
- **nameserver** --IEN116 name service (obsolete, 42).
- **netbios-dgm** --NetBios datagram service (138).
- **netbios-ns** --NetBios name service (137).
- **netbios-ss** --NetBios session service (139).
- **non500-isakmp** --Internet Security Association and Key Management Protocol (4500).
- **ntp** --Network Time Protocol (123).
- **pim-auto-rp** --PIM Auto-RP (496).
- **rip** --Routing Information Protocol (router, in.routed, 520).
- **snmp** --Simple Network Management Protocol (161).
- **snmptrap** --SNMP Traps (162).
- **sunrpc** --Sun Remote Procedure Call (111).
- **syslog** --System Logger (514).
- **tacacs** --TAC Access Control System (49).
- **talk** --Talk (517).
- **tftp** --Trivial File Transfer Protocol (69).

- **time** --Time (37).
- **who** --Who service (rwho, 513).
- **xdmcp** --X Display Manager Control Protocol (177).

The valid values for the **option** *option* keyword and argument are as follows:

- 0 to 255--IP Options value.
- **add-ext** --Matches the packets with Address Extension Option (147).
- **any-options** --Matches the packets with ANY Option.
- **com-security** --Matches the packets with Commercial Security Option (134).
- **dps** --Matches the packets with Dynamic Packet State Option (151).
- **encode** --Matches the packets with Encode Option (15).
- **eool** --Matches the packets with End of Options (0).
- **ext-ip** --Matches the packets with the Extended IP Option (145).
- **ext-security** --Matches the packets with the Extended Security Option (133).
- **finn** --Matches the packets with the Experimental Flow Control Option (205).
    - **imitd**--Matches the packets with IMI Traffic Desriptor Option (144).
    - **lsr**--Matches the packets with Loose Source Route Option (131).
    - **match-all**--Matches the packets if all specified flags are present.
    - **match-any**--Matches the packets if any specified flag is present.
    - **mtup**--Matches the packets with MTU Probe Option (11).
    - **mtur**--Matches the packets with MTU Reply Option (12).
    - **no-op**--Matches the packets with No Operation Option (1).
    - **psh**--Match the packets on the PSH bit.
    - **nsapa**--Matches the packets with NSAP Addresses Option (150).
    - **reflect**--Creates reflexive access list entry.
    - **record-route**--Matches the packets with Record Route Option (7).
    - **rst**--Matches the packets on the RST bit.
    - **router-alert**--Matches the packets with Router Alert Option (148).
    - **sdb**--Matches the packets with Selective Directed Broadcast Option (149).
    - **security**--Matches the packets with Basic Security Option (130).
    - **ssr**--Matches the packets with Strict Source Routing Option (137).
    - **stream-id**--Matches the packets with Stream ID Option (136).
    - **syn**--Match the packets on the SYN bit.
- **timestamp** --Matches the packets with the Time Stamp Option (68).

- **traceroute** --Matches the packets with the Trace Route Option (82).
- **ump** --Matches the packets with the Upstream Multicast Packet Option (152).
- **visa** --Matches the packets with the Experimental Access Control Option (142).
- **zsu** --Matches the packets with the Experimental Measurement Option (10).

The valid values for the **tos** *value* keyword and argument are as follows:

- 0 to 15--Type of service value.
- **max-reliability** --Matches the packets with the maximum reliable ToS (2).
- **max-throughput** --Matches the packets with the maximum throughput ToS (4).
- **min-delay** --Matches the packets with the minimum delay ToS (8).
- **min-monetary-cost** --Matches packets with the minimum monetary cost ToS (1).
- **normal** --Matches the packets with the normal ToS (0).

Access List or OGACL Processing of Fragments

The behavior of access-list entries regarding the use or lack of the **fragments** keyword are summarized in the table below:

Table 1: Access list or OGACL Processing of Fragments

If the Access-List Entry Has...	Then...
...no **fragments** keyword (the default behavior), and assuming all of the access-list entry information matches,	For an access-list entry containing only Layer 3 information: • The entry is applied to nonfragmented packets, initial fragments, and noninitial fragments. For an access list entry containing Layer 3 and Layer 4 information: • The entry is applied to nonfragmented packets and initial fragments: • If the entry is a **permit**statement, the packet or fragment is permitted. • If the entry is a **deny**statement, the packet or fragment is denied. • The entry is also applied to noninitial fragments in the following manner. Because noninitial fragments contain only Layer 3 information, only the Layer 3 portion of an access-list entry can be applied. If the Layer 3 portion of the access-list entry matches, and • If the entry is a **permit**statement, the noninitial fragment is permitted. • If the entry is a **deny** statement, the next access-list entry is processed. **Note** The **deny** statements are handled differently for noninitial fragments versus nonfragmented or initial fragments.
...the **fragments** keyword, and assuming all of the access-list entry information matches,	**Note** The access-list entry is applied only to noninitial fragments. The **fragments** keyword cannot be configured for an access-list entry that contains any Layer 4 information.

Be aware that you should not simply add the **fragments** keyword to every access list entry because the first fragment of the IP packet is considered a nonfragment and is treated independently of the subsequent fragments. An initial fragment will not match an access list **permit** or **deny** entry that contains the **fragments**keyword, the packet is compared to the next access list entry, and so on, until it is either permitted or denied by an access list entry that does not contain the **fragments** keyword. Therefore, you may need two access list entries for every **deny** entry. The first **deny** entry of the pair will not include the **fragments** keyword, and applies to the initial fragment. The second **deny** entry of the pair will include the **fragments** keyword and applies to the subsequent fragments. In the cases where there are multiple **deny** access-list entries for the same host but with different Layer 4 ports, a single **deny** access-list entry with the **fragments** keyword for that host is all that needs to be added. Thus all the fragments of a packet are handled in the same manner by the access list.

Packet fragments of IP datagrams are considered individual packets and each counts individually as a packet in access list accounting and access list violation counts.

Note The **fragments**keyword cannot solve all cases involving access lists and IP fragments.

Fragments and Policy Routing

Fragmentation and the fragment control feature affect policy routing if the policy routing is based on the **match ip addres**s command and the access list had entries that match on Layer 4 through 7 information. It is possible that noninitial fragments pass the access list and are policy routed, even if the first fragment was not policy routed or the reverse.

By using the **fragments** keyword in access list entries as described earlier, a better match between the action taken for initial and noninitial fragments can be made and it is more likely policy routing will occur as intended.

The **portgroup** *srcport-groupname or* **portgroup** *destport-groupname*keywords and arguments allow you to create an object group based on a source or destination group.

Examples

The following example creates an access list that denies all TCP packets:

```
Router> enable
Router# configure terminal
Router(config)# ip access-list extended my_ogacl_policy
Router(config-ext-nacl)# deny tcp any any
Router(config-ext-nacl)# exit
Router(config)# exit
```

Related Commands

Command	Description
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.
show ip access-list	Displays the contents of IP access lists or OGACLs.

Command	Description
show object-group	Displays information about object groups that are configured.

deny (Catalyst 6500 series switches)

To set conditions for a named access list, use the **deny** configuration command in access-list configuration mode. To remove a deny condition from an access list, use the **no** form of this command.

deny *protocol* {*src-addr src-wildcard*| **object-group** *object-group-name*| **any**| **host** {*addr*| *name*}} {*dest-addr dest-wildcard*| **any**| **eq** *port*| **gt** *port*| **host** {*addr*| *name*}| **lt** *port*| **neq** *port*| **portgroup** *srcport-groupname*| **object-group** *dest-addr-groupname*| **range** *port*| [**dscp** *type*| **fragments**| **option** *option*| **precedence** *precedence*| **log**| **log-input**| **time-range** *time-range-name*| **tos** *tos*| **ttl** *ttl-value*]}

nodeny *protocol* {*src-addr src-wildcard*| **object-group** *object-group-name*| **any**| **host** {*addr*| *name*}} {*dest-addr dest-wildcard*| **any**| **eq** *port*| **gt** *port*| **host** {*addr*| *name*}| **lt** *port*| **neq** *port*| **portgroup** *srcport-groupname*| **object-group** *dest-addr-groupname*| **range** *port*| [**dscp** *type*| **fragments**| **option** *option*| **precedence** *precedence*| **log**| **log-input**| **time-range** *time-range-name*| **tos** *tos*| **ttl** *ttl-value*]}

Syntax Description

protocol	Name or number of a protocol; valid values are **eigrp**, **gre**, **icmp**, **igmp**, **igrp**, **ip**, **ipinip**, **nos**, **ospf**, **tcp**, or **udp**, or an integer in the range 0 to 255 representing an IP protocol number. To match any Internet protocol (including Internet Control Message Protocol (ICMP), TCP, and User Datagram Protocol (UDP), use the keyword **ip**. See the "Usage Guidelines" section for additional qualifiers.
src-addr	Number of the source network or host from which the packet is being sent in a 32-bit quantity in four-part, dotted-decimal format.
src-wildcard	Wildcard bits to be applied to source network in four-part, dotted-decimal format. Place ones in the bit positions you want to ignore.
object-group *object-group-name*	Specifies the source or destination name of the object group.
any	Specifies any source or any destination host as an abbreviation for the *source-addr*or *destination-addr value*and the *source-wildcard* or *destination-wildcard* value of 0.0.0.0 255.255.255.255.
host *addr*	Specifies the source or destination address of a single host.
host *name*	Specifies the source or destination name of a single host.
tcp	Specifies the TCP protocol.

udp	Specifies the UDP protocol.
object-group *source-addr-group-name*	Specifies the source address group name.
destination-addr	Number of the network or host to which the packet is being sent in a 32-bit quantity in four-part, dotted-decimal format.
destination-wildcard	Wildcard bits to be applied to the destination in a 32-bit quantity in four-part, dotted-decimal format. Place ones in the bit positions you want to ignore.
eq *port*	Matches only packets on a given port number; see the "Usage Guidelines" section for valid values.
gt *port*	Matches only the packets with a greater port number; see the "Usage Guidelines" section for valid values.
lt *port*	Matches only the packets with a lower port number; see the "Usage Guidelines" section for valid values.
neq *port*	Matches only the packets that are not on a given port number; see the "Usage Guidelines" section for valid values.
portgroup *srcport-group-name*	Specifies the source port object group name.
object-group *dest-addr-group-name*	Specifies the destination address group name.
portgroup *destport-group-name*	Specifies the destination port object group name.
dscp *type*	(Optional) Matches the packets with the given Differentiated Services Code Point (DSCP) value; see the "Usage Guidelines" section for valid values.
fragments	(Optional) Applies the access list entry to noninitial fragments of packets; the fragment is either permitted or denied accordingly. For more details about the **fragments** keyword, see the "Access List Processing of Fragments" and "deny, on page 33" sections in the "Usage Guidelines" section.
option *option*	(Optional) Matches the packets with the given IP options value number; see the "Usage Guidelines" section for valid values.
precedence *precedence*	(Optional) Specifies the precedence filtering level for packets; valid values are a number from 0 to 7 or by a name. See the "Usage Guidelines" section for a list of valid names.

log	(Optional) Causes an informational logging message about the packet that matches the entry to be sent to the console. (The level of messages logged to the console is controlled by the **logging console** command.) The message for a standard list includes the access list number, whether the packet was permitted or denied, the source address, and the number of packets. The message for an extended list includes the access list number; whether the packet was permitted or denied; the protocol; whether the protocol was TCP, UDP, ICMP, or a number; and, if appropriate, the source and destination addresses and source and destination port numbers. For both standard and extended lists, the message is generated for the first packet that matches, and then at 5-minute intervals, including the number of packets permitted or denied in the prior 5-minute interval. The logging facility might drop some logging message packets if there are too many to be handled or if there is more than one logging message to be handled in 1 second. This behavior prevents the router from reloading because of too many logging packets. Therefore, the logging facility should not be used as a billing tool or an accurate source of the number of matches to an access list.
log-input	(Optional) Matches the log against this entry, including the input interface.
time-range *time-range-name*	(Optional) Specifies a time-range entry name.
tos *tos*	(Optional) Specifies the service filtering level for packets; valid values are a number from 0 to 15 or by a name as listed in the “Usage Guidelines” section of the **access-list**(IP extended) command.
option option	(Optional) Matches packets with the IP options value; see the “Usage Guidelines” section for the valid values.
fragments	(Optional) Applies the access list entry to noninitial fragments of packets; the fragment is either permitted or denied accordingly. For more details about the **fragments** keyword, see the deny, on page 33 and “deny, on page 33” sections in the “Usage Guidelines” section.

ttl *ttl-value*	(Optional) Matches packets with a given Time-to-live (ttl) value.

Command Default

There is no specific condition under which a packet is denied passing the named access list.

Command Modes

Access-list configuration (config-ext-nacl)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.

Usage Guidelines

Use this command following the **ip access-list** command to specify conditions under which a packet cannot pass the named access list.

The **portgroup** keyword appears only when you configure an extended ACL

The *address* or *object-group-name* value is created using the **object-group** command.

The **addrgroup** *object-group-name*keyword and argument allow you to create logical groups of users (or servers), which you can use to define access policy using ACLs. For example, with one ACL entry you can permit the object group named engineering to access all engineering servers. Otherwise, you would need one ACL entry for every person in the engineering group.

If the operator is positioned after the *source-addr* and *source-wildcard* values, it must match the source port.

If the operator is positioned after the *destination-addr* and *destination-wildcard* values, it must match the destination port.

If you are entering the port number of a TCP or UDP port, you can enter the decimal number or name of a TCP or UDP port. A port number is a number from 0 to 65535. TCP and UDP port names are listed in the "Usage Guidelines" section of the **access-list**(IP extended) command. TCP port names can be used only when filtering TCP. UDP port names can be used only when filtering UDP.

The valid values for the **dscp** *type* keyword and argument are as follows:

- 0 to 63--Differentiated services code point value.
- **af11** --Match packets with AF11 dscp (001010).
- **af12** --Match packets with AF12 dscp (001100).
- **af13** --Match packets with AF13 dscp (001110).
- **af21** --Match packets with AF21 dscp (010010).
- **af22** --Match packets with AF22 dscp (010100).
- **af23** --Matches the patches with the AF23 dscp (010110).
- **af31** --Matches the patches with the AF31 dscp (011010).
- **af32** --Matches the patches with the AF32 dscp (011100).

- **af33** --Matches the patches with the AF33 dscp (011110).
- **af41** --Matches the patches with the AF41 dscp (100010).
- **af42** --Matches the patches with the AF42 dscp (100100).
- **af43** --Matches the patches with the AF43 dscp (100110).
- **cs1** --Matches the patches with the CS1(precedence 1) dscp (001000).
- **cs2** --Matches the patches with the CS2(precedence 2) dscp (010000).
- **cs3** --Matches the patches with the CS3(precedence 3) dscp (011000).
- **cs4** --Matches the patches with the CS4(precedence 4) dscp (100000).
- **cs5** --Matches the patches with the CS5(precedence 5) dscp (101000).
- **cs6** --Matches the patches with the CS6(precedence 6) dscp (110000).
- **cs7** --Matches the patches with the CS7(precedence 7) dscp (111000).
- **default** --Matches the patches with the default dscp (000000).
- **ef** --Matches the patches with the EF dscp (101110).

The valid values for the **eq** *port* keyword and argument are as follows:

- 0 to 65535--Port number.
- **bgp** --Border Gateway Protocol (179).
- **chargen** --Character generator (19).
- **cmd** --Remote commands (rcmd, 514).
- **daytime** --Daytime (13).
- **discard** --Discard (9).
- **domain** --Domain Name Service (53).
- **echo** --Echo (7).
- **exec** --Exec (rsh, 512).
- **finger** --Finger (79).
- **ftp** --File Transfer Protocol (21).
- **ftp-data** --FTP data connections (20).
- **gopher** --Gopher (70).
- **hostname** --NIC hostname server (101).
- **ident** --Ident Protocol (113).
- **irc** --Internet Relay Chat (194).
- **klogin** --Kerberos login (543).
- **kshell** --Kerberos shell (544).
- **login** --Login (rlogin, 513).

- **lpd** --Printer service (515).
- **nntp** --Network News Transport Protocol (119).
- **pim-auto-rp** --PIM Auto-RP (496).
- **pop2** --Post Office Protocol v2 (109).
- **pop3** --Post Office Protocol v3 (110).
- **smtp** --Simple Mail Transport Protocol (25).
- **sunrpc** --Sun Remote Procedure Call (111).
- **syslog** --Syslog (514).
- **tacacs** --TAC Access Control System (49).
- **talk** --Talk (517).
- **telnet** --Telnet (23).
- **time** --Time (37).
- **uucp** --Unix-to-Unix Copy Program (540).
- **whois** --Nicname (43).
- **www** --World Wide Web (HTTP, 80).

The valid values for the **gt** *port* keyword and argument are as follows:

- 0-65535--Port number.
- **biff** --Biff (mail notification, comsat, 512).
- **bootpc** --Bootstrap Protocol (BOOTP) client (68).
- **bootps** --Bootstrap Protocol (BOOTP) server (67).
- **discard** --Discard (9).
- **dnsix** --DNSIX security protocol auditing (195).
- **domain** --Domain Name Service (DNS, 53).
- **echo** --Echo (7).
- **isakmp** --Internet Security Association and Key Management Protocol (500).
- **mobile-ip** --Mobile IP registration (434).
- **nameserver** --IEN116 name service (obsolete, 42).
- **netbios-dgm** --NetBios datagram service (138).
- **netbios-ns** --NetBios name service (137).
- **netbios-ss** --NetBios session service (139).
- **non500-isakmp** --Internet Security Association and Key Management Protocol (4500).
- **ntp** --Network Time Protocol (123).
- **pim-auto-rp** --PIM Auto-RP (496).

- **rip** --Routing Information Protocol (router, in.routed, 520).
- **snmp** --Simple Network Management Protocol (161).
- **snmptrap** --SNMP Traps (162).
- sunrpc--Sun Remote Procedure Call (111).
- **syslog** --System Logger (514).
- **tacacs** --TAC Access Control System (49).
- **talk** --Talk (517).
- **tftp** --Trivial File Transfer Protocol (69).
- **time** --Time (37).
- **who** --Who service (rwho, 513).
- **xdmcp** --X Display Manager Control Protocol (177).

The valid values for the **lt** *port* keyword and argument are as follows:

- 0-65535--Port number.
- **biff** --Biff (mail notification, comsat, 512).
- **bootpc** --Bootstrap Protocol (BOOTP) client (68).
- **bootps** --Bootstrap Protocol (BOOTP) server (67).
- **discard** --Discard (9).
- **dnsix** --DNSIX security protocol auditing (195).
- **domain** --Domain Name Service (DNS, 53).
- **echo** --Echo (7).
- **isakmp** --Internet Security Association and Key Management Protocol (500).
- **mobile-ip** --Mobile IP registration (434).
- **nameserver** --IEN116 name service (obsolete, 42).
- **netbios-dgm** --NetBios datagram service (138).
- **netbios-ns** --NetBios name service (137).
- **netbios-ss** --NetBios session service (139).
- **non500-isakmp** --Internet Security Association and Key Management Protocol (4500).
- **ntp** --Network Time Protocol (123).
- **pim-auto-rp** --PIM Auto-RP (496).
- **rip** --Routing Information Protocol (router, in.routed, 520).
- **snmp** --Simple Network Management Protocol (161).
- **snmptrap** --SNMP Traps (162).
- sunrpc--Sun Remote Procedure Call (111).

- **syslog** --System Logger (514).
- **tacacs** --TAC Access Control System (49).
- **talk** --Talk (517).
- **tftp** --Trivial File Transfer Protocol (69).
- **time** --Time (37).
- **who** --Who service (rwho, 513).
- **xdmcp** --X Display Manager Control Protocol (177).

The valid values for the **neg** *port* keyword and argument are as follows:

- 0 to 65535--Port number.
- **biff** --Biff (mail notification, comsat, 512).
- **bootpc** --Bootstrap Protocol (BOOTP) client (68).
- **bootps** --Bootstrap Protocol (BOOTP) server (67).
- **discard** --Discard (9).
- **dnsix** --DNSIX security protocol auditing (195).
- **domain** --Domain Name Service (DNS, 53).
- **echo** --Echo (7).
- **isakmp** --Internet Security Association and Key Management Protocol (500).
- **mobile-ip** --Mobile IP registration (434).
- **nameserver** --IEN116 name service (obsolete, 42).
- **netbios-dgm** --NetBios datagram service (138).
- **netbios-ns** --NetBios name service (137).
- **netbios-ss** --NetBios session service (139).
- **non500-isakmp** --Internet Security Association and Key Management Protoc (4500).
- **ntp** --Network Time Protocol (123).
- **pim-auto-rp** --PIM Auto-RP (496).
- **rip** --Routing Information Protocol (router, in.routed, 520).
- **snmp** --Simple Network Management Protocol (161).
- **snmptrap** --SNMP Traps (162).
- **sunrpc** --Sun Remote Procedure Call (111).
- **syslog** --System Logger (514).
- **tacacs** --TAC Access Control System (49).
- **talk** --Talk (517).
- **tftp** --Trivial File Transfer Protocol (69).

- **time** --Time (37).
- **who** --Who service (rwho, 513).
- **xdmcp** --X Display Manager Control Protocol (177).

The valid values for the **option** *option* keyword and argument are as follows:

- 0 to 255--IP Options value.
- **add-ext** --Matches the packets with Address Extension Option (147).
- **any-options** --Matches the packets with ANY Option.
- **com-security** --Matches the packets with Commercial Security Option (134).
- **dps** --Matches the packets with Dynamic Packet State Option (151).
- **encode** --Matches the packets with Encode Option (15).
- **eool** --Matches the packets with End of Options (0).
- **ext-ip** --Matches the packets with the Extended IP Option (145).
- **ext-security** --Matches the packets with the Extended Security Option (133).
- **finn** --Matches the packets with the Experimental Flow Control Option (205).
    - **imitd**--Matches the packets with IMI Traffic Desriptor Option (144).
    - **lsr**--Matches the packets with Loose Source Route Option (131).
    - **match-all**--Matches the packets if all specified flags are present.
    - **match-any**--Matches the packets if any specified flag is present.
    - **mtup**--Matches the packets with MTU Probe Option (11).
    - **mtur**--Matches the packets with MTU Reply Option (12).
    - **no-op**--Matches the packets with No Operation Option (1).
    - **psh**--Match the packets on the PSH bit.
    - **nsapa**--Matches the packets with NSAP Addresses Option (150).
    - **reflect**--Creates reflexive access list entry.
    - **record-route**--Matches the packets with Record Route Option (7).
    - **rst**--Matches the packets on the RST bit.
    - **router-alert**--Matches the packets with Router Alert Option (148).
    - **sdb**--Matches the packets with Selective Directed Broadcast Option (149).
    - **security**--Matches the packets with Basic Security Option (130).
    - **ssr**--Matches the packets with Strict Source Routing Option (137).
    - **stream-id**--Matches the packets with Stream ID Option (136).
    - **syn**--Match the packets on the SYN bit.
- **timestamp** --Matches the packets with the Time Stamp Option (68).

- **traceroute** --Matches the packets with the Trace Route Option (82).
- **ump** --Matches the packets with the Upstream Multicast Packet Option (152).
- **visa** --Matches the packets with the Experimental Access Control Option (142).
- **zsu** --Matches the packets with the Experimental Measurement Option (10).

The valid values for the **tos** *value* keyword and argument are as follows:

- 0 to 15--Type of service value.
- **max-reliability** --Matches the packets with the maximum reliable ToS (2).
- **max-throughput** --Matches the packets with the maximum throughput ToS (4).
- **min-delay** --Matches the packets with the minimum delay ToS (8).
- **min-monetary-cost** --Matches packets with the minimum monetary cost ToS (1).
- **normal** --Matches the packets with the normal ToS (0).

Access List Processing of Fragments

The behavior of access-list entries regarding the use or lack of the **fragments** keyword are summarized in the table below:

Table 2: Access list Processing of Fragments

If the Access-List Entry Has...	Then...
...no **fragments** keyword (the default behavior), and assuming all of the access-list entry information matches,	For an access-list entry containing only Layer 3 information: • The entry is applied to nonfragmented packets, initial fragments, and noninitial fragments. For an access list entry containing Layer 3 and Layer 4 information: • The entry is applied to nonfragmented packets and initial fragments: • If the entry is a **permit**statement, the packet or fragment is permitted. • If the entry is a **deny**statement, the packet or fragment is denied. • The entry is also applied to noninitial fragments in the following manner. Because noninitial fragments contain only Layer 3 information, only the Layer 3 portion of an access-list entry can be applied. If the Layer 3 portion of the access-list entry matches, and • If the entry is a **permit**statement, the noninitial fragment is permitted. • If the entry is a **deny** statement, the next access-list entry is processed. **Note** The **deny** statements are handled differently for noninitial fragments versus nonfragmented or initial fragments.
...the **fragments** keyword, and assuming all of the access-list entry information matches,	**Note** The access-list entry is applied only to noninitial fragments.The **fragments** keyword cannot be configured for an access-list entry that contains any Layer 4 information.

Be aware that you should not simply add the **fragments** keyword to every access list entry because the first fragment of the IP packet is considered a nonfragment and is treated independently of the subsequent fragments. An initial fragment will not match an access list **permit** or **deny** entry that contains the **fragments**keyword, the packet is compared to the next access list entry, and so on, until it is either permitted or denied by an access list entry that does not contain the **fragments** keyword. Therefore, you may need two access list entries for every **deny** entry. The first **deny** entry of the pair will not include the **fragments** keyword, and applies to the initial fragment. The second **deny** entry of the pair will include the **fragments** keyword and applies to the subsequent fragments. In the cases where there are multiple **deny** access-list entries for the same host but with different Layer 4 ports, a single **deny** access-list entry with the **fragments** keyword for that host is all that needs to be added. Thus all the fragments of a packet are handled in the same manner by the access list.

Packet fragments of IP datagrams are considered individual packets and each counts individually as a packet in access list accounting and access list violation counts.

Note The **fragments**keyword cannot solve all cases involving access lists and IP fragments.

Fragments and Policy Routing

Fragmentation and the fragment control feature affect policy routing if the policy routing is based on the **match ip addres**s command and the access list had entries that match on Layer 4 through 7 information. It is possible that noninitial fragments pass the access list and are policy routed, even if the first fragment was not policy routed or the reverse.

By using the **fragments** keyword in access list entries as described earlier, a better match between the action taken for initial and noninitial fragments can be made and it is more likely policy routing will occur as intended.

The **portgroup** *srcport-groupname or* **portgroup** *destport-groupname*keywords and arguments allow you to create an object group based on a source or destination group.

Examples

The following example creates an access list that denies all TCP packets:

```
Router(config)# ip access-list extended my-pbacl-policy
Router(config-ext-nacl)# deny tcp any any
Router(config-ext-nacl)# exit
Router(config)# exit
```

Related Commands

Command	Description
ip access-group	Controls access to an interface.
ip access-list	Defines an IP access list by name.
logging console	Limits messages logged to the console based on severity.
object-group	Defines object groups to optimize your configuration
permit (Catalyst 6500 series switches)	Sets conditions for a named IP access list.
show ip access-lists	Displays the contents of all current IP access lists.

deny (IP)

To set conditions in a named IP access list that will deny packets, use the **deny** command in access list configuration mode. To remove a deny condition from an access list, use the **no** form of this command.

[*sequence-number*] **deny** *source* [*source-wildcard*]

[*sequence-number*] **deny** *protocol source source-wildcard destination destination-wildcard* [**option** *option-name*] [**precedence** *precedence*] [**tos** *tos*] [**ttl** *operator value*] **[log]** [**time-range** *time-range-name*] **[fragments]**

no *sequence-number*

no deny *source* [*source-wildcard*]

no deny *protocol source source-wildcard destination destination-wildcard*

Internet Control Message Protocol (ICMP)

[*sequence-number*] **deny icmp** *source source-wildcard destination destination-wildcard* [*icmp-type* [*icmp-code*]| *icmp-message*] [**precedence** *precedence*] [**tos** *tos*] [**ttl** *operator value*] **[log]** [**time-range** *time-range-name*] **[fragments]**

Internet Group Management Protocol (IGMP)

[*sequence-number*] **deny igmp** *source source-wildcard destination destination-wildcard* [*igmp-type*] [**precedence** *precedence*] [**tos** *tos*] [**ttl** *operator value*] **[log]** [**time-range** *time-range-name*] **[fragments]**

Transmission Control Protocol (TCP)

[sequence-number] deny tcp *source source-wildcard* [*operator port* [*port*]] *destination destination-wildcard* [*operator* [*port*]] [**established** {**match-any**| **match-all**} {+-} *flag-name*| **precedence** *precedence*| **tos** *tos*| **ttl** *operator value*| **log**| **time-range** *time-range-name*| **fragments**]

User Datagram Protocol (UDP)

[*sequence-number*] **deny udp** *source source-wildcard* [*operator port* [*port*]] *destination destination-wildcard* [*operator* [*port*]] [**precedence** *precedence*] [**tos** *tos*] [**ttl** *operator value*] **[log]** [**time-range** *time-range-name*] **[fragments]**

Syntax Description

sequence-number	(Optional) Sequence number assigned to the deny statement. The sequence number causes the system to insert the statement in that numbered position in the access list.

source	Number of the network or host from which the packet is being sent. There are three alternative ways to specify the source: • Use a 32-bit quantity in four-part dotted-decimal format. • Use the **any**keyword as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255. • Use **host** *source*as an abbreviation for a *source*and *source-wildcard*of *source*0.0.0.0.
source-wildcard	Wildcard bits to be applied to the source . There are three alternative ways to specify the source wildcard: • Use a 32-bit quantity in four-part dotted-decimal format. Place 1s in the bit positions that you want to ignore. • Use the **any**keyword as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255. • Use **host** *source*as an abbreviation for a *source*and *source-wildcard*of *source*0.0.0.0.
protocol	Name or number of an Internet protocol. The *protocol* argument can be one of the keywords **eigrp**, **gre**, **icmp**, **igmp**, **ip**, **ipinip**, **nos**, **ospf**, **tcp**, or **udp**, or an integer in the range from 0 to 255 representing an Internet protocol number. To match any Internet protocol (including ICMP, TCP, and UDP), use the **ip**keyword. **Note** When the **icmp**, **igmp**, **tcp,** and **udp** keywords are entered, they must be followed with the specific command syntax that is shown for the ICMP, IGMP, TCP, and UDP forms of the **deny** command.
icmp	Denies only ICMP packets. When you enter the **icmp** keyword, you must use the specific command syntax shown for the ICMP form of the **deny** command.
igmp	Denies only IGMP packets. When you enter the **igmp** keyword, you must use the specific command syntax shown for the IGMP form of the **deny** command.
tcp	Denies only TCP packets. When you enter the **tcp** keyword, you must use the specific command syntax shown for the TCP form of the **deny** command.

udp	Denies only UDP packets. When you enter the **udp** keyword, you must use the specific command syntax shown for the UDP form of the **deny** command.
destination	Number of the network or host to which the packet is being sent. There are three alternative ways to specify the destination: • Use a 32-bit quantity in four-part dotted-decimal format. • Use the **any**keyword as an abbreviation for the *destination*and *destination-wildcard*of 0.0.0.0 255.255.255.255. • Use **host** *destination* as an abbreviation for a *destination*and *destination-wildcard* of *destination* 0.0.0.0.
destination-wildcard	Wildcard bits to be applied to the destination. There are three alternative ways to specify the destination wildcard: • Use a 32-bit quantity in four-part dotted-decimal format. Place 1s in the bit positions that you want to ignore. • Use the **any** keyword as an abbreviation for a *destination*and *destination-wildcard* of 0.0.0.0 255.255.255.255. • Use **host** *destination* as an abbreviation for a *destination*and *destination-wildcard* of *destination* 0.0.0.0.
option *option-name*	(Optional) Packets can be filtered by IP Options, as specified by a number from 0 to 255 or by the corresponding IP Option name, as listed in the table in the "Usage Guidelines" section.
precedence *precedence*	(Optional) Packets can be filtered by precedence level, as specified by a number from 0 to 7 or by a name.
tos *tos*	(Optional) Packets can be filtered by type of service (ToS) level, as specified by a number from 0 to 15, or by a name as listed in the "Usage Guidelines" section of the **access-list**(IP extended) command.

ttl *operator value*	(Optional) Compares the TTL value in the packet to the TTL value specified in this **deny** statement. • The *operator* can be **lt** (less than), **gt** (greater than), **eq** (equal), **neq** (not equal), or **range** (inclusive range). • The *value* can range from 0 to 255. • If the operator is **range**, specify two values separated by a space. • For Release 12.0S, if the operator is **eq** or **neq**, only one TTL value can be specified. • For all other releases, if the operator is **eq** or **neq**, as many as 10 TTL values can be specified, separated by a space. If the TTL in the packet matches just one of the possibly 10 values, the entry is considered to be matched.
log	(Optional) Causes an informational logging message about the packet that matches the entry to be sent to the console. (The level of messages logged to the console is controlled by the **logging console** command.)
time-range *time-range-name*	(Optional) Name of the time range that applies to this **deny** statement. The name of the time range and its restrictions are specified by the **time-range** and **absolute** or **periodic** commands, respectively.
fragments	(Optional) The access list entry applies to noninitial fragments of packets; the fragment is either permitted or denied accordingly. For more details about the **fragments** keyword, see the “deny (IP), on page 58” and “deny (IP), on page 58” sections in the “Usage Guidelines” section.
icmp-type	(Optional) ICMP packets can be filtered by ICMP message type. The type is a number from 0 to 255.
icmp-code	(Optional) ICMP packets that are filtered by ICMP message type can also be filtered by the ICMP message code. The code is a number from 0 to 255.
icmp-message	(Optional) ICMP packets can be filtered by an ICMP message type name or an ICMP message type and code name. The possible names are listed in the “Usage Guidelines” section of the **access-list**(IP extended) command.

igmp-type	(Optional) IGMP packets can be filtered by IGMP message type or message name. A message type is a number from 0 to 15. IGMP message names are listed in the "Usage Guidelines" section of the **access-list**(IP extended) command.
operator	(Optional) Compares source or destination ports. Operators include **lt** (less than), **gt** (greater than), **eq** (equal), **neq** (not equal), and **range** (inclusive range). If the operator is positioned after the source and source-wildcard arguments, it must match the source port. If the operator is positioned after the destination and destination-wildcard arguments, it must match the destination port. The range operator requires two port numbers. Up to ten port numbers can be entered for the **eq** (equal) and **neq** (not equal) operators. All other operators require one port number.
port	(Optional) The decimal number or name of a TCP or UDP port. A port number is a number from 0 to 65535. TCP and UDP port names are listed in the "Usage Guidelines" section of the **access-list**(IP extended) command. TCP port names can be used only when filtering TCP. UDP port names can be used only when filtering UDP.
established	(Optional) For the TCP protocol only: Indicates an established connection. A match occurs if the TCP datagram has the ACK or RST bit set. The nonmatching case is that of the initial TCP datagram to form a connection. **Note** The **established** keyword can be used only with the old command-line interface (CLI) format. To use the new CLI format, you must use the **match-any** or **match-all** keywords followed by the + or **-** keywords and *flag-name* argument.

match-any | **match-all**	(Optional) For the TCP protocol only: A match occurs if the TCP datagram has certain TCP flags set or not set. You use the **match-any**keyword to allow a match to occur if any of the specified TCP flags are present, or you can use the **match-all**keyword to allow a match to occur only if all of the specified TCP flags are present. You must follow the **match-any**and **match-all**keywords with the +or **-**keyword and the *flag-name*argument to match on one or more TCP flags.
+ | **-** *flag-name*	(Optional) For the TCP protocol only: The + keyword allows IP packets if their TCP headers contain the TCP flags that are specified by the *flag-name* argument. The **-** keyword filters out IP packets that do not contain the TCP flags specified by the *flag-name* argument. You must follow the + and **-** keywords with the *flag-name* argument. TCP flag names can be used only when filtering TCP. Flag names for the TCP flags are as follows: **urg**, **ack**, **psh**, **rst**, **syn**, and **fin**.

Command Default

There are no specific conditions under which a packet is denied passing the named access list.

Command Modes

Access list configuration

Command History

Release	Modification
11.2	This command was introduced.
12.0(1)T	The **time-range** *time-range-name*keyword and argument were added.
12.0(11)	The **fragments**keyword was added.
12.2(13)T	The igrp keyword was removed because the IGRP protocol is no longer available in Cisco IOS software.
12.2(14)S	The *sequence-number*argument was added.
12.2(15)T	The *sequence-number*argument was added.
12.3(4)T	The **option** *option-name* keyword and argument were added. The **match-any**, **match-all,** +,and **-**keywords and the *flag-name* argument were added.
12.3(7)T	Command functionality was modified to allow up to ten port numbers to be added after the **eq** and **neq** operators so that an access list entry can be created with noncontiguous ports.

Release	Modification
12.4(2)T	The **ttl** *operator value* keyword and arguments were added.
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.
12.2SX	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 following the **ip access-list** command to specify conditions under which a packet cannot pass the named access list.

The **time-range** keyword allows you to identify a time range by name. The **time-range**, **absolute**, and **periodic** commands specify when this **deny** statement is in effect.

log Keyword

A log message includes the access list number, whether the packet was permitted or denied; the protocol, whether it was TCP, UDP, ICMP, or a number; and, if appropriate, the source and destination addresses and source and destination port numbers. The message is generated for the first packet that matches, and then at 5-minute intervals, including the number of packets permitted or denied in the prior 5-minute interval.

Use the **ip access-list log-update** command to generate logging messages when the number of matches reaches a configurable threshold (rather than waiting for a 5-minute-interval). See the **ip access-list log-update** command for more information.

The logging facility might drop some logging message packets if there are too many to be handled or if there is more than one logging message to be handled in 1 second. This behavior prevents the router from crashing because of too many logging packets. Therefore, the logging facility should not be used as a billing tool or an accurate source of the number of matches to an access list.

If you enable Cisco Express Forwarding (CEF) and then create an access list that uses the **log** keyword, the packets that match the access list are not CEF-switched. They are fast-switched. Logging disables CEF.

Access List Filtering of IP Options

Access control lists can be used to filter packets with IP Options to prevent routers from being saturated with spurious packets containing IP Options. To see a complete table of all IP Options, including ones currently not in use, refer to the latest Internet Assigned Numbers Authority (IANA) information that is available from its URL: www.iana.org.

Cisco IOS software allows you to filter packets according to whether they contain one or more of the legitimate IP Options by entering either the IP Option value or the corresponding name for the *option-name* argument as shown in the table below.

Table 3: IP Option Values and Names

IP Option Value or Name	Description
0 to 255	IP Options values.

IP Option Value or Name	Description
add-ext	Match packets with Address Extension Option (147).
any-options	Match packets with any IP Option.
com-security	Match packets with Commercial Security Option (134).
dps	Match packets with Dynamic Packet State Option (151).
encode	Match packets with Encode Option (15).
eool	Match packets with End of Options (0).
ext-ip	Match packets with Extended IP Options (145).
ext-security	Match packets with Extended Security Option (133).
finn	Match packets with Experimental Flow Control Option (205).
imitd	Match packets with IMI Traffic Descriptor Option (144).
lsr	Match packets with Loose Source Route Option (131).
mtup	Match packets with MTU Probe Option (11).
mtur	Match packets with MTU Reply Option (12).
no-op	Match packets with No Operation Option (1).
nsapa	Match packets with NSAP Addresses Option (150).
psh	Matches the packets on the PSH bit.
record-route	Match packets with Router Record Route Option (7).
reflect	Creates reflexive access list entry.
rst	Matches the packets on the RST bit.
router-alert	Match packets with Router Alert Option (148).
sdb	Match packets with Selective Directed Broadcast Option (149).
security	Match packets with Base Security Option (130).

IP Option Value or Name	Description
ssr	Match packets with Strict Source Routing Option (137).
stream-id	Match packets with Stream ID Option (136).
syn	Matches the packets on the SYN bit.
timestamp	Match packets with Time Stamp Option (68).

Filtering IP Packets Based on TCP Flags

The access list entries that make up an access list can be configured to detect and drop unauthorized TCP packets by allowing only the packets that have very specific groups of TCP flags set or not set. Users can select any desired combination of TCP flags with which to filter TCP packets. Users can configure access list entries in order to allow matching on a flag that is set and on a flag that is not set. Use the **+** and **-** keywords with a flag name to specify that a match is made based on whether a TCP header flag has been set. Use the **match-any** and **match-all** keywords to allow the packet if any or all, respectively, of the flags specified by the + or **-** keyword and *flag-name* argument have been set or not set.

Access List Processing of Fragments

The behavior of access list entries regarding the use or lack of use of the **fragments** keyword can be summarized as follows:

If the Access-List Entry Has...	Then...
...no **fragments** keyword (the default behavior), and assuming all of the access-list entry information matches,	For an access list entry that contains only Layer 3 information: • The entry is applied to nonfragmented packets, initial fragments, and noninitial fragments. For an access list entry that contains Layer 3 and Layer 4 information: • The entry is applied to nonfragmented packets and initial fragments. • If the entry is a **permit**statement, then the packet or fragment is permitted. • If the entry is a **deny**statement, then the packet or fragment is denied. • The entry is also applied to noninitial fragments in the following manner. Because noninitial fragments contain only Layer 3 information, only the Layer 3 portion of an access list entry can be applied. If the Layer 3 portion of the access list entry matches, and • If the entry is a **permit**statement, then the noninitial fragment is permitted. • If the entry is a **deny** statement, then the next access list entry is processed. **Note** The **deny** statements are handled differently for noninitial fragments versus nonfragmented or initial fragments.
...the **fragments** keyword, and assuming all of the access-list entry information matches,	The access list entry is applied only to noninitial fragments. The **fragments** keyword cannot be configured for an access list entry that contains any Layer 4 information.

Be aware that you should not add the **fragments** keyword to every access list entry because the first fragment of the IP packet is considered a nonfragment and is treated independently of the subsequent fragments. An initial fragment will not match an access list **permit** or **deny** entry that contains the **fragments**keyword. The packet is compared to the next access list entry, and so on, until it is either permitted or denied by an access list entry that does not contain the **fragments** keyword. Therefore, you may need two access list entries for every **deny** entry. The first **deny** entry of the pair will not include the **fragments** keyword and applies to the initial fragment. The second **deny** entry of the pair will include the **fragments** keyword and applies to the subsequent fragments. In the cases in which there are multiple **deny** access list entries for the same host but with different Layer 4 ports, a single **deny** access list entry with the **fragments** keyword for that host is all that needs to be added. Thus all the fragments of a packet are handled in the same manner by the access list.

Packet fragments of IP datagrams are considered individual packets, and each counts individually as a packet in access list accounting and access list violation counts.

Note The **fragments**keyword cannot solve all cases that involve access lists and IP fragments.

Fragments and Policy Routing

Fragmentation and the fragment control feature affect policy routing if the policy routing is based on the **match ip address** command and the access list has entries that match on Layer 4 through 7 information. It is possible that noninitial fragments pass the access list and are policy-routed, even if the first fragment is not policy-routed.

By using the **fragments** keyword in access list entries as described earlier, a better match between the action taken for initial and noninitial fragments can be made, and it is more likely that policy routing will occur as intended.

Creating an Access List Entry with Noncontiguous Ports

For Cisco IOS Release 12.3(7)T and later releases, you can specify noncontiguous ports on the same access control entry, which greatly reduces the number of access list entries required for the same source address, destination address, and protocol. If you maintain large numbers of access list entries, we recommend that you consolidate them when possible by using noncontiguous ports. You can specify up to ten port numbers following the **eq** and **neq** operators.

Examples

The following example sets conditions for a standard access list named Internetfilter:

```
ip access-list standard Internetfilter
 deny 192.168.34.0  0.0.0.255
 permit 172.16.0.0  0.0.255.255
 permit 10.0.0.0  0.255.255.255
! (Note: all other access implicitly denied.)
```

The following example denies HTTP traffic on Monday through Friday from 8:00 a.m. to 6:00 p.m.:

```
time-range no-http
 periodic weekdays 8:00 to 18:00
!
ip access-list extended strict
 deny tcp any any eq http time-range no-http
!
interface ethernet 0
 ip access-group strict in
```

The following example adds an entry with the sequence number 25 to extended IP access list 150:

```
ip access-list extended 150
 25 deny ip host 172.16.3.3 host 192.168.5.34
```

The following example removes the entry with the sequence number 25 from the extended access list example shown above:

```
 no 25
```

The following example sets a deny condition for an extended access list named filter2. The access list entry specifies that a packet cannot pass the named access list if it contains the Strict Source Routing IP Option, which is represented by the IP option value ssr.

```
ip access-list extended filter2
 deny ip any any option ssr
```

The following example sets a deny condition for an extended access list named kmdfilter1. The access list entry specifies that a packet cannot pass the named access list if the RST and FIN TCP flags have been set for that packet:

```
ip access-list extended kmdfilter1
 deny tcp any any match-any +rst +fin
```

The following example shows several **deny** statements that can be consolidated into one access list entry with noncontiguous ports. The **show access-lists** command is entered to display a group of access list entries for the access list named abc.

```
Router# show access-lists abc
Extended IP access list abc
 10 deny tcp any eq telnet any eq 450
 20 deny tcp any eq telnet any eq 679
 30 deny tcp any eq ftp any eq 450
 40 deny tcp any eq ftp any eq 679
```

Because the entries are all for the same **deny** statement and simply show different ports, they can be consolidated into one new access list entry. The following example shows the removal of the redundant access list entries and the creation of a new access list entry that consolidates the previously displayed group of access list entries:

```
ip access-list extended abc
 no 10
 no 20
 no 30
 no 40
 deny tcp any eq telnet ftp any eq 450 679
```

The following examples shows the creation of the consolidated access list entry:

```
Router# show access-lists abc
Extended IP access list abc
 10 deny tcp any eq telnet ftp any eq 450 679
```

The following access list filters IP packets containing Type of Service (ToS) level 3 with TTL values 10 and 20. It also filters IP packets with a TTL greater than 154 and applies that rule to noninitial fragments. It permits IP packets with a precedence level of flash and a TTL not equal to 1, and sends log messages about such packets to the console. All other packets are denied.

```
ip access-list extended canton
 deny ip any any tos 3 ttl eq 10 20
 deny ip any any ttl gt 154 fragments
 permit ip any any precedence flash ttl neq 1 log
```

Related Commands

Command	Description
absolute	Specifies an absolute time when a time range is in effect.
access-list (IP extended)	Defines an extended IP access list.
access-list (IP standard)	Defines a standard IP access list.
ip access-group	Controls access to an interface.
ip access-list	Defines an IP access list by name.

Command	Description
ip access-list log-update	Sets the threshold number of packets that cause a logging message.
ip access-list resequence	Applies sequence numbers to the access list entries in an access list.
ip options	Drops or ignores IP Options packets that are sent to the router.
logging console	Sends system logging (syslog) messages to all available TTY lines and limits messages based on severity.
match ip address	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, or performs policy routing on packets.
periodic	Specifies a recurring (weekly) time range for functions that support the time-range feature.
permit (IP)	Sets conditions under which a packet passes a named IP access list.
remark	Writes a helpful comment (remark) for an entry in a named IP access list.
show access-lists	Displays a group of access-list entries.
show ip access-list	Displays the contents of all current IP access lists.
time-range	Specifies when an access list or other feature is in effect.

deny (IPv6)

To set deny conditions for an IPv6 access list, use the **deny** command in IPv6 access list configuration mode. To remove the deny conditions, use the **no** form of this command.

deny *protocol* {*source-ipv6-prefix/prefix-length*| **any**| **host** *source-ipv6-address*| **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length*| **any**| **host** *destination-ipv6-address*| **auth**} [*operator* [*port-number*]] [**dest-option-type** [*doh-number*| *doh-type*]] [**dscp** *value*] [**flow-label** *value*] **[fragments] [hbh] [log] [log-input] [mobility]** [**mobility-type** [*mh-number*| *mh-type*]] **[routing]** [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*] **[undetermined-transport]**

no deny *protocol* {*source-ipv6-prefix/prefix-length*| **any**| **host** *source-ipv6-address*| **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length*| **any**| **host** *destination-ipv6-address*| **auth**} [*operator* [*port-number*]] [**dest-option-type** [*doh-number*| *doh-type*]] [**dscp** *value*] [**flow-label** *value*] **[fragments] [hbh] [log] [log-input] [mobility]** [**mobility-type** [*mh-number*| *mh-type*]] **[routing]** [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*] **[undetermined-transport]**

Internet Control Message Protocol

deny icmp {*source-ipv6-prefix/prefix-length*| **any**| **host** *source-ipv6-address*| **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length*| **any**| **host** *destination-ipv6-address*| **auth**} [*operator* [*port-number*]] [*icmp-type* [*icmp-code*]| *icmp-message*] [**dest-option-type** [*doh-number*| *doh-type*]] [**dscp** *value*] [**flow-label** *value*] **[fragments] [hbh] [log] [log-input] [mobility]** [**mobility-type** [*mh-number*| *mh-type*]] **[routing]** [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*]

Transmission Control Protocol

deny tcp {*source-ipv6-prefix/prefix-length*| **any**| **host** *source-ipv6-address*| **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length*| **any**| **host** *destination-ipv6-address*| **auth**} [*operator* [*port-number*]] **[ack]** [**dest-option-type** [*doh-number*| *doh-type*]] [**dscp** *value*] **[established] [fin]** [**flow-label** *value*] **[fragments] [hbh] [log] [log-input] [mobility]** [**mobility-type** [*mh-number*| *mh-type*]] [**neq** {*port*| *protocol*}] **[psh]** [**range** {*port*| *protocol*}] **[routing]** [**routing-type** *routing-number*] **[rst]** [**sequence** *value*] **[syn]** [**time-range** *name*] **[urg]**

User Datagram Protocol

deny udp {*source-ipv6-prefix/prefix-length*| **any**| **host** *source-ipv6-address*| **auth**} [*operator* [*port-number*]] {*destination-ipv6-prefix/prefix-length*| **any**| **host** *destination-ipv6-address*| **auth**} [*operator* [*port-number*]] [**dest-option-type** [*doh-number*| *doh-type*]] [**dscp** *value*] [**flow-label** *value*] **[fragments] [hbh] [log] [log-input] [mobility]** [**mobility-type** [*mh-number*| *mh-type*]] [**neq** {*port*| *protocol*}] [**range** {*port*| *protocol*}] **[routing]** [**routing-type** *routing-number*] [**sequence** *value*] [**time-range** *name*]

Syntax Description

protocol	Name or number of an Internet protocol. It can be one of the keywords **ahp**, **esp**, **icmp**, **ipv6**, **pcp**, **sctp**, **tcp**, **udp**, or **hbh**, or an integer in the range from 0 to 255 representing an IPv6 protocol number.

source-ipv6-prefix/prefix-length	The source IPv6 network or class of networks about which to set deny conditions. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
any	An abbreviation for the IPv6 prefix ::/0.
host *source-ipv6-address*	The source IPv6 host address about which to set deny conditions. This *source-ipv6-address* argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
operator [*port-number*]	(Optional) Specifies an operand that compares the source or destination ports of the specified protocol. Operands are **lt** (less than), **gt** (greater than), **eq** (equal), **neq** (not equal), and **range** (inclusive range). If the operator is positioned after the *source-ipv6-prefix/prefix-length* argument, it must match the source port. If the operator is positioned after the *destination-ipv6/prefix-length* argument, it must match the destination port. The **range** operator requires two port numbers. All other operators require one port number. The optional *port-number* argument is a decimal number or the name of a TCP or UDP port. A port number is a number from 0 to 65535. TCP port names can be used only when filtering TCP. UDP port names can be used only when filtering UDP.
destination-ipv6-prefix/prefix-length	The destination IPv6 network or class of networks about which to set deny conditions. This argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.
host *destination-ipv6-address*	The destination IPv6 host address about which to set deny conditions. This *destination-ipv6-address* argument must be in the form documented in RFC 2373 where the address is specified in hexadecimal using 16-bit values between colons.

auth	Allows matching traffic against the presence of the authentication header in combination with any protocol.
dest-option-type	(Optional) Matches IPv6 packets against the hop-by-hop option extension header within each IPv6 packet header.
doh-number	(Optional) Integer in the range from 0 to 255 representing an IPv6 destination option extension header.
doh-type	(Optional) Destination option header types. The possible destination option header type and its corresponding *doh-number* value are home-address—201.
dscp *value*	(Optional) Matches a differentiated services code point value against the traffic class value in the Traffic Class field of each IPv6 packet header. The acceptable range is from 0 to 63.
flow-label *value*	(Optional) Matches a flow label value against the flow label value in the Flow Label field of each IPv6 packet header. The acceptable range is from 0 to 1048575.
fragments	(Optional) Matches non-initial fragmented packets where the fragment extension header contains a non-zero fragment offset. The **fragments** keyword is an option only if the *operator* [*port-number*] arguments are not specified.
hbh	(Optional) Specifies a hop-by-hop options header.
log	(Optional) Causes an informational logging message about the packet that matches the entry to be sent to the console. (The level of messages logged to the console is controlled by the **logging console** command.) The message includes the access list name and sequence number, whether the packet was denied; the protocol, whether it was TCP, UDP, ICMP, or a number; and, if appropriate, the source and destination addresses and source and destination port numbers. The message is generated for the first packet that matches, and then at 5-minute intervals, including the number of packets denied in the prior 5-minute interval.

log-input	(Optional) Provides the same function as the **log** keyword, except that the logging message also includes the input interface.
mobility	(Optional) Extension header type. Allows matching of any IPv6 packet including a mobility header, regardless of the value of the mobility-header-type field within that header.
mobility-type	(Optional) Mobility header type. Either the *mh-number* or *mh-type* argument must be used with this keyword.
mh-number	(Optional) Integer in the range from 0 to 255 representing an IPv6 mobility header type.
mh-type	(Optional) Name of a mobility header type. Possible mobility header types and their corresponding *mh-number* value are as follows: • 0—bind-refresh • 1—hoti • 2—coti • 3—hot • 4—cot • 5—bind-update • 6—bind-acknowledgment • 7—bind-error
routing	(Optional) Matches source-routed packets against the routing extension header within each IPv6 packet header.
routing-type	(Optional) Allows routing headers with a value in the type field to be matched independently. The *routing-number* argument must be used with this keyword.
routing-number	Integer in the range from 0 to 255 representing an IPv6 routing header type. Possible routing header types and their corresponding *routing-number* value are as follows: • 0—Standard IPv6 routing header • 2—Mobile IPv6 routing header

sequence *value*	(Optional) Specifies the sequence number for the access list statement. The acceptable range is from 1 to 4294967295.
time-range *name*	(Optional) Specifies the time range that applies to the deny statement. The name of the time range and its restrictions are specified by the **time-range** and **absolute** or **periodic** commands, respectively.
undetermined-transport	(Optional) Matches packets from a source for which the Layer 4 protocol cannot be determined. The **undetermined-transport** keyword is an option only if the *operator* [*port-number*] arguments are not specified.
icmp-type	(Optional) Specifies an ICMP message type for filtering ICMP packets. ICMP packets can be filtered by ICMP message type. The ICMP message type can be a number from 0 to 255, some of which include the following predefined strings and their corresponding numeric values: • 144—dhaad-request • 145—dhaad-reply • 146—mpd-solicitation • 147—mpd-advertisement
icmp-code	(Optional) Specifies an ICMP message code for filtering ICMP packets. ICMP packets that are filtered by ICMP message type can also be filtered by the ICMP message code. The code is a number from 0 to 255.
icmp-message	(Optional) Specifies an ICMP message name for filtering ICMP packets. ICMP packets can be filtered by an ICMP message name or ICMP message type and code. The possible names are listed in the "Usage Guidelines" section.
ack	(Optional) For the TCP protocol only: acknowledgment (ACK) bit set.
established	(Optional) For the TCP protocol only: Indicates an established connection. A match occurs if the TCP datagram has the ACK or RST bits set. The nonmatching case is that of the initial TCP datagram to form a connection.

fin	(Optional) For the TCP protocol only: Fin bit set; no more data from sender.
neq {*port* | *protocol*}	(Optional) Matches only packets that are not on a given port number.
psh	(Optional) For the TCP protocol only: Push function bit set.
range {*port* | *protocol*}	(Optional) Matches only packets in the range of port numbers.
rst	(Optional) For the TCP protocol only: Reset bit set.
syn	(Optional) For the TCP protocol only: Synchronize bit set.
urg	(Optional) For the TCP protocol only: Urgent pointer bit set.

Command Default

No IPv6 access list is defined.

Command Modes

IPv6 access list configuration (config-ipv6-acl)#

Command History

Release	Modification
12.0(23)S	This command was introduced.
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.
12.4(2)T	The *icmp-type* argument was enhanced. The **dest-option-type**, **mobility**, **mobility-type**, and **routing-type** keywords were added. The *doh-number*, *doh-type*, *mh-number*, *mh-type*, and *routing-number* arguments 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.
12.2(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 introduced on Cisco ASR 1000 Aggregation Series Routers.

Release	Modification
12.4(20)T	The **auth** keyword was added.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE.
15.2(3)T	This command was modified. Support was added for the **hbh** keyword.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The **deny** (IPv6) command is similar to the **deny** (IP) command, except that it is IPv6-specific.

Use the **deny** (IPv6) command following the **ipv6 access-list** command to define the conditions under which a packet passes the access list or to define the access list as a reflexive access list.

Specifying IPv6 for the *protocol* argument matches against the IPv6 header of the packet.

By 1default, the first statement in an access list is number 10, and the subsequent statements are numbered in increments of 10.

You can add **permit**, **deny**, **remark**, or **evaluate** statements to an existing access list without retyping the entire list. To add a new statement anywhere other than at the end of the list, create a new statement with an appropriate entry number that falls between two existing entry numbers to indicate where it belongs.

In Cisco IOS Release 12.2(2)T or later releases, 12.0(21)ST, and 12.0(22)S, IPv6 access control lists (ACLs) are defined and their deny and permit conditions are set by using the **ipv6 access-list** command with the **deny** and **permit** keywords in global configuration mode. In Cisco IOS Release 12.0(23)S or later releases, IPv6 ACLs are defined by using the **ipv6 access-list** command in global configuration mode and their permit and deny conditions are set by using the **deny** and **permit** commands in IPv6 access list configuration mode. Refer to the **ipv6 access-list** command for more information on defining IPv6 ACLs.

Note In Cisco IOS Release 12.0(23)S or later releases, every IPv6 ACL has implicit **permit icmp any any nd-na**, **permit icmp any any nd-ns**, and **deny ipv6 any any** statements as its last match conditions. (The former two match conditions allow for ICMPv6 neighbor discovery.) An IPv6 ACL must contain at least one entry for the implicit **deny ipv6 any any** statement to take effect. The IPv6 neighbor discovery process makes use of the IPv6 network layer service; therefore, by default, IPv6 ACLs implicitly allow IPv6 neighbor discovery packets to be sent and received on an interface. In IPv4, the Address Resolution Protocol (ARP), which is equivalent to the IPv6 neighbor discovery process, makes use of a separate data link layer protocol; therefore, by default, IPv4 ACLs implicitly allow ARP packets to be sent and received on an interface.

Both the *source-ipv6-prefix/prefix-length* and *destination-ipv6-prefix/prefix-length* arguments are used for traffic filtering (the source prefix filters traffic based upon the traffic source; the destination prefix filters traffic based upon the traffic destination).

Note IPv6 prefix lists, not access lists, should be used for filtering routing protocol prefixes.

The **fragments** keyword is an option only if the *operator* [*port-number*] arguments are not specified.

The **undetermined-transport** keyword is an option only if the *operator* [*port-number*] arguments are not specified.

The following is a list of ICMP message names:

- beyond-scope
- destination-unreachable
- echo-reply
- echo-request
- header
- hop-limit
- mld-query
- mld-reduction
- mld-report
- nd-na
- nd-ns
- next-header
- no-admin
- no-route
- packet-too-big
- parameter-option
- parameter-problem
- port-unreachable
- reassembly-timeout
- renum-command
- renum-result
- renum-seq-number
- router-advertisement
- router-renumbering
- router-solicitation
- time-exceeded
- unreachable

Examples

The following example configures the IPv6 access list named toCISCO and applies the access list to outbound traffic on Ethernet interface 0. Specifically, the first deny entry in the list keeps all packets that have a destination

TCP port number greater than 5000 from exiting out of Ethernet interface 0. The second deny entry in the list keeps all packets that have a source UDP port number less than 5000 from exiting out of Ethernet interface 0. The second deny also logs all matches to the console. The first permit entry in the list permits all ICMP packets to exit out of Ethernet interface 0. The second permit entry in the list permits all other traffic to exit out of Ethernet interface 0. The second permit entry is necessary because an implicit deny all condition is at the end of each IPv6 access list.

```
ipv6 access-list toCISCO
 deny tcp any any gt 5000
 deny ::/0 lt 5000 ::/0 log
 permit icmp any any
 permit any any
interface ethernet 0
 ipv6 traffic-filter toCISCO out
```

The following example shows how to allow TCP or UDP parsing although an IPsec AH is present:

```
IPv6 access list example1
    deny tcp host 2001::1 any log sequence 5
    permit tcp any any auth sequence 10
    permit udp any any auth sequence 20
```

Related Commands

Command	Description
ipv6 access-list	Defines an IPv6 access list and enters IPv6 access list configuration mode.
ipv6 traffic-filter	Filters incoming or outgoing IPv6 traffic on an interface.
permit (IPv6)	Sets permit conditions for an IPv6 access list.
show ipv6 access-list	Displays the contents of all current IPv6 access lists.

deny (MAC ACL)

To set conditions for a MAC access list, use the **deny** command in MAC access-list extended configuration mode. To remove a condition from an access list, use the **no** form of this command.

deny {*src_mac_mask*| **host name** *src_mac_name*| **any**} {*dest_mac_mask*| **host name** *dst_mac_name*| **any**} [{*protocol_keyword*| *ethertype_number ethertype_mask*} [**vlan** *vlan_ID*] [**cos** *cos_value*]]

no deny {*src_mac_mask*| **host name** *src_mac_name*| **any**} {*dest_mac_mask*| **host name** *dst_mac_name*| **any**} [{*protocol_keyword*| *ethertype_number ethertype_mask*} [**vlan** *vlan_ID*] [**cos** *cos_value*]]

Syntax Description

src_mac_mask	Specifies the MAC address mask that identifies a selected block of source MAC addresses. A value of 1 represents a wildcard in that position.
host name *src_mac_name*	Specifies a source host that has been named using the **mac host name** command.
any	Specifies any source or any destination host as an abbreviation for the *src_mac_mask*or *dest_mac_mask*value of 1111.1111.1111, which declares all digits to be wildcards .
dest_mac_mask	Specifies the MAC address mask that identifies a selected block of destination MAC addresses.
host name *dst_mac_name*	Specifies a destination host that has been named using the **mac host name** command.
protocol_keyword	(Optional) Specifies a named protocol (for example, ARP).
ethertype_number	(Optional) The EtherType number specifies the protocol within the Ethernet packet.
ethertype_mask	(Optional) The EtherType mask allows a range of EtherTypes to be specified together. This is a hexadecimal number from 0 to FFFF. An EtherType mask of 0 requires an exact match of the EtherType.
vlan *vlan_ID*	(Optional) Specifies a VLAN.
cos *cos_value*	(Optional) Specifies the Layer 2 priority level for packets. The range is from 0 to 7.

Command Default

This command has no defaults.

Command Modes

MAC access-list extended configuration (config-ext-macl)

Command History

Release	Modification
12.2(33)SXI	This command was introduced.

Usage Guidelines

Use this command following the **ip access-list** command to define the conditions under which a packet passes the access list.

- The **vlan** and **cos** keywords are not supported in MAC ACLs used for VACL filtering.
- The **vlan** keyword for VLAN-based QoS filtering in MAC ACLs can be globally enabled or disabled and is disabled by default.
- Enter MAC addresses as three 2-byte values in dotted hexadecimal format. For example, 0123.4567.89ab.
- Enter MAC address masks as three 2-byte values in dotted hexadecimal format. Use 1 bits as wildcards. For example, to match an address exactly, use 0000.0000.0000 (can be entered as 0.0.0).
- An entry without a protocol parameter matches any protocol.
- Enter an EtherType and an EtherType mask as hexadecimal values from 0 to FFFF.
- This list shows the EtherType values and their corresponding protocol keywords:
    - 0x0600--xns-idp--Xerox XNS IDP
    - 0x0BAD--vines-ip--Banyan VINES IP
    - 0x0baf--vines-echo--Banyan VINES Echo
    - 0x6000--etype-6000--DEC unassigned, experimental
    - 0x6001--mop-dump--DEC Maintenance Operation Protocol (MOP) Dump/Load Assistance
    - 0x6002--mop-console--DEC MOP Remote Console
    - 0x6003--decnet-iv--DEC DECnet Phase IV Route
    - 0x6004--lat--DEC Local Area Transport (LAT)
    - 0x6005--diagnostic--DEC DECnet Diagnostics
    - 0x6007--lavc-sca--DEC Local-Area VAX Cluster (LAVC), SCA
    - 0x6008--amber--DEC AMBER
    - 0x6009--mumps--DEC MUMPS
    - 0x0800--ip--Malformed, invalid, or deliberately corrupt IP frames
    - 0x8038--dec-spanning--DEC LANBridge Management
    - 0x8039--dsm--DEC DSM/DDP
    - 0x8040--netbios--DEC PATHWORKS DECnet NETBIOS Emulation

- 0x8041--msdos--DEC Local Area System Transport
- 0x8042--etype-8042--DEC unassigned
- 0x809B--appletalk--Kinetics EtherTalk (AppleTalk over Ethernet)
- 0x80F3--aarp--Kinetics AppleTalk Address Resolution Protocol (AARP)

Examples

This example shows how to create a MAC-Layer ACL named mac_layer that denies dec-phase-iv traffic with source address 0000.4700.0001 and destination address 0000.4700.0009, but allows all other traffic:

```
Router(config)# mac access-list extended mac_layer

Router(config-ext-macl)# deny 0000.4700.0001 0.0.0 0000.4700.0009 0.0.0 dec-phase-iv

Router(config-ext-macl)# permit any any
```

Related Commands

Command	Description
permit (MAC ACL)	Sets permit conditions for a named MAC access list.
mac access-list extended	Defines a MAC access list by name.
mac host	Assigns a name to a MAC address.
show mac access-group	Displays the contents of all current MAC access groups.

deny (WebVPN)

To set conditions in a named Secure Sockets Layer Virtual Private Network (SSL VPN) access list that will deny packets, use the **deny** command in webvpn acl configuration mode. To remove a deny condition from an access list, use the **no** form of this command.

deny [**url** [**any**| *url-string*]] [**ip| tcp| udp| http| https| cifs**] [**any**| *source-ip source-mask*] [**any**| *destination-ip destination-mask*] [**time-range** *time-range-name*] **[syslog]**

no deny url [**any**| *url-string*] [**ip| tcp| udp| http| https| cifs**] [**any**| *source-ip source-mask*] [**any**| *destination-ip destination-mask*] [**time-range** *time-range-name*] **[syslog]**

Syntax Description

url	(Optional) Filtering rules are applied to the URL. • Use the **any** keyword as an abbreviation for any URL.
url-string	(Optional) URL string defined as follows: **scheme://host[:port][/path]** • **scheme** --Can be HTTP, Secure HTTPS (HTTPS), or Common Internet File System (CIFS). This field is required in the URL string. • **host** --Can be a hostname or a host IP (host mask). The host can have one wildcard (*). • **port** --Can be any valid port number (1-65535). It is possible to have multiple port numbers separated by a comma (,). The port range is expressed using a dash (-). • **path** --Can be any valid path string. In the path string, the $user is translated to the current user name.
ip	(Optional) Denies only IP packets. When you enter the **ip** keyword, you must use the specific command syntax shown for the IP form of the deny command.
tcp	(Optional) Denies only TCP packets. When you enter the **tcp** keyword, you must use the specific command syntax shown for the TCP form of the deny command.
udp	(Optional) Denies only UDP packets. When you enter the **udp** keyword, you must use the specific command syntax shown for the UDP form of the deny command.

http	(Optional) Denies only HTTP packets. When you enter the **http** keyword, you must use the specific command syntax shown for the HTTP form of the deny command.
https	(Optional) Denies only HTTPS packets. When you enter the **https** keyword, you must use the specific command syntax shown for the HTTPS form of the deny command.
cifs	(Optional) Denies only CIFS packets. When you enter the **cifs**keyword, you must use the specific command syntax shown for the CIFS form of the deny command.
source-ip source-mask	(Optional) Number of the network or host from which the packet is being sent. There are three alternative ways to specify the source: • Use a 32-bit quantity in four-part dotted-decimal format. • Use the **any** keyword as an abbreviation for a source and source mask of 0.0.0.0 255.255.255.255. • Use **host** source as an abbreviation for a source and source-wildcard of source 0.0.0.0.
destination-ip destination-mask	(Optional) Number of the network or host to which the packet is being sent. There are three alternative ways to specify the destination: • Use a 32-bit quantity in four-part dotted-decimal format. • Use the **any** keyword as an abbreviation for a source and source mask of 0.0.0.0 255.255.255.255. • Use **host** source as an abbreviation for a source and source-wildcard of source 0.0.0.0.
time-range *time-range-name*	(Optional) Name of the time range that applies to this **deny** statement. The name of the time range and its restrictions are specified by the **time-range** and **absolute** or **periodic** commands, respectively.
syslog	(Optional) System logging messages are generated.

Command Default

There are no specific conditions under which a packet is denied passing the named access list.

Command Modes

Webvpn acl configuration

Command History

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

Usage Guidelines

Use this command following the **acl** command to specify conditions under which a packet cannot pass the named access list.

The **time-range** keyword allows you to identify a time range by name. The **time-range**, **absolute**, and **periodic** commands specify when this deny statement is in effect.

Examples

The following example shows that all packets from the URL “https://10.168.2.228:34,80-90,100-/public” will be denied:

```
webvpn context context1
 acl acl1
```

deny url “https://10.168.2.228:34,80-90,100-/public”

Related Commands

Command	Description
absolute	Specifies an absolute time for a time range.
periodic	Specifies a recurring (weekly) time range for functions that support the time-range feature.
permit (webvpn acl)	Sets conditions to allow a packet to pass a named SSL VPN access list.
time-range	Enables time-range configuration mode and defines time ranges for functions (such as extended access lists).

description (dot1x credentials)

To specify a description for an 802.1X profile, use the **description** command in dot1x credentials configuration mode. To remove the description, use the **no** form of this command.

description *text*

no description

Syntax Description

text	Text description. The description can be up to 80 characters.

Command Default

A description 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.

An 802.1X credential structure is necessary when configuring a supplicant (client). This credentials structure may contain a username, password, and description.

Examples

The following example shows which credentials profile should be used when configuring a supplicant, and it provides a description of the credentials profile:

```
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 which 802.1X credentials profile to use.

description (identify zone)

To enter a description of a zone, use the **description** command in security zone configuration mode. To remove the description of the zone, use the **no** form of this command.

description *line-of-description*

no description *line-of-description*

Syntax Description

line-of-description	Description of the zone. You can enter up to 40 characters.

Command Default

None

Command Modes

Security zone configuration

Command History

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

Usage Guidelines

You can use this subcommand after entering the **zone security** or **zone-pair security**command.

Examples

The following example specifies that zone z1 is a testzone:

```
zone security z1
 description testzone
```

Related Commands

Command	Description
zone-pair security	Creates a zone-pair that is the type security.
zone security	Creates a zone.

description (identity policy)

To enter a description for an identity policy, use the **description** command in identity policy configuration mode. To remove the description, use the **no** form of this command.

description *line-of-description*

no description *line-of-description*

Syntax Description

line-of-description	Description of the identity policy.

Command Default

A description is not entered for the identity policy.

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.

Examples

The following example shows that a default identity policy and its description ("policyname1") have been specified:

```
Router (config)# identity policy policyname1
Router (config-identity-policy)# description policyABC
```

Related Commands

Command	Description
description (identity profile)	Enters a description for an identity profile.

description (identity profile)

To enter a description for an identity profile, use the **description** command in identity profile configuration mode. To remove the description of the identity profile, use the **no** form of this command.

description *line-of-description*

no description *line-of-description*

Syntax Description

line-of-description	Description of the identity profile.

Command Default

A description is not entered for the identity profile.

Command Modes

Identity profile configuration (config-identity-prof)

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.
12.3(8)T	This command was previously configured in dot1x configuration mode.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

The **identity profile**command and one of its keywords (**default**, **dot1x**, or **eapoudp**) must be entered in global configuration mode before the **description** command can be used.

Examples

The following example shows that a default identity profile and its description ("ourdefaultpolicy") have been specified:

```
Router (config)# identity profile default
Router (config-identity-prof)# description ourdefaultpolicy
```

Related Commands

Command	Description
description (identity policy)	Enters a description for an identity policy.
identity profile	Creates an identity profile and enters identity profile configuration mode.

description (IKEv2 keyring)

To add the description of an Internet Key Exchange Version 2 (IKEv2) peer or profile, use the **description** command in the IKEv2 keyring peer configuration mode. To delete the description, use the **no** form of this command.

description *line-of-description*

no description *line-of-description*

Syntax Description

line-of-description	Description given to an IKE peer or profile.

Command Default

The peer or profile is not described.

Command Modes

IKEv2 keyring peer configuration (config-ikev2-keyring-peer)

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 provide a descriptive line about the IKEv2 peer, peer group, or profile.

Examples

The following example shows that the description “connection from site A” has been added to an IKEv2 peer:

```
Router(config)# crypto ikev2 keyring keyr 1
Router(configikev2-keyring)# peer peer1
Router(config-ikev2-keyring-peer)# description connection from site A
```

Related Commands

Command	Description
address (ikev2 keyring)	Specifies the IPv4 address or the range of the peers in IKEv2 keyring.
crypto ikev2 keyring	Defines an IKEv2 keyring.

Command	Description
hostname (ikev2 keyring)	Specifies the hostname for the peer in the IKEv2 keyring.
identity (ikev2 keyring)	Identifies the peer with IKEv2 types of identity.
peer	Defines a peer or a peer group for the keyring.
pre-shared-key **(ikev2 keyring)**	Defines a preshared key for the IKEv2 peer.

description (isakmp peer)

To add the description of an Internet Key Exchange (IKE) peer, use the **description** command in ISAKMP peer configuration mode. To delete the description, use the **no** form of this command.

description *line-of-description*

no description *line-of-description*

Syntax Description

line-of-description	Description given to an IKE peer.

Command Default

No default behavior or values

Command Modes

ISAKMP peer configuration

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.

Usage Guidelines

IKE peers that "sit" behind a Network Address Translation (NAT) device cannot be uniquely identified; therefore, they have to share the same peer description.

Examples

The following example shows that the description "connection from site A" has been added for an IKE peer:

```
Router# crypto isakmp peer address 10.2.2.9
Router (config-isakmp-peer)# description connection from site A
```

Related Commands

Command	Description
clear crypto session	Deletes crypto sessions (IPSec and IKE SAs).
show crypto isakmp peer	Displays peer descriptions.
show crypto session	Displays status information for active crypto sessions in a router.

destination host

To configure the fully qualified domain name (FQDN) of a Diameter peer, use the **destination host**command in diameter peer configuration submode. To disable the configured FQDN, use the **no** form of this command.

destination host *string*

no destination host *string*

Syntax Description

string	The FQDN of the Diameter peer.

Command Default

No FQDN is configured.

Command Modes

Diameter peer configuration

Command History

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

Examples

The following example shows how to configure the destination host:

```
Router(config-dia-peer)# destination host
 host1.example.com.
```

Related Commands

Command	Description
destination realm	Configures the destination realm of a Diameter peer.
diameter peer	Configures a Diameter peer and enters Diameter peer configuration submode.

destination realm

To configure the destination realm of a Diameter peer, use the **destination realm**command in diameter peer configuration submode. To disable the configured realm, use the **no** form of this command.

destination realm *string*

no destination realm *string*

Syntax Description

string	The destination realm (part of the domain @*realm*) in which a Diameter peer is located.

Command Default

No realm is configured.

Command Modes

Diameter peer configuration

Command History

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

Usage Guidelines

The realm might be added by the authentication, authorization, and accounting (AAA) client when sending a request to AAA. However, if the client does not add the attribute, then the value configured while in Diameter peer configuration submode is used when sending messages to the destination Diameter peer. If a value is not configured while in Diameter peer configuration submode, the value specified by the **diameter destination realm**global configuration command is used.

Examples

The following example shows how to configure the destination realm:

```
router (config-dia-peer)# destination realm
 example.com
```

Related Commands

Command	Description
diameter destination realm	Configures a global Diameter destination realm.
diameter peer	Configures a Diameter peer and enters Diameter peer configuration submode.

device (identity profile)

To statically authorize or reject individual devices, use the **device** command in identity profile configuration mode. To disable the authorization or rejection, use the **no** form of this command.

device {**authorize** {**ip address** *ip-address* **policy** *policy-name*| **mac-address** *mac-address*| **type** {**cisco**| **ip**| **phone**}}| **not-authorize**}

no device {**authorize** {**ip address** *ip-address* **policy** *policy-name*| **mac-address** *mac-address*| **type** {**cisco**| **ip**| **phone**}}| **not-authorize**}

Syntax Description

authorize	Configures an authorized device.
ip address	Specifies a device by its IP address.
ip-address	The IP address.
policy	Applies an associated policy with the device.
policy-name	Name of the policy.
mac-address	Specifies a device by its MAC address.
mac-address	The MAC address.
type	Specifies a device by its type.
cisco	Specifies a Cisco device.
ip	Specifies an IP device.
phone	Specifies a Cisco IP phone.
not-authorize	Configures an unauthorized device.

Command Default

A device is not statically authorized or rejected.

Command Modes

Identity profile configuration (config-identity-prof)

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.

Release	Modification
12.3(8)T	The **unauthorize** keyword was changed to **not authorize**. The *cisco-device* argument was deleted. The **ip address** keyword and *ip-address* argument were added. The **ip** and **phone** keywords were added.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

The **identity profile**command and **default**, **dot1x**, or **eapoudp** keywords must be entered in global configuration mode before the **device** command can be used.

Examples

The following configuration example defines an identity profile for Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP) to statically authorize host 192.168.1.3 with "policyname1" as the associated identity policy:

```
Router(config)# identity profile eapoudp
Router(config-identity-prof)# device authorize ip-address 192.168.1.3 policy policyname1
```

Related Commands

Command	Description
identity profile eapoudp	Creates an identity profile.

device-role

To specify the role of the device attached to the port, use the **device-role** command in neighbor discovery (ND) inspection policy configuration mode or router advertisement (RA) guard policy configuration mode.

device-role {**host**| **monitor**| **router**}

Syntax Description

host	Sets the role of the device to host.
monitor	Sets the role of the device to monitor.
router	Sets the role of the device to router.

Command Default

The device role is host.

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.
15.2(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 **device-role** command specifies the role of the device attached to the port. By default, the device role is host, and therefore all the inbound router advertisement and redirect messages are blocked. If the device role is enabled using the **router** keyword, all messages (router solicitation [RS], router advertisement [RA], or redirect) are allowed on this port.

When the **router** or **monitor** keyword is used, the multicast RS messages are bridged on the port, regardless of whether limited broadcast is enabled. However, the **monitor** keyword does not allow inbound RA or redirect messages. When the **monitor** keyword is used, devices that need these messages will receive them.

Note

With the introduction of Cisco IOS Release 15.2(4)S1, the trusted port has precedence over the device role for accepting RAs over a port to the router. Prior to this release, the device role router had precedence over the trusted port. The device role of the router still needs to be configured in order for the RS to be sent over the port.

Examples

The following example defines a Neighbor Discovery Protocol (NDP) policy name as policy1, places the device in ND inspection policy configuration mode, and configures the device as the host:

```
Router(config)# ipv6 nd inspection policy policy1
Router(config-nd-inspection)# device-role host
```

The following example defines an RA guard policy name as raguard1, places the device in RA guard policy configuration mode, and configures the device as the host:

```
Router(config)# ipv6 nd raguard policy raguard1
Router(config-ra-guard)# device-role host
```

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.

device-sensor accounting

To add device sensor protocol data to accounting records and to generate accounting events when new sensor data is detected, use the **device-sensor accounting** command in global configuration mode. To disable adding device sensor protocol data to accounting records and to disable generating accounting events, use the **no** form of this command.

device-sensor accounting

no device-sensor accounting

Syntax Description

This command has no arguments or keywords.

Command Default

The device sensor protocol data is added to the accounting records and accounting events are generated when new sensor data is detected.

Command Modes

Global configuration (config)

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

The device sensor is used to glean endpoint information from Cisco Discovery Protocol (CDP), Link Layer Discovery Protocol (LLDP), and DHCP messages and make this information available to registered clients in the context of an access session. You can use the **device-sensor accounting** command to include the data gleaned by the device sensor in RADIUS accounting messages.

Examples

The following example shows how to add the device sensor protocol data to accounting records:

```
Device> enable
Device# configure terminal
Device(config)# device-sensor accounting
Device(config)# end
```

Related Commands

Command	Description
debug device-sensor	Enables debugging for the device sensor.
show device-sensor cache	Displays device sensor cache entries.

device-sensor filter-list cdp

To create a Cisco Discovery Protocol filter containing a list of Type-Length-Value (TLV) fields that can be included or excluded in the device sensor output, use the **device-sensor filter-list cdp** command in global configuration mode. To remove the Cisco Discovery Protocol filter containing the list of TLV fields, use the **no** form of this command.

device-sensor filter-list cdp list *tlv-list-name*

no device-sensor filter-list cdp list *tlv-list-name*

Syntax Description

list	Specifies a Cisco Discovery Protocol TLV filter list.
tlv-list-name	Cisco Discovery Protocol TLV filter list name.

Command Default

Cisco Discovery Protocol TLV filter list is not available.

Command Modes

Global configuration (config)

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 **device-sensor filter-list cdp list** *tlv-list-name* command to configure the name of the Cisco Discovery Protocol TLV filter list and enter Cisco Discovery Protocol sensor configuration mode. You can configure the list of TLVs in Cisco Discovery Protocol sensor configuration mode using the **tlv** {**name** *tlv-name* | **number** *tlv-number*} command. Use the **name** *tlv-name* keyword-argument pair to specify the name of the TLV. Enter **?** for querying the available TLV names. Use the **number** *tlv-name* keyword-argument pair to specify the TLV number to be added to the Cisco Discovery Protocol TLV filter list.

Use the **no tlv** {**name** *tlv-name* | **number** *tlv-number*} command to remove individual TLVs from the Cisco Discovery Protocol TLV filter list.

Use the **no device-sensor filter-list cdp list** *tlv-list-name* command to remove the entire TLV list containing all the TLVs.

Examples

The following example shows how to create a Cisco Discovery Protocol filter containing a list of TLVs:

```
Device> enable
Device# configure terminal
```

```
Device(config)# device-sensor filter-list cdp list cdp-list
Device(config-sensor-cdplist)# tlv name address-type
Device(config-sensor-cdplist)# tlv name device-name
Device(config-sensor-cdplist)# tlv number 34
Device(config-sensor-cdplist)# end
```

Related Commands

Command	Description
debug device-sensor	Enables debugging for the 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 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.
show device-sensor cache	Displays device sensor cache entries.

device-sensor filter-list dhcp

To create a DHCP filter containing a list of options that can be included or excluded in the device sensor output, use the **device-sensor filter-list dhcp** command in global configuration mode. To remove the DHCP filter containing the list of options, use the **no** form of this command.

device-sensor filter-list dhcp list *option-list-name*

no device-sensor filter-list dhcp list *option-list-name*

Syntax Description

list	Specifies a DHCP options filter list.
option-list-name	Name of DHCP options filter list.

Command Default

DHCP options filter list is not available.

Command Modes

Global configuration (config)

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 **device-sensor filter-list dhcp list** *option-list-name* command to configure the name of the DHCP options filter list and enter into DHCP sensor configuration mode. You can configure the list of options in DHCP sensor configuration mode using the **option** {**name** *option-name* | **number** *option-number*} command. Use the **name** *option-name* keyword-argument pair to specify the name of the TLV. Enter **?** for querying the available TLV names. Use the **number** *option-name* keyword-argument pair to specify the TLV number to be added to the DHCP options filter list.

Use the **no option** {**name** *option-name* | **number** *option-number*} command to remove individual options from the DHCP options filter list.

Use the **no device-sensor filter-list dhcp list** *option-list-name* command to remove the entire TLV list containing all the TLVs.

Examples

The following example shows how to create a DHCP filter containing a list of options:

```
Device> enable
Device# configure terminal
Device(config)# device-sensor filter-list dhcp list dhcp-list
Device(config-sensor-dhcplist)# option name address-type
Device(config-sensor-dhcplist)# option name device-name
Device(config-sensor-dhcplist)# option number 34
Device(config-sensor-dhcplist)# end
```

Related Commands

Command	Description
debug device-sensor	Enables debugging for the 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 TLV fields 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.
show device-sensor cache	Displays device sensor cache entries.

device-sensor filter-list lldp

To create a Link Layer Discovery Protocol (LLDP) filter containing a list of Type-Length-Value (TLV) fields that can be included or excluded in the device sensor output, use the **device-sensor filter-list lldp** command in global configuration mode. To remove the LLDP filter containing the list of TLV fields, use the **no** form of this command.

device-sensor filter-list lldp list *tlv-list-name*

no device-sensor filter-list lldp list *tlv-list-name*

Syntax Description

list	Specifies an LLDP TLV filter list.
tlv-list-name	Name of the LLDP TLV filter list.

Command Default

LLDP TLV filter list is not available.

Command Modes

Global configuration (config)

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 **device-sensor filter-list lldp list** *tlv-list-name* command to configure the name of the LLDP TLV filter list and enter LLDP sensor configuration mode. You can configure the list of TLVs in LLDP sensor configuration mode using the **tlv** {**name** *tlv-name* | **number** *tlv-number*} command. Use the **name** *tlv-name* keyword-argument pair to specify the name of the TLV. Enter **?** for querying the available TLV names. Use the **number** *tlv-name* keyword-argument pair to specify the TLV number to be added to the LLDP TLV filter list.

Use the **no tlv** {**name** *tlv-name* | **number** *tlv-number*} command to remove individual TLVs from the LLDP TLV filter list.

Use the **no device-sensor filter-list lldp list** *tlv-list-name* command to remove the entire TLV list containing all the TLVs.

Examples

The following example shows how to create an LLDP filter containing a list of TLVs:

```
Device> enable
Device# configure terminal
```

```
Device(config)# device-sensor filter-list lldp list lldp-list
Device(config-sensor-lldplist)# tlv name address-type
Device(config-sensor-lldplist)# tlv name device-name
Device(config-sensor-lldplist)# tlv number 34
Device(config-sensor-lldplist)# end
```

Related Commands

Command	Description
debug device-sensor	Enables debugging for the 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 TLV fields 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.
show device-sensor cache	Displays device sensor cache entries.

device-sensor filter-spec

To apply a specific protocol filter containing a list of Type-Length-Value (TLV) fields to the device sensor output, use the **device-sensor filter-spec** command in global configuration mode. To remove the protocol filter list from the device sensor output, use the **no** form of this command.

device-sensor filter-spec {**cdp** | **dhcp** | **lldp**} {**exclude** {**all** | **list** *list-name*} | **include list** *list-name*}

no device-sensor filter-spec {**cdp** | **dhcp** | **lldp**} {**exclude** {**all** | **list** *list-name*} | **include list** *list-name*}

Syntax Description

cdp	Applies a Cisco Discovery Protocol TLV filter list to the device sensor output.
dhcp	Applies a DHCP TLV filter list to the device sensor output.
lldp	Applies a Link Layer Discovery Protocol (LLDP) TLV filter list to the device sensor output.
exclude	Specifies the TLVs that should be excluded from the device sensor output.
all	Disables all notifications for the associated protocol.
list *list-name*	Specifies the name of the protocol TLV filter list.
include	Specifies the TLVs that should be included in the device sensor output.

Command Default

All TLVs are included in notifications and will trigger notifications.

Command Modes

Global configuration (config)

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 **device-sensor filter-spec** command to specify the TLVs that must be included in all sensor outputs (session notifications sent to internal sensor clients and accounting requests).

Certain TLVs and message types such as DISCOVER, OFFER, REQUEST, ACK, and IP addresses are excluded because they are used as transport for higher layer protocols and will change frequently without conveying any useful information about the endpoint.

OFFER messages will also be ignored as they may be received from multiple servers and will not convey any useful endpoint data.

Examples

The following example shows how to apply a Cisco Discovery Protocol TLV filter list to the device sensor output:

```
Device> enable
Device# configure terminal
Device(config)# device-sensor filter-spec cdp include list cdp-list1
Device(config)# end
```

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.
show device-sensor cache	Displays device sensor cache entries.

device-sensor notify

To enable client notifications and accounting events for Type-Length-Value (TLV) changes, use the **device-sensor notify** command in global configuration mode. To disable client notifications and accounting events for TLV changes, use the **no** form of this command.

device-sensor notify {**all-changes** | **new-tlvs**}

no device-sensor notify {**all-changes** | **new-tlvs**}

Syntax Description

all-changes	Enables client notifications and accounting events for all TLV changes.
new-tlvs	Enables client notifications and accounting events for only new TLV changes.

Command Default

Client notifications and accounting events are generated only for new TLVs.

Command Modes

Global configuration (config)

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

By default, for each supported peer protocol, client notifications and accounting events will be generated only when an incoming packet includes a TLV that was not previously received in the context of a given session.

To enable client notifications and accounting events for all TLV changes, where either a new TLV has been received or a previously received TLV was received with a different value, use the **device-sensor notify all-changes** command.

To return to the default behavior, use the **device-sensor notify new-tlvs** or the **default device-sensor notify** command.

Examples

The following example shows how to enable client notifications and accounting events for all TLV changes:

```
Device> enable
Device# configure terminal
Device(config)# device-sensor notify all-changes
Device(config)# end
```

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.
show device-sensor cache	Displays device sensor cache entries.

dhcp (IKEv2)

To assign an IP address to the remote access client using a DHCP server, use the **dhcp**command in IKEv2 authorization policy configuration mode. To remove the assigned IP address, use the **no** form of this command.

dhcp {**giaddr** *ip-address*| **server** {*ip-address*| *hostname*}| **timeout** *seconds*}

no dhcp {**giaddr**| **server**| **timeout**}

Syntax Description

giaddr *ip-address*	Specifies the gateway IP address (giaddr).
server	Specifies addresses for the DHCP server.
ip-address	IP address of the DHCP server.
hostname	Hostname of the DHCP server. The hostname is resolved during configuration.
timeout *seconds*	Specifies the wait time in seconds before the next DHCP server in the list is tried.

Command Default

An IP address is not assigned by a DHCP server.

Command Modes

IKEv2 client group 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.

Usage Guidelines

If this command is not configured, an IP address is assigned to a remote device using either a local pool that is configured on a device or a framed IP address attribute that is defined in RADIUS.

Note You can specify only one DHCP server. It is assumed that the DHCP server can be reached via the global routing table, and therefore, the DHCP packets are forwarded to the global routing table.

Examples

The following example shows that the IP address of the DHCP server is 192.0.2.1 and that the time to wait until the next DHCP server on the list is tried is 6 seconds:

```
Device(config)# crypto ikev2 client configuration group home
Device(config-ikev2-client-config-group)# key abcd
Device(config-ikev2-client-config-group)# dhcp server 192.0.2.1
Device(config-ikev2-client-config-group)# dhcp timeout 6
```

Related Commands

Command	Description
crypto ikev2 authorization policy	Specifies an IKEv2 authorization policy group.

dhcp server (isakmp)

To assign an IP address or hostname using a DHCP server, use the **dhcp server**command in crypto ISAKMP group configuration mode. To remove the assigned IP address or hostname, use the **no** form of this command.

dhcp server {*ip-address*| *hostname*}

no dhcp server {*ip-address*| *hostname*}

Syntax Description

ip-address	Address of the DHCP server.
hostname	Hostname of the DHCP server.

Command Default

IP address is not assigned by a DHCP server.

Command Modes

Crypto ISAKMP group configuration (config-isakmp-group)

Command History

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

Usage Guidelines

If this command is not configured, an IP address is assigned to a remote device using either a local pool that is configured on a router or a framed IP address attribute that is defined in RADIUS.

Note Up to five DHCP servers can be configured one at a time.

Note The DHCP proxy feature does not include functionality for the DHCP server to "push" the DNS, WINS server, or domain name to the remote client.

Examples

The following example shows that the IP address of the DHCP server is 10.2.3.4 and that the time to wait until the next DHCP server on the list is tried is 6 seconds:

```
Router (config)# crypto isakmp client configuration group home
 Router (config-isakmp-group)# key abcd
 Router (config-isakmp-group)# dhcp server 10.2.3.4
 Router (config-isakmp-group)# dhcp timeout 6
```

Related Commands

Command	Description
crypto isakmp client configuration group	Specifies to which group a policy profile will be defined.

dhcp timeout

To set the wait time before the next DHCP server on the list is tried, use the **dhcp timeout**command in crypto ISAKMP group configuration mode. To remove the wait time that was set, use the **no** form of this command.

dhcp timeout *time*

no dhcp timeout *time*

Syntax Description

time	Response time in seconds. Value = 4 through 30.

Command Modes

Crypto ISAKMP group configuration (config-isakmp-group)

Command History

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

Examples

The following example shows that the IP address of the DHCP server is 10.2.3.4 and that the time to wait until the next DHCP server on the list is tried is 6 seconds:

```
Router (config)# crypto isakmp client configuration group home
 Router (config-isakmp-group)# dhcp server 10.2.3.4
 Router (config-isakmp-group)# key abcd
 Router (config-isakmp-group)# dhcp timeout 6
```

Related Commands

Command	Description
crypto isakmp client configuration group	Specifies to which group a policy profile will be defined.

dialer aaa

To allow a dialer to access the authentication, authorization, and accounting (AAA) server for dialing information, use the dialer aaa command in interface configuration mode. To disable this function, use the no form of this command.

dialer aaa [**password** *string*| **suffix** *string*]

no dialer aaa [**password** *string*| **suffix** *string*]

Syntax Description

password *string*	(Optional) Defines a nondefault password for authentication. The password string can be a maximum of 128 characters.
suffix *string*	(Optional) Defines a suffix for authentication. The suffix string can be a maximum of 64 characters.

Command Default

This feature is not enabled by default.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.1(5)T	The password and **suffix** 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.

Usage Guidelines

This command is required for large scale dial-out and Layer 2 Tunneling Protocol (L2TP) dial-out functionality. With this command, you can specify a suffix, a password, or both. If you do not specify a password, the default password will be “cisco.”

Note Only IP addresses can be specified as usernames for the **dialer aaa suffix** command.

Examples

This example shows a user sending out packets from interface Dialer1 with a destination IP address of 10.1.1.1. The username in the access-request message is "10.1.1.1@ciscoDoD" and the password is "cisco."

```
interface dialer1
 dialer aaa
 dialer aaa suffix @ciscoDoD password cisco
```

Related Commands

Command	Description
accept dialout	Accepts requests to tunnel L2TP dial-out calls and creates an accept-dialout VPDN subgroup.
dialer congestion-threshold	Specifies congestion threshold in connected links.
dialer vpdn	Enables a Dialer Profile or DDR dialer to use L2TP dial-out.

diameter origin host

To configure the fully qualified domain name (FQDN) of the host of a Diameter node, use the **diameter origin host** command in global configuration mode. To disable the configured FQDN, use the **no** form of this command.

diameter origin host *string*

no diameter origin host *string*

Syntax Description

string	Character string that describes the FQDN for a specific Diameter node.

Command Default

No realm is configured.

Command Modes

Global configuration

Command History

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

Usage Guidelines

Because there is no host configured by default, it is mandatory to configure this information. The origin host information is sent in requests to a Diameter peer. Global Diameter protocol parameters are used if Diameter parameters have not been defined at a Diameter peer level.

Examples

The following example shows how to configure a Diameter origin host:

```
Router(config)# diameter origin host
 host1.example.com.
```

Related Commands

Command	Description
diameter origin realm	Configures origin realm information for a Diameter node.
diameter peer	Defines a Diameter peer and enters Diameter peer configuration mode.

diameter origin realm

To configure origin realm information for a Diameter node, use the **diameter origin realm** command in global configuration mode. To disable the configured realm information, use the **no** form of this command.

diameter origin realm *string*

no diameter origin realm *string*

Syntax Description

string	Character string that describes the realm information for a specific Diameter node.

Command Default

No realm is configured.

Command Modes

Global configuration

Command History

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

Usage Guidelines

Because there is no realm configured by default, it is mandatory to configure this information. Origin realm information is sent in requests to a Diameter peer.

Examples

The following example shows how to configure a Diameter origin realm:

```
Router (config)# diameter origin realm
 example.com
```

Related Commands

Command	Description
diameter origin host	Configures the FQDN of the host of a Diameter node.
diameter peer	Defines a Diameter peer and enters Diameter peer configuration mode.

diameter peer

To configure a device as a Diameter Protocol peer and enter the Diameter peer configuration submode, use the **diameter peer** command in global configuration mode. To disable Diameter Protocol configuration for a peer, use the **no** form of this command.

diameter peer *name*

no diameter peer *name*

Syntax Description

name	Character string used to name the peer node to be configured for the Diameter Credit Control Application (DCCA).

Command Default

No Diameter peer is configured.

Command Modes

Global configuration

Command History

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

Usage Guidelines

This command enables the Diameter peer configuration submode. From the submode, you can configure other DCCA parameters. The configuration is applied when you exit the submode.

Examples

The following example shows how to configure a Diameter peer:

```
Router (config)# diameter peer
 dia_peer_1
```

Related Commands

Command	Description
address ipv4	Defines a route to the host of the Diameter peer using IPv4.
destination host	Configures the FQDN of a Diameter peer.
destination realm	Configures the destination realm in which a Diameter peer is located.

Command	Description
ip vrf forwarding	Associates a VRF with a Diameter peer.
security ipsec	Configures IPSec as the security protocol for the Diameter peer-to-peer connection.
show diameter peer	Displays the Diameter peer configuration.
source interface	Configures the interface to connect to the Diameter peer.
timer	Configures Diameter base protocol timers for peer-to-peer communication.
transport {tcp} port	Configures the transport protocol for connections to the Diameter peer.

diameter redundancy

To enable the Diameter node to be a Cisco IOS Redundancy Facility (RF) client and track session states, use the **diameter redundanc**y command in global configuration mode. To disable this feature, use the **no** form of this command.

diameter redundancy

no diameter redundancy

Syntax Description

This command has no arguments or keywords.

Command Default

Diameter redundancy is not configured.

Command Modes

Global configuration

Command History

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

Usage Guidelines

When you configure Diameter redundancy on a device, that device will not initiate any TCP connection while it is a standby node. Upon transition to active status, the device initiates a TCP connection to the Diameter peer.

Note This command is required for service-aware Packet Data Protocol (PDP) session redundancy. For more information about service-aware PDP session redundancy, see the “GTP-Session Redundancy for Service-Aware PDPs Overview” section of the *Cisco GGSN Release 5.2 Configuration Guide* .

Examples

The following example shows how to configure Diameter redundancy:

```
Router (config)# diameter redundancy
```

Related Commands

Command	Description
diameter origin host	Configures the FQDN of the host of this Diameter node.

Command	Description
diameter origin realm	Configures the realm of origin in which this Diameter node is located.
diameter timer	Configures Diameter base protocol timers to use if none have been configured at the Diameter peer level.
diameter vendor support	Configures a Diameter node to advertise the vendor AVPs it supports in capability exchange messages with Diameter peers.

diameter timer

To set either the frequency of transport connection attempts or the interval for sending watchdog messages, use the **diameter timer**command in global configuration mode. To return to the default values, use the **no** form of this command.

diameter timer {**connection| transaction| watch-dog**} **value**

no diameter timer {**connection| transaction| watch-dog**} **value**

Syntax Description

connection	Maximum interval, in seconds, for the Gateway General Packet Radio Service (GPRS) Support Node (GGSN) to attempt reconnection to a Diameter peer after being disconnected due to 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.
watch-dog	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 value for each timer is 30 seconds.

Command Modes

Global 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 examples show how to configure the Diameter timers:

```
Router config# diameter timer connection 20
Router config# diameter timer watch-dog 25
```

Related Commands

Command	Description
aaa group server diameter	Defines a Diameter AAA server group.
diameter peer	Configures a Diameter peer and enters Diameter peer configuration submode.
timer	Configures the Diameter base protocol timers for a Diameter peer.

diameter vendor supported

To configure a Diameter node to advertise the vendor-specific attribute value pairs (AVPs) it recognizes, use the **diameter vendor supported** command in global configuration mode. To remove the supported vendor configuration, use the **no** form of this command.

diameter vendor supported {**Cisco**| **3gpp**| **Vodafone**}

no diameter vendor supported {**Cisco**| **3gpp**| **Vodafone**}

Syntax Description

Cisco	Configures the Diameter node to advertise support for the Cisco-specific AVPs.
3gpp	Configures the Diameter node to advertise support for the AVPs that support the Third-Generation Partnership Project (3GPP).
Vodafone	Configures the Diameter node to advertise support for the Vodafone-specific AVPs.

Command Default

No vendor identifier is configured.

Command Modes

Global configuration

Command History

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

Usage Guidelines

Individual vendors can define AVPs specific to their implementation of the Diameter Credit Control Application (DCCA), or for individual applications. You can configure multiple instances of this command, as long as each instance has a different vendor identifier.

Examples

The following example shows how to configure DCCA to advertise support for a the Cisco-specific AVPs:

```
Router (config)# diameter vendor supported Cisco
```

Related Commands

Command	Description
diameter origin host	Configures the FQDN of the host of this Diameter node.
diameter origin realm	Configures the realm of origin in which this Diameter node is located.
diameter redundancy	Enables the Diameter node to be a Cisco IOS RF client and track session states.
diameter timer	Configures Diameter base protocol timers to use if none have been configured at the Diameter peer level.

disable open-media-channel

To prevent the creation of Real-time Transport Protocol (RTP) or RTP Control (RTCP) media channels when a Session Initiation Protocol (SIP) class map is used for SIP inspection, use the **disable open-media-channel** command in parameter-map type configuration mode. To enable the creation of RTP or RTCP media channels, use the **no** form of this command or remove this parameter map from the inspect action.

disable open-media-channel

no disable open-media-channel

Syntax Description

This command has no arguments or keywords.

Command Default

RTP and RTPC media channels are opened by the SIP inspection process.

Command Modes

Parameter-map type configuration (config-profile)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

Cisco IOS Firewall Trust Relay Point (TRP) support enables Cisco IOS Firewall to process Simple Traversal of User Datagram Protocol (UDP) (STUN) messages. The STUN messages open ports (pinholes) for secondary channels (RTP and RTCP), which are necessary for implementation of TRPs in voice networks.

Cisco IOS Firewall supports partial SIP inspection that allows the SIP Application-level Gateway (ALG) to parse the SIP message in a packet to check for protocol conformance.

To configure partial SIP inspection in voice networks, you must use the **disable open-media-channel** command to configure SIP ALG so that it does not open pinholes for media information found in the SDP message.

When Cisco IOS TRP is used in voice network for firewall traversal, Partial SIP-ALG (enabled when this parameter map is attached to the inspect action) provides security for SIP control channel and STUN with Cisco Flow data (CFD) provides security for the RTP and RTCP channels. If Partial SIP-ALG is not used, the normal SIP-ALG will open RTP and RTCP channels by itself.

Examples

The following example shows how to create a parameter map that does not open a media channel when attached to a SIP class map:

```
Router(config)# parameter-map type protocol-info sip pmap-sip
Router(config-profile)# disable open-media-channel
```

Related Commands

Command	Description
parameter-map type protocol-info	Creates or modifies a protocol-specific parameter map and enters parameter-map type configuration mode.

disconnect ssh

To terminate a Secure Shell (SSH) connection on your router, use the **disconnect ssh** command in privileged EXEC mode.

disconnect ssh [vty] *session-id*

Syntax Description

vty	(Optional) Virtual terminal for remote console access.
session-id	The session-id is the number of connection displayed in the **show ip ssh** command output.

Command Default

No default behavior or values.

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.
12.2(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

The **clear line vty** *n* command, where *n* is the connection number displayed in the **show ip ssh** command output, may be used instead of the **disconnect ssh** command.

When the EXEC connection ends, whether normally or abnormally, the SSH connection also ends.

Examples

The following example terminates SSH connection number 1:

```
disconnect ssh 1
```

Related Commands

Command	Description
clear line vty	Returns a terminal line to idle state using the privileged EXEC command.

dn

To associate the identity of a router with the distinguished name (DN) in the certificate of the router, use the **dn** command in crypto identity configuration mode. To remove this command from your configuration, use the **no** form of this command.

dn *name=string* [*, name=string*]

no dn *name=string* [*, name=string*]

Syntax Description

name string	Identity used to restrict access to peers with specific certificates. Optionally, you can associate more than one identity.

Command Default

If this command is not enabled, the router can communicate with any encrypted interface that is not restricted on its IP address.

Command Modes

Crypto identity configuration (crypto-identity)

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 **dn** command to associate the identity of the router, which is defined in the **crypto identity**command, with the DN that the peer used to authenticate itself.

Note The name defined in the crypto identity command must match the *string* defined in the dn command. That is, the identity of the peer must be the same as the identity in the exchanged certificate.

This command allows you set restrictions in the router configuration that prevent those peers with specific certificates, especially certificates with particular DNs, from having access to selected encrypted interfaces.

An encrypting peer matches this list if it contains the attributes listed in any one line defined within the *name=string*.

Examples

The following example shows how to configure an IPsec crypto map that can be used only by peers that have been authenticated by the DN and if the certificate belongs to “green”:

```
crypto map map-to-green 10 ipsec-isakmp
 set peer 172.21.114.196
 set transform-set my-transformset
 match address 124
 identity to-green
!
crypto identity to-green
 dn ou=green
```

Related Commands

Command	Description
crypto identity	Configures the identity of the router with a given list of DNs in the certificate of the router.
fqdn	Associates the identity of the router with the hostname that the peer used to authenticate itself.

dn (IKEv2)

To enable and derive an IKEv2 name mangler from identity of type distinguished name (DN), use the **dn** command in IKEv2 name mangler configuration mode. To remove the name derived from DN, use the **no** form of this command.

dn {**common-name| country| domain| locality| organization| organization-unit| state**}

no dn

Syntax Description

common-name	Derives the name mangler from the common name portion in the DN.
country	Derives the name mangler from the country portion in the DN.
domain	Derives the name mangler from the domain portion in the DN.
locality	Derives the name mangler from the locality portion in the DN.
organization	Derives the name mangler from the organization portion in the DN.
organization-unit	Derives the name mangler from the organization-unit portion in the DN.
state	Derives the name mangler from the state portion in the DN.

Command Default

No default behavior or values.

Command Modes

IKEv2 name mangler configuration (config-ikev2-name-mangler)

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.

Usage Guidelines

Use this command to derive the name mangler from any field in the remote identity of type DN.

Examples

The following example shows how to derive a name for the name mangler from the country field of the DN:

```
Router(config)# crypto ikev2 name-mangler mangler2
Router(config-ikev2-name-mangler)# dn country
```

Related Commands

Command	Description
crypto ikev2 name mangler	Defines a name mangler.

dnis (AAA preauthentication)

To preauthenticate calls on the basis of the Dialed Number Identification Service (DNIS) number, use the **dnis** command in AAA preauthentication configuration mode. To remove the **dnis** command from your configuration, use the **no** form of this command.

dnis [**if-avail|** **required**] **[accept-stop]** [**password** *string*]

no dnis [**if-avail|** **required**] **[accept-stop]** [**password** *string*]

Syntax Description

if-avail	(Optional) Implies that if the switch provides the data, RADIUS must be reachable and must accept the string in order for preauthentication to pass. If the switch does not provide the data, preauthentication passes.
required	(Optional) Implies that the switch must provide the associated data, that RADIUS must be reachable, and that RADIUS must accept the string in order for preauthentication to pass. If these three conditions are not met, preauthentication fails.
accept-stop	(Optional) Prevents subsequent preauthentication elements from being tried once preauthentication has succeeded for a call element.
password *string*	(Optional) Password to use in the Access-Request packet. The default is *cisco*.

Command Default

The **if-avail** and **required** keywords are mutually exclusive. If the **if-avail** keyword is not configured, the preauthentication setting defaults to **required**.

The default password string is cisco.

Command Modes

AAA preauthentication configuration

Command History

Release	Modification
12.1(2)T	This command was introduced.

Usage Guidelines

You may configure more than one of the AAA preauthentication commands (**clid**, **ctype**, **dnis**) to set conditions for preauthentication. The sequence of the command configuration decides the sequence of the preauthentication conditions. For example, if you configure **dnis**, then **clid**, then **ctype**, then this is the order of the conditions considered in the preauthentication process.

In addition to using the preauthentication commands to configure preauthentication on the Cisco router, you must set up the preauthentication profiles on the RADIUS server.

Examples

The following example enables DNIS preauthentication using a RADIUS server and the password Ascend-DNIS:

```
aaa preauth
 group radius
 dnis password Ascend-DNIS
```

The following example specifies that incoming calls be preauthenticated on the basis of the DNIS number:

```
aaa preauth
 group radius
 dnis required
```

Related Commands

Command	Description
aaa preauth	Enters AAA preauthentication mode.
clid	Preauthenticates calls on the basis of the CLID number.
ctype	Preauthenticates calls on the basis of the call type.
dnis bypass (AAA preauthentication configuration)	Specifies a group of DNIS numbers that will be bypassed for preauthentication.
group (authentication)	Selects the security server to use for AAA preauthentication.
isdn guard-timer	Sets a guard timer to accept or reject a call in the event that the RADIUS server fails to respond to a preauthentication request.

dnis (RADIUS)

To preauthenticate calls on the basis of the DNIS (Dialed Number Identification Service) number, use the **dnis** command in AAA preauthentication configuration mode. To remove the **dnis** command from your configuration, use the **no** form of this command.

dnis [**if-avail| required**] **[accept-stop]** [**password** *password*]

no dnis [**if-avail| required**] **[accept-stop]** [**password** *password*]

Syntax Description

if-avail	(Optional) Implies that if the switch provides the data, RADIUS must be reachable and must accept the string in order for preauthentication to pass. If the switch does not provide the data, preauthentication passes.
required	(Optional) Implies that the switch must provide the associated data, that RADIUS must be reachable, and that RADIUS must accept the string in order for preauthentication to pass. If these three conditions are not met, preauthentication fails.
accept-stop	(Optional) Prevents subsequent preauthentication elements such as clid or ctype from being tried once preauthentication has succeeded for a call element.
password *password*	(Optional) Defines the password for the preauthentication element.

Command Default

The **if-avail** and **required** keywords are mutually exclusive. If the **if-avail** keyword is not configured, the preauthentication setting defaults to **required**.

The default password string is cisco.

Command Modes

AAA preauthentication configuration

Command History

Release	Modification
12.1(2)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

You may configure more than one of the authentication, authorization, and accounting (AAA) preauthentication commands (**clid**, **ctype**, **dnis**) to set conditions for preauthentication. The sequence of the command configuration decides the sequence of the preauthentication conditions. For example, if you configure **dnis**, then **clid**, then **ctype**, in this order, then this is the order of the conditions considered in the preauthentication process.

In addition to using the preauthentication commands to configure preauthentication on the Cisco router, you must set up the preauthentication profiles on the RADIUS server.

Examples

The following example specifies that incoming calls be preauthenticated on the basis of the DNIS number:

```
aaa preauth
 group radius
 dnis required
```

Related Commands

Command	Description
clid	Preauthenticates calls on the basis of the CLID number.
ctype	Preauthenticates calls on the basis of the call type.
dnis bypass (AAA preauthentication configuration)	Specifies a group of DNIS numbers that will be bypassed for preauthentication.
group (RADIUS)	Specifies the AAA RADIUS server group to use for preauthentication.

dnis bypass (AAA preauthentication configuration)

To specify a group of DNIS (Dialed Number Identification Service) numbers that will be bypassed for preauthentication, use the **dnis bypass** command in AAA preauthentication configuration mode. To remove the **dnis bypass** command from your configuration, use the **no** form of this command.

dnis bypass *dnis-group-name*

no dnis bypass *dnis-group-name*

Syntax Description

dnis-group-name	Name of the defined DNIS group.

Command Default

No DNIS numbers are bypassed for preauthentication.

Command Modes

AAA preauthentication configuration

Command History

Release	Modification
12.1(2)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

Before using this command, you must first create a DNIS group with the **dialer dnis group** command.

Examples

The following example specifies that preauthentication be performed on all DNIS numbers except for two DNIS numbers (12345 and 12346), which have been defined in the DNIS group called hawaii:

```
aaa preauth
 group radius
 dnis required
 dnis bypass hawaii
dialer dnis group hawaii
 number 12345
 number 12346
```

Related Commands

Command	Description
dialer dnis group	Creates a DNIS group.
dnis (RADIUS)	Preauthenticates calls on the basis of the DNIS number.

dns

To specify the primary and secondary Domain Name Service (DNS) servers, use the **dns** command in ISAKMP group configuration mode or IKEv2 authorization policy configuration mode. To remove this command from your configuration, use the **no** form of this command.

[**ipv6**]**dns** *primary-server* [*secondary-server*]

no [**ipv6**]**dns** *primary-server* [*secondary-server*]

Syntax Description

ipv6	(Optional) Specifies an IPv6 address for the DNS server. To specify an IPv4 address, execute the command without this keyword.
primary-server	Name of the primary DNS server.
secondary-server	(Optional) Name of the secondary DNS server.

Command Default

A DNS server is not specified.

Command Modes

ISAKMP group configuration (config-isakmp-group) IKEv2 authorization policy configuration (config-ikev2-author-policy)

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.
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.

Usage Guidelines

Use the dns command to specify the primary and secondary DNS servers for the group.

You must enable the following commands before enabling the **dns** 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 DNS server for the default group name:

```
crypto isakmp client configuration group default
 key cisco
 dns 10.2.2.2 10.3.2.3
 pool dog
 acl 199
```

Related Commands

Command	Description
acl	Configures split tunneling.
crypto ikev2 authorization policy	Specifies an IKEv2 authorization policy.
crypto isakmp client configuration group	Specifies the policy profile of the group that will be defined.
domain (isakmp-group)	Specifies the DNS domain to which a group belongs.

dnsix-dmdp retries through dynamic

dnsix-dmdp retries

To s et the retransmit count used by the Department of Defense Intelligence Information System Network Security for Information Exchange (DNSIX) Message Delivery Protocol (DMDP), use the **dnsix-dmdp retries** command in global configuration mode. To restore the default number of retries, use the **no**form of this command.

dnsix-dmdp retries *count*

no dnsix-dmdp retries *count*

Syntax Description

count	Number of times DMDP will retransmit a message. It can be an integer from 0 to 200. The default is 4 retries, or until acknowledged.

Command Default

Retransmits messages up to 4 times, or until acknowledged.

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.(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 sets the number of times DMDP will attempt to retransmit a message to 150:

```
dnsix-dmdp retries 150
```

Related Commands

Command	Description
dnsix-nat authorized-redirection	Specifies the address of a collection center that is authorized to change the primary and secondary addresses of the host to receive audit messages.
dnsix-nat primary	Specifies the IP address of the host to which DNSIX audit messages are sent.

Command	Description
dnsix-nat secondary	Specifies an alternate IP address for the host to which DNSIX audit messages are sent.
dnsix-nat source	Starts the audit-writing module and defines audit trail source address.
dnsix-nat transmit-count	Causes the audit-writing module to collect multiple audit messages in the buffer before sending the messages to a collection center.

dnsix-nat authorized-redirection

To sp ecify the address of a collection center that is authorized to change the primary and secondary addresses of the host to receive audit messages, use the **dnsix-nat authorized-redirection** command in global configuration mode. To delete an address, use the **no** form of this command.

dnsix-nat authorized-redirection *ip-address*

no dnsix-nat authorized-redirection *ip-address*

Syntax Description

ip-address	IP address of the host from which redirection requests are permitted.

Command Default

An empty list of addresses.

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.(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 multiple **dnsix-nat authorized-redirection** commands to specify a set of hosts that are authorized to change the destination for audit messages. Redirection requests are checked against the configured list, and if the address is not authorized the request is rejected and an audit message is generated. If no address is specified, no redirection messages are accepted.

Examples

The following example specifies that the address of the collection center that is authorized to change the primary and secondary addresses is 192.168.1.1:

```
dnsix-nat authorization-redirection 192.168.1.1
```

dnsix-nat primary

To s pecify the IP address of the host to which Department of Defense Intelligence Information System Network Security for Information Exchange (DNSIX) audit messages are sent, use the **dnsix-nat primary** command in global configuration mode. To delete an entry, use the **no** form of this command.

dnsix-nat primary *ip-address*

no dnsix-nat primary *ip-address*

Syntax Description

ip-address	IP address for the primary collection center.

Command Default

Messages are not sent.

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.(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

An IP address must be configured before audit messages can be sent.

Examples

The following example configures an IP address as the address of the host to which DNSIX audit messages are sent:

```
dnsix-nat primary 172.16.1.1
```

dnsix-nat secondary

To sp ecify an alternate IP address for the host to which Department of Defense Intelligence Information System Network Security for Information Exchange (DNSIX) audit messages are sent, use the **dnsix-nat secondary** command in global configuration mode. To delete an entry, use the **no** form of this command.

dnsix-nat secondary *ip-address*

no dnsix-nat secondary *ip-address*

Syntax Description

ip-address	IP address for the secondary collection center.

Command Default

No alternate IP address is known.

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.(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

When the primary collection center is unreachable, audit messages are sent to the secondary collection center instead.

Examples

The following example configures an IP address as the address of an alternate host to which DNSIX audit messages are sent:

```
dnsix-nat secondary 192.168.1.1
```

dnsix-nat source

To st art the audit-writing module and to define the audit trail source address, use the **dnsix-nat source**command in global configuration mode. To disable the Department of Defense Intelligence Information System Network Security for Information Exchange (DNSIX) audit trail writing module, use the **no** form of this command.

dnsix-nat source *ip-address*

no dnsix-nat source *ip-address*

Syntax Description

ip-address	Source IP address for DNSIX audit messages.

Command Default

Disabled

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.(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 issue the **dnsix-nat source** command before any of the other **dnsix-nat** commands. The configured IP address is used as the source IP address for DMDP protocol packets sent to any of the collection centers.

Examples

The following example enables the audit trail writing module, and specifies that the source IP address for any generated audit messages should be the same as the primary IP address of Ethernet interface 0:

```
dnsix-nat source 192.168.2.5
interface ethernet 0
 ip address 192.168.2.5 255.255.255.0
```

dnsix-nat transmit-count

To h ave the audit writing module collect multiple audit messages in the buffer before sending the messages to a collection center, use the **dnsix-nat transmit-count** command inglobal configuration mode. To revert to the default audit message count, use the **no** form of this command.

dnsix-nat transmit-count *count*

no dnsix-nat transmit-count *count*

Syntax Description

count	Number of audit messages to buffer before transmitting to the server. It can be an integer from 1 to 200.

Command Default

One message is sent at a time.

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.(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

An audit message is sent as soon as the message is generated by the IP packet-processing code. The audit writing module can, instead, buffer up to several audit messages before transmitting to a collection center.

Examples

The following example configures the system to buffer five audit messages before transmitting them to a collection center:

```
dnsix-nat transmit-count 5
```

dns-timeout

To specify the Domain Name System (DNS) idle timeout (the length of time for which a DNS lookup session will continue to be managed while there is no activity), use the **dns-timeout** command in parameter-map type inspect configuration mode. To disable the timeout, use the **no** form of this command.

dns-timeout *seconds*

no dns-timeout *seconds*

Syntax Description

seconds	Length of time, in seconds, for which a DNS name lookup session will still be managed while there is no activity. The default is 5.

Command Default

The DNS idle timeout is disabled.

Command Modes

Parameter-map type inspect configuration

Command History

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

Usage Guidelines

You can use the **dns-timeout**subcommand when you are creating an inspect type parameter map. You can enter the **dns-timeout**subcommand after you enter the **parameter-map type inspect** command.

Use the **dns-timeout**command if you have DNS inspection configured and want to control the timeout of DNS sessions.

If DNS inspection is not configured, but you enter the **dns-timeout** command, the command does not take effect (that is, it is not applied to a DNS session).

For more detailed information about creating a parameter map, see the **parameter-map type inspect** command.

Examples

The following example specifies that if there is no activity, a DNS lookup session will continue to be managed for 25 seconds:

```
parameter-map type inspect insp-params
 dns-timeout 25
```

Related Commands

Command	Description
ip inspect dns-timeout	Specifies the DNS idle timeout (the length of time during which a DNS name lookup 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.

domain (AAA)

To configure username domain options for the RADIUS application, use the **domain** command in dynamic authorization local server configuration mode. To disable the username domain options configured, use the **no** form of this command.

domain {**delimiter** *character*| **stripping [right-to-left]**}

no domain {**delimiter** *character*| **stripping [right-to-left]**}

Syntax Description

delimiter *character*	Specifies the domain delimiter. One of the following options can be specified: @, /, **$**, **%**, \, # or **-**
stripping	Compares the incoming username with the names oriented to the left of the @ domain delimiter.
right-to-left	Terminates the string at the first delimiter going from right to left.

Command Default

No username domain options are configured.

Command Modes

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

Command History

Release	Modification
12.2(31)SB14	This command was introduced.
12.2(33)SRC5	This command was integrated into Cisco IOS Release 12.2(33)SRC5.
Cisco IOS XE Release 2.3	This command was modified. This command was implemented on ASR 1000 series routers.
15.1(2)T	This command was integrated into Cisco IOS Release 15.1(2)T. This command was also modified. The **right-to-left** keyword was added.

Usage Guidelines

If domain stripping is not configured, the full username provided in the authentication, authorization, and accounting (AAA) packet of disconnect (POD) messages is compared with the online subscribers. Configuring domain stripping allows you to send disconnect messages with only the username present before the @ domain delimiter. The network access server (NAS) compares and matches this username with any online subscriber with a potential domain.

For instance, when domain stripping is configured and you send a POD message with the username “test,” a comparison between the POD message and online subscribers takes place, and subscribers with the username “test@cisco.com” or “test” match the specified username “test.”

Examples

The following configuration example is used to match a username from right to left. If the username is user1@cisco.com@test.com, then the username to be matched by the POD message is user1@cisco.com.

```
Router# configure terminal
Router(config)# aaa server radius dynamic-author
Router(config-locsvr-da-radius)# domain stripping right-to-left
Router(config-locsvr-da-radius)# domain delimiter @
Router(config-locsvr-da-radius)# end
```

The following configuration example is used to match a username from left to right. If the username is user1@cisco.com@test.com, then the username to be matched by the POD message is user1.

```
Router# configure terminal
Router(config)# aaa server radius dynamic-author
Router(config-locsvr-da-radius)# domain stripping
Router(config-locsvr-da-radius)# domain delimiter @
Router(config-locsvr-da-radius)# end
```

Related Commands

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

domain (isakmp-group)

To specify the Domain Name Service (DNS) domain to which a group belongs, use the **domain** command in Internet Security Association Key Management Protocol (ISAKMP) group configuration mode. To remove this command from your configuration, use the **no** form of this command.

domain *name*

no domain *name*

Syntax Description

name	Name of the DNS domain.

Command Default

A DNS domain is not specified.

Command Modes

ISAKMP group configuration (config-isakmp-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.

Usage Guidelines

Use the domain command to specify group domain membership.

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

Examples

The following example shows that members of the group “cisco” also belong to the domain “cisco.com”:

```
crypto isakmp client configuration group cisco
  key cisco
  dns 10.2.2.2 10.3.2.3
  pool dog
  acl 199
  domain cisco.com
```

Related Commands

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

domain-stripping

To configure domain stripping at the server group level, use the **domain-stripping** command in server group RADIUS configuration mode. To disable the configuration, use the **no** form of this command.

domain-stripping [**strip-suffix** *word*] **[right-to-left]** [**prefix-delimiter** *word*] [**delimiter** *word*]

no domain-stripping [**strip-suffix** *word*] **[right-to-left]** [**prefix-delimiter** *word*] [**delimiter** *word*]

Syntax Description

strip-suffix	(Optional) Configures the suffix, which needs to be stripped.
word	(Optional) Suffix that needs to be stripped.
right-to-left	(Optional) Terminates the string at the first delimiter going from right to left.
prefix-delimiter	(Optional) Configures a set of prefix delimiters.
delimiter	(Optional) Configures a set of suffix delimiters.

Command Default

Stripping is disabled. The entire username (including the domain name) is sent to the RADIUS server.

Command Modes

Server group RADIUS configuration (config-sg-radius)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.
15.2(3)T	This command was integrated into Cisco IOS Release 15.2(3)T.

Usage Guidelines

Use the **radius-server domain-stripping** command to remove the domain name from the username received at the global level. All authentication, authorization, and accounting (AAA) requests with “user@example.com” will go to the remote RADIUS server with the reformatted username “user.” The domain name is removed from the request .

Use the **domain-stripping** command to configure domain stripping at the server group level. Per-server group configuration will override the global configuration. That is, if domain stripping is not enabled globally but enabled in the server group, it is enabled only for that server group. Also, if virtual routing and forwarding (VRF)-specific domain stripping is configured globally and in the server group for a different VRF, domain stripping is enabled in both the VRFs. After domain stripping and broadcast accounting are configured, you can create separate accounting records as per the configurations.

Examples

The following example shows how to configure domain stripping at the server group level:

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa group server radius rad1
Device(config-sg-radius)# domain-stripping right-to-left delimiter @$/
Device(config-sg-radius)# end
```

Related Commands

Command	Description
aaa group server radius	Adds the RADIUS server group.

dot1x control-direction

Note Effective with Cisco IOS Release 12.2(33)SXI, the **dot1x control-direction** command is replaced by the **authentication control-direction** command. See the **authentication control-direction** command for more information.

To change an IEEE 802.1X controlled port to unidirectional or bidirectional, use the **dot1x control-direction** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

dot1x control-direction {**both**| **in**}

no dot1x control-direction

Syntax Description

both	Enables bidirectional control on the port.
in	Enables unidirectional control on the port.

Command Default

The port is set to bidirectional mode.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(25)SEC	This command was introduced.
12.4(6)T	This command was integrated into Cisco IOS Release 12.4(6)T.
12.4(4)XC	This command was integrated into Cisco IOS Release 12.4(4)XC for Cisco 870 Integrated Services Switchs (ISRs) only.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SXI	This command was replaced by the **authentication control-direction** command.

Usage Guidelines

The IEEE 802.1x standard defines a client-server-based access control and authentication protocol that restricts unauthorized devices from connecting to a LAN through publicly accessible ports. 802.1x controls network access by creating two distinct virtual access points at each port. One access point is an uncontrolled port; the other is a controlled port. All traffic through the single port is available to both access points. 802.1x authenticates each user device that is connected to a switch port and assigns the port to a VLAN before making available any services that are offered by the switch or the LAN. Until the device is authenticated, 802.1x access control allows only Extensible Authentication Protocol over LAN (EAPOL) traffic through the port to which the device is connected. After authentication is successful, normal traffic can pass through the port.

Unidirectional State

When you configure a port as unidirectional with the **dot1x control-direction in** interface configuration command, the port changes to the spanning-tree forwarding state.

When Unidirectional Controlled Port is enabled, the connected host is in the sleeping mode or power-down state. The host does not exchange traffic with other devices in the network. The host connected to the unidirectional port cannot send traffic to the network, the host can only receive traffic from other devices in the network.

Bidirectional State

When you configure a port as bidirectional with the **dot1x control-direction both** interface configuration command, the port is access-controlled in both directions. In this state, the switch port receives or sends only EAPOL packets; all other packets are dropped.

Using the **both** keyword or using the **no** form of this command changes the port to its bidirectional default setting.

Catalyst 6500 Series Switch

Setting the port as bidirectional enables 802.1X authentication with wake-on-LAN (WoL).

Cisco IOS Release 12.4(4)XC

For Cisco IOS Release 12.4(4)XC, on Cisco 870 ISRs only, this command can be configured on Layer 2 (for switch ports) and Layer 3 (for switched virtual interfaces). However, the command can function at only one layer at a time; that is, if it is configured on Layer 2, it cannot also be configured on Layer 3 and vice versa.

Examples

The following example shows how to enable unidirectional control:

```
Switch(config-if)# dot1x control-direction in
```

The following examples show how to enable bidirectional control:

```
Switch(config-if)# dot1x control-direction both
```

or

```
Switch(config-if)# no dot1x control-direction
```

You can verify your settings by entering the show dot1x all privileged EXEC command. The show dot1x all command output is the same for all devices except for the port names and the state of the port. If a host is attached to the port but is not yet authenticated, a display similar to the following appears:

```
Supplicant MAC 0002.b39a.9275
AuthSM State = CONNECTING
BendSM State = IDLE
PortStatus = UNAUTHORIZED
```

If you enter the dot1x control-direction in command to enable unidirectional control, the following appears in the show dot1x all command output:

```
ControlDirection = In
```

If you enter the dot1x control-direction in command and the port cannot support this mode because of a configuration conflict, the following appears in the show dot1x all command output:

```
ControlDirection = In (Disabled due to port settings):
```

The following example shows how to reset the global 802.1X parameters:

```
Switch(config)# dot1x default
```

Examples

The following example shows how to enable 802.1X authentication with WoL and set the port as bidirectional:

```
Switch(config)# interface gigabitethernet 5/1
Switch(config-if)# dot1x control-direction both
```

Examples

The following example shows Layer 3 802.1X support on a switched virtual interface (using a Cisco 870 ISR):

```
interface FastEthernet0
 description  switchport connect to a client
!
interface FastEthernet1
 description  switchport connect to a client
!
interface FastEthernet2
 description  switchport connect to a client
!
interface FastEthernet3
 description  switchport connect to a client
!
interface FastEthernet4
 description  Connect to the public network
!
interface Vlan1
 description  Apply 802.1x functionality on SVI
 dot1x pae authenticator
 dot1x port-control auto
 dot1x reauthentication
 dot1x control-direction in
```

Related Commands

Command	Description
show dot1x	Displays details for an identity profile.

dot1x credentials

To specify which 802.1X credential profile to use when configuring a supplicant (client) or to apply a credentials structure to an interface and to enter dot1x credentials configuration mode, use the **dot1x credentials** command in global configuration or interface configuration mode. To remove the credential profile, use the **no** form of this command.

dot1x credentials *name*

no dot1x credentials

Syntax Description

name	Name of the credentials profile.

Command Default

A credentials profile is not specified.

Command Modes

Global configuration Interface configuration

Command History

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

Usage Guidelines

An 802.1X credential structure is necessary when configuring a supplicant. This credentials structure may contain a username, password, and description.

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
anonymous-id (dot1x credential)	Specifies the anonymous identity that is associated with a credentials profile.

Command	Description
description (dot1x credential)	Specifies the description for an 802.1X credentials profile.
password (dot1x credential)	Specifies the password for an 802.1X credentials profile.
username (dot1x credential)	Specifies the username for an 802.1X credentials profile.

dot1x critical (global configuration)

To configure the IEEE 802.1X critical authentication parameters, use the **dot1x critical** command in global configuration mode.

dot1x critical {**eapol**| **recovery delay** *milliseconds*}

Syntax Description

eapol	Specifies that the switch sends an EAPOL-Success message when the switch successfully authenticates the critical port.
recovery delay *milliseconds*	Specifies the recovery delay period that the switch waits to reinitialize a critical port when an unavailable RADIUS server becomes available; valid values are from 1 to 10000, in milliseconds.

Command Default

The default settings are as follows:

- **eapol** --Disabled
- *milliseconds* --1000 milliseconds

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.
12.2(33)SXI	The **recovery delay** keyword was replaced by the **authentication critical recovery delay** command.

Examples

This example shows how to specify that the switch sends an EAPOL-Success message when the switch successfully authenticates the critical port:

```
Switch(config)# dot1x critical eapol
```

This example shows how to set the recovery delay period that the switch waits to reinitialize a critical port when an unavailable RADIUS server becomes available:

```
Switch(config)# dot1x critical recovery delay 1500
```

Related Commands

Command	Description
dot1x critical (interface configuration)	Enables 802.1X critical authentication on an interface.

dot1x critical (interface configuration)

To enable 802.1X critical authentication, and optionally, 802.1X critical authentication recovery and authentication, on an interface, use the **dot1x critical** command in interface configuration mode. To disable 802.1X critical authentication, and optionally, 802.1X critical authentication recovery and authentication, use the **no** form of this command.

dot1x critical [**recovery action reinitialize**]

no dot1x critical [**recovery action reinitialize**]

Syntax Description

recovery action reinitialize	(Optional) Enables 802.1X critical authentication recovery and specifies that the port is authenticated when an authentication server is available.

Command Default

The 802.1X critical authentication is enabled on an interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.

Examples

This example shows how to enable 802.1X critical authentication on an interface:

```
Router(config-if)# dot1x critical
```

This example shows how to enable 802.1X critical authentication recovery and authenticate the port when an authentication server is available:

```
Router(config-if)# dot1x critical recovery action reinitialize
```

This example shows how to disable 802.1X critical authentication on an interface:

```
Router(config-if)# no
 dot1x critical
```

Related Commands

Command	Description
dot1x critical (global configuration)	Configures the 802.1X critical authentication parameters.

dot1x default

To reset the global 802.1X authentication parameters to their default values as specified in the latest IEEE 802.1X standard, use the **dot1x default** command in global configuration or interface configuration mode.

dot1x default

Syntax Description

This command has no arguments or keywords.

Command Default

The default values are as follows:

- The per-interface 802.1X protocol enable state is disabled (force-authorized).
- The number of seconds between reauthentication attempts is 3600 seconds.
- The quiet period is 60 seconds.
- The retransmission time is 30 seconds.
- The maximum retransmission number is 2 times.
- The multiple host support is disabled.
- The client timeout period is 30 seconds.
- The authentication server timeout period is 30 seconds.

Command Modes

Global configuration (config) Interface configuration (config-if)

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.
12.2(14)SX	This command was implemented on the Supervisor Engine 720 in Cisco IOS Release 12.2(14)SX.
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.
12.2(17d)SXB	This command was implemented on the Supervisor Engine 2 in Cisco IOS Release 12.2(17d)SXB.
12.4(6)T	Interface configuration was added as a configuration mode for this command.

Release	Modification
12.4(4)XC	This command was integrated into Cisco IOS Release 12.4(4)XC for Cisco 870 Integrated Services Routers (ISRs) only.
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 12.2(33)SXH.

Usage Guidelines

The IEEE 802.1x standard defines a client-server-based access control and authentication protocol that restricts unauthorized devices from connecting to a LAN through publicly accessible ports. 802.1x controls network access by creating two distinct virtual access points at each port. One access point is an uncontrolled port; the other is a controlled port. All traffic through the single port is available to both access points. 802.1x authenticates each user device that is connected to a switch port and assigns the port to a VLAN before making available any services that are offered by the switch or the LAN. Until the device is authenticated, 802.1x access control allows only Extensible Authentication Protocol (EAP) over LAN (EAPOL) traffic through the port to which the device is connected. After authentication is successful, normal traffic can pass through the port.

Use the **show dot1x**command to verify your current 802.1X settings.

Cisco IOS Release 12.4(4)XC

For Cisco IOS Release 12.4(4)XC, on Cisco 870 ISRs only, this command can be configured on Layer 2 (for switch ports) and Layer 3 (for switched virtual interfaces). However, the command can function at only one layer at a time; that is, if it is configured on Layer 2, it cannot also be configured on Layer 3 and vice versa.

Examples

The following example shows how to reset the global 802.1X parameters:

```
Router(config)# dot1x default
```

The following example show how to reset the global 802.1X parameters on FastEthernet interface 0:

```
Router(config)# interface FastEthernet0
Router(config-if)# dot1x default
```

Related Commands

Command	Description
dot1x critical (global configuration)	Configures the 802.1X critical authentication parameters.
dot1x critical (interface configuration)	Enables 802.1X critical authentication on an interface.
dot1x max-req	Sets the maximum number of times that the device sends an EAP request/identity frame to a client (assuming that a response is not received) before restarting the authentication process.
dot1x re-authentication (EtherSwitch)	Enables periodic reauthentication of the client for the Ethernet switch network module.

Command	Description
dot1x timeout (EtherSwitch)	Sets retry timeouts for the Ethernet switch network module.
show dot1x	Displays 802.1X information.
show dot1x (EtherSwitch)	Displays the 802.1X statistics, administrative status, and operational status for the device or for the specified interface.

dot1x guest-vlan

To specify an active VLAN as an IEEE 802.1x guest VLAN, use the **dot1x guest-vlan**command in interface configuration mode. To return to the default setting, use the **no** form of this command.

dot1x guest-vlan vlan-id

no dot1x guest-vlan

Syntax Description

vlan-id	Specify an active VLAN as an IEEE 802.1x guest VLAN. The range is 1 to 4094.

Command Default

No guest VLAN is configured.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(14)EA1	This command was introduced.
12.2(25)SE	This command was modified to change the default guest VLAN behavior.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
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)S	This command was integrated into Cisco IOS Release 15.3(1)S.

Usage Guidelines

You can configure a guest VLAN on a static-access port.

For each IEEE 802.1x port, you can configure a guest VLAN to provide limited services to clients (a device or workstation connected to the switch) not running IEEE 802.1x authentication. These users might be upgrading their systems for IEEE 802.1x authentication, and some hosts, such as Windows 98 systems, might not be IEEE 802.1x capable.

When you enable a guest VLAN on an IEEE 802.1x port, the software assigns clients to a guest VLAN when it does not receive a response to its Extensible Authentication Protocol over LAN (EAPOL) request/identity frame or when EAPOL packets are not sent by the client.

With Cisco IOS Release 12.4(11)T and later, the switch port maintains the EAPOL packet history. If another EAPOL packet is detected on the interface during the lifetime of the link, the guest VLAN feature is disabled.

If the port is already in the guest VLAN state, the port returns to the unauthorized state, and authentication restarts. The EAPOL history is reset upon loss of link.

Any number of non-IEEE 802.1x-capable clients are allowed access when the switch port is moved to the guest VLAN. If an IEEE 802.1x-capable client joins the same port on which the guest VLAN is configured, the port is put into the unauthorized state in the RADIUS-configured or user-configured access VLAN, and authentication is restarted.

Guest VLANs are supported on IEEE 802.1x switch ports in single-host or multi-host mode.

You can configure any active VLAN except a Remote Switched Port Analyzer (RSPAN) VLAN or a voice VLAN as an IEEE 802.1x guest VLAN. The guest VLAN feature is not supported on internal VLANs (routed ports) or trunk ports; it is supported only on access ports.

After you configure a guest VLAN for an IEEE 802.1x port to which a DHCP client is connected, you might need to get a host IP address from a DHCP server. You can change the settings for restarting the IEEE 802.1x authentication process on the switch before the DHCP process on the client times out and tries to get a host IP address from the DHCP server. You should decrease the settings for the IEEE 802.1x authentication process using the **dot1x max-reauth-req**and **dot1x timeout tx-period** interface configuration commands. The amount of decrease depends on the connected IEEE 802.1x client type.

Examples

This example shows how to specify VLAN 5 as an IEEE 802.1x guest VLAN:

```
Switch(config-if)# dot1x guest-vlan 5
```

This example shows how to set 3 as the quiet time on the switch, to set 15 as the number of seconds that the switch waits for a response to an EAP-request/identity frame from the client before resending the request, and to enable VLAN 2 as an IEEE 802.1x guest VLAN when an IEEE 802.1x port is connected to a DHCP client:

```
Switch(config-if)# dot1x timeout max-reauth-req 3
Switch(config-if)# dot1x timeout tx-period 15
Switch(config-if)# dot1x guest-vlan 2
```

You can display the IEEE 802.1x administrative and operational status for the device or for the specified interface by entering the **show dot1x interface***interface-id*] privileged EXEC command.

Related Commands

Command	Description
dot1x max-reauth-req	Specifies the number of times that the switch retransmits an EAP-request/identity frame to the client before restarting the authentication process.
dot1x timeout	Sets authentication retry timeouts.
show dot1x	Displays details for an identity profile.

dot1x guest-vlan supplicant

To allow the 802.1x-capable supplicants to enter the guest VLAN, use the **dot1x guest-vlan supplicant**command in global configuration mode. To prevent the 802.1x-capable supplicants from entering the guest VLAN, use the **no** form of this command.

dot1x guest-vlan supplicant

no dot1x guest-vlan supplicant

Syntax Description

This command has no arguments or keywords.

Command Default

The 802.1x-capable supplicants are prevented from entering the guest VLAN.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.

Examples

This example shows how to allow the 802.1x-capable supplicants to enter the guest VLAN:

```
Router(config)# dot1x guest-vlan supplicant
```

This example shows how to prevent the 802.1x-capable supplicants from entering the guest VLAN:

```
Router(config)# no dot1x guest-vlan supplicant
```

Related Commands

Command	Description
dot1x critical (global configuration)	Configures the 802.1X critical authentication parameters.
dot1x critical (interface configuration)	Enables 802.1X critical authentication on an interface.

dot1x host-mode

Note Effective with Cisco IOS Release 12.2(33)SXI, the **dot1x host-mode**command is replaced by the **authentication host-mode** command. See the **authentication host-mode**command for more information.

To allow hosts on an IEEE 802.1X-authorized port, use the **dot1x host-mode** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

dot1x host-mode {**multi-auth**| **multi-host**| **single-host**}

no dot1x host-mode {**multi-auth**| **multi-host**| **single-host**}

Syntax Description

multi-auth	Specifies that all clients are authenticated individually on the port. The multi-auth mode is not supported on switch ports and is the default mode for switch ports.
multi-host	Ensures that the first client and all subsequent clients are allowed access to the port if the first client is successfully authenticated.
single-host	Ensures that only the first client is authenticated. All other clients are ignored and may cause a violation. The single-host mode is the default mode for switch ports.

Command Default

Hosts are not allowed on an 802.1X-authorized port.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(14)EA1	This command was introduced for switches. It replaced the **dot1x multiple-hosts** command.
12.4(6)T	This command was integrated into Cisco IOS Release 12.4(6)T.
12.4(4)XC	This command was integrated into Cisco IOS Release 12.4(4)XC for Cisco 870 Integrated Services Switchs (ISRs) only.
12.2(33)SXI	This command was replaced by the **authentication host-mode** command.

Usage Guidelines

Before you use this command, use the **dot1x port-control auto**command to enables IEEE 802.1X port-based authentication, and cause the port to begin in the unauthorized state.

The **multi-auth** mode authenticates each new client separately.

In **multi-host** mode, only one of the attached hosts has to be successfully authorized for all hosts to be granted network access (the **multi-host** mode authenticates one client, but after the client is authenticated, traffic is allowed from all other MAC addresses.). If the port becomes unauthorized (reauthentication fails or an Extensible Authentication Protocol over LAN [EAPOL] logoff message is received), all attached clients are denied access to the network.

The **single-host** mode allows only one client per port; that is, one MAC address is authenticated, and all others are blocked.

Cisco IOS Release 12.4(4)XC

For Cisco IOS Release 12.4(4)XC, on Cisco 870 ISRs only, this command can be configured on Layer 2 (for switch ports) and Layer 3 (for switched virtual interfaces). However, the command can function at only one layer at a time; that is, if it is configured on Layer 2, it cannot also be configured on Layer 3 and vice versa.

Examples

The following example shows how to enable IEEE 802.1X globally, to enable IEEE 802.1x on a port, and to enable multiple-hosts mode:

```
Switch(config)# dot1x system-auth-control
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x host-mode multi-host:
```

Examples

The following example shows Layer 3 802.1X support on a switched virtual interface (using a Cisco 870 ISR):

```
interface FastEthernet0
 description  switchport connect to a client
!
interface FastEthernet1
 description  switchport connect to a client
!
interface FastEthernet2
 description  switchport connect to a client
!
interface FastEthernet3
 description  switchport connect to a client
!
interface FastEthernet4
 description  Connect to the public network
!
interface Vlan1
 description  Apply 802.1x functionality on SVI
 dot1x pae authenticator
 dot1x port-control auto
 dot1x reauthentication
```

Related Commands

Command	Description
dot1x port-control	Enables 802.1X port-based authentication.

Command	Description
show dot1x	Displays details for an identity profile.

dot1x initialize

Note Effective with Cisco IOS Release 12.2(33)SXI, the **dot1x initialize** command is replaced by the **clear authentication session** command. See the **clear authentication session** command for more information.

To initialize 802.1X clients on all 802.1X-enabled interfaces, use the **dot1x initialize** command in privileged EXEC mode. This command does not have a **no** form.

dot1x initialize [**interface** *interface-name*]

Syntax Description

interface *interface-name*	(Optional) Specifies an interface to be initialized. If this keyword is not entered, all interfaces are initialized.

Command Default

State machines are not enabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(14)EA1	This command was introduced.
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.

Usage Guidelines

Use this command to initialize the 802.1X state machines and to set up a fresh environment for authentication. After you enter this command, the port status becomes unauthorized.

Examples

The following example shows how to manually initialize a port:

```
Router# dot1x initialize interface gigabitethernet2/0/2
```

You can verify the unauthorized port status by entering the **show dot1x** [**interface** *interface-name*] command.

Related Commands

Command	Description
show dot1x	Displays details for an identity profile.

dot1x mac-auth-bypass

To enable a switch to authorize clients based on the client MAC address, use the **dot1x mac-auth-bypass**command in interface configuration mode. To disable MAC authentication bypass, use the **no** form of this command.

dot1x mac-auth-bypass [eap]

no dot1x mac-auth-bypass

Syntax Description

eap	(Optional) Configures the switch to use Extensible Authentication Protocol (EAP) for authorization.

Command Default

MAC authentication bypass is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(33)SXH	This command was introduced.
15.1(4)M	This command was integrated into Cisco IOS Release 15.1(4)M.

Usage Guidelin

Note To use MAC authentication bypass on a routed port, ensure that MAC address learning is enabled on the port.

When the MAC authentication bypass feature is enabled on an 802.1X port, the switch uses the MAC address as the client identity. The authentication server has a database of client MAC addresses that are allowed network access. If authorization fails, the switch assigns the port to the guest VLAN if a VLAN is configured.

Examples

This example shows how to enable MAC authentication bypass:

```
Router(config)# interface fastethernet 5/1
Router(config-if)# dot1x mac-auth-bypass
```

This example shows how to configure the switch to use EAP for authorization:

```
Router(config)# interface fastethernet 5/1
Router(config-if)# dot1x mac-auth-bypass eap
```

This example shows how to disable MAC authentication bypass:

```
Router(config)# interface fastethernet 5/1
Router(config-if)# no dot1x mac-auth-bypass
```

Related Commands

Command	Description
dot1x critical (global configuration)	Configures the 802.1X critical authentication parameters.
dot1x critical (interface configuration)	Enables 802.1X critical authentication on an interface.

dot1x max-reauth-req

To set the maximum number of times the authenticator sends an Extensible Authentication Protocol (EAP) request/identity frame (assuming that no response is received) to the client , use the **dot1x max-reauth-req**command in interface configuration mode. To set the maximum number of times to the default setting of 2, use the **no** form of this command.

dot1x max-reauth-req *number*

no dot1x max-reauth-req

Syntax Description

number	Maximum number of times. The range is 1 through 10. The default is 2.

Command Default

The command default is 2.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(18)SE	This command was introduced.
12.2(25)SEC	The *number* argument was added.
12.4(6)T	This command was integrated into Cisco IOS Release 12.4(6)T.
12.4(4)XC	This command was integrated into Cisco IOS Release 12.4(4)XC for Cisco 870 Integrated Services Routers (ISRs) only.

Usage Guidelines

You should change the default value of this command only to adjust for unusual circumstances, such as unreliable links or specific behavioral problems with certain clients and authentication servers.

Cisco IOS Release 12.4(4)XC

For Cisco IOS Release 12.4(4)XC, on Cisco 870 ISRs only, this command can be configured on Layer 2 (for switch ports) and Layer 3 (for switched virtual interfaces). However, the command can function at only one layer at a time, that is, if it is configured on Layer 2, it cannot also be configured on Layer 3 and vice versa.

Verifying Settings

You can verify your settings by entering the show dot1x [interface interface-id] command.

Examples

The following example shows how to set 4 as the number of times that the authentication process is restarted before changing to the unauthorized state:

```
Router(config-if)# dot1x max-reauth-req 4
```

Examples

The following example shows Layer 3 802.1X support on a switched virtual interface (using a Cisco 870 ISR):

```
interface FastEthernet0
 description  switchport connect to a client
!
interface FastEthernet1
 description  switchport connect to a client
!
interface FastEthernet2
 description  switchport connect to a client
!
interface FastEthernet3
 description  switchport connect to a client
!
interface FastEthernet4
 description  Connect to the public network
!
interface Vlan1
 description  Apply 802.1x functionality on SVI
 dot1x pae authenticator
 dot1x port-control auto
 dot1x reauthentication
```

Related Commands

Command	Description
dot1x max-req	Sets the maximum number of times that a device can send an EAP request/identity frame to a client (assuming that a response is not received) before restarting the authentication process .
dot1x timeout tx-period	Sets the number of seconds that the switch waits for a response to an EAP request or identity frame from the client before resending the request.
show dot1x	Displays IEEE 802.1X status for the specified port.

dot1x max-req

To set the maximum number of times that a networking device or Ethernet switch network module can send an Extensible Authentication Protocol (EAP) request/identity frame to a client (assuming that a response is not received) before restarting the authentication process, use the **dot1x max-req**command in interface configuration or global configuration mode. To set the number of times to the default setting of 2, use the **no** form of this command.

dot1x max-req *retry-number*

no dot1x max-req

Syntax Description

retry-number	Maximum number of retries. The value is from 1 through 10. The default value is 2. The value is applicable to all EAP packets except for Request ID.

Command Default

The default number of retries is 2.

Command Modes

Interface configuration (config-if) Global configuration (config)

Command History

Release	Modification
12.1(6)EA2	This command was introduced on the Cisco Ethernet switch network module.
12.2(14)SX	This command was implemented on the Supervisor Engine 720 in Cisco IOS Release 12.2(14)SX.
12.2(15)ZJ	This command was implemented on the Cisco Ethernet switch network module on the following platforms in Cisco IOS Release 12.2(15)ZJ: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series.
12.1(11)AX	This command was integrated into Cisco IOS Release 12.1(11)AX.
12.1(14)EA1	This command was integrated into Cisco IOS Release 12.1(14)EA1 and the configuration mode was changed to interface configuration mode except on the EtherSwitch network module.
12.3(2)XA	This command was integrated into Cisco IOS Release 12.3(2)XA and implemented on the following router platforms: Cisco 806, Cisco 831, Cisco 836, Cisco 837, Cisco 1701, Cisco 1710, Cisco 1721, Cisco 1751-V, and Cisco 1760.

Release	Modification
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T and implemented on the following router platforms: Cisco 1751, Cisco 2610XM, Cisco 2611XM, Cisco 2620XM, Cisco 2621XM, Cisco 2650XM, Cisco 2651XM, Cisco 2691, Cisco 3640, Cisco 3640A, and Cisco 3660.
12.2(17d)SXB	This command was implemented on the Supervisor Engine 2 in Cisco IOS Release 12.2(17d)SXB.
12.4(4)XC	This command was integrated into Cisco IOS Release 12.4(4)XC for Cisco 870 Integrated Services Routers (ISRs) only.
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.

Usage Guidelines

The IEEE 802.1x standard defines a client-server-based access control and authentication protocol that restricts unauthorized devices from connecting to a LAN through publicly accessible ports. 802.1x controls network access by creating two distinct virtual access points at each port. One access point is an uncontrolled port; the other is a controlled port. All traffic through the single port is available to both access points. 802.1x authenticates each user device that is connected to a switch port and assigns the port to a VLAN before making available any services that are offered by the switch or the LAN. Until the device is authenticated, 802.1x access control allows only Extensible Authentication Protocol (EAP) over LAN (EAPOL) traffic through the port to which the device is connected. After authentication is successful, normal traffic can pass through the port.

Note You should change the default value of this command only to adjust for unusual circumstances, such as unreliable links or specific behavioral problems with certain clients and authentication servers.

Cisco IOS Release 12.4(4)XC

For Cisco IOS Release 12.4(4)XC, on Cisco 870 ISRs only, this command can be configured on Layer 2 (for switch ports) and Layer 3 (for switched virtual interfaces). However, the command can function at only one layer at a time, that is, if it is configured on Layer 2, it cannot also be configured on Layer 3 and vice versa.

Examples

The following example shows that the maximum number of times that the networking device will send an EAP request or identity message to the client PC is 6:

```
Router(config) configure terminal
Router(config)# interface ethernet 0
Router(config-if)# dot1x max-req 6
```

The following example shows how to set the number of times that a switch sends an EAP request or identity frame to 5 before restarting the authentication process:

```
Router(config-if)# dot1x max-req 5
```

Related Commands

Command	Description
dot1x port-control	Enables manual control of the authorization state of a controlled port.
dot1x re-authentication	Globally enables periodic reauthentication of the client PCs on the 802.1X interface.
dot1x reauthentication (EtherSwitch)	Enables periodic reauthentication of the Ethernet switch network module client on the 802.1X interface.
dot1x timeout	Sets retry timeouts.
dot1x timeout (EtherSwitch)	Sets retry timeouts for the Ethernet switch network module.
show dot1x	Displays details for an identity profile.
show dot1x (EtherSwitch)	Displays the 802.1X statistics, administrative status, and operational status for the device or for the specified interface.

dot1x max-start

To set the maximum number of Extensible Authentication Protocol (EAP) start frames that a supplicant sends (assuming that no response is received) to the client before concluding that the other end is 802.1X unaware, use the **dot1x max-start**command in global configuration or interface configuration mode. To remove the maximum number-of-times setting, use the **no** form of this command.

dot1x max-start *number*

no dot1x max-start

Syntax Description

number	Maximum number of times that the router sends an EAP start frame. The value is from 1 to 65535. The default is 3.

Command Default

The default maximum number setting is 3.

Command Modes

Global configuration Interface configuration

Command History

Release	**Modification**
12.3(11)T	This command was introduced.
12.4(6)T	Global configuration mode was added for this command.
12.4(4)XC	This command was integrated into Cisco IOS Release 12.4(4)XC for Cisco 870 Integrated Services Routers (ISRs) only.
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

For Cisco IOS Release 12.4(4)XC, on Cisco 870 ISRs only, this command can be configured on Layer 2 (for switch ports) and Layer 3 (for switched virtual interfaces). However, the command can function at only one layer at a time, that is, if it is configured on Layer 2, it cannot also be configured on Layer 3 and vice versa.

Examples

The following example shows that the maximum number of EAP over LAN- (EAPOL-) Start requests has been set to 5:

```
Router (config)# interface Ethernet1
Router (config-if)# dot1x pae supplicant
Router (config-if)# dot1x max-start 5
```

Examples

The following example shows Layer 3 802.1X support on a switched virtual interface (using a Cisco 870 ISR):

```
interface FastEthernet0
 description  switchport connect to a client
!
interface FastEthernet1
 description  switchport connect to a client
!
interface FastEthernet2
 description  switchport connect to a client
!
interface FastEthernet3
 description  switchport connect to a client
!
interface FastEthernet4
 description  Connect to the public network
!
interface Vlan1
 description  Apply 802.1x functionality on SVI
 dot1x pae authenticator
 dot1x port-control auto
```

dot1x reauthentication

Related Commands

Command	Description
dot1x pae	Sets the PAE type during 802.1X authentication.
interface	Configures an interface type.

dot1x multi-hosts

To allow multiple hosts (clients) on an 802.1X-authorized port in interface configuration command mode, use the **dot1x multi-hosts** command. Use the **no** form of this command to disallow multiple hosts.

dot1x multi-hosts

no dot1x multi-hosts

Syntax Description

This command has no arguments or keywords.

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(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.

Usage Guidelines

Before entering this command, ensure that the **dot1x port-control**command is set to **auto** for the specified interface.

Examples

This example shows how to allow multiple hosts:

```
Router(config-if)# dot1x multi-hosts
Router(config-if)#
```

This example shows how to disallow multiple hosts:

```
Router(config-if)# no dot1x multi-hosts
Router(config-if)#
```

Related Commands

Command	Description
dot1x port-control	Sets the port control value.
show dot1x	Displays 802.1X information.

dot1x multiple-hosts

Note This command was replaced by the **dot1x host-mode** command effective with Cisco IOS Release 12.1(14)EA1 and Release 12.4(6)T.

To allow multiple hosts (clients) on an 802.1X-authorized switch port that has the **dot1x port-control** interface configuration command set to **auto**, use the **dot1x multiple-hosts** command in interface configuration mode. To return to the default setting, use the **no** form of this command.

dot1x multiple-hosts

no dot1x multiple-hosts

Syntax Description

This command has no arguments or keywords.

Command Default

Multiple hosts are disabled.

Command Modes

Interface configuration

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.
12.1(14)EA1	This command was replaced by the **dot1x host-mode** command in Cisco IOS Release 12.1(14)EA1.
12.4(6)T	This command was replaced by the **dot1x host-mode** command on the T-train.

Usage Guidelines

This command is supported only on switch ports.

This command enables you to attach multiple clients to a single 802.1X-enabled port. In this mode, only one of the attached hosts must be successfully authorized for all hosts to be granted network access. If the port becomes unauthorized (reauthentication fails or an Extensible Authentication Protocol over LAN [EAPOL]-logoff message is received), all attached clients are denied access to the network.

Use the **show dot1x**(EtherSwitch)privileged EXEC command with the **interface** keyword to verify your current 802.1X multiple host settings.

Examples

The following example shows how to enable 802.1X on Fast Ethernet interface 0/1 and to allow multiple hosts:

```
Router(config)# interface fastethernet0/1
Router(config-if)# dot1x port-control auto
Router(config-if)# dot1x multiple-hosts
```

Related Commands

Command	Description
dot1x default	Enables manual control of the authorization state of the port.
show dot1x (EtherSwitch)	Displays the 802.1X statistics, administrative status, and operational status for the device or for the specified interface.

dot1x pae

To set the Port Access Entity (PAE) type, use the **dot1x pae** command in interface configuration mode. To disable the PAE type that was set, use the **no** form of this command.

dot1x pae [**supplicant**| **authenticator**| **both**]

no dot1x pae [**supplicant**| **authenticator**| **both**]

Syntax Description

supplicant	(Optional) The interface acts only as a supplicant and will not respond to messages that are meant for an authenticator.
authenticator	(Optional) The interface acts only as an authenticator and will not respond to any messages meant for a supplicant.
both	(Optional) The interface behaves both as a supplicant and as an authenticator and thus will respond to all dot1x messages.

Command Default

PAE type is not set.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(11)T	This command was introduced.
12.4(4)XC	This command was integrated into Cisco IOS Release 12.4(4)XC for Cisco 870 Integrated Services Routers (ISRs) only.
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

If the **dot1x system-auth-control**command has not been configured, the **supplicant** keyword will be the only keyword available for use with this command. (That is, if the **dot1x system-auth-control**command has not been configured, you cannot configure the interface as an authenticator.)

Cisco IOS Release 12.4(4)XC

For Cisco IOS Release 12.4(4)XC, on Cisco 870 ISRs only, this command can be configured on Layer 2 (for switch ports) and Layer 3 (for switched virtual interfaces). However, the command can function at only one layer at a time, that is, if it is configured on Layer2, it cannot also be configured on Layer 3 and vice versa.

Examples

The following example shows that the interface has been set to act as a supplicant:

```
Router (config)# interface Ethernet1
Router (config-if)# dot1x pae supplicant
```

Examples

The following example shows Layer 3 802.1X support on a switched virtual interface (using a Cisco 870 ISR):

```
interface FastEthernet0
 description  switchport connect to a client
!
interface FastEthernet1
 description  switchport connect to a client
!
interface FastEthernet2
 description  switchport connect to a client
!
interface FastEthernet3
 description  switchport connect to a client
!
interface FastEthernet4
 description  Connect to the public network
!
interface Vlan1
 description  Apply 802.1x functionality on SVI
 dot1x pae authenticator
 dot1x port-control auto
```

dot1x reauthentication

Related Commands

Command	Description
dot1x system-auth-control	Enables 802.1X SystemAuthControl (port-based authentication).
interface	Configures an interface type.

dot1x port-control

Note Effective with Cisco IOS Release 12.2(33)SXI, the **dot1x port-control** command is replaced by the **authentication port-control** command. See the **authentication port-control** command for more information.

To enable manual control of the authorization state of a controlled port, use the **dot1x port-control** command in interface configuration mode. To disable the port-control value, use the **no** form of this command.

dot1x port-control {**auto**| **force-authorized**| **force-unauthorized**}

no dot1x port-control

Syntax Description

auto	Enables 802.1X port-based authentication and causes the port to begin in the unauthorized state, allowing only Extensible Authentication Protocol over LAN (EAPOL) frames to be sent and received through the port.
force-authorized	Disables 802.1X on the interface and causes the port to change to the authorized state without any authentication exchange required. The port transmits and receives normal traffic without 802.1X-based authentication of the client. The **force-authorized** keyword is the default.
force-unauthorized	Denies all access through this interface by forcing the port to change to the unauthorized state, ignoring all attempts by the client to authenticate.

Command Default

The default is force-authorized.

Command Modes

Interface configuration

Command History

Release	Modification
12.1(6)EA2	This command was introduced for the Cisco Ethernet switch network module.
12.1(11)AX	This command was integrated into Cisco IOS Release 12.1(11)AX.
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.

Release	Modification
12.2(15)ZJ	This command was implemented on the following platforms for the Cisco Ethernet switch network module: Cisco 2600 series, Cisco 3600 series, and Cisco 3700 series.
12.3(2)XA	This command was introduced on the following Cisco Switches: Cisco 806, Cisco 831, Cisco 836, Cisco 837, Cisco 1701, Cisco 1710, Cisco 1721, Cisco 1751-V, and Cisco 1760.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T. Switch support was added for the following platforms: Cisco 1751, Cisco 2610XM, Cisco 2611XM, Cisco 2620XM, Cisco 2621XM, Cisco 2650XM, Cisco 2651XM, Cisco 2691, Cisco 3640, Cisco 3640A, and Cisco 3660.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was added for Cisco IOS Release 12.2(17d)SXB.
12.4(4)XC	This command was integrated into Cisco IOS Release 12.4(4)XC for Cisco 870 Integrated Services Switchs (ISRs) only.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXI	This command was replaced by the **authentication port-control** command.

Usage Guidelines

For Ethernet Switch Network Modules

The following guidelines apply to Ethernet switch network modules:

- The 802.1X protocol is supported on Layer 2 static-access ports.
- You can use the **auto** keyword only if the port is not configured as one of these types:
  - Trunk port--If you try to enable 802.1X on a trunk port, an error message appears, and 802.1X is not enabled. If you try to change the mode of an 802.1X-enabled port to trunk, the port mode is not changed.
  - EtherChannel port--Before enabling 802.1X on the port, you must first remove it from the EtherChannel. If you try to enable 802.1X on an EtherChannel or on an active port in an EtherChannel, an error appears, and 802.1X is not enabled. If you enable 802.1X on a not-yet active port of an EtherChannel, the port does not join the EtherChannel.
  - Switch Port Analyzer (SPAN) destination port--You can enable 802.1X on a port that is a SPAN destination port; however, 802.1X is disabled until the port is removed as a SPAN destination. You can enable 802.1X on a SPAN source port.

To globally disable 802.1X on the device, you must disable it on each port. There is no global configuration command for this task.

For Cisco IOS Release 12.4(4)XC

For Cisco IOS Release 12.4(4)XC, on Cisco 870 ISRs only, this command can be configured on Layer 2 (for switch ports) and Layer 3 (for switched virtual interfaces). However, the command can function at only one layer at a time; that is, if it is configured on Layer 2, it cannot also be configured on Layer 3 and vice versa.

Verifying Settings

You can verify your settings by entering the **show dot1x** ommand and checking the Status column in the 802.1X Port Summary section of the display. An enabled status means that the port-control value is set to auto or to force-unauthorized.

Examples

The following example shows that the authentication status of the client PC will be determined by the authentication process:

```
Switch(config)# configure terminal
Switch(config)# interface ethernet 0
Switch(config-if)# dot1x port-control auto
```

Examples

The following example shows Layer 3 802.1X support on a switched virtual interface (using a Cisco 870 ISR):

```
interface FastEthernet0
 description  switchport connect to a client
!
interface FastEthernet1
 description  switchport connect to a client
!
interface FastEthernet2
 description  switchport connect to a client
!
interface FastEthernet3
 description  switchport connect to a client
!
interface FastEthernet4
 description  Connect to the public network
!
interface Vlan1
 description  Apply 802.1x functionality on SVI
 dot1x pae authenticator
 dot1x port-control auto
```

dot1x reauthentication

Related Commands

Command	Description
dot1x max-req	Sets the maximum number of times that a switch or Ethernet switch network module can send an EAP request/identity frame to a client (assuming that a response is not received) before restarting the authentication process.
dot1x re-authentication	Globally enables periodic reauthentication of the client on the 802.1X interface.
dot1x reauthentication (EtherSwitch)	Enables periodic reauthentication of the client on the 802.1X interface.

Command	Description
dot1x timeout	Sets retry timeouts.
dot1x timeout (EtherSwitch)	Sets retry timeouts for the Ethernet switch network module.
show dot1x	Displays details for an identity profile.
show dot1x (EtherSwitch)	Displays the 802.1X statistics, administrative status, and operational status for the switch or for the specified interface.

dot1x re-authenticate (EtherSwitch)

To manually initiate a reauthentication of all 802.1X-enabled ports or the specified 802.1X-enabled port on a router with an Ethernet switch network module installed, use the **dot1x re-authenticate** command in privileged EXEC mode.

dot1x re-authenticate [**interface interface-type interface-number**]

Syntax Description

interface *interface-type interface-number*	(Optional) Specifies the slot and port number of the interface to reauthenticate.

Command Default

There is no default setting.

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

You can use this command to reauthenticate a client without waiting for the configured number of seconds between reauthentication attempts (reauthperiod) and automatic reauthentication.

Examples

The following example shows how to manually reauthenticate the device connected to Fast Ethernet interface 0/1:

```
Router# dot1x re-authenticate interface fastethernet 0/1
Starting reauthentication on FastEthernet0/1.
```

dot1x re-authenticate (privileged EXEC)

Note Effective with Cisco IOS Release 12.2(33)SXI, the **dot1x re-authenticate** command is replaced by the **clear authentication session** command. See the **clear authentication session** command for more information.

To manually initiate a reauthentication of the specified 802.1X-enabled ports, use the **dot1x re-authenticate** command in privileged EXEC mode.

dot1x re-authenticate [**interface** *interface-name interface-number*]

Syntax Description

interface *interface-name interface-number*	(Optional) Interface on which reauthentication is to be initiated.

Command Default

There is no default setting.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(11)AX	This command was introduced.
12.3(2)XA	This command was integrated into Cisco IOS Release12.3(2)XA.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.4(4)XC	This command was integrated into Cisco IOS Release 12.4(4)XC for Cisco 870 Integrated Services Routers (ISRs) only.

Usage Guidelines

You can use this command to reauthenticate a client without having to wait for the configured number of seconds between reauthentication attempts (re-authperiod) and automatic reauthentication.

Cisco IOS Release 12.4(4)XC

For Cisco IOS Release 12.4(4)XC, on Cisco 870 ISRs only, this command can be configured on Layer 2 (for switch ports) and Layer 3 (for switched virtual interfaces). However, the command can function at only one layer at a time, that is, if it is configured on Layer 2, it cannot also be configured on Layer 3 and vice versa.

Examples

The following example shows how to manually reauthenticate the device that is connected to a port:

```
Router# dot1x re-authenticate interface gigabitethernet2/0/1
```

Examples

The following example shows Layer 3 802.1X support on a switched virtual interface (using a Cisco 870 ISR):

```
interface FastEthernet0
 description  switchport connect to a client
!
interface FastEthernet1
 description  switchport connect to a client
!
interface FastEthernet2
 description  switchport connect to a client
!
interface FastEthernet3
 description  switchport connect to a client
!
interface FastEthernet4
 description  Connect to the public network
!
interface Vlan1
 description  Apply 802.1x functionality on SVI
 dot1x pae authenticator
 dot1x port-control auto
```

dot1x reauthentication

Related Commands

Command	Description
dot1x reauthentication	Globally enables periodic reauthentication of the client PCs on the 802.1X interface.
dot1x timeout	Sets retry timeouts.

dot1x reauthentication

Note Effective with Cisco IOS Release 12.2(33)SXI, the **dot1x reauthentication** command is replaced by the **authentication periodic**command. See the **authentication periodic** command for more information.

To enable periodic reauthentication of the client PCs on the 802.1X interface, use the **dot1x reauthentication** command in interface configuration mode. To disable periodic reauthentication, use the **no** form of this command.

dot1x reauthentication

no dot1x reauthentication

Syntax Description

This command has no arguments or keywords.

Command Default

Periodic reauthentication is not set.

Command Modes

Interface configuration

Command History

Release	Modification
12.2(14)SX	This command was introduced on the Supervisor Engine 720.
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(17d)SXB	This command was implemented on the Supervisor Engine 2 in Cisco IOS Release 12.2(17d)SXB.
12.4(4)XC	This command was integrated into Cisco IOS Release 12.4(4)XC for Cisco 870 Integrated Services Routers (ISRs) only.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXI	This command was replaced by the **authentication periodic** command.

Usage Guidelines

The reauthentication period can be set using the **dot1x timeout** command.

Cisco IOS Release 12.4(4)XC

For Cisco IOS Release 12.4(4)XC, on Cisco 870 ISRs only, this command can be configured on Layer 2 (for switch ports) and Layer 3 (for switched virtual interfaces). However, the command can function at only one layer at a time; that is, if it is configured on Layer 2, it cannot also be configured on Layer 3 and vice versa.

Examples

The following example shows that reauthentication has been enabled and the reauthentication period as been set for 1800 seconds:

```
Router(config)# configure terminal
Router(config)# interface ethernet 0
Router(config-if)# dot1x reauthentication
Router(config-if)# dot1x timeout reauth-period 1800
```

Examples

The following example shows Layer 3 802.1X support on a switched virtual interface using a Cisco 870 ISR:

```
interface FastEthernet0
 description  switchport connect to a client
!
interface FastEthernet1
 description  switchport connect to a client
!
interface FastEthernet2
 description  switchport connect to a client
!
interface FastEthernet3
 description  switchport connect to a client
!
interface FastEthernet4
 description  Connect to the public network
!
interface Vlan1
 description  Apply 802.1x functionality on SVI
 dot1x pae authenticator
 dot1x port-control auto
```

dot1x reauthentication

Examples

The following example shows how to enable periodic reauthentication of the client:

```
Router(config-if)# dot1x reauthentication
Router(config-if)#
```

The following example shows how to disable periodic reauthentication of the client:

```
Router(config-if)# no dot1x reauthentication
Router(config-if)#
```

Related Commands

Command	Description
dot1x max-req	Sets the maximum number of times that a router can send an EAP request/identity frame to a client PC (assuming that a response is not received) before concluding that the client PC does not support 802.1X.
dot1x port-control	Sets an 802.1X port control value.

Command	Description
dot1x timeout	Sets retry timeouts.
show dot1x	Displays 802.1X information.

dot1x re-authentication (EtherSwitch)

To enable periodic reauthentication of the client for an Ethernet switch network module, use the **dot1x re-authentication** command in global configuration mode. To disable periodic reauthentication, use the **no** form of this command.

dot1x re-authentication

no dot1x re-authentication

Syntax Description

This command has no arguments or keywords.

Command Default

Periodic reauthentication is disabled.

Command Modes

Global configuration

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

You configure the amount of time between periodic reauthentication attempts by using the **dot1x timeout re-authperiod** global configuration command.

Examples

The following example shows how to disable periodic reauthentication of the client:

```
Router(config)# no dot1x re-authentication
```

The following example shows how to enable periodic reauthentication and set the number of seconds between reauthentication attempts to 4000 seconds:

```
Router(config)# dot1x re-authentication
Router(config)# dot1x timeout re-authperiod 4000
```

Related Commands

Command	Description
dot1x timeout (EtherSwitch)	Sets retry timeouts for the Ethernet switch network module.

Command	Description
show dot1x (EtherSwitch)	Displays the 802.1X statistics, administrative status, and operational status for the device or for the specified interface.

dot1x supplicant interface

To configure the dot1x supplicant for a given interface, use the **dot1x supplicant interface**command in privileged EXEC mode. To disable the configuration, use the **no** form of this command.

dot1x supplicant {**start| stop**} *profile-name* **interface** *type number*

Syntax Description

start	Starts the supplicant for a given interface.
stop	Stops the supplicant for a given interface.
profile-name	Profile name.
type number	Interface type and number.

Command Default

The dot1x supplicant interface is not configured.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.

Examples

The following example shows how to configure the dot1x supplicant for a Gigabit Ethernet interface:

```
Router# dot1x supplicant start n1 interface GigabitEthernet 0/0/1
```

Related Commands

Command	Description
dot1x default	Resets the global 802.1X authentication parameters to their default values as specified in the latest IEEE 802.1X standard.

dot1x system-auth-control

To globally enable 802.1X SystemAuthControl (port-based authentication), use the **dot1x system-auth-control**command in global configuration mode. To disable SystemAuthControl, use the **no** form of this command.

dot1x system-auth-control

no dot1x system-auth-control

Syntax Description

This command has no arguments or keywords.

Command Default

System authentication is disabled by default. If this command is disabled, all ports behave as if they are force authorized.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(2)XA	This command was introduced.
12.2(14)SX	This command was implemented on the Supervisor Engine 720.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to 12.2(17d)SXB.
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 IEEE 802.1x standard defines a client-server-based access control and authentication protocol that restricts unauthorized devices from connecting to a LAN through publicly accessible ports. 802.1x controls network access by creating two distinct virtual access points at each port. One access point is an uncontrolled port; the other is a controlled port. All traffic through the single port is available to both access points. 802.1x authenticates each user device that is connected to a switch port and assigns the port to a VLAN before making available any services that are offered by the switch or the LAN. Until the device is authenticated, 802.1x access control allows only Extensible Authentication Protocol (EAP) over LAN (EAPOL) traffic through the port to which the device is connected. After authentication is successful, normal traffic can pass through the port.

The **no** form of the command removes any 802.1X-related configurations.

Catalyst 6500 Series Switch and Cisco 7600 Series

You must enable Authentication, Authorization, and Accounting (AAA) and specify the authentication method list before enabling 802.1X. A method list describes the sequence and authentication methods to be queried to authenticate a user.

Examples

The following example shows how to enable SystemAuthControl:

```
Router(config)# dot1x system-auth-control
```

Related Commands

Command	Description
aaa authentication dot1x	Specifies one or more AAA methods for use on interfaces running IEEE 802.1X.
aaa new-model	Enables the AAA access-control model.
debug dot1x	Displays 802.1X debugging information.
description	Specifies a description for an 802.1X profile.
device	Statically authorizes or rejects individual devices.
dot1x initialize	Initializes 802.1X state machines on all 802.1X-enabled interfaces.
dot1x max-req	Sets the maximum number of times that a router or Ethernet switch network module can send an EAP request/identity frame to a client (assuming that a response is not received) before restarting the authentication process.
dot1x port-control	Enables manual control of the authorized state of a controlled port.
dot1x re-authenticate	Manually initiates a reauthentication of the specified 802.1X-enabled ports.
dot1x reauthentication	Globally enables periodic reauthentication of the client PCs on the 802.1X interface.
dot1x timeout	Sets retry timeouts.
identity profile	Creates an identity profile and enters identity profile configuration mode.
show dot1x	Displays details and statistics for an identity profile.
template	Specifies a virtual template from which commands may be cloned.

dot1x timeout

To configure the value for retry timeouts, use the **dot1x timeout** command in global configuration or interface configuration mode. To return to the default value for retry timeouts to, use the **no** form of this command.

All Platforms Except the Cisco 7600 Series Switch

dot1x timeout {**auth-period** *seconds*| **held-period** *seconds*| **quiet-period** *seconds*| **ratelimit-period** *seconds*| **reauth-period** {*seconds*| **server**}| **server-timeout** *seconds*| **start-period** *seconds*| **supp-timeout** *seconds*| **tx-period** *seconds*}

no dot1x timeout {**auth-period** *seconds*| **held-period** *seconds*| **quiet-period** *seconds*| **ratelimit-period** *seconds*| **reauth-period** {*seconds*| **server**}| **server-timeout** *seconds*| **start-period** *seconds*| **supp-timeout** *seconds*| **tx-period** *seconds*}

Cisco 7600 Series Switch

dot1x timeout {**reauth-period** *seconds*| **quiet-period** *seconds*| **tx-period** *seconds*| **supp-timeout** *seconds*| **server-timeout** *seconds*}

no dot1x timeout {**reauth-period| quiet-period| tx-period| supp-timeout| server-timeout**}

Syntax Description

auth-period *seconds*	Configures the time, in seconds, the supplicant (client) waits for a response from an authenticator (for packets other than Extensible Authentication Protocol over LAN [EAPOL]-Start) before timing out. • The range is from 1 to 65535. The default is 30.
held-period *seconds*	Configures the time, in seconds for which a supplicant will stay in the HELD state (that is, the length of time it will wait before trying to send the credentials again after a failed attempt). • The range is from 1 to 65535. The default is 60.
quiet-period *seconds*	Configures the time, in seconds, that the authenticator (server) remains quiet (in the HELD state) following a failed authentication exchange before trying to reauthenticate the client. • For all platforms except the Cisco 7600 series Switch, the range is from 1 to 65535. The default is 120. • For the Cisco 7600 series Switch, the range is from 0 to 65535. The default is 60.

ratelimit-period *seconds*	Throttles the EAP-START packets that are sent from misbehaving client PCs (for example, PCs that send EAP-START packets that result in the wasting of switch processing power). • The authenticator ignores EAPOL-Start packets from clients that have successfully authenticated for the rate-limit period duration. • The range is from 1 to 65535. By default, rate limiting is disabled.
reauth-period {*seconds* | **server**}	Configures the time, in seconds, after which an automatic reauthentication should be initiated. • The **server**keyword indicates that the reauthentication period value for the client should be obtained from the authentication, authorization, and accounting (AAA) server as the Session-Timeout (RADIUS Attribute 27) value. If the **server** keyword is used, the action upon reauthentication is also decided by the server and sent as the Termination-Action (RADIUS Attribute 29) value. The termination action could be either "terminate" or "reauthenticate." If the **server** keyword is not used, the termination action is always "reauthenticate." • For all platforms except the Cisco 7600 series switch, the range is from 1 to 65535. The default is 3600. • For the Cisco 7600 series switch, the range is from 1 to 4294967295. The default is 3600. See the "Usage Guidelines" section for additional information. **Note** Effective with Cisco IOS Release 12.2(33)SXI, this phrase is replaced by the **authentication timer reauthenticate**command. See the **authentication timer reauthenticate**command for more information.

server-timeout *seconds*	Configures the interval, in seconds, between two successive EAPOL-Start frames when they are being retransmitted. • For all platforms except the Cisco 7600 series switch, the range is from 1 to 65535. The default is 30. • For the Cisco 7600 series switch, the range is from 30 to 65535. The default is 30. If the server does not send a response to an 802.1X packet within the specified period, the packet is sent again.
start-period *seconds*	Configures the interval, in seconds, between two successive EAPOL-Start frames when they are being retransmitted. • The value is from 1 to 65535. The default is 30.
supp-timeout *seconds*	Sets the authenticator-to-supplicant retransmission time for all EAP messages other than EAP Request ID. • For all platforms except the Cisco 7600 series Switch, the range is from 1 to 65535. The default is 30. • For the Cisco 7600 series Switch, the range is from 30 to 65535. The default is 30.
tx-period *seconds*	Configures the number of seconds between retransmission of EAP request ID packets (assuming that no response is received) to the client. • For all platforms except the Cisco 7600 series switch, the range is from 1 to 65535. The default is 30. • For the Cisco 7600 series switch, the range is from 30 to 65535. The default is 30. • If an 802.1X packet is sent to the supplicant and the supplicant does not send a response after the retry period, the packet will be sent again.

Command Default

Periodic reauthentication and periodic rate-limiting are not done.

Command Modes

Global configuration Interface configuration

Cisco 7600 Switch

Interface configuration

Command History

Release	Modification
12.2(14)SX	This command was introduced on the Supervisor Engine 720.
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(18)SE	Ranges for the **server-timeout**, **supp-timeout**, and **tx-period** keywords were changed.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was added for Cisco IOS Release 12.2(17d)SXB.
12.3(11)T	The **auth-period**, **held-period**, and **start-period** keywords were added.
12.2(25)SEC	The range for the **tx-period** keyword was changed, and the **reauth-period** and **server-timeout** keywords were added.
12.1(11)AX	This command was introduced.
12.1(14)EA1	The **supp-timeout** and **server-timeout** keywords were added. The configuration mode for the command was changed to interface configuration mode.
12.4(6)T	The **supp-timeout** keyword was added, and this command was integrated into Cisco IOS Release 12.4(6)T.
12.4(4)XC	This command was integrated into Cisco IOS Release 12.4(4)XC for Cisco 870 Integrated Services Switchs (ISRs) only.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXI	The **reauth-period** keyword was replaced by the **authentication timer reauthenticate**command.

Usage Guidelines

For Cisco IOS Release 12.4(4)XC, on Cisco 870 ISRs only, this command can be configured on Layer 2 (for switch ports) and Layer 3 (for switched virtual interfaces). However, the command can function at only one layer at a time; that is, if it is configured on Layer 2, it cannot also be configured on Layer 3 and vice versa.

Cisco 7600 Switch

You must enable periodic reauthentication before you enter the **dot1x timeout reauth-period** command. Enter the **dot1x reauthentication** command to enable periodic reauthentication. The **dot1x timeout reauth-period** command affects the behavior of the system only if periodic reauthentication is enabled.

Examples

The following example shows that various 802.1X retransmission and timeout periods have been set:

```
Switch(config)# configure terminal
Switch(config)# interface ethernet 0
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x reauthentication
Switch(config-if)# dot1x timeout auth-period 2000
Switch(config-if)# dot1x timeout held-period 2400
Switch(config-if)# dot1x timeout reauth-period 1800
Switch(config-if)# dot1x timeout quiet-period 600
Switch(config-if)# dot1x timeout start-period 90
Switch(config-if)# dot1x timeout supp-timeout 300
Switch(config-if)# dot1x timeout tx-period 60
Switch(config-if)# dot1x timeout server-timeout 60
```

The following example shows how to return to the default reauthorization period:

```
Switch(config-if)# no dot1x timeout reauth-period
```

Examples

The following example shows how to set 802.1X retransmission and timeout periods on the Cisco 7600 Switch:

```
Switch(config-if)# dot1x timeout reauth-period 4000
Switch(config-if)# dot1x timeout tx-period 60
Switch(config-if)# dot1x timeout supp-timeout 25
Switch(config-if)# dot1x timeout server-timeout 25
```

Examples

The following example shows Layer 3 802.1X support on a switched virtual interface (using a Cisco 870 ISR):

```
interface FastEthernet0
 description  switchport connect to a client
!
interface FastEthernet1
 description  switchport connect to a client
!
interface FastEthernet2
 description  switchport connect to a client
!
interface FastEthernet3
 description  switchport connect to a client
!
interface FastEthernet4
 description  Connect to the public network
!
interface Vlan1
 description  Apply 802.1x functionality on SVI
 dot1x pae authenticator
 dot1x port-control auto
```

dot1x reauthentication

Related Commands

Command	Description
dot1x max-req	Sets the maximum number of times that a switch or Ethernet switch module can send an EAP request/identity frame to a client (assuming that a response is not received) before restarting the authentication process.
dot1x port-control	Sets an 802.1X port control value.
dot1x re-authentication	Globally enables periodic reauthentication of the client PCs on the 802.1X interface.
show dot1x	Displays 802.1X information.

dot1x timeout (EtherSwitch)

To set the number of retry seconds between 802.1X authentication exchanges when an Ethernet switch network module is installed in the router, use the **dot1x timeout**command in global configuration mode. To return to the default setting, use the **no** form of this command.

dot1x timeout {**quiet-period** *seconds*| **re-authperiod** *seconds*| **tx-period** *seconds*}

no dot1x timeout {**quiet-period** *seconds*| **re-authperiod** *seconds*| **tx-period** *seconds*}

Syntax Description

quiet-period *seconds*	Specifies the time in seconds that the Ethernet switch network module remains in the quiet state following a failed authentication exchange with the client. The range is from 0 to 65535 seconds. The default is 60 seconds.
re-authperiod *seconds*	Specifies the number of seconds between reauthentication attempts. The range is from 1 to 4294967295. The default is 3660 seconds.
tx-period *seconds*	Time in seconds that the switch should wait for a response to an EAP-request/identity frame from the client before retransmitting the request. The range is from 1 to 65535 seconds. The default is 30 seconds.

Command Default

quiet-period : 60 seconds **re-authperiod**: 3660 seconds**tx-period**: 30 seconds

Command Modes

Global configuration

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

You should change the default values of this command only to adjust for unusual circumstances such as unreliable links or specific behavioral problems with certain clients or authentication servers.

quiet-period Keyword

During the quiet period, the Ethernet switch network module does not accept or initiate any authentication requests. If you want to provide a faster response time to the user, enter a smaller number than the default.

re-authperiod Keyword

The **re-authperiod** keyword affects the behavior of the the Ethernet switch network module only if you have enabled periodic reauthentication by using the **dot1x re-authentication** global configuration command.

Examples

The following example shows how to set the quiet time on the switch to 30 seconds:

```
Router(config)# dot1x timeout quiet-period 30
```

The following example shows how to enable periodic reauthentication and set the number of seconds between reauthentication attempts to 4000 seconds:

```
Router(config)# dot1x re-authentication
Router(config)# dot1x timeout re-authperiod 4000
```

The following example shows how to set 60 seconds as the amount of time that the switch waits for a response to an EAP-request/identity frame from the client before retransmitting the request:

```
Router(config)# dot1x timeout tx-period 60
```

Related Commands

Command	Description
dot1x max-req	Sets the maximum number of times that the device sends an EAP-request/identity frame before restarting the authentication process.
dot1x re-authentication (EtherSwitch)	Enables periodic reauthentication of the client for the Ethernet switch network module.
show dot1x (EtherSwitch)	Displays the 802.1X statistics, administrative status, and operational status for the device or for the specified interface.

dpd

To configure Dead Peer Detection (DPD), use the **dpd**command in IKEv2 profile configuration mode. To delete DPD, use the **no** form of this command.

dpd *interval retry-interval* {**on-demand| periodic**}

no dpd

Syntax Description

interval	Specifies the keepalive interval in seconds. The range is 10 to 3600.
retry-interval	Specifies the retry interval in seconds when there is no reply from the peer.
on-demand	Specifies the on-demand mode to send the keepalive only in the absence of any incoming data traffic, to check the liveness of the peer before sending any data.
periodic	Specifies the periodic mode to send keepalives regularly at a specified interval.

Command Default

DPD is disabled by default.

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.

Usage Guidelines

Use this command to configure DPD globally for peers matching a profile. The DPD configuration in an Internet Key Exchange Version 2 (IKEv2) profile overrides the global DPD configuration.

Examples

The following example shows how to configure the periodic mode for DPD:

```
Router(config)# crypto ikev2 profile prf1
Router(config-ikev2-profile)# dpd 1000 250 periodic
```

Related Commands

Command	Description
crypto ikev2 dpd	Defines DPD globally for all peers.
crypto ikev2 profile	Defines IKEv2 profile.

drop (type access-control)

Note Effective with Cisco IOS Release 15.2(4)M, the **drop** command is not available in Cisco IOS software.

To configure a traffic class to discard packets belonging to a specific class, use the **drop** command in policy-map class configuration mode. To disable the packet discarding action in a traffic class, use the **no** form of this command.

drop [all]

no drop [all]

Syntax Description

all	(Optional) Discards the entire stream of packets belonging to the traffic class.

Command Default

The packet discarding action in a traffic class is disabled.

Command Modes

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

Command History

Release	Modification
15.1(3)T	This command was introduced.
15.2(4)M	This command was removed from the Cisco IOS software.

Usage Guidelines

Once the match criteria are applied to packets belonging to the specific traffic class using the **match class session** command in a class map, these packets can be discarded by configuring the **drop** command with the **all** keyword in a policy map. Packets match only on the packet session (flow) entry of the Flexible Packet Matching (FPM) access control list (ACL) pattern matching tool, and skip user-configured classification filters. When the **drop** command is specified with the **all** keyword, this command can only be associated with a class map that was created with the **class-map** command and **type access-control** keyword and used in a policy map that can be attached to one or more interfaces to specify a service policy that is created with the **policy-map** command and **type access-control** keyword.

Examples

The following example shows how to create and configure a traffic class called class1 for use in a policy map called **policy1**. The policy map (service policy) is attached to output serial interface 2/0. All packets that match access group 101 are placed in class1. Packets that belong to this class are discarded.

```
Router(config)# class-map class1
Router(config-cmap)# match access-group 101
Router(config-cmap)# exit
Router(config)# policy-map policy1
Router(config-pmap)# class class1
Router(config-pmap-c)# drop
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface serial2/0
Router(config-if)# service-policy output policy1
Router(config-if)# end
```

The following example shows how to configure a class map and policy map to specify the protocol stack class, the match criteria and action to take, and a combination of classes using session-based (flow-based) and nonsession-based actions. The **drop all** command is associated with the action to be taken on the policy.

```
Router(config)# class-map type access-control match-all my-HTTP
Router(config-cm)# match field tcp destport eq 8080
Router(config-cm)# match start tcp payload-start offset 20 size 10 regex “GET”
Router(config)# class-map type access-control match-all my-FTP
Router(config-cmap)# match field tcp destport eq 21
Router(config)# class-map type access-control match all class1
Router(config-cmap)# match class my-HTTP session
Router(config-cmap)# match start tcp payload-start offset 40 size 20 regex “abc.*def”
Router(config)# policy-map type access-control my_http_policy
Router(config-pmap)# class class1
Router(config-pmap-c)# drop all
Router(config)# interface gigabitEthernet 0/1
Router(config-if)# service-policy type access-control input my_http_policy
```

Related Commands

Command	Description
class	Specifies the name of a predefined traffic class, which was configured with the **class-map** command. The **class** command also classifies traffic to the traffic policy and enters policy-map class configuration mode.
class-map type access-control	Creates a class map to be used for matching packets to a specified class and enters class-map configuration mode for determining the exact pattern to look for in the protocol stack of interest.
log	Generates log messages for a predefined traffic class.
match class session	Configures match criteria for a class map used to identify a session (flow) containing packets of interest, which is then applied to all packets transmitted during the session.
policy-map type access-control	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy, and enters policy-map configuration mode.
show class-map	Displays all class maps and their matching criteria.

Command	Description
show policy-map	Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps.
show policy-map interface	Displays the packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific PVC on the interface.

drop (zone-based policy)

To drop packets that are sent to the router, use the **drop** command in policy-map-class configuration mode.

drop [log]

Syntax Description

log	(Optional) Displays logging messages about dropped packets.

Command Default

Packets are not dropped.

Command Modes

Policy-map-class configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.
15.1(1)S	This command was introduced into Cisco IOS Release 15.1(1)S.

Usage Guidelines

You can use this command only after entering the **policy-map type inspect** and **class type inspect** commands.

In Cisco IOS Release 15.1(2)T and earlier releases, if you use the **drop** command to configure a zone-based firewall with IP multicast traffic, all multicast updates are dropped by the zone-based firewall.

In Cisco IOS Release 15.1(3)T and later releases, all multicast updates are passed by the zone-based firewall even if you explicitly configure the **drop** command for a zone-based firewall with IP multicast traffic.

Examples

The following example creates an inspect policy map named p1 and specifies that packets will be dropped on the traffic at c1:

```
policy-map type inspect p1
 class type inspect c1
  drop
```

The following example defines a policy map that will drop HTTP traffic:

```
access-list 101 permit ip 192.168.1 0.0.0.255 any
 class-map type inspect match-all c1
  match access-group 101
  match protocol http
policy-map type inspect p1
 class type inspect c1
 drop
```

Related Commands

Command	Description
class type inspect	Specifies the traffic (class) on which an action is to be performed.
policy-map type inspect	Creates Layer 3 and Layer 4 inspect type policy maps.

drop-unsecure

To drop messages with no or invalid options or an invalid signature, use the **drop-unsecure**command in neighbor discovery (ND) inspection policy configuration mode or or router advertisement (RA) guard policy configuration mode. To disable this function, use the **no** form of this command.

drop-unsecure

no drop-unsecure

Syntax Description

This command has no arguments or keywords.

Command Default

No ND inspection policies are configured.

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.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The **drop-unsecure** command drops messages with no or invalid Cryptographically Generated Address (CGA) options or Rivest, Shamir, and Adleman (RSA) signature as per RFC 3971, *Secure Discovery (SeND)*. However, note that messages with an RSA signature or CGA options that do not conform with or are not verified per RFC 3972, *Cryptographically Generated Addresses (CGA)*, are dropped.

Use the **drop-unsecure** 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 enables the router to drop messages with invalid CGA options or an invalid RSA signature:

```
Router(config)# ipv6 nd-inspection policy policy1
Router(config-nd-inspection)# drop-unsecure
```

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.

dtls port

To configure a desired port for the Datagram Transport Layer Security (DTLS) to listen, use the **dtls portcommand** in WebVPN gateway configuration mode. To disable the port, use the **no** form of this command.

dtls port *port-number*

no dtls port *port-number*

Syntax Description

port-number	DTLS port number. Range: 1025 to 65535. Default: 443.

Command Default

The default DTLS port is 443.

Command Modes

WebVPN gateway configuration (config-webvpn-gateway)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

DTLS listens on port 443 by default. You can configure the desired DTLS port using the **dtls port** command.

Examples

The following example shows how to configure 1055 as the DTLS port for a WebVPN gateway “gateway1”:

```
Router# configure terminal
Router(config)# webvpn gateway gateway1
Router(config-webvpn-gateway)# dtls port 1055
```

Related Commands

Command	Description
svc dtls	Enables DTLS support on the Cisco IOS SSL VPN.

dynamic

To define a named dynamic IP access list, use the **dynamic** command in access-list configuration mode . To remove the access lists, use the **no** form of this command.

dynamic *dynamic-name* [**timeout** *minutes*] {**deny**| **permit**} *protocol source source-wildcard destination destination-wildcard* [**precedence** *precedence*] [**tos** *tos*] **[log] [fragments]**

no dynamic *dynamic-name*

Internet Control Message Protocol (ICMP)

dynamic *dynamic-name* [**timeout** *minutes*] {**deny**| **permit**} **icmp** *source source-wildcard destination destination-wildcard* [*icmp-type* [*icmp-code*]| *icmp-message*] [**precedence** *precedence*] [**tos** *tos*] **[log] [fragments]**

Internet Group Management Protocol (IGMP)

dynamic *dynamic-name* [**timeout** *minutes*] {**deny**| **permit**} **igmp** *source source-wildcard destination destination-wildcard* [*igmp-type*] [**precedence** *precedence*] [**tos** *tos*] **[log] [fragments]**

Transmission Control Protocol (TCP)

dynamic *dynamic-name* [**timeout** *minutes*] {**deny**| **permit**} **tcp** *source source-wildcard* [*operator* [*port*]] *destination destination-wildcard* [*operator* [*port*]] **[established]** [**precedence** *precedence*] [**tos** *tos*] **[log] [fragments]**

User Datagram Protocol (UDP)

dynamic *dynamic-name* [**timeout** *minutes*] {**deny**| **permit**} **udp** *source source-wildcard* [*operator* [*port*]] *destination destination-wildcard* [*operator* [*port*]] [**precedence** *precedence*] [**tos** *tos*] **[log] [fragments]**

Syntax Description

dynamic-name	Identifies this access list as a dynamic access list. Refer to lock-and- key access documented in the “Configuring Lock-and-Key Security (Dynamic Access Lists)” chapter in the *Cisco IOSSecurity Configuration Guide* .
timeout *minutes*	(Optional) Specifies the absolute length of time (in minutes) that a temporary access-list entry can remain in a dynamic access list. The default is an infinite length of time and allows an entry to remain permanently. Refer to lock-and-key access documented in the “Configuring Lock-and-Key Security (Dynamic Access Lists)” chapter in the *Cisco IOSSecurity Configuration Guide* .
deny	Denies access if the conditions are matched.
permit	Permits access if the conditions are matched.

protocol	Name or number of an Internet protocol. It can be one of the keywords **eigrp**, **gre**, **icmp**, **igmp**, **ip**, **ipinip**, **nos**, **ospf**, **tcp**, or **udp**, or an integer in the range from 0 to 255 representing an Internet protocol number. To match any Internet protocol (including ICMP, TCP, and UDP), use the **ip**keyword. Some protocols allow further qualifiers described later.
source	Number of the network or host from which the packet is being sent. There are three alternative ways to specify the source: • Use a 32-bit quantity in four-part, dotted decimal format. • Use the **any**keyword as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255. • Use **host** *source* as an abbreviation for a *source* and *source-wildcard* of *source* 0.0.0.0.
source-wildcard	Wildcard bits to be applied to source. There are three alternative ways to specify the source wildcard: • Use a 32-bit quantity in four-part, dotted decimal format. Place 1s in the bit positions you want to ignore. • Use the **any** keyword as an abbreviation for a *source* and *source-wildcard* of 0.0.0.0 255.255.255.255. • Use **host** *source* as an abbreviation for a *source* and *source-wildcard*of *source* 0.0.0.0.
destination	Number of the network or host to which the packet is being sent. There are three alternative ways to specify the destination: • Use a 32-bit quantity in four-part, dotted decimal format . • Use the **any**keyword as an abbreviation for the *destination* and *destination-wildcard* of 0.0.0.0 255.255.255.255. • Use **host** *destination* as an abbreviation for a *destination* and *destination-wildcard* of *destination* 0.0.0.0.

destination-wildcard	Wildcard bits to be applied to the destination. There are three alternative ways to specify the destination wildcard: • Use a 32-bit quantity in four-part, dotted-decimal format. Place 1s in the bit positions you want to ignore. • Use the **any**keyword as an abbreviation for a *destination* and *destination-wildcard* of 0.0.0.0 255.255.255.255. • Use **host** *destination* as an abbreviation for a *destination* and *destination-wildcard* of *destination* 0.0.0.0.
precedence *precedence*	(Optional) Packets can be filtered by precedence level, as specified by a number from 0 to 7, or by name as listed in the section "Usage Guidelines."
tos *tos*	(Optional) Packets can be filtered by type of service (ToS) level, as specified by a number from 0 to 15, or by name as listed in the section "Usage Guidelines."
log	(Optional) Causes an informational logging message about the packet that matches the entry to be sent to the console. (The level of messages logged to the console is controlled by the **logging console** command.) The message includes the access list number, whether the packet was permitted or denied; the protocol, whether it was TCP, UDP, ICMP, or a number; and, if appropriate, the source and destination addresses and source and destination port numbers. The message is generated for the first packet that matches, and then at 5-minute intervals, including the number of packets permitted or denied in the prior 5-minute interval. The logging facility might drop some logging message packets if there are too many to be handled or if there is more than one logging message to be handled in 1 second. This behavior prevents the router from crashing due to too many logging packets. Therefore, the logging facility should not be used as a billing tool or an accurate source of the number of matches to an access list.

fragments	(Optional) The access-list entry applies to noninitial fragments of packets; the fragment is either permitted or denied accordingly. For more details about the **fragments** keyword, see the “Access List Processing of Fragments” and “Fragments and Policy Routing” sections in the “Usage Guidelines” section.
icmp-type	(Optional) ICMP packets can be filtered by ICMP message type. The type is a number from 0 to 255.
icmp-code	(Optional) ICMP packets that are filtered by ICMP message type can also be filtered by the ICMP message code. The code is a number from 0 to 255.
icmp-message	(Optional) ICMP packets can be filtered by an ICMP message type name or ICMP message type and code name. The possible names are found in the section “Usage Guidelines.”
igmp-type	(Optional) IGMP packets can be filtered by IGMP message type or message name. A message type is a number from 0 to 15. IGMP message names are listed in the section “Usage Guidelines.”
operator	(Optional) Compares source or destination ports. Possible operands include **lt** (less than), **gt** (greater than), **eq** (equal), **neq** (not equal), and **range** (inclusive range). If the operator is positioned after the *source* and *source-wildcard*, it must match the source port. If the operator is positioned after the *destination* and *destination-wildcard*, it must match the destination port. The **range** operator requires two port numbers. All other operators require one port number.
port	(Optional) The decimal number or name of a TCP or UDP port. A port number is a number from 0 to 65535 . TCP and UDP port names are listed in the section “Usage Guidelines” of the **access-list**(IP extended) command. TCP port names can only be used when filtering TCP. UDP port names can only be used when filtering UDP.
established	(Optional) For the TCP protocol only: Indicates an established connection. A match occurs if the TCP datagram has the ACK or RST bits set. The nonmatching case is that of the initial TCP datagram to form a connection.

Command Default

An extended access list defaults to a list that denies everything. An extended access list is terminated by an implicit deny statement.

Command Modes

Access-list configuration

Command History

Release	Modification
11.2	This command was introduced.
12.0(11)	The **fragments**keyword was added.
12.2(13)T	The igrp keyword was removed because the IGRP protocol is no longer available in Cisco IOS software.
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 can use named access lists to control the transmission of packets on an interface and restrict contents of routing updates. The Cisco IOS software stops checking the extended access list after a match occurs.

Fragmented IP packets, other than the initial fragment, are immediately accepted by any extended IP access list. Extended access lists used to control vty access or restrict the contents of routing updates must not match against the TCP source port, the ToS value, or the precedence of the packet.

Note Named IP access lists will not be recognized by any software release prior to Cisco IOS Release 11.2.

Note After an access list is created, any subsequent additions (possibly entered from the terminal) are placed at the end of the list. In other words, you cannot selectively add or remove access list command lines from a specific access list.

The following is a list of precedence names:

- **critical**
- **flash**
- **flash-override**
- **immediate**
- **internet**

- **network**
- **priority**
- **routine**

The following is a list of ToS names:

- **max-reliability**
- **max-throughput**
- **min-delay**
- **min-monetary-cost**
- **normal**

The following is a list of ICMP message type and code names:

- **administratively-prohibited**
- **alternate-address**
- **conversion-error**
- **dod-host-prohibited**
- **dod-net-prohibited**
- **echo**
- **echo-reply**
- **general-parameter-problem**
- **host-isolated**
- **host-precedence-unreachable**
- **host-redirect**
- **host-tos-redirect**
- **host-tos-unreachable**
- **host-unknown**
- **host-unreachable**
- **information-reply**
- **information-request**
- **mask-reply**
- **mask-request**
- **mobile-redirect**
- **net-redirect**
- **net-tos-redirect**
- **net-tos-unreachable**

- **net-unreachable**
- **network-unknown**
- **no-room-for-option**
- **option-missing**
- **packet-too-big**
- **parameter-problem**
- **port-unreachable**
- **precedence-unreachable**
- **protocol-unreachable**
- **reassembly-timeout**
- **redirect**
- **router-advertisement**
- **router-solicitation**
- **source-quench**
- **source-route-failed**
- **time-exceeded**
- **timestamp-reply**
- **timestamp-request**
- **traceroute**
- **ttl-exceeded**
- **unreachable**

The following is a list of IGMP message names:

- **dvmrp**
- **host-query**
- **host-report**
- **pim**
- **trace**

The following is a list of TCP port names that can be used instead of port numbers. Refer to the current assigned numbers RFC to find a reference to these protocols. Port numbers corresponding to these protocols can also be found if you type a ? in the place of a port number.

- **bgp**
- **chargen**
- **daytime**

- **discard**
- **domain**
- **echo**
- **finger**
- **ftp**
- **ftp-data**
- **gopher**
- **hostname**
- **irc**
- **klogin**
- **kshell**
- **lpd**
- **nntp**
- **pop2**
- **pop3**
- **smtp**
- **sunrpc**
- **syslog**
- **tacacs-ds**
- **talk**
- **telnet**
- **time**
- **uucp**
- **whois**
- **www**

The following is a list of UDP port names that can be used instead of port numbers. Refer to the current assigned numbers RFC to find a reference to these protocols. Port numbers corresponding to these protocols can also be found if you type a ? in the place of a port number.

- **biff**
- **bootpc**
- **bootps**
- **discard**
- **dns**
- **dnsix**

- **echo**
- **mobile-ip**
- **nameserver**
- **netbios-dgm**
- **netbios-ns**
- **ntp**
- **rip**
- **snmp**
- **snmptrap**
- **sunrpc**
- **syslog**
- **tacacs-ds**
- **talk**
- **tftp**
- **time**
- **who**
- **xdmcp**

Access List Processing of Fragments

The behavior of access-list entries regarding the use or lack of the **fragments** keyword can be summarized as follows:

If the Access-List Entry has...	Then..
...no **fragments** keyword (the default behavior), and assuming all of the access-list entry information matches,	For an access-list entry containing only Layer 3 information: • The entry is applied to nonfragmented packets, initial fragments and noninitial fragments. For an access-list entry containing Layer 3 and Layer 4 information: • The entry is applied to nonfragmented packets and initial fragments. • If the entry is a **permit**statement, the packet or fragment is permitted. • If the entry is a **deny**statement, the packet or fragment is denied. • The entry is also applied to noninitial fragments in the following manner. Because noninitial fragments contain only Layer 3 information, only the Layer 3 portion of an access-list entry can be applied. If the Layer 3 portion of the access-list entry matches, and • If the entry is a **permit**statement, the noninitial fragment is permitted. • If the entry is a **deny** statement, the next access-list entry is processed. **Note** The **deny** statements are handled differently for noninitial fragments versus nonfragmented or initial fragments.
...the **fragments** keyword, and assuming all of the access-list entry information matches,	**Note** The access-list entry is applied only to noninitial fragments.The **fragments** keyword cannot be configured for an access-list entry that contains any Layer 4 information.

Be aware that you should not simply add the **fragments** keyword to every access-list entry because the first fragment of the IP packet is considered a nonfragment and is treated independently of the subsequent fragments. An initial fragment will not match an access list **permit** or **deny** entry that contains the **fragments**keyword, the packet is compared to the next access-list entry, and so on, until it is either permitted or denied by an access-list entry that does not contain the **fragments** keyword. Therefore, you may need two access-list entries for every **deny** entry. The first **deny** entry of the pair will not include the **fragments** keyword, and applies to the initial fragment. The second **deny** entry of the pair will include the **fragments** keyword and applies to the subsequent fragments. In the cases where there are multiple **deny** access-list entries for the same host but with different Layer 4 ports, a single **deny** access-list entry with the **fragments** keyword for that host is all that needs to be added. Thus all the fragments of a packet are handled in the same manner by the access list.

Packet fragments of IP datagrams are considered individual packets and each counts individually as a packet in access list accounting and access list violation counts.

Note The **fragments**keyword cannot solve all cases involving access lists and IP fragments.

Fragments and Policy Routing

Fragmentation and the fragment control feature affect policy routing if the policy routing is based on the **match ip addres**s command and the access list had entries that match on Layer 4 through 7 information. It is possible that noninitial fragments pass the access list and are policy routed, even if the first fragment was not policy routed or the reverse.

By using the **fragments** keyword in access-list entries as described earlier, a better match between the action taken for initial and noninitial fragments can be made and it is more likely policy routing will occur as intended.

Examples

The following example defines a dynamic access list named abclist:

```
ip access-group abclist in
!
ip access-list extended abclist
 dynamic testlist timeout 5
 permit ip any any
 permit tcp any host 10.302.21.2 eq 23
```

Related Commands

Command	Description
clear access-template	Clears a temporary access-list entry from a dynamic access list manually.
distribute-list in (IP)	Filters networks received in updates.
distribute-list out (IP)	Suppresses networks from being advertised in updates.
ip access-group	Controls access to an interface.
ip access-list	Defines an IP access list by name.
logging console	Limits messages logged to the console based on severity.
show access-lists	Displays the contents of current IP and rate-limit access lists.
show ip access-list	Displays the contents of all current IP access lists.

E

eap

Note This command is removed effective with Cisco IOS Release 12.4(6)T.

To specify Extensible Authentication Protocol- (EAP-) specific parameters, use the **eap** command in identity profile configuration mode. To disable the parameters that were set, use the **no** form of this command.

eap {**username** *name*| **password** *password*}

no eap {**username** *name*| **password** *password*}

Syntax Description

username *name*	Username that will be sent to Request-Id packets.
password *password*	Password that should be used when replying to an Message Digest 5 (MD5) challenge.

Command Default

EAP parameters are not set.

Command Modes

Identity profile configuration

Command History

Release	Modification
12.3(11)T	This command was introduced.
12.4(6)T	This command was removed.
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 if your router is configured as a supplicant. This command provides the means for configuring the identity and the EAP MD5 password that will be used by 802.1X to authenticate.

Examples

The following example shows that the EAP username “user1” has been configured:

```
Router (config)# identity profile dot1x
Router (config-identity-prof)# eap username user1
```

Related Commands

Command	Description
identity profile	Creates an identity profile.

eap (IKEv2 profile)

To derive the name mangler from the remote identity of type Extensible Authentication Protocol (EAP), use the **eap**command in IKEv2 name mangler configuration mode. To remove the name derived from EAP, use the **no** form of this command.

eap {**all**| **dn** {**country**| **domain**| **locality**| **organization**| **organization-unit**| **state**} {**prefix**| **suffix** {**delimiter**{**.**| **@**| ****}}}}

no eap

Syntax Description

all	Derives the name mangler from the entire EAP identity.
dn	Derives the name from identities of type DN in EAP.
common-name	Derives the name from the common name portion in the DN.
country	Derives the name from the country name specified in the DN.
domain	Derives the name from the domain name specified in the DN.
locality	Derives the name from the locality specified in the DN.
organization	Derives the name from the organization specified in the DN.
organization-unit	Derives the name from the organization-unit specified in the DN.
state	Derives the name from the state name specified in the DN.
prefix	Derives the name from the prefix in EAP.
suffix	Derives the name from the suffix in EAP.
delimiter {. | @ | \}	Refers to the specified delimiter in the prefix or suffix.

Command Default

No default behavior or values.

Command Modes

IKEv2 name mangler configuration (config-ikev2-name-mangler)

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.

Usage Guidelines

Use this command to derive the name mangler from any field in the remote identity of type EAP.

Examples

The following example shows how to derive a name for the name mangler from a specific delimiter in EAP prefix:

```
Router(config)# crypto ikev2 name-mangler mangler2
Router(config-ikev2-name-mangler)# eap prefix delimiter @
```

Related Commands

Command	Description
crypto ikev2 name mangler	Defines a name mangler.

eckeypair

To configure the trustpoint to use an Elliptic Curve (EC) key on which certificate requests are generated using ECDSA signatures, use the **eckeypair** command in ca-trustpoint configuration mode. To remove the encryption key, use the **no** form of this command.

eckeypair *label*

no eckeypair *label*

Syntax Description

label	Specifies the EC key label that is configured using the **crypto key generate rsa** or **crypto key generate ec keysize** command in global configuration mode. See the Configuring Internet Key Exchange for IPsec VPNs feature module for more information.

Command Default

The trustpoint is not configured with an EC key.

Command Modes

Ca-trustpoint configuration mode (ca-trustpoint)

Command History

Release	Modification
15.1(2)T	This command was introduced in Cisco IOS Release 15.1(2)T.

Usage Guidelines

If an ECDSA signed certificate is imported without a trustpoint configuration, then the label defaults to the FQDN value.

Examples

The following example configures the EC key label in a certificate enrollment in a PKI:

```
Router(config)#
crypto pki trustpoint mytp
Router(ca-trustpoint)# eckeypair Router_1_Key
```

Related Commands

Command	Description
crypto key generate ec keysize	Generates EC keys.
crypto key generate rsa	Generates RSA keys.

Command	Description
crypto pki trustpoint	Declares the trustpoint and a given name and enters ca-trustpoint configuration mode.

email (IKEv2 profile)

To derive the name mangler from the remote identity of type e-mail, use the **email**command in IKEv2 name mangler configuration mode. To remove the name derived from the e-mail, use the **no** form of this command.

email {**all**| **domain**| **username**}

no email

Syntax Description

all	Derives the name mangler from the entire FQDN.
domain	Derives the name mangler from the domain name in e-mail.
hostname	Derives the name mangler from the username in e-mail.

Command Default

No default behavior or values.

Command Modes

IKEv2 name mangler configuration (config-ikev2-name-mangler)

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.

Usage Guidelines

Use this command to derive the name mangler from any field in the remote identity of type e-mail.

Examples

The following example shows how to derive a name for the name mangler from the username in e-mail:

```
Router(config)# crypto ikev2 name-mangler mangler2
Router(config-ikev2-name-mangler)# email username
```

Related Commands

Command	Description
crypto ikev2 name mangler	Defines a name mangler.

enable

To change the privilege level for a CLI session or to use a CLI view for a CLI session, use the **enable** command in either user EXEC, privileged EXEC, or diagnostic mode.

enable [privilege-level] [**view** [*view-name*]]

Syntax Description

privilege-level	(Optional) Privilege level at which to log in.
view	(Optional) Enters into root view, which enables users to configure CLI views. **Note** This keyword is required if you want to configure a CLI view.
view-name	(Optional) Enters or exits a specified command-line interface (CLI) view. This keyword can be used to switch from one CLI view to another CLI view.

Command Default

Privilege-level 15 (privileged EXEC)

Command Modes

User EXEC (>)

Privileged EXEC (#)

Diagnostic Mode (diag)

Command History

Release	Modification
10.0	This command was introduced.
12.3(7)T	The **view** keyword and *view-name* argument were added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	The **view** keyword and *view-name* argument were 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.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(22)SB.
Cisco IOS XE Release 2.1	This command became available on the ASR 1000 Series Routers, and became available in diagnostic mode for the first time.

Usage Guidelines

By default, using the **enable** command without the *privilege-level* argument in user EXEC mode causes the router to enter privileged EXEC mode (privilege-level 15).

Entering privileged EXEC mode enables the use of privileged commands. Because many of the privileged commands set operating parameters, privileged access should be password-protected to prevent unauthorized use. If the system administrator has set a password with the **enable password** global configuration command, you are prompted to enter the password before being allowed access to privileged EXEC mode. The password is case sensitive.

If an **enable** password has not been set, only enable mode can be accessed through the console connection.

Security levels can be set by an administrator using the **enable password** and **privilege level** commands. Up to 16 privilege levels can be specified, using the numbers 0 through 15. Using these privilege levels, the administrator can allow or deny access to specific commands. Privilege level 0 is associated with user EXEC mode, and privilege level 15 is associated with privileged EXEC mode.

For more information on defined privilege levels, see the *Cisco IOSSecurity Configuration Guide* and the *Cisco IOS Security Command Reference* publications.

If a level is not specified when entering the **enable** command, the user will enter the default mode of privileged EXEC (level 15).

Accessing a CLI View

CLI views restrict user access to specified CLI and configuration information. To configure and access CLI views, users must first enter into root view, which is accomplished via the **enable view** command (without the *view-name* argument). Thereafter, users are prompted for a password, which is the same password as the privilege level 15 password.

The *view-name* argument is used to switch from one view to another view.

To prevent dictionary attacks, a user is prompted for a password even if an incorrect view name is given. The user is denied access only after an incorrect view name and password are given.

Examples

In the following example, the user enters privileged EXEC mode (changes to privilege-level 15) by using the **enable** command without a privilege-level argument. The system prompts the user for a password before allowing access to the privileged EXEC mode. The password is not printed to the screen. The user then exits back to user EXEC mode using the **disable** command. Note that the prompt for user EXEC mode is the greater than symbol (>), and the prompt for privileged EXEC mode is the number sign (#).

```
Router> enable
Password: <letmein>
Router# disable
Router>
```

The following example shows which commands are available inside the CLI view “first” after the user has logged into this view:

```
Router# enable view first
Password:
00:28:23:%PARSER-6-VIEW_SWITCH:successfully set to view 'first'.
Router# ?
Exec commands:
  configure  Enter configuration mode
  enable     Turn on privileged commands
  exit       Exit from the EXEC
  show       Show running system information
```

```
Router# show ?
  ip       IP information
  parser   Display parser information
  version  System hardware and software status
Router# show ip ?

  access-lists            List IP access lists
  accounting              The active IP accounting database
  aliases                 IP alias table
  arp                     IP ARP table
  as-path-access-list     List AS path access lists
  bgp                     BGP information
  cache                   IP fast-switching route cache
  casa                    display casa information
  cef                     Cisco Express Forwarding
  community-list          List community-list
  dfp                     DFP information
  dhcp                    Show items in the DHCP database
  drp                     Director response protocol
  dvmrp                   DVMRP information
  eigrp                   IP-EIGRP show commands
  extcommunity-list       List extended-community list
  flow                    NetFlow switching
  helper-address          helper-address table
  http                    HTTP information
  igmp                    IGMP information
  irdp                    ICMP Router Discovery Protocol
.
.
```

The following example shows how to use the **enable view** command to switch from the root view to 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
disable	Exits from privileged EXEC mode to user EXEC mode, or, if privilege levels are set, to the specified privilege level.
enable password	Sets a local password to control access to various privilege levels.
privilege level (global)	Sets a privilege level for a command.

Command	Description
privilege level (line)	Sets a privilege level for a command for a specific line.

enable password

To set a local password to control access to various privilege levels, use the **enable password** command in global configuration mode. To remove the password requirement, use the **no**form of this command.

enable password [**level** *level*] {*password*| [*encryption-type*] *encrypted-password*}

no enable password [**level** *level*]

Syntax Description

level *level*	(Optional) Level for which the password applies. You can specify up to 16 privilege levels, using numbers 0 through 15. Level 1 is normal EXEC-mode user privileges. If this argument is not specified in the command or the **no** form of the command, the privilege level defaults to 15 (traditional enable privileges).
password	Password users type to enter enable mode.
encryption-type	(Optional) Cisco-proprietary algorithm used to encrypt the password. Currently the only encryption type available is 5. If you specify *encryption-type*, the next argument you supply must be an encrypted password (a password already encrypted by a Cisco router).
encrypted-password	Encrypted password you enter, copied from another router configuration.

Command Default

No password is defined. The default is level 15.

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.(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 Guidelin

Caution If neither the enable password command nor the enable secret command is configured, and if there is a line password configured for the console, the console line password will serve as the enable password for all VTY (Telnet and Secure Shell [SSH]) sessions.

Use this command with the **level** option to define a password for a specific privilege level. After you specify the level and the password, give the password to the users who need to access this level. Use the **privilege level** configuration command to specify commands accessible at various levels.

You will not ordinarily enter an encryption type. Typically you enter an encryption type only if you copy and paste into this command a password that has already been encrypted by a Cisco router.

Caution If you specify an encryption type and then enter a clear text password, you will not be able to reenter enable mode. You cannot recover a lost password that has been encrypted by any method.

If the **service password-encryption** command is set, the encrypted form of the password you create with the **enable password** command is displayed when a **more nvram:startup-config**command is entered.

You can enable or disable password encryption with the **service password-encryption**command.

An enable password is defined as follows:

- Must contain from 1 to 25 uppercase and lowercase alphanumeric characters.
- Can have leading spaces, but they are ignored. However, intermediate and trailing spaces are recognized.
- Can contain the question mark (?) character if you precede the question mark with the key combinationCrtl-v when you create the password; for example, to create the password *abc?123,* do the following:
    - Enter **abc**.
    - Type **Crtl-v**.
    - Enter **?123**.

When the system prompts you to enter the enable password, you need not precede the question mark with the Ctrl-v; you can simply enter abc?123 at the password prompt.

Examples

The following example enables the password “ pswd2” for privilege level 2:

```
enable password level 2 pswd2
```

The following example sets the encrypted password “$1$i5Rkls3LoyxzS8t9”, which has been copied from a router configuration file, for privilege level 2 using encryption type 7:

```
enable password level 2 5 $1$i5Rkls3LoyxzS8t9
```

Related Commands

Command	Description
disable	Exits privileged EXEC mode and returns to user EXEC mode.
enable	Enters privileged EXEC mode.
enable secret	Specifies an additional layer of security over the **enable password** command.
privilege	Configures a new privilege level for users and associate commands with that privilege level.
service password-encryption	Encrypts passwords.
show privilege	Displays your current level of privilege.

enable secret

To specify an additional layer of security over the **enable password** command, use the **enable secret** command in global configuration mode. To turn off the **enable secret** function, use the **no** form of this command.

enable secret [**level** *level*] {**[0]** *unencrypted-password*| *encryption-type encrypted-password*}

no enable secret [**level** *level*] [*encryption-type encrypted-password*]

Syntax Description

level *level*	(Optional) Specifies the level for which the password applies. You can specify up to 15 privilege levels, using numerals 1 through 15. Level 1 is normal EXEC-mode user privileges. If the *level* argument is not specified in the command or in the **no** form of the command, the privilege level defaults to 15 (traditional enable privileges).
0	(Optional) Specifies an unencrypted clear-text password. The password is converted to a Secure Hash Algorithm (SHA) 256 secret and gets stored in the router.
unencrypted-password	Password for users to enter enable mode. This password should be different from the password created with the **enable password** command.
encryption-type	Cisco-proprietary algorithm used to encrypt the password. The encryption types available for this command are 4 and 5. • **4** —Specifies an SHA-256 encrypted secret string. The SHA256 secret string is copied from the router configuration. • **5** —Specifies a message digest alogrithm 5 (MD5) encrypted secret.
encrypted-password	Encrypted password that is copied from another router configuration.

Command Default

No password is defined.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.0	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.
15.0(1)S	This command was integrated into Cisco IOS Release 15.0(1)S. Support for the encryption type **4** was added.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S. Support for the encryption type **4** was added.
15.1(4)M	This command was modified. Support for the encryption type **4** was added.
Cisco IOS Release 3.3SG	This command was modified. Support for the encryption type **5** was removed.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
Cisco IOS XE Release 3.8S	This command was modified. The warning message for removal of support for the encryption type **5** was modified.

Usage Guidelin

Caution If neither the **enable password** command or the **enable secret** command is configured, and if a line password is configured for the console, the console line password will serve as the enable password for all vty (Telnet and Secure Shell [SSH]) sessions.

Use the **enable secret** command to provide an additional layer of security over the enable password. The **enable secret** command provides better security by storing the enable secret password using a nonreversible cryptographic function. The added layer of security encryption provides is useful in environments where the password crosses the network or is stored on a TFTP server.

Typically you enter an encryption type only when you paste an encrypted password that you copied from a router configuration file into this command.

Caution If you specify an encryption type and then enter a clear-text password, you will not be able to reenter enable mode. You cannot recover a lost password that has been encrypted by any method.

If you use the same password for the **enable password** and **enable secret** commands, you receive an error message warning that this practice is not recommended, but the password will be accepted. By using the same password, however, you undermine the additional security the **enable secret** command provides.

Note After you set a password using the **enable secret** command, a password set using the **enable password** command works only if the **enable secret** is disabled or an older version of Cisco IOS software is being used, such as when running an older rxboot image. Additionally, you cannot recover a lost password that has been encrypted by any method.

If the **service password-encryption** command is set, the encrypted form of the password you create is displayed when the **more nvram:startup-config** command is entered.

You can enable or disable password encryption with the **service password-encryption** command.

An enable password is defined as follows:

- Must contain 1 to 25 alphanumeric characters, both uppercase and lowercase.
- Can have leading spaces, but they are ignored. However, intermediate and trailing spaces are recognized.
- Can contain the question mark (?) character if you precede the question mark with the key combinationCrtl-v when you create the password; for example, to create the password *abc?123,* do the following:
  - Enter **abc**.
  - Press **Crtl-v**.
  - Enter **?123**.

When the system prompts you to enter the enable password, you need not precede the question mark with the Ctrl-v; you can enter **abc?123** at the password prompt.

Note During a downgrade from Cisco IOS XE Release 3.3SG to Cisco IOS XE Release 3.2SG, if a SHA256-encrypted enable password is configured, then the SHA256-encrypted password will be lost without any warning, and the secret password will have to be reconfigured.

Examples

The following example shows how to specify the password with the **enable secret** command:

```
Device> enable
Device# configure terminal
Device(config)# enable secret password
```

After specifying a password with the **enable secret** command, users must enter this password to gain access. Any passwords set through **enable password** command will no longer work.

```
Password: password
```

The following example shows how to enable the encrypted password “$1$FaD0$Xyti5Rkls3LoyxzS8”, which has been copied from a router configuration file, for privilege level 2 using the encryption type 4:

```
Device> enable
Device# configure terminal
Device(config)# enable password level 2 4 $1$FaD0$Xyti5Rkls3LoyxzS8
```

The following example is a sample warning message that is displayed when a user enters the **enable secret 5** *encrypted-password* command:

```
Device(config)# enable secret 5 $1$FaD0$Xyti5Rkls3LoyxzS8

Warning: The CLI will be deprecated soon
'enable secret 5 <password>'
Please move to 'enable secret <password>' CLI
```

Related Commands

Command	Description
enable	Enters privileged EXEC mode.
enable password	Sets a local password to control access to various privilege levels.
more nvram:startup-config	Displays the startup configuration file contained in NVRAM or specified by the CONFIG_FILE environment variable.
service password-encryption	Encrypt passwords.

enabled (IPS)

To change the enabled status of a given signature or signature category, use the **enabled**command in signature-definition-status (config-sigdef-status) or IPS-category-action (config-ips-category-action) configuration mode. To return to the default action, use the **no** form of this command.

enabled {**true**| **false**}

no enabled

Syntax Description

true	Enables a specified signature or all signatures within a specified category.
false	Disables a specified signature or all signatures within a specified category.

Command Default

All commands are enabled.

Command Modes

Signature-definition-status configuration (config-sigdef-status) IPS-category-action configuration (config-ips-category-action)

Command History

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

Usage Guidelines

Use the **enabled**command to change the status of a signature or signature category to active (true) or inactive (false).

Examples

The following example shows how to change the status of signature 9000:0 to enabled:

```
Router(config)# ip ips signature-definitio
n
Router(config-sig)# signature 9000 0
Router(config-sig-sig)# status
Router(config-sigdef-status)# enabled true
```

Related Commands

Command	Description
category	Specifies a signature category that is to be used for multiple signature actions or conditions.

Command	Description
signature	Specifies a signature for which the CLI user tunings will be changed.
status	Changes the enabled or retired status of a given signature or signature category.

encryption (IKE policy)

To specify the encryption algorithm within an Internet Key Exchange (IKE) policy, use the **encryption**command in Internet Security Association Key Management Protocol (ISAK MP) policy configuration mode. IKE policies define a set of parameters to be used during IKE negotiation. To reset the encryption algorithm to the default value, use the **no** form of this command.

encryption {**des**| **3des**| **aes**| **aes 192**| **aes 256**}

no encryption

Syntax Description

des	56-bit Data Encryption Standard (DES)-CBC as the encryption algorithm.
3des	168-bit DES (3DES) as the encryption algorithm.
aes	128-bit Advanced Encryption Standard (AES) as the encryption algorithim.
aes 192	192-bit AES as the encryption algorithim.
aes 256	256-bit AES as the encryption algorithim.

The 56-bit DES-CBC encryption algorithm

Command Modes

ISAKMP policy configuration

Command History

Release	Modification
11.3 T	This command was introduced.
12.0(2)T	The **3des** option was added.
12.2(13)T	The following keywords were added: aes, aes 192, and aes 256 .
12.4(4)T	IPv6 support 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.

Usage Guidelines

Use this command to specify the encryption algorithm to be used in an IKE policy.

If a user enters an IKE encryption method that the hardware does not support, a warning message will be displayed immediately after the **encryption** command is entered.

Examples

The following example configures an IKE policy with the 3DES encryption algorithm (all other parameters are set to the defaults):

```
crypto isakmp policy
 encryption 3des
 exit
```

The following example is a sample warning message that is displayed when a user enters an IKE encryption method that the hardware does not support:

```
encryption aes 256
WARNING:encryption hardware does not support the configured
encryption method for ISAKMP policy 1
```

Related Commands

Command	Description
authentication (IKE policy)	Specifies the authentication method within an IKE policy.
crypto isakmp policy	Defines 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 policy	Displays the parameters for each IKE policy.

encryption (IKEv2 proposal)

To specify one or more encryption algorithms for an Internet Key Exchange Version 2 (IKEv2) proposal, use the **encryption**command in IKE v2 proposal configuration mode. To remove the encryption algorithm, use the **no** form of this command.

encryption 3des aes-cbc-128 aes-cbc-192 aes-cbc-256

no encryption

Syntax Description

3des	Specifies 168-bit DES (3DES) as the encryption algorithm.
aes-cbc-128	Specifies 128-bit Advanced Encryption Standard-Cipher Block Chaining (AES-CBC) as the encryption algorithim.
aes-cbc-192	Specifies 192-bit AES-CBC as the encryption algorithim.
aes-cbc-256	Specifies 256-bit AES-CBC as the encryption algorithim.

Command Default

The encryption algorithm is not specified.

Command Modes

IKEv2 proposal configuration (config-ikev2-proposal)

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 specify the encryption algorithm to be used in an IKEv2 proposal. The default encryption algorithm in the default proposal is 128-bit AES-CBC and 3 DES encryption algorithm.

Note You cannot selectively remove an encryption algorithm when multiple encryption algorithms are configured.

Examples

The following example configures an IKE proposal with the 3DES encryption algorithm:

```
Router(config)#
crypto ikev2 proposal proposal1
Router(config-ikev2-proposal)#
encryption 3des
```

Related Commands

Command	Description
crypto ikev2 proposal	Defines an IKEv2 proposal.
group (ikev2 proposal)	Specifies the DH group identifier in an IKEv2 proposal.
integrity (ikev2 proposal)	Specifies the integrity algorithm in an IKEv2 proposal.
show crypto ikev2 proposal	Displays the parameters for each IKEv2 proposal.

enforce-checksum

To enforce checksum verification for Flexible Packet Matching (FPM), use the **enforce-checksum** command in fpm package-info mode. To disable the checksum verification, use the **no** form of this command.

enforce-checksum

no enforce-checksum

Syntax Description

This command has no keywords and arguments.

Command Default

enforce checksum is enabled.

Command Modes

fpm package-info (config-fpm-pak-info)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **enforce-checksum** command ensures that the FPM verifies the checksum of the package during load and that the package has not been tampered. This command is useful when you want to define your own filters inside the FPM packages by disabling enforce-checksum using **no enforce-checksum** command. However, it is recommended to keep the **enforce-checksum**enabled.

Examples

The following example shows how to enable the **enforce-checksum** command:

```
Router# configure terminal
Router(config)# fpm package-info
Router(config-fpm-pak-info)# enforce-checksum
```

engine (IPS)

To enter signature-definition-action-engine configuration mode, which allows you to change router actions for a specified signature, use the **engine**command in signature-definition-action configuration mode.

engine

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

If you wish to change router actions for a specific signature, you must issue the engine command to enter the appropriate configuration mode, which allows you to issue the **event-action** command and specify any supported action.

Examples

The following example shows how to configure signature 5726 to reset all TCP connections and produce an alert:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ip ips signature-definition

Router(config-sigdef)# signature 5726 0

Router(config-sigdef-sig)# engine

Router(config-sigdef-sig-engine)# event-action reset-tcp-connection produce-alert

Router(config-sigdef-sig-engine)# exit
Router(config-sigdef-sig)# exit
Router(config-sigdef)#^ZDo you want to accept these changes? [confirm]
Router#
*Nov 9 21:50:55.847: %IPS-6-ENGINE_BUILDING: multi-string - 3 signatures - 12 of 11 engines
*Nov 9 21:50:55.859: %IPS-6-ENGINE_READY: multi-string - build time 12 ms - packets for
this engine will be scanned
*Nov 9 21:50:55.859: %SYS-5-CONFIG_I: Configured from console by cisco on console
```

Related Commands

Command	Description
event-action	Changes router actions for a signature or signature category.
signature	Specifies a signature for which the CLI user tunings will be changed.

enrollment

To specify the enrollment parameters of your certification authority (CA), use the **enrollment** command in ca-trustpoint configuration mode. To remove any of the configured parameters, use the **no** form of this command.

enrollment {**mode ra**| **retry count** *number*| **retry period** *minutes*| **url** *url*}

no enrollment {**mode ra**| **retry count** *number*| **retry period** *minutes*| **url** *url*}

Syntax Description

mode ra	Specifies registration authority (RA) mode as the mode supported by the CA.
retry count *number*	Specifies the number of times that a router will resend a certificate request when it does not receive a response from the previous request. The range is from 1 to 100. The default is 10.
retry period *minutes*	Specifies the wait period between certificate request retries. The range is from 1 to 60.
url url	Specifies the URL of the CA where your router should send certificate requests.

Command Default

RA mode is disabled.

After the router sends the first certificate request to the CA, it waits for 1 minute before sending a second request. After the second request, the interval between requests (the retry period) increases exponentially, with an additional 1 minute interval added at each increment.

The router sends a maximum of ten requests.

Your router does not know the CA URL until you specify it using url url.

Command Modes

CA-trustpoint configuration (ca-trustpoint)

Command History

Release	Modification
12.2(8)T	This command was introduced.
12.2(13)T	The **url** *url* option was enhanced to support TFTP enrollment.
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 mode keyword to specify the mode supported by the CA. This keyword is required if your CA system provides an RA.

Use the retry period minutes option to change the retry period from the default value. After requesting a certificate, the router waits to receive a certificate from the CA. If the router does not receive a certificate within a period of time (the retry period), the router will send another certificate request. The router will continue to send requests until it receives a valid certificate, until the CA returns an enrollment error, or until the configured number of retries is exceeded.

By default, the router sends a maximum of ten requests; you can change this parameter using the retry count number option . It stops sending requests when it receives a valid certificate, when the CA returns an enrollment error, or when the configured number of requests is reached.

Use the url url option to specify or change the URL of the CA. You can specify enrollment with the Simple Certificate Enrollment Protocol (SCEP) using a HTTP URL or TFTP (using a TFTP URL).

If you are using (SCEP) for enrollment, url must be in the form http://CA_name , where CA_name is the CA's host Domain Name System (DNS) name or IP address. If you are using TFTP for enrollment, *url* must be in the form tftp://certserver/file_specification .

TFTP enrollment is used to send the enrollment request and retrieve the certificate of the CA and the certificate of the router. If the file_specification is included in the URL, the router will append an extension onto the file specification. When the **crypto ca authenticate** command is entered, the router will retrieve the certificate of the CA from the specified TFTP server. As appropriate, the router will append the extension ".ca" to the filename or the fully qualified domain name (FQDN). If the **url** *url* option does not include a file specification, the router's FQDN will be used.

Note The **crypto ca trustpoint**commandreplaces the **crypto ca identity**and **crypto ca trusted-root**commands and all related subcommands (all ca-identity and trusted-root configuration mode commands). If you enter a ca-identity or trusted-root subcommand, theconfiguration mode and command will be written back as ca-trustpoint.

Examples

The following example shows how to declare a CA named ka and how to specify registration authority mode. It also shows how to set a retry count of 8 and a retry period of 2 minutes:

```
Router(config)# crypto ca trustpoint ka
Router(ca-trustpoint)# enrollment mode ra
Router(ca-trustpoint)# enrollment retry count 8
Router(ca-trustpoint)# enrollment retry period 2
```

The following example shows how to declare a CA named ka and how to specify the URL of the CA as http://example:80:

```
Router(config)# crypto ca trustpoint ka
Router(ca-trustpoint)# enrollment url http://example:80
```

Related Commands

Command	Description
crypto ca authenticate	Authenticates the CA (by getting the CA's certificate).

Command	Description
crypto ca trustpoint	Declares the CA that your router should use.
enrollment command	Specifies the HTTP command that is sent to the CA for enrollment.
enrollment credential	Specifies an existing trustpoint from another vendor that is to be enrolled with the Cisco IOS certificate server.
enrollment http-proxy	Enables access to the CA by HTTP through the proxy server.
enrollment profile	Specifies that an enrollment profile can be used for certificate authentication and enrollment.
enrollment selfsigned	Specifies self-signed enrollment for a trustpoint.
enrollment terminal	Specifies manual cut-and-paste certificate enrollment.
enrollment url	Specifies the enrollment parameters of a CA.

enrollment command

To specify the HTTP command that is sent to the certification authority (CA) for enrollment, use the **enrollment command** commandin ca-profile-enroll configuration mode.

enrollment command

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values

Command Modes

Ca-profile-enroll configuration

Command History

Release	Modification
12.2(13)ZH	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines

After enabling this command, you can use the **parameter** command to specify enrollment parameters for your enrollment profile.

Examples

The following example shows how to configure the enrollment profile name "E" for certificate enrollment:

```
crypto ca trustpoint Entrust
  enrollment profile E
  serial
crypto ca profile enrollment E
 authentication url  http://entrust:81
 authentication command  GET /certs/cacert.der
 enrollment url  http://entrust:81/cda-cgi/clientcgi.exe
 enrollment command  POST reference_number=$P2&authcode=$P1
&retrievedAs=rawDER&action=getServerCert&pkcs10Request=$REQ
 parameter 1 value aaaa-bbbb-cccc
 parameter 2 value 5001
```

Related Commands

Command	Description
crypto ca profile enrollment	Defines an enrollment profile.
parameter	Specifies parameters for an enrollment profile.

enrollment credential

To specify an existing trustpoint from another vendor that is to be enrolled with the Cisco IOS certificate server, use the **enrollment credential** command in ca-profile-enroll configuration mode.

enrollment credential *label*

Syntax Description

label	Name of the certification authority (CA) trustpoint of another vendor.

Command Default

No default behavior or values.

Command Modes

Ca-profile-enroll configuration

Command History

Release	Modification
12.3(11)T	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.

Usage Guidelines

To configure a router that is already enrolled with a CA of another vendor that is to be enrolled with a Cisco IOS certificate server, you must configure a certificate enrollment profile (via the **crypto pki profile enrollment**command). Thereafter, you should issue the **enrollment credential** command, which specifies the trustpoint of another vendor that has to be enrolled with a Cisco IOS certificate server.

Examples

The following example shows how to configure a client router and a Cisco IOS certificate server to exchange enrollment requests via a certificate enrollment profile:

```
! Define the trustpoint “msca-root” that points to the non-Cisco IOS CA and enroll and !
authenticate the client with the non-Cisco IOS CA.
crypto pki trustpoint msca-root
 enrollment mode ra
 enrollment url http://msca-root:80/certsrv/mscep/mscep.dll
 ip-address FastEthernet2/0
 revocation-check crl
!
! Configure trustpoint “cs” for Cisco IOS CA.
crypto pki trustpoint cs
 enrollment profile cs1
 revocation-check crl
!
! Define enrollment profile “cs1,” which points to Cisco IOS CA and mention (via the !
enrollment credential command) that “msca-root” is being initially enrolled with the ! Cisco
 IOS CA.
crypto pki profile enrollment cs1
 enrollment url  http://cs:80
 enrollment credential  msca-root!
! Configure the certificate server, and issue and the
grant auto trustpoint co
mmand to ! instruct the certificate server to accept enrollment request only from clients
who are ! already enrolled with trustpoint “msca-root.”
crypto pki server cs
 database level minimum
 database url nvram:
 issuer-name CN=cs
 grant auto trustpoint msca-root
!
crypto pki trustpoint cs
 revocation-check crl
rsakeypair cs
!
crypto pki trustpoint msca-root
 enrollment mode ra
 enrollment url http://msca-root:80/certsrv/mscep/mscep.dll
 revocation-check crl
```

Related Commands

Command	Description
crypto pki profile enrollment	Defines an enrollment profile.

enrollment http-proxy

To access the certification authority (CA) by HTTP through the proxy server, use the **enrollment http-proxy** command in ca-trustpoint configuration mode.

enrollment http-proxy *host-name port-num*

Syntax Description

host-name	Defines the proxy server used to get the CA.
port-num	Specifies the port number used to access the CA.

Command Default

If this command is not enabled, the CA will not be accessed via HTTP.

Command Modes

Ca-trustpoint 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.

Usage Guidelines

The **enrollment http-proxy** command must be used in conjunction with the **enrollment** command, which specifies the enrollment parameters for the CA.

Examples

The following example shows how to access the CA named “ka” by HTTP through the bomborra proxy server:

```
crypto ca trustpoint ka
 enrollment url http://kahului
 enrollment http-proxy bomborra 8080
 crl optional
```

Related Commands

Command	Description
crypto ca trustpoint	Declares the CA that your router should use.
enrollment	Specifies the enrollment parameters of your CA.

enrollment mode ra

The **enrollment mode ra**command is replaced by the enrollment command command. See the enrollment command command for more information.

enrollment profile

To specify that an enrollment profile can be used for certificate authentication and enrollment, use the **enrollment profile**command in ca-trustpoint configuration mode. To delete an enrollment profile from your configuration, use the **no** form of this command.

enrollment profile *label*

no enrollment profile *label*

Syntax Description

label	Creates a name for the enrollment profile.

Command Default

Your router does not recognize any enrollment profiles until you declare one using this command.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.2(13)ZH	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines

Before you can enable this command, you must enter the **crypto ca trustpoint** command.

The **enrollment profile** command enables your router to accept an enrollment profile, which can be configured via the **crypto ca profile enrollment** command. The enrollment profile, which consists of two templates, can be used to specify different URLs or methods for certificate authentication and enrollment.

Examples

The following example shows how to declare the enrollment profile named “E”:

```
crypto ca trustpoint Entrust
  enrollment profile E
  serial
crypto ca profile enrollment E
 authentication url  http://entrust:81
 authentication command  GET /certs/cacert.der
 enrollment url  http://entrust:81/cda-cgi/clientcgi.exe
 enrollment command  POST reference_number=$P2&authcode=$P1
&retrievedAs=rawDER&action=getServerCert&pkcs10Request=$REQ
 parameter 1 value aaaa-bbbb-cccc
 parameter 2 value 5001
```

Related Commands

Command	Description
crypto ca profile enrollment	Defines an enrollment profile.
crypto ca trustpoint	Declares the CA that your router should use.

enrollment retry count

The **enrollment retry count**command is replaced by the enrollment command. See the enrollmentcommand for more information.

enrollment retry period

The **enrollment retry period**command is replaced by the enrollment command. See the enrollmentcommand for more information.

enrollment selfsigned

To specify self-signed enrollment for a trustpoint, use the **enrollment selfsigned** command in ca-trustpoint configuration mode. To delete self-signed enrollment from a trustpoint, use the **no** form of this command.

enrollment selfsigned

no enrollment selfsigned

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default behavior or values.

Command Modes

ca-trustpoint configuration (ca-trustpoint)

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(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

Before you can use the **enrollment selfsigned** command, you must enable the **crypto pki trustpoint**command , which defines the trustpoint and enters ca-trustpoint configuration mode.

If you do not use this command, you should specify another enrollment method for the router by using an enrollment command such as **enrollment url** or **enrollment terminal**.

Examples

The following example shows a self-signed certificate being designated for a trustpoint named local:

```
crypto pki trustpoint local
 enrollment selfsigned
```

Related Commands

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

enrollment terminal (ca-profile-enroll)

To specify manual cut-and-paste certificate enrollment, use the **enrollment terminal**command in ca-profile-enroll configuration mode. To delete a current enrollment request, use the **no** form of this command.

enrollment terminal

no enrollment terminal

Syntax Description

This command has no arguments or keywords.

Command Default

A certificate enrollment request is not specified.

Command Modes

Ca-profile-enroll configuration

Command History

Release	Modification
12.2(13)ZH	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.

Usage Guidelines

A user may manually cut-and-paste certificate authentication requests and certificates when a network connection between the router and certification authority (CA) is unavailable. After this command is enabled, the certificate request is printed on the console terminal so that it can be manually copied (cut) by the user.

Note Although most routers accept manual enrollment, the process can be tedious if a large number of routers have to be enrolled.

Examples

The following example shows how to configure the enrollment profile named “E” to perform certificate authentication via HTTP and manual certificate enrollment:

```
crypto ca profile enrollment E
 authentication url  http://entrust:81
 authentication command  GET /certs/cacert.der
 enrollment terminal
 parameter 1 value aaaa-bbbb-cccc
 parameter 2 value 5001
```

Related Commands

Command	Description
crypto ca profile enrollment	Defines an enrollment profile.

enrollment terminal (ca-trustpoint)

To specify manual cut-and-paste certificate enrollment, use the **enrollment terminal**command in ca-trustpoint configuration mode. To delete a current enrollment request, use the **no** form of this command.

enrollment terminal [pem]

no enrollment terminal [pem]

Syntax Description

pem	(Optional) Adds privacy-enhanced mail (PEM) boundaries to the certificate request.

Command Default

No default behavior or values

Command Modes

Ca-trustpoint configuration (ca-trustpoint)

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.3(4)T	The **pem** keyword was added.
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.
12.4(24)T	Support for IPv6 Secure Neighbor Discovery (SeND) was added.

Usage Guidelines

A user may want to manually cut-and-paste certificate requests and certificates when he or she does not have a network connection between the router and certification authority (CA). When this command is enabled, the router displays the certificate request on the console terminal, allowing the user to enter the issued certificate on the terminal.

The pem Keyword

Use the **pem** keyword to issue certificate requests (via the **crypto ca enroll**command) or receive issued certificates (via the **crypto ca import certificate** command) in PEM-formatted files through the console terminal. If the CA server does not support simple certificate enrollment protocol (SCEP), the certificate request can be presented to the CA server manually.

Note When generating certificate requests in PEM format, your router does not have to have the CA certificate, which is obtained via the **crypto ca authenticate** command.

Examples

The following example shows how to manually specify certificate enrollment via cut-and-paste. In this example, the CA trustpoint is "MS."

```
crypto ca trustpoint MS
 enrollment terminal
 crypto ca authenticate MS
!
crypto ca enroll MS
crypto ca import MS certificate
```

Related Commands

Command	Description
crypto ca authenticate	Authenticates the CA (by getting the certificate of the CA).
crypto ca enroll	Obtains the certificates of your router from the certification authority.
crypto ca import	Imports a certificate manually via TFTP or cut-and-paste at the terminal.
crypto ca trustpoint	Declares the CA that your router should use.

enrollment url (ca-identity)

The **enrollment url (ca-identity)**command is replaced by the **enrollment url (ca-trustpoint)**command. See the **enrollment url (ca-trustpoint)** command for more information.

enrollment url (ca-profile-enroll)

To specify the URL of the certification authority (CA) server to which to send enrollment requests, use the **enrollment url** command in ca-profile-enroll configuration mode. To delete the enrollment URL from your enrollment profile, use the **no** form of this command.

enrollment url *url*[**vrf** *vrf-name*]

no enrollment url *url*[**vrf** *vrf-name*]

Syntax Description

url	URL of the CA server to which your router should send certificate requests.
vrf *vrf-name*	The VRF name.

Command Default

Your router does not recognize the CA URL until you specify it using this command.

Command Modes

Ca-profile-enroll configuration (ca-profile-enroll)#

Command History

Release	Modification
12.2(13)ZH	This command was introduced.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T.
15.1(4)T	This command was modified. The **vrf** *vrf-name* keyword-argument pair was added.

Usage Guidelines

This command allows the user to specify a different URL or a different method for authenticating a certificate and enrolling a certificate; for example, manual authentication and TFTP enrollment.

Note the following when specifying the *url* argument:

- If you are using Simple Certificate Enrollment Protocol (SCEP) for enrollment, the value must be in the form http://CA_name, where CA_name is the host Domain Name System (DNS) name or IP address of the CA.
- If you are using TFTP for enrollment, the value must be in the form tftp://certserver/file_specification. (If the URL does not include a file specification, the fully qualified domain name [FQDN] of the router will be used.)

Examples

The following example shows how to enable certificate enrollment via HTTP for the profile name “E”:

```
crypto pki trustpoint Entrust
  enrollment profile E
  serial
crypto pki profile enrollment E
 authentication url  http://entrust:81
 authentication command  GET /certs/cacert.der
 enrollment url  http://entrust:81/cda-cgi/clientcgi.exe
 enrollment command  POST reference_number=$P2&authcode=$P1
&retrievedAs=rawDER&action=getServerCert&pkcs10Request=$REQ
 parameter 1 value aaaa-bbbb-cccc
 parameter 2 value 5001
```

The following example shows how to configure the enrollment and certificate revocation list (CRL) via the same VRF:

```
crypto pki trustpoint trustpoint1
 enrollment url http://10.10.10.10:80
 vrf vrf1
 revocation-check crl
```

The following example shows how to configure the enrollment and certificate revocation list (CRL) via different VRF:

```
crypto pki profile enrollment pki_profile
 enrollment url  http://10.10.10.10:80  vrf vrf2

crypto pki trustpoint trustpoint1
 enrollment profile pki_profile
 vrf vrf1
 revocation-check crl
```

Related Commands

Command	Description
crypto pki profile enrollment	Defines an enrollment profile.

enrollment url (ca-trustpoint)

To specify the enrollment parameters of a certification authority (CA), use the **enrollment url** command in ca-trustpoint configuration mode. To remove any of the configured parameters, use the **no** form of this command.

enrollment [mode] [**retry period** *minutes*] [**retry count** *number*] **url** *url* **[pem]**

no enrollment [mode] [**retry period** *minutes*] [**retry count** *number*] **url** *url* **[pem]**

Syntax Description

mode	(Optional) Specifies the registration authority (RA) mode, if your CA system provides an RA. By default, RA mode is disabled.
retry period *minutes*	(Optional) Specifies the period, in minutes, in which the router waits before sending the CA another certificate request. Valid values are from 1 to 60. The default is 1.
retry count *number*	(Optional) Specifies the number of times a router will resend a certificate request when it does not receive a response from the previous request. Valid values are from 1 to 100. The default is 10.
url *url*	Specifies the URL of the file system where your router should send certificate requests. For enrollment method options, see the table below.
pem	(Optional) Adds privacy-enhanced mail (PEM) boundaries to the certificate request.

Command Default

Your router does not know the CA URL until you specify it using the **url** *url* keyword and argument.

Command Modes

Ca-trustpoint configuration (config-ca-trustpoint)

Command History

Release	Modification
11.3T	This command was introduced as the **enrollment url** (ca-identity) command.
12.2(8)T	This command was introduced. This command replaced the **enrollment url** (ca-identity) command.
12.2(13)T	This command was modified. The **url** *url* option was enhanced to support TFTP enrollment.

Release	Modification
12.3(4)T	This command was modified. The **pem** keyword was added, and the **url** *url* option was enhanced to support an additional enrollment method--the Cisco IOS File System (IFS).
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(24)T	This command was modified. Support for IPv6 Secure Neighbor Discovery (SeND) was added.
15.2(1)T	This command was modified. Support for specifying the IPv6 address in a URL for the CA was added.

Usage Guidelines

Use the **mode** keyword to specify the mode supported by the CA. This keyword is required if your CA system provides an RA.

Use the **retry period** *minutes* option to change the retry period from the default of 1 minute between retries. After requesting a certificate, the router waits to receive a certificate from the CA. If the router does not receive a certificate within a specified period of time (the retry period), the router will send another certificate request. By default, the router will send a maximum of ten requests until it receives a valid certificate, until the CA returns an enrollment error, or until the configured number of retries (specified through the **retry count** *number* option) is exceeded.

Use the **pem** keyword to issue certificate requests (using the **crypto pki enroll** command) or receive issued certificates (using the **crypto pki import certificate** command) in PEM-formatted files.

Note When generating certificate requests in PEM format, your router does not have to have the CA certificate, which is obtained using the **crypto ca authenticate** command.

The *url* argument specifies or changes the URL of the CA. The table below lists the available enrollment methods.

Table 4: Certificate Enrollment Methods

Enrollment Method	Description
WORD	Enrolls through the Simple Certificate Enrollment Protocol (SCEP) (an HTTP URL). **Note** If you are using SCEP for enrollment, the URL must be in the form http://*CA_name*, where *CA_name* is the host Domain Name System (DNS) name, IPv4 address, or IPv6 address of the CA.

Enrollment Method	Description
archive:	Enrolls through the archive: file system.
disk0:	Enrolls through the disc0 file system.
disk1:	Enrolls through the disc1 file system.
ftp:	Enrolls through the FTP file system.
http:	Enrolls through the HTTP file system. The URL must be in the following formats: • http://*CA_name:80*, where *CA_name* is the Domain Name System (DNS) • http://*ipv4-address*:80. For example: http://10.10.10.1:80. • *http://[ipv6-address]:80*. For example: http://[2001:DB8:1:1::1]:80. The IPv6 address is in hexadecimal notation and must be enclosed in brackets in the URL.
https:	Enrolls through the HTTPS file system. The URL must use the same formats as the HTTP: file system formats described above.
null:	Enrolls through the null file system
nvram:	Enrolls through Non-volatile Random-access Memory (NVRAM) file system
pram:	Enrolls through Parameter Random-access Memory (PRAM) file system
rcp:	Enrolls through the remote copy protocol (rcp) file system
scp:	Enrolls through the secure copy protocol (scp) file system
snmp:	Enrolls through the Simple Network Management Protocol (SNMP)
system:	Enrolls through the system file system
tftp:	Enrolls through the Trivial File Transfer Protocol (TFTP): file system. **Note** The URL must be in the form: tftp://*CA_name/file_specification*

Enrollment Method	Description
tmpsys:	Enrolls through the IOS tmpsys file system.
unix:	Enrolls through the UNIX file system.

TFTP enrollment is used to send the enrollment request and retrieve the certificate of the CA and the certificate of the router. If the file_specification is included in the URL, the router appends an extension onto the file specification. When the **crypto pki authenticate** command is entered, the router retrieves the certificate of the CA from the specified TFTP server. As appropriate, the router appends the extension ".ca" to the filename or the fully qualified domain name (FQDN). (If the **url** *url* option does not include a file specification, the FQDN of the router is used.)

Note The **crypto pki trustpoint**commandreplaces the **crypto ca identity**and **crypto ca trusted-root**commands and all related commands (all **ca-identity** and **trusted-root** configuration mode commands). If you enter a **ca-identity** or **trusted-root** command, theconfiguration mode and command is written back as pki-trustpoint.

An IPv6 address can be added to the URL for the CA in the Trustpoint configuration. It is important that this address be in brackets.

Examples

The following example shows how to declare a CA named "trustpoint" and specify the URL of the CA as http://example:80:

```
crypto pki trustpoint trustpoint
 enrollment url http://example:80
```

The following example shows how to declare a CA named "trustpoint" and specify the IPv6 URL of the CA as http://[2001:DB8:1:1::1]:80:

```
crypto pki trustpoint trustpoint
 enrollment url http://[2001:DB8:1:1::1]:80
```

Related Commands

Command	Description
crl query	Queries the certificate revocation list (CRL) to ensure that the certificate of the peer has not been revoked.
crypto pki authenticate	Authenticates the CA (by getting the certificate of the CA).
crypto pki enroll	Obtains the certificate or certificates of your router from the CA.
crypto pki trustpoint	Declares the CA that your router should use.

Command	Description
ocsp url	Specifies the URL of an online certificate status protocol (OCSP) server to override the OCSP server URL (if one exists) in the Authority Info Access (AIA) extension of the certificate.

eou allow

To allow additional Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP) options, use the **eou allow** command in global configuration mode. To disable the options that have been set, use the **no** form of this command.

eou allow {**clientless**| **ip-station-id**}

no eou allow {**clientless**| **ip-station-id**}

Syntax Description

clientless	Allows authentication of clientless hosts (systems that do not run Cisco Trust Agent).
ip-station-id	Allows an IP address in the station-id field.

Command Default

No additional EAPoUDP options are allowed.

Command Modes

Global configuration (config)

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 **eou allow** command used with the **clientless** keyword requires that a user group be configured on the Cisco Access Control Server (ACS) using the same username and password that are specified using the **eou clientless** command.

Examples

The following example shows that clientless hosts are allowed:

```
Router (config)# eou allow clientless
```

Related Commands

Command	Description
eou clientless	Sets user group credentials for clientless hosts.

eou clientless

To set user group credentials for clientless hosts, use the **eou clientless** command in global configuration mode. To remove the user group credentials, use the **no** form of this command.

eou clientless {**password** *password*| **username** *username*}

no eou clientless {**password**| **username**}

Syntax Description

password password	Sets a password.
username *username*	Sets a username.

Command Default

Username and password values are clientless.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(8)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

For this command to be effective, the **eou allow**command must also be enabled.

Examples

The following example shows that a clientless host with the username "user1" has been configured:

```
Router (config)# eou clientless username user1
```

The following example shows that a clientless host with the password "user123" has been configured:

```
Router (config)# eou clientless password user123
```

Related Commands

Command	Description
eou allow	Allows additional EAPoUDP options.

eou default

To set global Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP) parameters to the default values, use the **eou default**command in global or interface configuration mode.

eou default

Syntax Description

This command has no arguments or keywords.

Command Default

The EAPoUDP parameters are set to their default values.

Command Modes

Global configuration (config) Interface configuration (config-if)

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

You can configure this command globally by using global configuration mode or for a specific interface by using interface configuration mode.

Using this command, you can reset existing values to their default values.

Examples

The following configuration example shows that EAPoUDP parameters have been set to their default values:

```
Router (config)# eou default
```

eou initialize

To manually initialize Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP) state machines, use the **eou initialize**command in global configuration mode. This command has no **no** form.

eou initialize {**all**| **authentication** {**clientless**| **eap**| **static**}| **interface** *interface-name*| **ip** *ip-address*| **mac** *mac-address*| **posturetoken** *string*}

Syntax Description

all	Initiates reauthentication of all EAPoUDP clients. This keyword is the default.
authentication	Specifies the authentication type.
clientless	Clientless authentication type.
eap	EAP authentication type.
static	Static authentication type.
interface *interface-name*	Specifies a specific interface.
ip *ip-address*	Specifies a specific IP address.
mac *mac-address*	Specifies a specific MAC address.
posturetoken *string*	Specifies a specific posture token.

Command Default

None

Command Modes

Global configuration (config)

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

If this command is used, existing EAPoUDP state machines will be reset.

Examples

The following example shows that all EAPoUDP state machines have been reauthenticated:

```
Router (config)# eou initialize all
```

Related Commands

Command	Description
eou revalidate	Revalidates an EAPoUDP association.

eou logging

To enable Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP) system logging events, use the **eou logging**command in global configuration mode. To remove EAPoUDP logging, use the **no** form of this command.

eou logging

no eou logging

Syntax Description

This command has no arguments or keywords.

Command Default

Logging is disabled.

Command Modes

Global configuration (config)

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.

Examples

The following example shows that EAPoUDP logging has been enabled:

```
Router (config)# eou logging
```

The following is sample EAPoUDP logging output:

```
Apr  9 10:04:09.824: %EOU-6-SESSION: IP=10.0.0.1| HOST=DETECTED| Interface=FastEthernet0/0
*Apr  9 10:04:09.900: %EOU-6-CTA: IP=10.0.0.1| CiscoTrustAgent=DETECTED
*Apr  9 10:06:19.576: %EOU-6-POLICY: IP=10.0.0.1| TOKEN=Healthy
*Apr  9 10:06:19.576: %EOU-6-POLICY: IP=10.0.0.1| ACLNAME=#ACSACL#-IP-HealthyACL-40921e54
*Apr  9 10:06:19.576: %EOU-6-POSTURE: IP=10.0.0.1| HOST=AUTHORIZED|
Interface=FastEthernet0/0.420
*Apr  9 10:06:19.580: %EOU-6-AUTHTYPE: IP=10.0.0.1| AuthType=EAP
*Apr  9 10:06:04.424: %EOU-6-SESSION: IP=192.168.2.1| HOST=REMOVED|
Interface=FastEthernet0/0.420
```

eou max-retry

To set the number of maximum retry attempts for Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP), use the **eou max-retry**command in global or interface configuration mode. To remove the number of retries that were entered, use the **no** form of this command.

eou max-retry *number-of-retries*

no eou max-retry *number-of-retries*

Syntax Description

number-of-retries	Number of maximum retries that may be attempted. The value ranges from 1 through 10. The default is 3.

Command Default

The default number of retries is 3.

Command Modes

Global configuration (config) Interface configuration (config-if)

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.4	The value range was changed from 1 through 3 to 1 through 10.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

You can configure this command globally by using global configuration mode or for a specific interface by using interface configuration mode.

Examples

The following example shows that the maximum number of retries for an EAPoUDP session has been set for 2:

```
Router (config)# eou max-retry 2
```

Related Commands

Command	Description
show eou	Displays information about EAPoUDP global values or EAPoUDP session cache entries.

eou port

To set the UDP port for Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP), use the **eou port**command in global configuration mode. This command has no **no** form.

eou port *port-number*

Syntax Description

port-number	Number of the port. The value ranges from 1 through 65535. The default value is 27186.

Command Default

The default *port-number* value is 27186.

Command Modes

Global configuration (config)

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

Ensure that the port you set does not conflict with other UDP applications.

Examples

The following example shows that the port for an EAPoUDP session has been set to 200:

```
Router (config)# eou port 200
```

Related Commands

Command	Description
show eou	Displays information about EAPoUDP.

eou rate-limit

To set the number of simultaneous posture validations for Extensible Authentication Protocol over UDP (EAPoUDP), use the **eou rate-limit**command in global configuration mode. This command has no **no** form.

eou rate-limit *number-of-validations*

Syntax Description

number-of-validations	Number of clients that can be simultaneously validated. The value ranges from 1 through 200. The default value is 20.

Command Default

No default behaviors or values

Command Modes

Global configuration (config)

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

If you set the rate limit to 0 (zero), rate limiting will be turned off.

If the rate limit is set to 100 and there are 101 clients, validation will not occur until one drops off.

To return to the default value, use the **eou default** command.

Examples

The following example shows that the number of posture validations has been set to 100:

```
Router (config)# eou rate-limit 100
```

Related Commands

Command	Description
eou default	Sets global EAPoUDP parameters to the default values.
show eou	Displays information about EAPoUDP.

eou revalidate

To revalidate an Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP) association, use the **eou revalidate**command in privileged EXEC mode. To disable the revalidation, use the **no** form of this command.

eou revalidate {**all**| **authentication** {**clientless**| **eap**| **static**}| **interface** *interface-name*| **ip** *ip-address*| **mac** *mac-address*| **posturetoken** *string*}

no eou revalidate {**all**| **authentication** {**clientless**| **eap**| **static**}| **interface** *interface-name*| **ip** *ip-address*| **mac** *mac-address*| **posturetoken** *string*}

Syntax Description

all	Enables revalidation of all EAPoUDP clients. This keyword option is the default.
authentication	Specifies the authentication type.
clientless	Clientless authentication type.
eap	EAP authentication type.
static	Static authentication type.
interface *interface-name*	Name of the interface. (See the table below for the types of interface that may be shown.)
ip *ip-address*	IP address of the client.
mac *mac-address*	The 48-bit hardware address of the client.
posturetoken *string*	Name of the posture token.

Command Default

None

Command Modes

Privileged EXEC (#)

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

If you use this command, existing EAPoUDP sessions will be revalidated.

The table below lists the interface types that may be used with the **interface** keyword.

Table 5: 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
Virtual-Template	Virtual template interface
Virtual-TokenRing	Virtual TokenRing interface

Examples

The following example shows that all EAPoUDP clients are to be revalidated:

```
Router# eou revalidate all
```

Related Commands

Command	Description
eou initialize	Manually initializes EAPoUDP state machines.

eou timeout

To set the Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP) timeout values, use the **eou timeout**command in global or interface configuration mode. To remove the value that was set, use the **no** form of this command.

eou timeout {**aaa** *seconds*| **hold-period** *seconds*| **retransmit** *seconds*| **revalidation** *seconds*| **status query** *seconds*}

no timeout {**aaa** *seconds*| **hold-period** *seconds*| **retransmit** *seconds*| **revalidation** *seconds*| **status query** *seconds*}

Syntax Description

aaa *seconds*	Authentication, authorization, and accounting (AAA) timeout period, in seconds. The value range is from 1 through 60. Default=60.
hold-period *seconds*	Hold period following failed authentication, in seconds. The value range is from 60 through 86400. Default=180.
retransmit *seconds*	Retransmit period, in seconds. The value range is from 1 through 60. Default=3.
revalidation *seconds*	Revalidation period, in seconds. The value range is from 300 through 86400. Default=36000.
status query *seconds*	Status query period after revalidation, in seconds. The value range is from 30 through 1800. Default=300.

Command Default

No default behavior or values

Command Modes

Global configuration (config) Interface configuration (config-if)

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

You can configure this command globally by using global configuration mode or for a specific interface by using interface configuration mode.

Examples

The following example shows that the status query period after revalidation is set to 30:

```
Router (config)# eou timeout status query 30
```

Related Commands

Command	Description
show eou	Displays information about EAPoUDP global values.

error-msg

To display a specific error message when a user logs on to a Secure Sockets Layer Virtual Private Network (SSL VPN) gateway, use the **error-msg** command in webvpn acl configuration mode. To remove the error message, use the **no** form of this command.

error-msg *message-string*

no error-msg *message-string*

Syntax Description

message-string	Error message to be displayed.

Command Default

No special error message is displayed.

Command Modes

Webvpn acl configuration

Command History

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

Usage Guidelines

If the **error-url** command is configured, the user is redirected to the error URL for every request that is not allowed. If the **error-url** command is not configured, the user gets a standard, gateway-generated information page showing themessage that was configured using the **error-msg** command.

Examples

This example shows that the following error message will be displayed when the user logs on to the SSL VPN gateway:

```
webvpn context context1
 acl acl1
  error-msg “If you have any questions, please contact <a
href+mailto:employee1@example.com>Employee1</a>.”
```

Related Commands

Command	Description
acl	Defines an ACL using a SSL VPN gateway at the Application Layer level and enters webvpn acl configuration mode.
error-url	Defines a URL as an ACL violation page using a SSL VPN gateway.

Command	Description
webvpn context	Configures a SSL VPN context and enters webvpn context configuration mode.

error-url

To define a URL as an access control list (ACL) violation page using a Secure Socket Layer Virtual Private Network (SSL VPN) gateway, use the **error-url** command in webvpn acl configuration mode. To remove the ACL violation page, use the **no** form of this command.

error-url access-deny-page-url

no error-url access-deny-page-url

Syntax Description

access-deny-page-url	URL to which a user is directed for an ACL violation.

Command Default

If this command is not configured, the gateway redirects the ACL violation page to a predefined URL.

Command Modes

Webvpn acl configuration

Command History

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

Usage Guidelines

If the **error-url** command is configured, the user is redirected to a predefined URL for every request that is not allowed. If the **error-url** command is not configured, the user gets a standard, gateway-generated error page.

Examples

The following example shows that the URL "http://www.example.com" has been defined as the ACL violation page:

```
webvpn context context1
 acl acl1
  error-url "http://www.example.com"
```

Related Commands

Command	Description
acl	Defines an ACL using a SSL VPN gateway at the Application Layer level.
error-msg	Displays a specific error message when a user logs on to a SSL VPN gateway.

Command	Description
webvpn context	Configures the SSL VPN context and enters webvpn context configuration mode.

evaluate

To nest a reflexive access list within an access list, use the **evaluate** command in access-list configuration mode. To remove a nested reflexive access list from the access list, use the **no** form of this command.

evaluate *name*

no evaluate *name*

Syntax Description

name	The name of the reflexive access list that you want evaluated for IP traffic entering your internal network. This is the name defined in the **permit** (reflexive) command.

Command Default

Reflexive access lists are not evaluated.

Command Modes

Access-list 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.

Usage Guidelines

This command is used to achieve reflexive filtering, a form of session filtering.

Before this command will work, you must define the reflexive access list using the **permit** (reflexive) command.

This command nests a reflexive access list within an extended named IP access list.

If you are configuring reflexive access lists for an external interface, the extended named IP access list should be one which is applied to inbound traffic. If you are configuring reflexive access lists for an internal interface, the extended named IP access list should be one which is applied to outbound traffic. (In other words, use the access list opposite of the one used to define the reflexive access list.)

This command allows IP traffic entering your internal network to be evaluated against the reflexive access list. Use this command as an entry (condition statement) in the IP access list; the entry “points” to the reflexive access list to be evaluated.

As with all access list entries, the order of entries is important. Normally, when a packet is evaluated against entries in an access list, the entries are evaluated in sequential order, and when a match occurs, no more entries are evaluated. With a reflexive access list nested in an extended access list, the extended access list entries are evaluated sequentially up to the nested entry, then the reflexive access list entries are evaluated sequentially, and then the remaining entries in the extended access list are evaluated sequentially. As usual, after a packet matches *any* of these entries, no more entries will be evaluated.

Examples

The following example shows reflexive filtering at an external interface. This example defines an extended named IP access list *inboundfilters*, and applies it to inbound traffic at the interface. The access list definition permits all Border Gateway Protocol and Enhanced Interior Gateway Routing Protocol traffic, denies all Internet Control Message Protocol traffic, and causes all Transmission Control Protocol traffic to be evaluated against the reflexive access list *tcptraffic*.

If the reflexive access list *tcptraffic* has an entry that matches an inbound packet, the packet will be permitted into the network. *tcptraffic* only has entries that permit inbound traffic for existing TCP sessions.

```
interface Serial 1
 description Access to the Internet via this interface
 ip access-group inboundfilters in
!
ip access-list extended inboundfilters
 permit 190 any any
 permit eigrp any any
 deny icmp any any
 evaluate tcptraffic
```

Related Commands

Command	Description
ip access-list	Defines an IP access list by name.
ip reflexive-list timeout	Specifies the length of time that reflexive access list entries will continue to exist when no packets in the session are detected.
permit (reflexive)	Creates a reflexive access list and enables its temporary entries to be automatically generated.

evaluate (IPv6)

To nest an IPv6 reflexive access list within an IPv6 access list, use the **evaluate** (IPv6) command in IPv6 access list configuration mode. To remove the nested IPv6 reflexive access list from the IPv6 access list, use the **no** form of this command.

evaluate *access-list-name* [**sequence** *value*]

no evaluate *access-list-name* [**sequence** *value*]

Syntax Description

access-list-name	The name of the IPv6 reflexive access list that you want evaluated for IPv6 traffic entering your internal network. This is the name defined in the **permit** (IPv6) command. Names cannot contain a space or quotation mark, or begin with a numeric.
sequence *value*	(Optional) Specifies the sequence number for the IPv6 reflexive access list. The acceptable range is from 1 to 4294967295.

Command Default

IPv6 reflexive access lists are not evaluated.

Command Modes

IPv6 access list configuration

Command History

Release	Modification
12.0(23)S	This command was introduced.
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(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 **evaluate** (IPv6) command is similar to the **evaluate** (IPv4) command, except that it is IPv6-specific.

This command is used to achieve IPv6 reflexive filtering, a form of session filtering.

Before this command will work, you must define the IPv6 reflexive access list using the **permit** (IPv6) command.

This command nests an IPv6 reflexive access list within an IPv6 access control list (ACL).

If you are configuring an IPv6 reflexive access list for an external interface, the IPv6 ACL should be one that is applied to inbound traffic. If you are configuring IPv6 reflexive access lists for an internal interface, the IPv6 ACL should be one that is applied to outbound traffic. (In other words, use the access list opposite of the one used to define the IPv6 reflexive access list.)

This command allows IPv6 traffic entering your internal network to be evaluated against the reflexive access list. Use this command as an entry (condition statement) in the IPv6 ACL; the entry "points" to the IPv6 reflexive access list to be evaluated.

As with all IPv6 ACL entries, the order of entries is important. Normally, when a packet is evaluated against entries in an IPv6 ACL, the entries are evaluated in sequential order, and when a match occurs, no more entries are evaluated. With an IPv6 reflexive access list nested in an IPv6 ACL, the IPv6 ACL entries are evaluated sequentially up to the nested entry, then the IPv6 reflexive access list entries are evaluated sequentially, and then the remaining entries in the IPv6 ACL are evaluated sequentially. As usual, after a packet matches any of these entries, no more entries will be evaluated.

Note IPv6 reflexive access lists do not have any implicit deny or implicit permit statements.

Examples

The **evaluate** command in the following example nests the temporary IPv6 reflexive access lists named TCPTRAFFIC and UDPTRAFFIC in the IPv6 ACL named OUTBOUND. The two reflexive access lists are created dynamically (session filtering is "triggered") when incoming TCP or UDP traffic matches the applicable permit entry in the IPv6 ACL named INBOUND. The OUTBOUND IPv6 ACL uses the temporary TCPTRAFFIC or UDPTRAFFIC access list to match (evaluate) outgoing TCP or UDP traffic related to the triggered session. The TCPTRAFFIC and UDPTRAFFIC lists time out automatically when no IPv6 packets match the permit statement that triggered the session (the creation of the temporary reflexive access list).

Note The order of IPv6 reflexive access list entries is not important because only permit statements are allowed in IPv6 reflexive access lists and reflexive access lists do not have any implicit conditions. The OUTBOUND IPv6 ACL simply evaluates the UDPTRAFFIC reflexive access list first and, if there were no matches, the TCPTRAFFIC reflexive access list second. Refer to the **permit** command for more information on configuring IPv6 reflexive access lists.

```
ipv6 access-list INBOUND
  permit tcp any any eq bgp reflect TCPTRAFFIC
  permit tcp any any eq telnet reflect TCPTRAFFIC
  permit udp any any reflect UDPTRAFFIC
ipv6 access-list OUTBOUND
  evaluate UDPTRAFFIC
  evaluate TCPTRAFFIC
```

Related Commands

Command	Description
ipv6 access-list	Defines an IPv6 access list and enters IPv6 access list configuration mode.

Command	Description
permit (IPv6)	Sets permit conditions for an IPv6 access list.
show ipv6 access-list	Displays the contents of all current IPv6 access lists.

event-action

To change router actions for a signature or signature category, use the **event-action**command in signature-definition-action-engine or IPS- category-action configuration mode. To revert to the default router action values, use the **no** form of this command.

event-action *action*

no event-action

Syntax Description

action	Router actions for a specified signature or signature category. The *action* argument can be any of the following options: • **deny-attacker-inline** • **deny-connection-inline** • **deny-packet-inline** • **produce-alert** • **reset-tcp-connection** **Note** Event actions for an individual signature must be entered on a single line. However, event actions associated with a category can be entered separately or on a single line.

Command Default

Default values for the signature or signature category will be used.

Command Modes

Signature-definition-action-engine configuration (config-sigdef-action-engine) IPS-category-action configuration (config-ips-category-action)

Command History

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

Usage Guidelines

Signature-Based Changes

After signature-based changes are complete, Cisco IOS Intrusion Prevention System (IPS) prompts the user to confirm whether or not the changes are acceptable. Confirming the changes instructs Cisco IOS IPS to compile the changes for the signature and modify memory structures to reflect the change. Also, Cisco IOS IPS will save the changes to the location specified via the **ip ips config location** command (for example, flash:ips5/*.xml).

You can issue the **show ip ips signatures**command to verify the event-action configuration. (The **show running-config**command does not show individual signature tuning information.)

Signature Category-Based Changes

After signature category-based changes are complete, the category tuning information is saved in the command-line interface (CLI) configuration.

Category configuration information is processed in the order that it is entered. Thus, it is recommended that the process of retiring all signatures occur before all other category tuning.

If a category is configured more than once, the parameters entered in the second configuration will be added to or will replace the previous configuration.

Examples

The following example shows how to configure signature 5726 to reset all TCP connections and produce an alert:

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ip ips signature-definition

Router(config-sigdef)# signature 5726 0

Router(config-sigdef-sig)# engine

Router(config-sigdef-sig-engine)# event-action reset-tcp-connection produce-alert

Router(config-sigdef-sig-engine)# exit
Router(config-sigdef-sig)# exit
Router(config-sigdef)#^ZDo you want to accept these changes? [confirm]
Router#
*Nov 9 21:50:55.847: %IPS-6-ENGINE_BUILDING: multi-string - 3 signatures - 12 of 11 engines
*Nov 9 21:50:55.859: %IPS-6-ENGINE_READY: multi-string - build time 12 ms - packets for
this engine will be scanned
*Nov 9 21:50:55.859: %SYS-5-CONFIG_I: Configured from console by cisco on console
```

The following example shows how to tune event-action parameters for the signature category “adware/spyware.” All the tuning information will be applied to all signatures that belong to the adware/spyware signature category.

```
Router(config)# ip ips signature category
Router(config-ips-category)# category attack adware/spyware
Router(config-ips-category-action)# event-action produce-alert
Router(config-ips-category-action)# event-action deny-packet-inline
Router(config-ips-category-action)# event-action reset-tcp-connection
Router(config-ips-category-action)# retired false
Router(config-ips-category-action)# ^Z
Do you want to accept these changes:[confirmm]y
```

Related Commands

Command	Description
engine	Enters the signature-definition-action-engine configuration mode, which allows you to change router actions for a specified signature.
ip ips config location	Specifies the location in which the router will save signature information.

Command	Description
signature	Specifies a signature for which the CLI user tunings will be changed.
show ip ips	Displays IPS information such as configured sessions and signatures.

exception access-group

To configure a device exception in a global consumer configuration, use the **exception access-group** command in TMS consumer configuration mode. To remove the device exception from the global TMS configuration, use the **no** form of this command.

Note Effective with Cisco IOS Release 12.4(20)T, the **exception access-group** command is not available in Cisco IOS software.

exception access-group *extended-acl*

no exception access-group *extended-acl*

Syntax Description

extended-acl	Name or number of the extended access list.

Command Default

None.

Command Modes

TMS consumer configuration (cfg-tms-cons)

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 **exception access-group** command is configured to attach a local device exception to a consumer process. A local device exception is an override configured on the consumer that negates a mitigation enforcement action sent from the controller or from a TMS Rules Engine configuration (mitigation type service policy) configured on the consumer.

For example, traffic from the 192.168.1.0/24 network is considered to be suspect. So, an ACL drop enforcement action is configured for all traffic sourced from this network. However, a device with a host address in this range (192.168.1.55) needs to transit over a specific consumer. A local device exception is configured on the consumer to override ACL drop enforcement action.

The device exception is configured locally. A host IP address (or any other subset of the network) is defined in an extended access list and then referenced by the **exception access-group** command. The **tms-class** command is configured to associate an interface with the device exception. The enforcement action configured on the controller is not applied to traffic that is permitted by the access list.

Examples

The following example configures an device exception for the 192.168.1.55 host address:

```
Router(config)# ip access-list extended NAMED_ACL

Router(config-ext-nacl)# permit tcp host 192.168.1.55 any

Router(config-ext-nacl)# exit

Router(config)# interface Ethernet 0/0

Router(config-if)# ip access-group NAMED_ACL in
Router(config-if)# tms-class

Router(config-if)# exit

Router(config)# tms consumer

Router(cfg-tms-cons)# exception access-group NAMED_ACL

Router(cfg-tms-cons)# service-policy type tms TMS_POL_1

Router(cfg-tms-cons)# end
```

Related Commands

Command	Description
tms consumer	Configures a consumer process on a router or networking device.
tms-class	Associates an interface with an ACL drop enforcement action.

exclusive-domain

To add or remove a domain name to or from the exclusive domain list so that the Cisco IOS firewall does not have to send lookup requests to the vendor server, use the **exclusive-domain** command in URL parameter-map configuration mode. To disable this capability, use the **no** form of this command.

exclusive-domain {**deny**| **permit**} *domain-name*

no exclusive-domain {**deny**| **permit**} *domain-name*

Syntax Description

deny	Removes the specified domain name from the exclusive domain list. Blocks all traffic destined for the specified domain name.
permit	Adds the specified domain name to the exclusive domain list. Permits all traffic destined for the specified domain name.
domain-name	Domain name that is added or removed from the exclusive domain name list; for example, www.example.com.

Command Default

Disabled.

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 **exclusive-domain**subcommand after you enter the **parameter-map type urlfilter** command. For detailed information about creating a parameter map, see the **parameter-map type urlfilter** command.

The **exclusive-domain** command allows you to specify a list of domain names (exclusive domains) so that the Cisco IOS firewall does not create a lookup request for the traffic that is destined for one of the domains in the exclusive list. Thus, you can avoid sending lookup requests to the web server for traffic that is destined for a host that is completely allowed to all users. You can enter the complete domain name or a partial domain name.

Complete Domain Name

If you add a complete domain name, such as www.example.com, to the exclusive domain list, all traffic whose URLs are destined for this domain (such as www.example.com/news and www.example.com/index) is excluded from the URL filtering policies of the vendor server. On the basis of the configuration, the URLs are permitted or blocked (denied).

Partial Domain Name

If you add only a partial domain name to the exclusive domain list, such as example.com, all URLs whose domain names end with this partial domain name (such as www.example.com/products and www.example.com/eng) are excluded from the URL filtering policies of the vendor server. On the basis of the configuration, the URLs are permitted or blocked (denied).

Examples

The following example adds cisco.com to the exclusive domain list:

```
parameter-map type urlfilter u1
 exclusive-domain permit example.com
```

Related Commands

Command	Description
ip urlfilter exclusive-domain	Adds or removes a domain name to or from the exclusive domain list so that the Cisco IOS firewall does not have to send lookup requests to the vendor server.
parameter-map type urlfilter	Creates or modifies a parameter map for URL filtering parameters.

F through H

filter-hash

Note Effective with Cisco IOS Release 15.2(4)M, the **filter-hash** command is not available in Cisco IOS software.

To specify the hash for verification and validation of decrypted contents, use the **filter-hash** command in Flexible Packet Matching (FPM) encryption filter configuration mode.

filter-hash *hash-value*

Syntax Description

hash-value	Hash value obtained from the encrypted traffic classification definition file (eTCDF).

Command Default

No hash value is specified.

Command Modes

FPM encryption filter configuration (c-map-match-enc-config)

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

If you have access to an eTCDF or if you know valid values to configure encrypted FPM filters, you can configure the same eTCDF through the command-line interface instead of using the preferred method of loading the eTCDF on the router. You must create a class map of type access-control using the **class-map type** command, and use the **match encrypted** command to configure the match criteria for the class map on the basis of encrypted FPM filters and enter FPM match encryption filter configuration mode. You can then use the appropriate commands to specify the algorithm, cipher key, cipher value, filter hash, filter ID, and filter version. You can copy the values from the eTCDF by opening the eTCDF in any text editor.

Use the **filter-hash** command to specify the hash for verification and validation of decrypted contents.

Examples

The following example shows how to specify the hash value from the eTCDF file for verification and validation of decrypted contents:

```
Router(config)# class-map type access-control match-all c1
Router(config-cmap)# match encrypted
Router(c-map-match-enc-config)# filter-hash AABBCCDD11223344
Router(c-map-match-enc-config)#
```

Related Commands

Command	Description
class-map type	Creates a class map to be used for matching packets to a specified class.
match encrypted	Configures the match criteria for a class map on the basis of encrypted FPM filters and enters FPM match encryption filter configuration mode.

filter-id

Note Effective with Cisco IOS Release 15.2(4)M, the **filter-id** command is not available in Cisco IOS software.

To specify a filter-level ID for encrypted filters, use the **filter-id** command in FPM match encryption filter configuration mode.

filter-id *id-value*

Syntax Description

id-value	Filter-level ID value.

Command Default

No filter ID is specified.

Command Modes

FPM match encryption filter configuration (c-map-match-enc-config)

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

If you have access to an encrypted traffic classification definition file (eTCDF) or if you know valid values to configure encrypted Flexible Packet Matching (FPM) filters, you can configure the same eTCDF through the command-line interface instead of using the preferred method of loading the eTCDF on the router. You must create a class map of type access-control using the **class-map type** command, and use the **match encrypted** command to configure the match criteria for the class map on the basis of encrypted FPM filters and enter FPM match encryption filter configuration mode. You can then use the appropriate commands to specify the algorithm, cipher key, cipher value, filter hash, filter ID, and filter version. You can copy the values from the eTCDF by opening the eTCDF in any text editor.

Use the **filter-id** command to specify a filter-level ID for encrypted filters.

Examples

The following example shows how to specify the filter ID value for an encrypted filter:

```
Router(config)# class-map type access-control match-all c1
Router(config-cmap)# match encrypted
Router(c-map-match-enc-config)# filter-id id2
Router(c-map-match-enc-config)#
```

Related Commands

Command	Description
class-map type	Creates a class map to be used for matching packets to a specified class.
match encrypted	Configures the match criteria for a class map on the basis of encrypted FPM filters and enters FPM match encryption filter configuration mode.

filter-version

Note Effective with Cisco IOS Release 15.2(4)M, the **filter-version** command is not available in Cisco IOS software.

To specify the filter-level version value for the encrypted filter, use the **filter-version** command in FPM match encryption filter configuration mode.

filter-version *version*

Syntax Description

version	Filter-level version value of the encrypted filter.

Command Default

No filter version is specified.

Command Modes

FPM match encryption filter configuration (c-map-match-enc-config)

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

If you have access to an encrypted traffic classification definition file (eTCDF) or if you know valid values to configure encrypted Flexible Packet Matching (FPM) filters, you can configure the same eTCDF through the command-line interface instead of using the preferred method of loading the eTCDF on the router. You must create a class map of type access-control using the **class-map type** command, and use the **match encrypted** command to configure the match criteria for the class map on the basis of encrypted FPM filters and enter FPM match encryption filter configuration mode. You can then use the appropriate commands to specify the algorithm, cipher key, cipher value, filter hash, filter ID, and filter version. You can copy the values from the eTCDF by opening the eTCDF in any text editor.

Use the **filter-version** command to specify the filter-level version value for the encrypted filter.

Examples

The following example shows how to specify the filter version for the encrypted filter:

```
Router(config)# class-map type access-control match-all c1
Router(config-cmap)# match encrypted
Router(c-map-match-enc-config)# filter-version v1
Router(c-map-match-enc-config)#
```

Related Commands

Command	Description
class-map type	Creates a class map to be used for matching packets to a specified class.
match encrypted	Configures the match criteria for a class map on the basis of encrypted FPM filters and enters FPM match encryption filter configuration mode.

filter tunnel

To configure a SSL VPN tunnel access filter, use **filter tunnel** command in webvpn group policy configuration mode. To remove the tunnel access filter, use the **no** form of this command.

filter tunnel {*extended-acl* | *acl-name*}

no filter tunnel

Syntax Description

extended-acl	Defines the filter on the basis of an extended access list (ACL). A named, numbered, or expanded access list is entered.
acl -name	Specifies the name for the access list.

Command Default

A SSL VPN tunnel access filter is not configured.

Command Modes

Webvpn group policy configuration

Command History

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

Usage Guidelines

The tunnel access filter is used to control network- and application-level access.

Examples

The following example shows how to configure a deny access filter for any host from the 192.0.2.0/24 network:

```
Device(config)# access-list 101 deny ip 192.0.2.0 0.0.0.255 any
Device(config)# webvpn context context1
Device(config-webvpn-context)# policy group ONE
Device(config-webvpn-group)# filter tunnel 101
```

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.

fingerprint

To preenter a fingerprint that can be matched against the fingerprint of a certification authority (CA) certificate during authentication, use the **fingerprint** command in ca-trustpoint configuration mode. To remove the preentered fingerprint, use the **no** form of this command.

fingerprint *ca-fingerprint*

no fingerprint *ca-fingerprint*

Syntax Description

ca-fingerprint	Certificate fingerprint.

Command Default

A fingerprint is not preentered for a trustpoint, and if the authentication request is interactive, you must verify the fingerprint that is displayed during authentication of the CA certificate. If the authentication request is noninteractive, the certificate will be rejected without a preentered fingerprint.

Command Modes

Ca-trustpoint configuration

Command History

Release	Modification
12.3(12)	This command was introduced. This release supports only message digest algorithm 5 (MD5) fingerprints.
12.3(13)T	Support was added for Secure Hash Algorithm 1 (SHA1), but only for Cisco IOS T releases.
12.4(24)T	Support for IPv6 Secure Neighbor Discovery (SeND) was added.

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.

Note An authentication request made using the CLI is considered an interactive request. An authentication request made using HTTP or another management tool is considered a noninteractive request.

Preenter the fingerprint if you want to avoid responding to the verify question during CA certificate authentication or if you will be requesting authentication noninteractively. The preentered fingerprint may be either the MD5 fingerprint or the SHA1 fingerprint of the CA certificate.

If you are authenticating a CA certificate and the fingerprint was preentered, if the fingerprint matches that of the certificate, the certificate is accepted. If the preentered fingerprint does not match, the certificate is rejected.

If you are requesting authentication noninteractively, the fingerprint must be preentered or the certificate will be rejected. The verify question will not be asked when authentication is requested noninteractively.

If you are requesting authentication interactively without preentering the fingerprint, the fingerprint of the certificate will be displayed, and you will be asked to verify it.

Examples

The following example shows how to preenter an MD5 fingerprint before authenticating a CA certificate:

```
Router(config)# crypto pki trustpoint myTrustpoint
Router(ca-trustpoint)# fingerprint 6513D537 7AEA61B7 29B7E8CD BBAA510B
Router(ca-trustpoint) exit
Router(config)# crypto pki authenticate myTrustpoint
Certificate has the following attributes:
       Fingerprint MD5: 6513D537 7AEA61B7 29B7E8CD BBAA510B
      Fingerprint SHA1: 998CCFAA 5816ECDE 38FC217F 04C11F1D DA06667E
Trustpoint Fingerprint: 6513D537 7AEA61B7 29B7E8CD BBAA510B
Certificate validated - fingerprints matched.
Trustpoint CA certificate accepted.
Router (config)#
```

The following is an example for Cisco Release 12.3(12). Note that the SHA1 fingerprint is not displayed because it is not supported by this release.

```
Router(config)# crypto ca trustpoint myTrustpoint
Router(ca-trustpoint)# fingerprint 6513D537 7AEA61B7 29B7E8CD BBAA510B
Router(ca-trustpoint)# exit
Router(config)# crypto ca authenticate myTrustpoint
Certificate has the following attributes:
           Fingerprint: 6513D537 7AEA61B7 29B7E8CD BBAA510B
Trustpoint Fingerprint: 6513D537 7AEA61B7 29B7E8CD BBAA510B
Certificate validated - fingerprints matched.
Trustpoint CA certificate accepted.
Router(config)#
```

Related Commands

Command	Description
crypto ca authenticate	Authenticates the CA (by getting the certificate of the CA).
crypto ca trustpoint	Declares the CA that your router should use.

firewall

To specify secure virtual LAN (VLAN) groups and to attach them to firewall modules, use the **firewall** command in global configuration mode. To disable the configuration, use the **no** form of this command.

firewall {**autostate**| **module** *number* **vlan-group** *number*| **multiple-vlan-interfaces**| **vlan-group** *number* *vlan-range*}

no firewall {**autostate**| **module** *number* **vlan-group** *number*| **multiple-vlan-interfaces**| **vlan-group** *number* *vlan-range*}

Syntax Description

autostate	Enables auto state.
module	Specifies the module number to which a VLAN group is attached.
number	Module number. Valid values are from 1 to 6.
vlan-group	Specifies the secure group to which the VLANs are attached.
number	Group number. The range is from 1 to 65535.
multiple-vlan-interfaces	Enables multiple VLAN interfaces mode for firewall modules.
vlan-range	VLAN range. Valid values are from 2 to 1001 and 1006 to 4094.

Command Default

No secure VLAN groups are attached to firewall modules.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SXI	This command was introduced.

Examples

The following example shows how to configure a VLAN group:

```
Router(config)# firewall vlan-group 34 1-20
```

Related Commands

Command	Description
show firewall vlan-group	Displays secure VLANs attached to a secure group.

fpm package-group

Note Effective with Cisco IOS Release 15.2(4)M, the **fpm package-group** command is not available in Cisco IOS software.

To configure flexible packet matching (fpm) package support, use the **fpm package-group** command in global configuration mode. To disable fpm package support, use the **no** form of this command.

fpm package-group [fpm-group-name]

no fpm package-group [fpm-group-name]

Syntax Description

fpm-group-name	Specifies the fpm package group name.

Command Default

FPM groups are not configured by default.

Command Modes

Global configuration (config)#

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 example enables fpm package-group:

```
Router(config)# fpm package-group fpm-group-76
```

Related Commands

Command	Description
fpm package-info	Enables fpm package transfer.

fpm package-info

Note Effective with Cisco IOS Release 15.2(4)M, the **fpm package-info** command is not available in Cisco IOS software.

To configure flexible packet matching (FPM) package transfer from an FPM server to a local server, use the **fpm package-info** command in global configuration mode. To disable fpm packet transfer, use the **no** form of this command.

fpm package-info

no fpm package-info

Syntax Description

This command has no keywords or arguments.

Command Default

The command is not configured by default.

Command Modes

Global configuration (config)#

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 example enables fpm package transfer:

```
Router(config)# fpm package-info
```

Related Commands

Command	Description
fpm package-group	Configures fpm package group support.
show fpm package-group	Displays fpm package matching support configuration details.
show fpm package-info	Displays fpm package transfer configuration details.

fqdn (IKEv2 profile)

To derive the name mangler from the remote identity of type Fully Qualified Domain Name (FQDN), use the **fqdn** command in IKEv2 name mangler configuration mode. To remove the name derived from FQDN, use the **no** form of this command.

fqdn {**all**| **domain**| **hostname**}

no fqdn

Syntax Description

all	Derives the name mangler from the entire FQDN.
domain	Derives the name mangler from the domain name of FQDN.
hostname	Derives the name mangler from the hostname of FQDN.

Command Default

No default behavior or values.

Command Modes

IKEv2 name mangler configuration (config-ikev2-name-mangler)

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.

Usage Guidelines

Use this command to derive the name mangler from the remote identity of type FQDN.

Examples

The following example shows how to derive a name for the name mangler from the hostname of FQDN:

```
Router(config)# crypto ikev2 name-mangler mangler2
Router(config-ikev2-name-mangler)# fqdn hostname
```

Related Commands

Command	Description
crypto ikev2 name mangler	Defines a name mangler.

grant auto rollover

To enable automatic granting of certificate reenrollment requests for a Cisco IOS subordinate certificate authority (CA) server or registration authority (RA) mode CA, use the **grant auto rollover** command in certificate server configuration mode. To disable automatic granting of certificate reenrollment requests for a Cisco IOS subordinate or RA-mode CA server, use the **no** form of this command.

grant auto rollover {**ca-cert**| **ra-cert**}

no grant auto rollover {**ca-cert**| **ra-cert**}

Syntax Description

ca-cert	Specifies that auto renewal is enabled for the subordinate CA rollover certificate.
ra-cert	Specifies that auto renewal is enabled for the RA-mode CA rollover certificate.

Command Default

Automatic granting of certificate reenrollment requests for a Cisco IOS subordinate CA server or RA-mode CA reenrollment requests is not enabled. Reenrollment requests will have to be granted manually.

Command Modes

Certificate server configuration (cs-server)

Command History

Release	Modification
12.4(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.

The first time a CA is enabled, a certificate request is sent to its superior CA. This initial request must be granted manually. The **grant auto rollover**command allows subsequent renewal certificate grant requests to be automatically processed by the CA for either a subordinate CA certificate (by designating the **ca-cert** keyword) or an RA-mode CA (by designating the **ra-cert** keyword), thereby eliminating the need for operator intervention.

Examples

The following example shows how the user can enable automatic granting of certificate reenrollment requests for a Cisco IOS subordinate CA server:

```
Router(config)#crypto pki server CA
Router(cs-server)#grant auto rollover ca-cert
```

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.
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 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.

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

grant auto trustpoint

To specify the certification authority (CA) trustpoint of another vendor from which the Cisco IOS certificate server automatically grants certificate enrollment requests, use the **grant auto trustpoint**command in certificate server configuration mode. To remove the name of the trustpoint holding the trusted CA certificate, use the **no** form of this command.

grant auto trustpoint *label*

no grant auto trustpoint *label*

Syntax Description

label	Name of the non-Cisco IOS CA trustpoint.

Command Default

No default behavior or values.

Command Modes

Certificate server configuration (cs-server)

Command History

Release	Modification
12.3(11)T	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 12.2(33)SRA.

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.

After the network administrator for the server configures and authenticates a trustpoint for the CA of another vendor, the **grant auto trustpoint** command is issued to reference the newly created trustpoint and enroll the router with a Cisco IOS CA.

Note The newly created trustpoint can only be used one time (which occurs when the router is enrolled with the Cisco IOS CA). After the initial enrollment is successfully completed, the credential information will be deleted from the enrollment profile.

The Cisco IOS certificate server will automatically grant only the requests from clients who were already enrolled with the CA of another vendor. All other requests must be manually granted--unless the server is set to be in auto grant mode (through the **grant automatic**command).

Caution

The **grant automatic**command can be used for testing and building simple networks and should be disabled before the network is accessible by the Internet. However, it is recommended that you do not issue this command if your network is generally accessible .

Examples

The following example shows how to configure a client router and a Cisco IOS certificate server to exchange enrollment requests through a certificate enrollment profile:

```
! Define the trustpoint “msca-root” that points to the non-Cisco IOS CA and enroll and !
authenticate the client with the non-Cisco IOS CA.
crypto pki trustpoint msca-root
 enrollment mode ra
 enrollment url http://msca-root:80/certsrv/mscep/mscep.dll
 ip-address FastEthernet2/0
 revocation-check crl
!
! Configure trustpoint “cs” for Cisco IOS CA.
crypto pki trustpoint cs
 enrollment profile cs1
 revocation-check crl
!
! Define enrollment profile “cs1,” which points to Cisco IOS CA and mention (via the !
enrollment credential command) that “msca-root” is being initially enrolled with the ! Cisco
 IOS CA.
crypto pki profile enrollment cs1
 enrollment url  http://cs:80
 enrollment credential  msca-root!
! Configure the certificate server, and issue the grant auto trustpoint command to ! instruct
 the certificate server to accept enrollment request only from clients who are ! already
enrolled with trustpoint “msca-root.”
crypto pki server cs
 database level minimum
 database url nvram:
 issuer-name CN=cs
 grant auto trustpoint msca-root
!
crypto pki trustpoint cs
 revocation-check crl
rsakeypair cs
!
crypto pki trustpoint msca-root
 enrollment mode ra
 enrollment url http://msca-root:80/certsrv/mscep/mscep.dll
 revocation-check crl
```

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.

Command	Description
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 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.

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

grant none

To specify all certificate requests to be rejected, use the **grant none** command in certificate server configuration mode. To disable automatic rejection of certificate enrollment, use the **no** form of this command.

grant none

no grant none

Syntax Description

This command has no arguments or keywords.

Command Default

Certificate enrollment is manual; that is, authorization is required.

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.

Examples

The following example shows how to automatically reject all certificate enrollment requests for the certificate server “myserver”:

```
Router#(config) ip http server
Router#(config) crypto pki server myserver
Router#(cs-server) database level minimum
Router#(cs-server)#
grant none
```

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.

Command	Description
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 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.

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

grant ra-auto

To specify that all enrollment requests from a Registration Authority (RA) be granted automatically, use the **grant ra-auto** command in certificate server configuration mode. To disable automatic certificate enrollment, use the **no** form of this command.

grant ra-auto

no grant ra-auto

Syntax Description

This command has no arguments or keywords.

Command Default

Certificate enrollment is manual; that is, authorization is required.

Command Modes

Certificate server configuration (cs-server)

Command History

Release	Modification
12.3(7)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.

When grant ra-auto mode is configured on the issuing certificate server, ensure that the RA mode certificate server is running in manual grant mode so that enrollment requests are authorized individually by the RA.

Note For the **grant ra-auto** command to work, you have to include “cn=ioscs RA” or “ou=ioscs RA” in the subject name of the RA certificate.

Examples

The following output shows that the issuing certificate server is configured to issue a certificate automatically if the request comes from an RA:

```
Router (config)# crypto pki server myserver
Router-ca (cs-server)# grant ra-auto
% This will cause all certificate requests that are already authorized by known RAs to be
automatically granted.
Are you sure you want to do this? [yes/no]:yes
```

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.
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.

Command	Description
grant none	Specifies all certificate requests to be rejected.
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.
show (cs-server)	Displays the PKI CS configuration.
shutdown (cs-server)	Allows a CS to be disabled without removing the configuration.

group (firewall)

To enter redundancy application group configuration mode, use the **group** command in redundancy application configuration mode. To remove the group configuration, use the **no** form of this command.

group *id*

no group *id*

Syntax Description

id	Redundancy group ID. Valid values are 1 and 2.

Command Default

No group is configured.

Command Modes

Redundancy application configuration (config-red-app)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Examples

The following example shows how to configure a redundancy group with group ID 1:

```
Router# configure terminal
Router(config)# redundancy
Router(config-red)# application redundancy
Router(config-red-app)# group 1
Router(config-red-app-grp)#
```

Related Commands

Command	Description
application redundancy	Enters redundancy application configuration mode.

group (authentication)

To specify the authentication, authorization, and accounting (AAA) TACACS+ server group to use for preauthentication, use the **group** command in AAA preauthentication configuration mode. To remove the **group** command from your configuration, use the **no** form of this command.

group tacacs+ *server-group*

no group tacacs+ *server-group*

Syntax Description

tacacs+	Uses a TACACS+ server for authentication.
server-group	Name of the server group to use for authentication.

Command Default

No method list is configured.

Command Modes

AAA preauthentication configuration

Command History

Release	Modification
12.1(2)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

You must configure the **group** command before you configure any other AAA preauthentication command (**clid**, **ctype**, **dnis**, or **dnis bypass**).

Examples

The following example enables Dialed Number Identification Service (DNIS) preauthentication using the abc123 server group and the password aaa-DNIS:

```
aaa preauth
 group abc123
 dnis password aaa-DNIS
```

Related Commands

Command	Description
aaa preauth	Enters AAA preauthentication mode.
dnis (authentication)	Enables AAA preauthentication using DNIS.

group (IKE policy)

To specify one or more Diffie-Hellman (DH) group identifier(s) for use in an Internet Key Exchange (IKE) policy, which defines a set of parameters to be used during IKE negotiation , use the **group**command in Internet Security Association Key Management Protocol (ISAKMP) policy configuration mode. To reset the DH group identifier to the default value, use the **no** form of this command.

group{**1**| **2**| **5**| **14**| **15**| **16**| **19**| **20**| **24**}

no group

Syntax Description

1	Specifies the 768-bit DH group.
2	Specifies the 1024-bit DH group.
5	Specifies the 1536-bit DH group.
14	Specifies the 2048-bit DH group.
15	Specifies the 3072-bit DH group.
16	Specifies the 4096-bit DH group.
19	Specifies the 256-bit elliptic curve DH (ECDH) group.
20	Specifies the 384-bit ECDH group.
24	Specifies the 2048-bit DH/DSA group.

Command Default

DH group 1

Command Modes

ISAKMP policy configuration (config-isakmp)

Command History

Release	Modification
11.3 T	This command was introduced.
12.1(1.3)T	Support was added for DH group 5.
12.4(4)T	Support for IPv6 was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.(33)SRA.

Release	Modification
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	Support was added for DH groups 14, 15, and 16 on the Cisco ASR 1000 series routers.
15.1(2)T	This command was modified. The **14**, **15**, **16**, **19**, and **20** keywords were added.

Usage Guidelin

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.

The group chosen must be strong enough (have enough bits) to protect the IPsec keys during negotiation. A generally accepted guideline recommends the use of a 2048-bit group after 2013 (until 2030). Either group 14 or group 24 can be selected to meet this guideline. Even if a longer-lived security method is needed, the use of Elliptic Curve Cryptography is recommended, but group 15 and group 16 can also be considered.

The ISAKMP group and the IPsec perfect forward secrecy (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 shows how to configure an IKE policy with the 1024-bit DH group (all other parameters are set to the defaults):

```
Router(config)# crypto isakmp policy 15
Router(config-isakmp) group 2
Router(config-isakmp)
 exit
```

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.
hash (IKE policy)	Specifies the hash algorithm within an IKE policy.
lifetime (IKE policy)	Specifies the lifetime of an IKE SA.

Command	Description
show crypto isakmp policy	Displays the parameters for each IKE policy.

group (IKEv2 proposal)

To specify one or more Diffie-Hellman (DH) group identifier(s) for use in an Internet Key Exchange Version 2 (IKEv2) proposal, use the **group**command in IKEv2 proposal configuration mode. To reset the DH group identifier to the default value, use the **no** form of this command.

group {**1**| **2**| **5**| **14**| **15**| **16**| **19**| **20**| **24**}

no group

Syntax Description

1	Specifies the 768-bit DH group.
2	Specifies the 1024-bit DH group.
5	Specifies the 1536-bit DH group.
14	Specifies the 2048-bit DH group
15	Specifies the 3072-bit DH group.
16	Specifies the 4096-bit DH group.
19	Specifies the 256-bit elliptic curve DH (ECDH) group.
20	Specifies the 384-bit ECDH group.
24	Specifies the 2048-bit DH/DSA group.

Command Default

DH group 2 and 5 in the IKEv2 proposal.

Command Modes

IKEv2 proposal configuration (config-ikev2-proposal)

Command History

Release	Modification
15.1(1)T	This command was introduced.
15.1(2)T	This command was modified. The **14**, **15**, **16**, **19**, and **20** keywords were added.
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

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.

The group chosen must be strong enough (have enough bits) to protect the IPsec keys during negotiation. A generally accepted guideline recommends the use of a 2048-bit group after 2013 (until 2030). Either group 14 or group 24 can be selected to meet this guideline. Even if a longer-lived security method is needed, the use of Elliptic Curve Cryptography is recommended, but group 15 and group 16 can also be considered.

Examples

The following example shows how to configure an IKEv2 proposal with the 1024-bit DH group:

```
Router(config)#
crypto ikev2 proposal proposal1
Router(config-ikev2-proposal)#
group 2
Router(config-ikev2-proposal)#
exit
```

Related Commands

Command	Description
crypto ikev2 proposal	Defines an IKEv2 proposal.
encryption (ikev2 proposal)	Specifies the encryption algorithm in an IKEv2 proposal.
integrity (ikev2 proposal)	Specifies the integrity algorithm in an IKEv2 proposal.
show crypto ikev2 proposal	Displays the algorithms configured in each IKEv2 proposal.

group (local RADIUS server)

To enter user group configuration mode and to configure shared settings for a user group, use the **group**command in local RADIUS server configuration mode. To remove the group configuration from the local RADIUS server, use the **no** form of this command.

group *group-name*

no group *group-name*

Syntax Description

group-name	Name of user group.

Command Default

No default behavior or values

Command Modes

Local RADIUS server 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.

Examples

The following example shows that shared settings are being configured for group “team1”:

```
group team1
```

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.

Command	Description
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.
user	Authorizes a user to authenticate using the local authentication server.
vlan	Specifies a VLAN to be used by members of a user group.

group (RADIUS)

To specify the authentication, authorization, and accounting (AAA) RADIUS server group to use for preauthentication, use the **group** command in AAA preauthentication configuration mode. To remove the **group** command from your configuration, use the **no** form of this command.

group *server-group*

no group *server-group*

Syntax Description

server-group	Specifies a AAA RADIUS server group.

Command Default

No default behavior or values.

Command Modes

AAA preauthentication configuration

Command History

Release	Modification
12.1(2)T	This command was introduced.

Usage Guidelines

You must configure a RADIUS server group with the **aaa group server radius** command in global configuration mode before using the **group** command in AAA preauthentication configuration mode.

You must configure the **group** command before you configure any other AAA preauthentication command (**clid**, **ctype**, **dnis**, or **dnis bypass**).

Examples

The following example shows the creation of a RADIUS server group called “maestro” and then specifies that DNIS preauthentication be performed using this server group:

```
aaa group server radius maestro
 server 10.1.1.1
 server 10.2.2.2
 server 10.3.3.3
aaa preauth
 group maestro
 dnis required
```

Related Commands

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

Command	Description
clid	Preauthenticates calls on the basis of the CLID number.
ctype	Preauthenticates calls on the basis of the call type.
dnis (RADIUS)	Preauthenticates calls on the basis of the DNIS number.
dnis bypass (AAA preauthentication configuration)	Specifies a group of DNIS numbers that will be bypassed for preauthentication.

group-lock

The **group-lock** command attribute is used to check if a user attempting to connect to a group belongs to this group. This attribute is used in conjunction with the extended authentication (Xauth) username. The user name must include the group to which it belongs. The group is then matched against the VPN group name (ID_KEY_ID) that is passed during the Internet Key Exchange (IKE). If the groups do not match, then the client connection is terminated.

To allow the extended authentication (Xauth) username to be entered when preshared key authentication is used with IKE, use the **group-lock** command in Internet Security Association Key Management Protocol (ISAKMP) group configuration mode. To remove the group lock, use the **no** form of this command.

Note Preshared keys are supported only. Certificates are not supported.

group-lock

no group-lock

Syntax Description

This command has no arguments or keywords.

Command Default

Group lock is not configured.

Command Modes

ISAKMP group configuration (config-isakmp-group)

Command History

Release	Modification
12.2(13)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

The Group-Lock attribute can be used if preshared key authentication is used with IKE. When the user enables the **group-lock** command attribute, one of the following extended Xauth usernames can be entered:

name/group

name\group

name@group

name%group

where the \ / @ % are the delimiters. The group that is specified after the delimiter is then compared against the group identifier that is sent during IKE aggressive mode. The groups must match or the connection is rejected.

Caution Do not use the Group-Lock attribute if you are using RSA signature authentication mechanisms such as certificates. Use the User-VPN-Group attribute instead.

The Group-Lock attribute is configured on a Cisco IOS router or in the RADIUS profile. This attribute has local (gateway) significance only and is not passed to the client.

Note If local authentication is used, then the Group-Lock attribute is the only option.

The username in the local or RADIUS database must be of the following format:

username[/,\,%,@]group.

Examples

The following example shows how Group-Lock attribute is configured in the CLI using the **group-lock** command:

Note 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 **group-lock** command.

```
crypto isakmp client configuration group cisco
  group-lock
```

The following example shows how an attribute-value (AV) pair for the User-VPN-Group attribute is added in the RADIUS configuration:

Note If RADIUS is used for user authentication, then use the User-VPN-Group attribute instead of the Group-Lock attribute.

```
ipsec:group-lock=1
```

Related Commands

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

group-object

To specify a nested reference to a type of user group within an object group, use the **group-object** command in object-group identity configuration mode. To remove the user group from the object group, use the **no** form of this command.

group-object *name*

no group-object *name*

Syntax Description

name	Nested user group name.

Command Default

No nested user group 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

In addition to a security group that is specified for the object group, a group object can be specified for a nested user group. The **group-object** command is used in the class map configuration of the Security Group Access (SGA) Zone-Based Policy firewall (ZBPF). Multiple nested user 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 **group-object** command is used in the class map configuration of the SGA ZBPF.

```
Router(config)# object-group security myobject1a
Router(config-object-group)# security-group tag-id 1
Router(config-object-group)# end
Router(config)# object-group security myobject1b
Router(config-object-group)# security-group tag-id 2
Router(config-object-group)# end
Router(config)# object-group security myobject1
Router(config-object-group)# group-object myobject1a
Router(config-object-group)# group-object myobject1b
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.
match group-object security	Matches traffic from a user in the security group.
object-group security	Creates an object group to identify traffic coming from a specific user or endpoint.
security-group	Specifies the membership of the security group for an object group.
show object-group	Displays the content of all user groups.

group size

To set the group size (sender ID length) for Suite B, use the **group size** command in GDOI local server configuration mode. To return a group size to the default size, use the **no** form of this command.

group size {**small** {**8** | **12** | **16**} | **medium** | **large**}

no group size [**small** [**8** | **12** | **16**] | **medium** | **large**]

Syntax Description

small {**8** | **12** | **16**}	Specifies an 8-, 12-, or 16-bit sender identifier (SID).
medium	Specifies a 24-bit SID.
large	Specifies a 32-bit SID (FIPS 140-2 operating mode).

Command Default

Medium

Command Modes

GDOI local server configuration (gdoi-local-server)

Command History

Release	Modification
15.2(4)M	This command was introduced.

Usage Guidelines

SID lengths of 8, 12, or 16 bits ensure interoperability with the GDOI standard that is described in RFC 6054, Using Counter Modes with Encapsulating Security Payload (ESP) and Authentication Header (AH) to Protect Group Traffic.

For most deployments, a group size of medium is recommended; therefore, using this command is optional. Any group size other than medium should be used only for interoperability (for which a small 8-bit, small 12-bit, or small 16-bit size should be used) or if you need to strictly adhere to FIPS 140-2 compliance (in which case, large is required). If you use this command, you should choose the group size based on the anticipated number of key servers (KSs) and group members (GMs).

When you change the group size in a group with cooperative KSs while Suite B (meaning ESP-GCM or ESP-GMAC) is configured and while the Suite B policy has been generated, you must change the group size on all secondary KSs before changing it on the primary KS.

Changing the group size causes the group to reinitialize (so that the new SID length can be used). The following prompt appears:

```
Device(gdoi-local-server)# group size large

% Changing Group Size from MEDIUM to LARGE will cause
% the group to re-initialize...
```

```
Are you sure you want to proceed? [yes/no]:
```

If the group size is decreasing and KS SIDs (KSSIDs) were configured that are not supported in the new group size (for example, 256 was configured with large and you changed it to medium, which has a maximum KSSID value of 127), the following prompt appears:

```
Device(gdoi-local-server)# group size medium

% Changing the Group Size from LARGE to MEDIUM will cause the group to
% re-initialize & the following configured Key Server SIDs will be lost:
%   256, 510-511

Are you sure you want to proceed? [yes/no]:
```

If cooperative KSs are configured, changing the group size on a secondary cooperative KS will not change the group size used and will not cause reinitialization until the primary cooperative KS changes the group size and reinitializes the group:

```
Device(gdoi-local-server)# group size large

% Secondary COOP-KS will change configured Group Size from MEDIUM to LARGE
% but will not use this Group Size until Primary COOP-KS changes as well.
```

If the group is currently reinitializing, changing the group size is denied:

```
Device(gdoi-local-server)# group size large

% Group Size Configuration Denied:
%   Please wait for group getvpn to finish re-initialization
%   and try changing the Group Size again.
```

If cooperative KSs are configured and the local KS is primary, changing the group size is denied if all of the secondary cooperative KS peers have not already changed their group size to the new group size:

```
Device(gdoi-local-server)# group size large

% Primary COOP-KS cannot change Group Size from MEDIUM to LARGE while the
% following Secondary COOP-KS peers have not changed to LARGE:
%   10.0.9.1 (Group Size: MEDIUM)
```

If cooperative KSs are configured and the local KS is primary, changing the group size is denied if all of the secondary cooperative KS peers are not alive (meaning that there is a network split):

```
Device(gdoi-local-server)# group size large

% Primary COOP-KS cannot change Group Size from MEDIUM to LARGE while
% there is a network split with the following COOP-KS peers:
%   10.0.8.1 (Role: Primary, Status: Dead)
```

Examples

The following example shows how to configure a SID length of 16-bit small:

```
Device# crypto gdoi group GETVPN
Device(config-gdoi-group) server local
Device(gdoi-local-server) group size small 16
```

Related Commands

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

gtp

To configure the inspection parameters for General Packet Radio Service (GPRS) Tunneling Protocol (GTP), use the **gtp** command in parameter-map profile configuration mode. To disable the inspection parameters for GTP, use the **no** form of this command.

gtp {**request-queue** *elements*| **timeout** {{**gsn**| **pdp-context**| **signaling**| **tunnel**} *minutes*| **request-queue** *seconds*}| **tunnel-limit** *number*}

no gtp {**request-queue**| **timeout** {**gsn**| **pdp-context**| **signaling**| **tunnel**| **request-queue**}| **tunnel-limit**}

Syntax Description

request-queue	Specifies the queue depth of GTP requests.
elements	Number of elements in a queue. The range is from 1 to 4294967295. The default is 200.
timeout	Configures the timeout values for GTP.
gsn	Specifies the timeout value for the inactive GPRS Support Node (GSN).
minutes	Timeout in minutes. The range is from 1 to 35791. The default is 30.
pdp-context	Specifies the timeout value for inactive Packet Data Protocol (PDP) -Context.
request-queue	Specifies the timeout value for the inactive request queue.
seconds	Timeout in seconds. The range is from 1 to 2147483. The default value is 60.
signaling	Specifies the timeout value for inactive signaling.
tunnel	Specifies the timeout value for an inactive tunnel. The default value is 30 minutes.
tunnel-limit	Specifies the number of maximum allowed GTP tunnels.
number	Number of allowed GTP tunnels. The range is from 1 to 4294967295. The default is 500.

Command Default

Inspect parameters are not configured for GTP.

Command Modes

Parameter-map profile configuration (config-profile)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.

Usage Guidelines

The **request-queue** keyword specifies the maximum number of GTP requests that will be queued while waiting for a response. When the specified limit is reached and a new request arrives, the request that has been in the queue for the longest time is removed. After the inactivity timer has elapsed, the request will be removed from the queue.

Examples

The following examples show how to configure the maximum number of GTP requests that will be queued while waiting for a response.

```
Router(config)# parameter-map type inspect pamap1
Router(config-profile)# gtp request-queue 100
```

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.

hardware statistics

To enable the collection of hardware statistics, use the **hardware statistics**command in IPv6or IPv4 access-list configuration mode. To disable this feature, use the **no** form of this command.

hardware statistics

no hardware statistics

Syntax Description

This commands has no arguments or keywords.

Command Default

This command is disabled by default.

Command Modes

IPv6 access-list configuration (config-ipv6-acl)

Command History

Release	Modification
12.2(50)SY	This command was introduced.

Usage Guidelines

The hardware statistics command affects only global access-list (ACL) counters.

Examples

The following example enables the collection of hardware statistics in an IPv6 configuration:

```
Router(config-ipv6-acl)# hardware statistics
```

hash (ca-trustpoint)

To specify the cryptographic hash algorithm function for the signature that the Cisco IOS client uses to sign its self-signed certificates, use the **hash** command in ca-trustpoint configuration mode. To return to the default cryptographic hash function, use the **no** form of this command.

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.

hash{**md5**| **sha1**| **sha256**| **sha384**| **sha512**}

no hash

Syntax Description

md5	Specifies that Message-Digest algorithm 5 (MD5) hash function is used.
sha1	Specifies that Secure Hash Algorithm (SHA-1) hash function is used as the default hash algorithm for RSA keys.
sha256	Specifies that the SHA-256 hash function is used as the hash algorithm for Elliptic Curve (EC) 256 bit keys.
sha384	Specifies that the SHA-384 hash function is used as the hash algorithm for EC 384 bit keys.
sha512	Specifies that the SHA-512 hash function is used as the hash algorithm for EC 384 bit keys.

Command Default

The Cisco IOS client uses the MD5 cryptographic hash function for self-signed certificates by default.

Command Modes

Ca-trustpoint configuration (ca-trustpoint)

Command History

Release	Modification
12.4(15)T	This command was introduced.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 series routers.

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.

Any specified **hash** command algorithm keyword option can be used to over-ride the default setting for the trustpoint. This setting then becomes the default cryptographic hash algorithm function for self-signed certificates by default.

Note The algorithm does not specify what kind of signature the certificate authority (CA) uses when it issues a certificate to the client.

Examples

The following example configures the trustpoint “MyTP” and sets the cryptographic hash function to SHA-384:

```
crypto pki trustpoint MyTP
   enrollment url http://MyTP
   ip-address FastEthernet0/0
   revocation-check none
   hash sha384
```

Related Commands

Command	Description
hash (cs-server)	Specifies the cryptographic hash function the Cisco IOS certificate server uses to sign certificates issued by the CA.

hash (cs-server)

To specify the cryptographic hash function the Cisco IOS certificate server uses to sign certificates issued by the certificate authority (CA), use the **hash** command in certificate server configuration mode. To return to the default cryptographic hash function, use the no form of this command.

hash {**md5**| **sha1**| **sha256**| **sha384**| **sha512**}

no hash

Syntax Description

md5	Specifies that the Message-Digest algorithm 5 (MD5), the default hash function is used.
sha1	Specifies that the Secure Hash Algorithm (SHA-1) hash function is used.
sha256	Specifies that the SHA-256 hash function is used.
sha384	Specifies that the SHA-384 hash function is used.
sha512	Specifies that the SHA-512 hash function is used.

Command Default

By default, to sign certificates issued by CA, the Cisco IOS client uses the MD5 cryptographic hash function.

Command Modes

Certificate server configuration (cs-server)

Command History

Release	Modification
12.3(4)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.

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.

The **hash** command in cs-server configuration mode sets the hash function for the signature that the Cisco IOS CA uses to sign all of the certificates issued by the server. If the CA is a root CA, it uses the hash function in its own, self-signed certificate.

Examples

The following example configures a certificate server, MyCS, and sets the cryptographic hash function to SHA-512 for the certificate server:

```
crypto pki server MyCS
database level complete
issuer-name CN=company,L=city,C=country
grant auto trustpoint
hash sha512
lifetime crl 168
```

The following is sample output from the **show crypto ca certificates** command. This output shows that the CA has been configured and that the hash function SHA-512 has been specified.

```
CA Certificate
Status: Available
Certificate Serial Number: 01
Certificate Usage: Signature
Issuer:
cn=company
l=city
c=country
Subject:
cn=company
l=city
c=country
Validity Date:
start date: 01:32:35 GMT Aug 3 2006
end date: 01:32:35 GMT Aug 2 2009
Associated Trustpoints: MyTP
Certificate Subject:
Name: MyCS.cisco.com
IP Address: 192.168.10.2
Status: Pending Key
Usage: General Purpose
Certificate Request Fingerprint SHA1: 05080A60 82DE9395 B35607C2 38F3A0C3 50609EF8
Associated Trustpoint: MyTP
```

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.

Command	Description
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.
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.

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

hash (IKE policy)

To specify the hash algorithm within an Internet Key Exchange policy, use the **hash**command in Internet Security Association Key Management Protocol (ISAKMP) policy configuration mode. IKE policies define a set of parameters to be used during IKE negotiation. To reset the hash algorithm to the default secure hash algorithm (SHA) -1 hash algorithm, us e the **no** form of this command.

hash {**sha**| **sha256**| **sha384**| **md5**}

no hash

Syntax Description

sha	Specifies SHA-1 (HMAC variant) as the hash algorithm.
sha256	Specifies SHA-2 family 256-bit (HMAC variant) as the hash algorithm.
sha384	Specifies SHA-2 family 384-bit (HMAC variant) as the hash algorithm.
md5	Specifies MD5 (HMAC variant) as the hash algorithm.

Command Default

The SHA-1 hash algorithm

Command Modes

ISAKMP policy configuration

Command History

Release	Modification
11.3 T	This command was introduced.
12.4(4)T	IPv6 support 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.
Cisco IOS XE Release 2.1	This command was introduced on Cisco ASR 1000 Series Routers.
15.1(2)T	This command was modified. The **sha256** and **sha384** keywords were added.

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.

Use this command to specify the hash algorithm to be used in an IKE policy.

Examples

The following example configures an IKE policy with the MD5 hash algorithm (all other parameters are set to the defaults):

```
crypto isakmp policy 15
 hash md5
 exit
```

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 Diffie-Hellman group identifier within an IKE policy.
lifetime (IKE policy)	Specifies the lifetime of an IKE SA.
show crypto isakmp policy	Displays the parameters for each IKE policy.

heading

To configure the heading that is displayed above URLs listed on the portal page of a SSL VPN, use the **heading** command in webvpn URL list configuration mode. To remove the heading, use the **no** form of this command.

heading *text-string*

no heading

Syntax Description

text-string	The URL list heading entered as a text string. The heading must be in quotation marks if it contains spaces.

Command Default

A heading is not configured.

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)#
```

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.

hide-url-bar

To prevent the URL bar from being displayed on the SSL VPN portal page, use the **hide-url-bar** command in webvpn group policy configuration mode. To display the URL bar on the portal page, use the **no** form of this command.

hide-url-bar

no hide-url-bar

Syntax Description

This command has no arguments or keywords.

Command Default

The URL bar is displayed on the SSL VPN portal page.

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 applies only to clientless mode access.

Examples

The following example hides the URL bar on the SSL VPN portal page:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# policy group ONE
Router(config-webvpn-group)# hide-url-bar
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.

holdtime

To configure the hold time for Internet Key Exchange Version 2 (IKEv2) gateways in a Hot Standby Router Protocol (HSRP) cluster, use the **holdtime** command in IKEv2 cluster configuration mode. To restore the default hold time, use the **no** form of this command.

holdtime *milliseconds*

no holdtime

Syntax Description

milliseconds	Interval, in milliseconds, before a peer is considered dead. The range is from 100 to 120000. The default is 3000.

Command Default

The default is 3000 milliseconds if the hold time is not configured.

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 **holdtime** command.

Examples

The following example shows how to set the hold time to receive messages from a peer to 100 milliseconds:

```
Device(config)# crypto ikev2 cluster
Device(config-ikev2-cluster)# holdtime 100
```

Related Commands

Command	Description
crypto ikev2 cluster	Defines an IKEv2 cluster policy in an HSRP cluster.

hop-limit

To verify the advertised hop-count limit, use the **hop-limit** command in RA guard policy configuration mode.

hop-limit {**maximum**| **minimum** } *limit*

Syntax Description

maximum *limit*	Verifies that the hop-count limit is lower than that set by the *limit* argument.
minimum *limit*	Verifies that the hop-count limit is greater than that set by the *limit* argument.

Command Default

No hop-count limit is specified.

Command Modes

RA guard policy configuration (config-ra-guard)

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 **hop-limit** command enables verification that the advertised hop-count limit is greater than or less than the value set by the *limit* argument. Configuring the **minimum** *limit* keyword and argument can prevent an attacker from setting a low hop-count limit value on the hosts to block them from generating traffic to remote destinations; that is, beyond their default router. If the advertised hop-count limit value is unspecified (which is the same as setting a value of 0), the packet is dropped.

Configuring the **maximum** *limit* keyword and argument enables verification that the advertised hop-count limit is lower than the value set by the *limit* argument. If the advertised hop-count limit value is unspecified (which is the same as setting a value of 0), the packet is dropped.

Examples

The following example shows how the command defines a router advertisement (RA) guard policy name as raguard1, places the router in RA guard policy configuration mode, and sets a minimum hop-count limit of 3:

```
Router(config)# ipv6 nd raguard policy raguard1
Router(config-ra-guard)# hop-limit minimum 3
```

Related Commands

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

host (webvpn url rewrite)

To select the name of the host site to be mangled on a Secure Socket Layer virtual private network (SSL VPN) gateway, use the **host** command in webvpn url rewrite configuration mode. To deselect a site, use the **no** form of this command.

host *host-name*

no host *host-name*

Syntax Description

host-name	Hostname of the site to be mangled.

Command Default

A host site is not selected.

Command Modes

Webvpn url rewrite (config-webvpn-url-rewrite)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Examples

The following example shows that the site www.examplecompany.com is to be mangled:

```
Router (config)# webvpn context
Router (config-webvpn-context)# url rewrite
Router (config-webvpn-url-rewrite)# host www.examplecompany.com
```

Related Commands

Command	Description
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.

hostname (IKEv2 keyring)

To specify the hostname for the peer in the Internet Key Exchange Version 2 (IKEv2) keyring, use the **hostname** command IKEv2 keyring peer configuration mode. To remove the hostname, use the **no** form of this command.

hostname *name*

no hostname

Syntax Description

name	Name for the peer.

Command Default

The hostname is not specified.

Command Modes

IKEv2 keyring peer configuration (config-ikev2-keyring-peer)

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

When configuring the IKEv2 keyring, use this command to identify the peer using hostname, which is:

- Independent of the IKEv2 identity.
- Available on an IKEv2 initiator only.
- Provided by IPsec to IKEv2 as part of a security association setup request to identify the peer.
- Used to identify the peer only with crypto maps and not with tunnel protection.

Examples

The following example shows how to configure the hostname for a peer when configuring an IKEv2 keyring:

```
Router(config)# crypto ikev2 keyring keyring-1
Router(config-ikev2-keyring)# peer peer1
Router(config-ikev2-keyring-peer)# description peer1
Router(config-ikev2-keyring-peer)# hostname peer1.example.com
```

Related Commands

Command	Description
address (ikev2 keyring)	Specifies the IPv4 address or the range of the peers in IKEv2 key.
crypto ikev2 keyring	Defines an IKEv2 keyring.
description (ikev2 keyring)	Describes an IKEv2 peer or a peer group for the IKEv2 keyring.
identity (ikev2 keyring)	Identifies the peer with IKEv2 types of identity.
peer	Defines a peer or a peer group for the keyring.
pre-shared-key **(ikev2 keyring)**	Defines a preshared key for the IKEv2 peer.

hostname (WebVPN)

To configure the hostname for a SSL VPN gateway, use the **hostname** command in webvpn gateway configuration mode. To remove the hostname from the SSL VPN gateway configuration, use the **no** form of this command.

hostname *name*

no hostname

Syntax Description

name	Specifies the hostname.

Command Default

The hostname is not configured.

Command Modes

Webvpn gateway configuration

Command History

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

Usage Guidelines

A hostname is configured for use in the URL and cookie-mangling process. In configurations where traffic is balanced among multiple SSL VPN gateways, the hostname configured with this command maps to the gateway IP address configured on the load-balancing device(s).

Examples

The following example configures a hostname for a SSL VPN gateway:

```
Router(config)# webvpn gateway GW_1
Router(config-webvpn-gateway)# hostname VPN_Server
```

Related Commands

Command	Description
webvpn gateway	Defines a SSL VPN gateway and enters webvpn gateway configuration mode.

http proxy-server

To direct Secure Socket Layer virtual private network (SSL VPN) user requests through a backend HTTP proxy server, use the **http proxy-server** command in webvpn policy group configuration mode. To redirect user requests to internal servers, use the **no** form of this command.

http proxy-server {*dns-name*| *ip-address*} **port** *port-number*

no http proxy-server

Syntax Description

dns-name	Domain Name System (DNS) to be directed to the HTTP proxy server.
ip-address	IP address to be directed to the HTTP proxy server.
port *port-number*	Port number of the backend HTTP proxy server.

Command Default

User requests are routed directly to internal servers.

Command Modes

Webvpn policy group configuration (config-webvpn-group)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Examples

The following example shows that requests from IP address 10.1.1.1 are to be routed to the proxy server (port number 2034):

```
Router (config)# webvpn context e1
Router (config-webvpn-context)# policy group g1
Router (config-webvpn-group)# http proxy-server 10.1.1.1 port 2034
Router (config-webvpn-group)# exit
Router (config-webvpn-context)# default-group-policy g1
```

http-redirect

To configure HTTP traffic to be carried over secure HTTP (HTTPS), use the **http-redirect** command in webvpn gateway configuration mode. To remove the HTTPS configuration from the SSL VPN gateway, use the **no** form of this command.

http-redirect [**port** *number*]

no http-redirect

Syntax Description

port *number*	(Optional) Specifies a port number. The value for this argument is a number from 1 to 65535.

Command Default

The following default value is used if this command is configured without entering the **port** keyword:

port *number* : 80

Command Modes

Webvpn gateway configuration

Command History

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

Usage Guidelines

When this command is enabled, the HTTP port is opened and the SSL VPN gateway listens for HTTP connections. HTTP connections are redirected to use HTTPS. Entering the **port**keyword and *number* argument configures the gateway to listen for HTTP traffic on the specified port. Entering the **no** form, disables HTTP traffic redirection. HTTP traffic is handled by the HTTP server if one is running.

Examples

The following example, starting in global configuration mode, redirects HTTP traffic (on TCP port 80) over to HTTPS (on TCP port 443):

```
Router(config)# webvpn gateway SSL_GATEWAY
Router(config-webvpn-gateway)# http-redirect
```

Related Commands

Command	Description
webvpn gateway	Defines a SSL VPN gateway and enters webvpn gateway configuration mode.

hw-module slot subslot only

Note This command is deleted effective with Cisco IOS Release 12.2SXI.

To change the mode of the Cisco 7600 SSC-400 card to allocate full buffers to the specified subslot, use the **hw-module slot subslot only** command in global configuration mode. If this command is not used, the total amount of buffers available is divided between the two subslots on the Cisco 7600 SSC-400.

Note This command automatically generates a reset on the Cisco 7600 SSC-400. See Usage Guidelines below for details.

hw-module slot *slot* **subslot** *subslot* **only**

Syntax Description

slot	Chassis slot number where the Cisco 7600 SSC-400 is located. Refer to the appropriate hardware manual for slot information. For SIPs and SSCs, refer to the platform-specific SPA hardware installation guide or the corresponding “Identifying Slots and Subslots for SIPs and SPAs” topic in the platform-specific SPA software configuration guide.
subslot	Secondary slot number on the SSC where the IPSec VPN SPA is installed.

Command Default

No default behavior or values.

Command Modes

Global configuration mode

Command History

Release	Modification
12.2(18)SXF2	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.
12.2SXI	This command was deleted.

Usage Guidelines

Follow these guidelines and restrictions when configuring a Cisco 7600 SSC-400 and IPSec VPN SPAs using the **hw-module slot subslot only**command:

- This command is useful when supporting IP multicast over GRE on the IPSec VPN SPA.
- When this command is executed, it automatically takes a reset action on the Cisco 7600 SSC-400 and issues the following prompt to the console:

```
 Module n will be reset? Confirm [n]:
```

The prompt will default to "N" (no). You must type "Y" (yes) to activate the reset action.

- When in this mode, if you manually plug in a second SPA, or if you attempt to reset the SPA (by entering a **no hw-module subslot shutdown** command, for example), a message is displayed on the router console which refers you to the customer documentation.

Examples

The following example allocates full buffers to the SPA that is installed in subslot 0 of the SIP located in slot 1 of the router and takes a reset action of the Cisco 7600 SSC-400.

```
Router(config)# hw-module slot 4 subslot 1 only
Module 4 will be reset? Confirm [no]: y
```

Note that the prompt will default to "N" (no). You must type "Y" (yes) to activate the reset action.

Related Commands

Command	Description
ip multicast-routing	Enables IP multicast routing.
ip pim	Enables Protocol Independent Multicast (PIM) on an interface.

icmp idle-timeout through ip http ezvpn

icmp idle-timeout

To configure the timeout for Internet Control Message Protocol (ICMP) sessions, use the **icmp idle-timeout** command in parameter-map type inspect configuration mode. To disable the timeout, use the **no** form of this command.

icmp idle-timeout *seconds* [**ageout-time** *seconds*]

no icmp idle-timeout

Syntax Description

seconds	ICMP timeout, in seconds. The default is 10. Valid values are from 1 to 2147483.
ageout-time *seconds*	(Optional) Specifies the aggressive aging time for ICMP packets. Valid values are from 1 to 2147483.

Command Default

The timeout default is 10 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 **icmp idle-timeout** command 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 shows how to specify the ICMP session timeout as 90 seconds:

```
parameter-map type inspect insp-params
 icmp idle-timeout 90
```

The following example shows how to specify the ICMP session aging out time as 50 seconds:

```
parameter-map type inspect insp-params
 icmp idle-timeout 90 ageout 50
```

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.

ida-client server url

To specify the IDA-server url that the IOS IDA client communicates with to download files from the Cisco.com server, use the **ida-client server url** command in global configuration mode. To revert back to the default value, use the **no** form of this command.

ida-client server url url

no ida-client server url url

Syntax Description

url	Specifies the IDA-server url. You must enter the following URL: https://www.cisco.com/cgi-bin/front.x/ida/locator/locator.pl

Command Default

The default IDA-server URL is: https://www.cisco.com/cgi-bin/ida/locator/locator.pl

Note Do not use the default URL in your configuration.

Command Modes

Global configuration

Command History

Release	Modification
15.0(1)M	This command was introduced.
15.1(1)T	This command was modified to include a default IDA-server URL.

Usage Guidelines

Enter the following URL for the **ida-client server url**command to specify the IDA-server URL:

```
Router(config)# ida-client server url
https://www.cisco.com/cgi-bin/front.x/ida/locator/locator.pl
```

Related Commands

Command	Description
ips signature update cisco	Initiates a one-time download of an IPS signatures from Cisco.com.
upgrade automatic abortversion	Cancels the scheduled reloading of the router with a new Cisco IOS software image.

Command	Description
upgrade automatic getversion	Downloads a Cisco IOS software image directly from www.cisco.com or from a non-Cisco server.
upgrade automatic runversion	Reloads the router with a new Cisco IOS software image.

identifier

To assign a GDOI key server (KS) sender identifier (KSSID) to a KS, use the **identifier** command in GDOI local server configuration mode. To disable a GDOI KS identifier, use the **no** form of this command.

identifier

no identifier

Syntax Description

This command has no arguments or keywords.

Command Default

No KSSIDs are assigned to the KS.

Command Modes

GDOI local server (gdoi-local-server)

Command History

Release	Modification
15.2(4)M	This command was introduced.

Usage Guidelines

This command enters GDOI local server ID configuration mode, which contains several subcommands for setting the KSSID:

- **default** (sets the values to their defaults)
- **exit** (saves the KSSID configuration and exits)
- **no** (negates a command)
- **range** *lowest-kssid* **-** *highest-kssid* (assigns a range of KSSIDs (unique in the entire group))
- **value** *kssid* (assigns a KSSID (unique in the entire group))

Each KS must be assigned at least one KSSID when using GCM or GMAC. The following table shows that the range of KSSIDs available depends on the group size configuration.

Table 6: Ranges of Available KSSIDs Based on Group Size

Configured Group Size	Range of Available KSSIDs
Small (8 bits)	0 to 1
Small (12 bits)	0 to 3
Small (16 bits)	0 to 15
Medium	0 to 127

Configured Group Size	Range of Available KSSIDs
Large	0 to 511

Each KS must be assigned at least one KSSID when using GCM or GMAC. You can configure a single KSSID, a range of KSSIDs, or both. KSSID values are not assigned to (and usable by) the KS until you exit GDOI local server ID configuration mode.

If you remove KSSIDs that were previously used since the last reinitialization, the group reinitializes (without traffic loss), and KSSIDs that were used will be reset. You are prompted to confirm this before configuring the KSSID set. For example:

```
Device(gdoi-local-server-id)# no value 1
Device(gdoi-local-server-id)# exit

% The following Key Server SIDs being removed were previously used:
%   1
% Removing these KS SIDs will re-initialize the group (without traffic loss).

Are you sure you want to proceed? [yes/no]:
```

If the group is currently reinitializing, removal of KSSIDs that have been previously used since the last reinitialization is denied. For example:

```
Device(gdoi-local-server-id)# no value 0
Device(gdoi-local-server-id)# exit

% Key Server SID Configuration Denied:
%   Please wait for group getvpn to finish re-initialization
%   and try removing used KS SIDs again.
```

If cooperative KSs are configured and the secondary cooperative KS has configured a new group size, but the primary cooperative KS has not changed the group size so that the secondary cooperative KS is using the new group size, entering the **identifier** command on the secondary cooperative KS is denied. For example:

```
Device(gdoi-local-server)# identifier

% Key Server SID Configuration Denied:
%   Need Primary COOP-KS to change Group Size from MEDIUM to LARGE, OR
%   Need Local KS to change Group Size from LARGE to MEDIUM.
```

If cooperative KSs are is configured, the KSSIDs configured on each KS must be unique. No two KSs can have the same KSSID value configured, and if a cooperative KS tries to configure a KSSID that another cooperative KS peer has already assigned to itself, the configuration is denied. For example:

```
Device(gdoi-local-server-id)# range 0-127
Device(gdoi-local-server-id)# end

% Key Server SID Configuration Denied:
%   The following Key Server SIDs being added overlap:
%   0-9, 20-29  (COOP-KS Peer: 10.0.7.1)
%   10-19, 30-39  (COOP-KS Peer: 10.0.9.1)
```

Examples

The following example shows how to configure a single KSSID and a range of KSSIDs. In this example, the **value 0** command allots the pool of SIDs to the KS that begin with KSSID value 0 (meaning that it is allotted the pool of SID values beginning with 0x0 and ending with 0x1FFFF):

```
Device# configure terminal
Device(config)# crypto gdoi group GETVPN
Device(config-gdoi-group)# server local
Device(gdoi-local-server)# identifier
Device(gdoi-local-server-id)# range 10 - 20
Device(gdoi-local-server-id)# value 0
Device(gdoi-local-server-id)# end
```

identity local

To specify the local Internet Key Exchange Version 2 (IKEv2) identity type, use the **identity local**command in IKEv2 profile configuration mode. To remove the identity, use the **no** form of this command.

identity local {**address**{*ipv4-address*| *ipv6-address*}| **dn**| **fqdn** *fqdn-string*| **email** *e-mail-string*| **key-id** *opaque-string*}

no identity

Syntax Description

address *{ipv4-address | ipv6-address}*	Uses the IPv4 or IPv6 address as the local identity.
dn	Uses the distinguished name as the local identity.
fqdn *fqdn-string*	Uses the Fully Qualified Domain Name (FQDN) as the local identity.
email *email-string*	Uses the e-mail ID as the local identity.
key-id *opaque-string*	Uses the proprietary type opaque string as the local identity.

Command Default

If the local authentication method is a preshared key, the default local identity is the IP address (IPv4 or IPv6). If the local authentication method is an RSA signature, the default local identity is Distinguished Name.

Command Modes

IKEv2 profile configuration (config-ikev2-profile)

Command History

Release	Modification
15.1(1)T	This command was introduced.
15.1(4)M	This command was modified. Support was added for 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.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

Use this command to specify the local IKEv2 identity type as an IPv4 address or IPv6 address, a DN, an FQDN, an e-mail ID, or a key ID. The local IKEv2 identity is used by the local IKEv2 peer to identify itself to the remote IKEv2 peers in the AUTH exchange using the IDi field.

Note You can configure one local IKEv2 identity type for a profile.

Examples

The following example shows how to specify an IPv4 address as the local IKEv2 identity:

```
Router(config)# crypto ikev2 profile profile1
Router(config-ikev2-profile)# identity local address 10.0.0.1
The following example shows how to specify an IPv6 address as the local IKEv2 identity:
Router(config)# crypto ikev2 profile profile1
Router(config-ikev2-profile)# identity local address 2001:DB8:0::1
```

Related Commands

Command	Description
crypto ikev2 profile	Defines an IKEv2 profile.

identity (IKEv2 keyring)

To identify a peer with Internet Key Exchange Version 2 (IKEv2) types of identity, use the **identity**command in IKEv2 keyring peer configuration mode. To remove the identity, use the **no** form of this command.

identity {**address**{*ipv4-address*| *ipv6-address*}| **fqdn domain** *domain-name*| **email domain** *domain-name*| **key-id** *domain-name*}

no identity {**address**{*ipv4-address*| *ipv6-address*}| **fqdn domain** *domain-name*| **email domain** *domain-name*| **key-id** *key-id*}

Syntax Description

address {*ipv4-address* | *ipv6-address*}	Uses the IPv4 or IPv6 address to identify the peer.
fqdn domain *domain-name*	Uses the Fully Qualified Domain Name (FQDN) to identify the peer.
email domain*domain-name*	Uses the e-mail ID to identify the peer.
key-id *key-id*	Uses the proprietary types to identify the peer.

Command Default

Identity types are not specified to a peer.

Command Modes

IKEv2 keyring peer configuration (config-ikev2-keyring-peer)

Command History

Release	Modification
15.1(1)T	This command was introduced.
15.1(4)M	This command was modified. Support was added for 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.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.
15.3(3)M	This command was modified. The **domain** *domain-name* keyword-argument pair was added.

Usage Guidelines

Use this command to identify the peer using IKEv2 types of identity such as an IPv4 or IPv6 address, an FQDN, an e-mail ID, or a key ID. Key lookup using IKEv2 identity is available only on the responder because the peer ID is not available on the initiator at the time of starting the IKEv2 session, and the initiator looks up keys during session startup.

Examples

The following example shows how to associate an FQDN to the peer:

```
Router(config)# crypto ikev2 keyring keyring-4
Router(config-keyring)# peer abc
Router(config-keyring-peer)# description abc domain
Router(config-keyring-peer)# identity fqdn example.com
```

Related Commands

Command	Description
address (ikev2 keyring)	Specifies the IPv4 or IPv6 address or the range of the peers in an IKEv2 keyring.
crypto ikev2 keyring	Defines an IKEv2 keyring.
description (ikev2 keying)	Describes an IKEv2 peer or a peer group for the IKEv2 keyring.
hostname (ikev2 keyring)	Specifies the hostname for the peer in the IKEv2 keyring.
peer	Defines a peer or a peer group for the keyring.
pre-shared-key (ikev2 keyring)	Defines a preshared key for the IKEv2 peer.

identity (IKEv2 profile)

To specify how the local or remote router identifies itself to the peer and communicates with the peer in the Rivest, Shamir and Adleman (RSA) authentication exchange, use the **identity** command in IKEv2 profile configuration mode. To delete a match, use the **no** form of this command.

identity [**local** {**dn** [**trustpoint** *trustpoint-name* [**serial** *certificate-serial*]]| **address** *ip-address*| **fqdn** *string*| **email** *string*}| **remote** {**dn [ou=..., o=...]**| **address** *ip-address*| **fqdn** *string*| **email** *string*}]

no identity [**local** {**dn** [**trustpoint** *trustpoint-name* [**serial** *certificate-serial*]]| **address** *ip-address*| **fqdn** *string*| **email** *string*}| **remote** {**dn [ou=..., o=...]**| **address** *ip-address*| **fqdn** *string*| **email** *string*}]

Syntax Description

local	Specifies the local router.
dn	Specifies the distinguished name (DN) of the local or remote router.
trustpoint *trustpoint-name*	(Optional) Specifies the PKI trustpoint name to use with the RSA signature authentication method on the local router.
serial *certificate-serial*	(Optional) Specifies the serial number of the trustpoint certificate on the local router.
address *ip-address*	Specifies the IP address of the remote or local router.
fqdn *fqdn-name*	Specifies the Fully Qualified Domain Name (FQDN) of the remote or local router.
email *e-mail ID*	Specifies the email ID of the remote or local router.
ou= ..., **o=**...	(Optional) Specifies the organizational Unit (OU) field of the subject name in the trustpoint certificate.

Command Default

An identity profile is not specified for a local or remote router regarding the RSA authentication exchange.

Command Modes

IKEv2 profile configuration (crypto-ikev2-profile)#

Command History

Release	Modification
15.1(1)T	This command was introduced.
15.1(2)T	This command was modified. The **local**, **dn**, **trustpoint**, **serial**, and **ou=** keywords were added to this command.

Usage Guidelines

Use the **identity** command to identify the local or remote router by its DN, trustpoint, IP address, FQDN, or email address.

Examples

The following example shows how an IKEv2 profile is matched on the remote identity. The following profile caters to peers that identify using **fqdn example.com** and authenticate with **rsa-signature** using **trustpoint-remote**. The local node authenticates with **pre-share** using **keyring-1**.

```
Router(config)# crypto ikev2 profile profile2
Router(config-ikev2-profile)# match identity remote fqdn example.com
Router(config-ikev2-profile)# identity local email router2@example.com
Router(config-ikev2-profile)# authentication local pre-share
Router(config-ikev2-profile)# authentication remote rsa-sig
Router(config-ikev2-profile)# keyring keyring-1
Router(config-ikev2-profile)# pki trustpoint trustpoint-remote verify
Router(config-ikev2-profile)# lifetime 300
Router(config-ikev2-profile)# dpd 5 10 on-demand
Router(config-ikev2-profile)# virtual-template 1
```

Related Commands

Command	Description
crypto ikev2 profile	Defines an IKEv2 profile.
match (IKEv2 profile)	Matches a profile on front-door VPN routing and forwarding (FVRF) or local parameters such as IP address or peer identity or peer certificate.
authentication (IKEv2 profile)	Specifies the local and remote authentication methods in an Internet Key Exchange Version 2 (IKEv2) profile.
keyring (IKEv2 profile)	Specifies a locally defined or accounting, authentication and authorization (AAA) based keyring.
pki trustpoint	Specifies the router to use the PKI trustpoints in the RSA signature authentication.

identity address ipv4

To identify a Group Domain of Interpretation (GDOI) group address, use the **identity address ipv4** command in GDOI group configuration mode. To remove the group address, use the **no** form of this command.

identity address ipv4 *address*

no identity address ipv4 *address*

Syntax Description

address	IP address of the group.

Command Default

A group address is not identified.

Command Modes

GDOI group configuration

Command History

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

Usage Guidelines

This command or the **identity number** command is required for a GDOI configuration.

Examples

The following example shows that the identity address is 10.2.2.2:

```
identity address ipv4 10.2.2.2
```

Related Commands

Command	Description
crypto gdoi group	Identifies a GDOI group.
identity number	Identifies a GDOI group number.

identity number

To identify a Group Domain of Interpretation (GDOI) group number, use the **identity number** command in GDOI group configuration mode. To remove the group number, use the **no** form of this command.

identity number *number*

no identity number *number*

Syntax Description

number	Number of the group.

Command Default

A GDOI group number is not identified.

Command Modes

GDOI group configuration

Command History

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

Usage Guidelines

This command or the **identity address ipv4** command is required for a GDOI configuration.

Examples

The following example shows the group number is 3333:

```
identity number 3333
```

Related Commands

Command	Description
crypto gdoi group	Identifies a GDOI group and enters GDOI group configuration mode.
identity address ipv4	Identifies a GDOI group address.

identity policy

To create an identity policy and to enter identity policy configuration mode, use the **identity policy**command in global configuration mode. To remove the policy, use the **no** form of this command.

identity policy *policy-name* [**access-group** *group-name*| **description** *line-of-description*| **redirect** *url*| **template**| [**virtual-template** *interface-number*]]

noidentity policy *policy-name* [**access-group** *group-name*| **description** *line-of-description*| **redirect** *url*| **template**| [**virtual-template** *interface-number*]]

Syntax Description

policy-name	Name of the policy.
access-group *group-name*	(Optional) Access list to be applied.
description *line-of-description*	(Optional) Description of the policy.
redirect *url*	(Optional) Redirects clients to a particular URL.
template	(Optional) Virtual template interface from which commands may be cloned.
virtual-template *interface-number*	(Optional) Virtual template number. The values range from 1 through 200.

Command Default

An identity policy is not created.

Command Modes

Global configuration (config)

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

An identity policy has to be associated with an identity profile.

Examples

The following example shows that an access policy named "policyname2" is being created. The access-group attribute is set to "allow-access." The redirect URL is set to "http://remediate-url.com." This access policy will be associated with a statically authorized device in the identity profile.

```
Router (config)# identity policy policyname2
Router (config-identity-policy)# access-group allow-access
Router (config-identity-policy)# redirect url http://remediate-url.com
```

Related Commands

Command	Description
identity profile	Creates an identity profile.

identity profile

To create an identity profile and to enter identity profile configuration mode, use the **identity profile**command in global configuration mode. To disable an identity profile, use the **no** form of this command.

identity profile {**default**| **dot1x**| **eapoudp**| **auth-proxy**}

no identity profile {**default**| **dot1x**| **eapoudp**| **auth-proxy**}

Syntax Description

default	Service type is default.
dot1x	Service type for 802.1X.
eapoudp	Service type for Extensible Authentication Protocol over UDP (EAPoUDP).
auth-proxy	Service type for authentication proxy.

Command Default

An identity profile is not created.

Command Modes

Global configuration (config)

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.
12.3(8)T	The **eapoudp** keyword was added.
12.4(6)T	The **dot1x** keyword was removed.
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 **identity profile** command and **default** keyword allow you to configure static MAC addresses of a client computer that does not support 802.1X and to authorize or unauthorize them statically. After you have issued the **identity profile** command and **default** keyword and the router is in identity profile configuration mode, you can specify the configuration of a template that can be used to create the virtual access interface to which unauthenticated supplicants (client computers) will be mapped.

The **identity profile** command and the **dot1x** keyword are used by the supplicant and authenticator. Using the **dot1x** keyword, you can set the username, password, or other identity-related information for an 802.1X authentication.

Using the **identity profile** command and the **eapoudp** keyword, you can statically authenticate or unauthenticate a device either on the basis of the device IP address or MAC address or on the type, and the corresponding network access policy can be specified using the **identity policy** command.

Examples

The following example shows that an identity profile and its description have been specified:

```
Router (config)# identity profile default
Router (config-identity-prof)# description description_entered_here
```

The following example shows that an EAPoUDP identity profile has been created:

```
Router (config)# identity policy eapoudp
```

Related Commands

Command	Description
debug dot1x	Displays 802.1X debugging information.
description	Specifies a description for an 802.1X profile.
device	Statically authorizes or rejects individual devices.
dot1x initialize	Initializes 802.1X state machines on all 802.1X-enabled interfaces.
dot1x max-req	Sets the maximum number of times that a router can send an EAP request/identity frame to a client PC.
dot1x max-start	Sets the maximum number of times the authenticator sends an EAP request/identity frame (assuming that no response is received) to the client.
dot1x pae	Sets the PAE type during 802.1X authentication.
dot1x port-control	Enables manual control of the authorization state of a controlled port.
dot1x re-authenticate	Manually initiates a reauthtication of the specified 802.1X-enabled ports.
dot1x re-authentication	Globally enables periodic reauthentication of the client PCs on the 802.1X interface.
dot1x system-auth-control	Enables 802.1X SystemAuthControl (port-based authentication).

Command	Description
dot1x timeout	Sets retry timeouts.
identity policy	Creates an identity policy.
show dot1x	Displays details for an identity profile.
template (identity profile)	Specifies a virtual template from which commands may be cloned.

identity profile eapoudp

To create an identity profile and to enter Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP) profile configuration mode, use the **identity profile eapoudp**command in global configuration mode. To remove the policy, use the **no** form of this command.

identity profile eapoudp

no identity profile eapoudp

Syntax Description

This command has no arguments or keywords.

Command Default

No EAPoUDP identity profile exists.

Command Modes

Global configuration (config)

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

Using this command, you can statically authenticate or unauthenticate a device either on the basis of the device IP address or MAC address or on the type, and the corresponding network access policy can be specified using the **identity policy** command.

Examples

The following example shows that an EAPoUDP identity profile has been created:

```
Router (config)# identity profile eapoudp
```

Related Commands

Command	Description
identity policy	Creates an identity policy.

idle-timeout (WebVPN)

Note Effective with Cisco IOS Release 12.4(6)T, the **idle-timeout (WebVPN)** command is not available in Cisco IOS software.

To set the default idle timeout for a Secure Sockets Layer Virtual Private Network (SSLVPN) if no idle timeout has been defined or if the idle timeout is zero (0), use the **idle-timeout** command in Web VPN configuration mode. To revert to the default value, use the **no** form of this command.

idle-timeout [**never**| *seconds*]

no idle-timeout [**never**| *seconds*]

Syntax Description

never	(Optional) The idle timeout function is disabled.
seconds	(Optional) Idle timeout in seconds. The values are from 180 seconds (3 minutes) to 86400 seconds (24 hours).

Command Default

If command is not configured, the default idle timeout is 1800 seconds (30 minutes).

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

Configuring this command prevents stale sessions.

Examples

The following example shows that the idle timeout has been set for 1200 seconds:

```
Router (config)#
webvpn
Router (config-webvpn)# idle-timeout 1200
The following example shows that the idle timeout function is disabled:
Router (config)# webvpn
Router (config-webvpn)# idle-timeout never
```

Related Commands

Command	Description
webvpn	Enters Web VPN configuration mode.

if-state nhrp

To enable the Next Hop Resolution Protocol (NHRP) to control the state of the tunnel interface, use the **if-state nhrp** command in interface configuration mode. To disable NHRP control of the tunnel interface state, use the **no** form of this command.

if-state nhrp

no if-state nhrp

Syntax Description

This command has no arguments or keywords.

Command Default

NHRP tunnel interface state control is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Usage Guidelines

If the system detects that one or more of the Next Hop Servers (NHSs) configured on the interface is up, then the tunnel interface state is also declared as ‘up’. If all NHSs configured on the interface are down, then the tunnel interface state is also declared as ‘down’.

The system does not consider NHSs configured with ‘no-reply’ when determining the interface state.

Examples

The following example shows how to enable NHRP control of the tunnel interface state:

```
Router(config)# interface tunnel 1
Router(config-if)# if-state nhrp
```

Related Commands

Command	Description
show ip interface	Displays the usability status of interfaces configured for IP.
show ip nhrp nhs	Displays NHRP NHS information.

import

To import a user-defined URL list into a webvpn context, use the **import** command in the webvpn URL list configuration mode. To disable the URL list, use the **no** form of this command.

import *device* **:** *file*

no import *device* **:** *file*

Syntax Description

device **:** *file*	- *device* **:** *file* --Storage device on the system and the file name. The file name should include the directory location.

Command Default

A user-defined URL list is not imported.

Command Modes

Webvpn URL list configuration (config-webvpn-url)

Command History

Release	Modification
12.4(22)T	This command was introduced.

Usage Guidelines

If this command is used under the **url-list** command, the **url-text** command is not allowed. The **import** command and the **url-list** commands are mutually exclusive when used for a particular URL list. (If you use them together, you will receive this message: "Please remove the imported url-list.")

Also, if a URL list is configured using the **url-text** command, the **import** command is not allowed. (If you use them together, you will receive this message: "Please remove all the URLs before importing a file.")

Examples

The following example shows that the URL list file "test-url.xml" is being imported from flash:

```
Router (config)# webvpn context
 Router (config-webvpn-context)# url-list test
 Router (config-webvpn-url)# import flash:est-url.xml
```

Related Commands

Command	Description
webvpn create template	Creates templates for multilanguage support for messages in an SSL VPN.

include-local-lan

To configure the Include-Local-LAN attribute to allow a nonsplit-tunneling connection to access the local subnetwork at the same time as the client, use the **include-local-lan** command in Internet Security Association Key Management Protocol (ISAKMP) group configuration mode or Internet Key Exchange Version 2 (IKEv2) authorization policy configuration mode. To disable the attribute that allows the nonsplit-tunneling connection, use the **no** form of this command.

include-local-lan

no include-local-lan

Syntax Description

This command has no arguments or keywords.

Command Default

A nonsplit-tunneling connection is not able to access the local subnet at the same time as the client.

Command Modes

ISAKMP group configuration (config-isakmp-group)

IKEv2 authorization policy configuration (config-ikev2-author-policy)

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

If split tunneling is not in use (that is, the SPLIT_INCLUDE attribute was not negotiated), you lose not only Internet access, but also access to resources on the local subnetworks. The Include-Local-LAN attribute allows the server to push the attribute to the client, which allows for a nonsplit-tunneling connection to access the local subnetwork at the same time as the client (that is, the connection is to the subnetwork to which the client is directly attached).

The Include-Local-LAN attribute is configured on a Cisco IOS router or in the RADIUS profile.

To configure the Include-Local-LAN attribute, use the **include-local-lan** command.

An example of an attribute-value (AV) pair for the Include-Local-LAN attribute is as follows:

```
ipsec:include-local-lan=1
```

You must enable the **crypto isakmp client configuration group** or **crypto ikev2 authorization policy** command, which specifies group policy information that has to be defined or changed, before enabling the **include-local-lan** command.

Note The Include-Local-LAN 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 Include-Local-LAN has been configured:

```
crypto isakmp client configuration group cisco
 include-local-lan
```

Related Commands

Command	Description
acl	Configures split tunneling.
crypto ikev2 authorization policy	Specifies an IKEv2 authorization policy.
crypto isakmp client configuration group	Specifies the DNS domain to which a group belongs.

incoming

To configure filtering for incoming IP traffic, use the **incoming** command in router IP traffic export (RITE) configuration mode. To disable filtering for incoming traffic, use the **no** form of this command.

incoming {**access-list** {*standard*| *extended*| *named*}| **sample one-in-every** *packet-number*}

no incoming {**access-list** {*standard*| *extended*| *named*}| **sample one-in-every** *packet-number*}

Syntax Description

access-list *standard* | *extended named*	An existing numbered (standard or extended) or named access control list (ACL). **Note** The filter is applied only to exported traffic, not normal router traffic.
sample one-in-every *packet-number*	Exports only one packet out of every specified number of packets. Valid range for the *packet-number* argument is 2 to 2147483647 packets. By default, all traffic is exported.

Command Default

If this command is not enabled, all incoming IP traffic will be filtered via sampling.

Command Modes

RITE configuration

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.

Usage Guidelines

When configuring a network device for exporting IP traffic, you can issue the **incoming** command to filter unwanted traffic via the following methods:

- ACLs, which accept or deny an IP packet for export
- Sampling, which allows you to export one in every few packets in which you are interested. Use this option when it is not necessary to export all incoming traffic. Also, sampling is useful when a monitored ingress interface can send traffic faster than the egress interface can transmit it.

Examples

The following example shows how to configure the profile “corp1,” which will send captured IP traffic to host “00a.8aab.90a0” at the interface “FastEthernet 0/1.” This profile is also configured to export one in every 50 packets and to allow incoming traffic only from the ACL “ham_ACL.”

```
Router(config)# ip traffic-export profile corp1
Router(config-rite)# interface FastEthernet 0/1
Router(config-rite)# bidirectional
Router(config-rite)# mac-address 00a.8aab.90a0
Router(config-rite)# outgoing sample one-in-every 50
Router(config-rite)# incoming access-list ham_acl
Router(config-rite)# exit
Router(config)# interface FastEthernet 0/0
Router(config-if)# ip traffic-export apply corp1
```

Related Commands

Command	Description
ip traffic-export profile	Creates or edits an IP traffic export profile and enables the profile on an ingress interface.
outgoing	Configures filtering for outgoing export traffic.

initial-contact force

To process an initial contact notification in Internet Key Exchange Version 2 (IKEv2) IKE_AUTH exchange to an IKEv2 client by deleting unwanted security associations (SAs) and previous IKEv2 sessions, use the **initial-contact force** command in IKEv2 profile configuration mode. To not process the initial contact notification, use the **no** form of this command.

initial-contact force

no initial-contact

Syntax Description

This command has no arguments or keywords.

Command Default

IKEv2 processes the initial contact notification received in an IKE_AUTH exchange after successful authentication and deletes the old IKEv2 SA and IPsec SAs for the same local and remote IKEv2 peer or identity.

Command Modes

IKEv2 profile configuration (config-ikev2-profile)

Command History

Release	Modification
15.2(2)T	This command was introduced.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.

Usage Guidelines

Before using the **initial-contact force** command, you must configure the **crypto ikev2 profile** command. Configuring this command in the IKEv2 profile enforces the default behavior of initial contact processing, even if initial contact notification is not received.

Examples

The following example shows how to configure the **initial-contact force** command:

```
Device(config)# crypto ikev2 profile profile1
Device(config-ikev2-profile)# initial-contact force
```

Related Commands

Command	Description
crypto ikev2 profile	Defines an IKEv2 profile.

initiate mode

To configure the Phase 1 mode of an Internet Key Exchange (IKE), use the **initiate mode**command in ISAKMP profile configuration mode. To remove the mode that was config ured, use the **no** form of this command.

initiate mode aggressive

no initiate mode aggressive

Syntax Description

aggressive	Aggressive mode is initiated.

Command Default

IKE initiates main mode.

Command Modes

ISAKMP profile configuration (config-isa-prof)

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.

Usage Guidelines

Use this command if you want to initiate an IKE aggressive mode exchange instead of a main mode exchange.

Examples

The following example shows that aggressive mode has been configured:

```
crypto isakmp profile vpnprofile
 initiate mode aggressive
```

inservice (WebVPN)

To enable a SSL VPN gateway or context process, use the **inservice**command in webvpn gateway configuration or webvpn context configuration mode. To disable a SSL VPN gateway or context process without removing the configuration from the router configuration file, use the **no** form of this command.

inservice

no inservice

Syntax Description

This command has no arguments or keywords.

Command Default

A SSL VPN gateway or context process is not enabled.

Command Modes

Webvpn gateway configuration Webvpn context configuration

Command History

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

Usage Guidelines

The enable form of this command initializes required system data structures, initializes TCP sockets, and performs other start-up tasks related to the SSL VPN gateway or context process. The gateway and context processes must both be “inservice” to enable SSL VPN.

Examples

The following example enables the SSL VPN gateway process named SSL_GATEWAY:

```
Router(config)# webvpn gateway SSL_GATEWAY
```

```
Router(config-webvpn-gateway)# inservice
```

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
webvpn context	Enters webvpn configuration mode to configure the SSL VPN context.
webvpn gateway	Defines a SSL VPN gateway and enters webvpn gateway configuration mode.

inspect

To enable Cisco IOS stateful packet inspection, use the **inspect** command in policy-map-class configuration mode. To disable stateful packet inspection, use the **no** form of this command.

inspect [*parameter-map-name*]

no inspect[*parameter-map-name*]

Syntax Description

parameter-map-name	(Optional) Name of a previously configured inspect parameter map. If you do not specify a parameter map name, the software uses the default values for all the parameters.

Command Default

Cisco IOS stateful packet inspection is disabled.

Command Modes

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

Command History

Release	Modification
12.4(6)T	This command was introduced.
15.1(2)T	This command was modified. Support for IPv6 was added.
Cisco IOS XE Release 3.4S	This command was integrated into Cisco IOS XE Release 3.4S.

Usage Guidelines

You can use this command after entering the **policy-map type inspect**, **class type inspect**, and **parameter-map type inspect** commands.

To enable Cisco IOS stateful packet inspection, enter the name of an inspect parameter map that was previously configured with the **parameter-map type inspect** command.

This command lets you specify the attributes that will be used for the inspection.

Examples

The following example specifies inspection parameters for alert and audit-trail, and requests the **inspect** action with the specified inspect parameter:

```
parameter-map type inspect insp-params
 alert on
 audit-trail on
policy-map type inspect mypolicy
 class type inspect inspect-traffic
  inspect inspect-params
```

Related Commands

Command	Description
class type inspect	Specifies the traffic (class) on which an action is to be performed.
parameter-map type inspect	Configures an inspect-type parameter map for connecting thresholds, timeouts, and other parameters pertaining to the **inspect** action.
policy-map type inspect	Creates a Layer 3 and Layer 4 or a Layer 7 (protocol-specific) inspect-type policy map.

inspect (config-profile)

To enable Cisco IOS stateful packet inspection, use the **inspect** command in parameter-map type inspect configuration mode. To disable stateful packet inspection, use the **no** form of this command.

inspect {*parameter-map-name* | **vrf** *vrf-name parameter-map-name*}

no inspect {*parameter-map-name* | **vrf** *vrf-name parameter-map-name*}

Syntax Description

parameter-map-name	Parameter map name.
vrf	Binds a VPN routing and forwarding (VRF) instance to a parameter map.
vrf-name	VRF name.

Command Default

VRF instances are not bound to parameter maps.

Command Modes

Parameter-map type inspect configuration (config-profile)

Command History

Release	Modification
Cisco IOS XE Release 3.5S	This command was introduced.

Usage Guidelines

You must configure the **parameter-map type inspect-global** command before you can configure the **inspect** command.

Examples

The following example shows how to enable Cisco IOS stateful packet inspection:

```
Router(config)# parameter-map type inspect-global
Router(config-profile)# inspect pmap1
```

The following example shows how to bind an inspect-VRF parameter map to the default VRF:

```
Router(config)# parameter-map type inspect-global
Router(config-profile)# inspect vrf vrf1 pmap1
```

Related Commands

Command	Description
parameter-map type inspect-global	Configures a global parameter map.

integrity

To specify one or more integrity algorithms for an Internet Key Exchange Version 2 (IKEv2) proposal, use the **integrity**command in IKEv2 proposal configuration mode. To remove the configuration of the hash algorithm, us e the **no** form of this command.

integrity sha1 sha256 sha384 sha512 md5

no integrity

Syntax Description

sha1	Specifies Secure Hash Algorithm (SHA-1 - HMAC variant) as the hash algorithm.
sha256	Specifies SHA-2 family 256-bit (HMAC variant) as the hash algorithm.
sha384	Specifies SHA-2 family 384-bit (HMAC variant) as the hash algorithm.
sha512	Specifies SHA-2 family 512-bit (HMAC variant) as the hash algorithm.
md5	Specifies Message-Digest algorithm 5 (MD5 - HMAC variant) as the hash algorithm.

Command Default

The default integrity algorithm is used.

Command Modes

IKEv2 proposal configuration (config-ikev2-proposal)

Command History

Release	Modification
15.1(1)T	This command was introduced.
15.1(2)T	This command was modified. The **sha256** and **sha384** keywords were added.
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

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.

Use this command to specify the integrity algorithm to be used in an IKEv2 proposal. The default integrity algorithms in the default proposal are SHA-1 and MD5.

Note

You cannot selectively remove an integrity algorithm when multiple integrity algorithms are configured.

Suite-B adds support for the SHA-2 family (HMAC variant) hash algorithm used to authenticate packet data and verify the integrity verification mechanisms for the IKEv2 proposal configuration. HMAC is a variant that provides an additional level of hashing.

Examples

The following example configures an IKEv2 proposal with the MD5 integrity algorithm:

```
Router(config)#
crypto ikev2 proposal proposal1
Router(config-ikev2-proposal)#
integrity md5
```

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 Diffie-Hellman group identifier in an IKEv2 proposal.
show crypto ikev2 proposal	Displays the parameters for each IKEv2 proposal.

interface (RITE)

To specify the outgoing interface for exporting traffic, use the **interface** command in router IP traffic export (RITE) configuration mode. To disable an interface, use the **no** form of this command.

interface *interface-name*

no interface *interface-name*

Syntax Description

interface-name	Name of interface in which IP packets are exported.

Command Default

If this command is not enabled, the exported IP traffic profile does not recognize an interface in which to send captured IP traffic.

Command Modes

RITE configuration

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.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

After you configure an IP traffic export profile via the **ip traffic-export profile** global configuration command, you should issue the **interface** command; otherwise, the profile will be unable to export the captured IP packets. If you do not specify the **interface** command, you will receive a warning, which states that the profile is incomplete, when you attempt to apply the profile to an interface via the **ip traffic-export apply profile** interface configuration command.

Note Currently, only Ethernet and Fast Ethernet interfaces are supported.

Examples

The following example shows how to configure the profile “corp1,” which will send captured IP traffic to host “00a.8aab.90a0” at the interface “FastEthernet 0/1.” This profile is also configured to export one in every 50 packets and to allow incoming traffic only from the access control list ACL “ham_ACL.”

```
Router(config)# ip traffic-export profile corp1
Router(config-rite)# interface FastEthernet 0/1
Router(config-rite)# bidirectional
Router(config-rite)# mac-address 00a.8aab.90a0
Router(config-rite)# outgoing sample one-in-every 50
Router(config-rite)# incoming access-list ham_acl
Router(config-rite)# exit
Router(config)# interface FastEthernet 0/0
Router(config-if)# ip traffic-export apply corp1
```

Related Commands

Command	Description
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.

interface (VASI)

To configure a virtual routing and forwarding (VRF)-Aware Software Infrastructure (VASI) interface, use the **interface** command in global configuration mode. To remove a VASI configuration, use the **no** form of this command.

interface {**vasileft** | **vasiright**} *number*

no interface {**vasileft** | **vasiright**} *number*

Syntax Description

vasileft	Configures the vasileft interface.
vasiright	Configures the vasiright interface.
number	Identifier of the VASI interface pair. The range is from 1 to 2000.

Command Default

The VASI interface is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 2.6	This command was introduced.
Cisco IOS XE Release 3.1S	This command was modified. The *number* argument was modified to accept 500 VASI interface pairs.
Cisco IOS XE Release 3.3S	This command was modified. The *number* argument was modified to accept 1000 VASI interface pairs.
Cisco IOS XE Release 3.10S	This command was modified. The *number* argument was modified to accept 2000 VASI interface pairs.

Usage Guidelines

The vasileft and vasiright interfaces must be configured before the VASI interface becomes active. The two halves of the interface pair must be configured separately. If only one half of the interface is configured and not the other half, then the VASI interface does not become active.

Examples

The following example shows how to configure vasileft and vasiright interfaces:

```
Device(config)# interface vasileft 200
Device(config-if)# vrf forwarding table1
Device(config-if)# ip address 192.168.0.1 255.255.255.0
Device(config-if)# exit
Device(config)# interface vasiright 200
Device(config-if)# vrf forwarding table2
Device(config-if)# ip address 192.168.1.1 255.255.255.0
Device(config-if)# exit
```

Related Commands

Command	Description
debug adjacency (VASI)	Displays debugging information for VASI adjacency.
debug interface (VASI)	Displays debugging information for a VASI interface descriptor block.
debug vasi	Displays VASI debugging information.
ip address	Sets a primary or secondary IP address for an interface.
show vasi pair	Displays the status of a VASI pair.
vrf forwarding	Associates a VRF instance or a virtual network with an interface or subinterface.

interface virtual-template

To create a virtual template interface that can be configured and applied dynamically in creating virtual access interfaces, use the **interface virtual-template** command in global configuration mode. To remove a virtual template interface, use the **no** form of this command.

interface virtual-template *number* [**type** *virtual-template-type*]

no interface virtual-template *number*

Syntax Description

number	Number used to identify the virtual template interface. Up to 200 virtual template interfaces can be configured. On the Cisco 10000 series router, up to 4095 virtual template interfaces can be configured.
type *virtual-template-type*	(Optional) Specifies the type of virtual template.

Command Default

No virtual template interface is defined.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.2F	This command was introduced.
12.2(4)T	This command was enhanced to increase the maximum number of virtual template interfaces from 25 to 200.
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	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.2(33)SB	This command's default configuration was modified for SNMP and implemented on the Cisco 10000 series router for the PRE3 and PRE4.
Cisco IOS XE Release 2.5	This command was implemented on Cisco ASR 1000 series routers.

Usage Guidelines

A virtual template interface is used to provide the configuration for dynamically created virtual access interfaces. It is created by users and can be saved in NVRAM.

After the virtual template interface is created, it can be configured in the same way as a serial interface.

Virtual template interfaces can be created and applied by various applications such as virtual profiles, virtual private dialup networks (VPDNs), PPP over ATM, protocol translation, and Multichassis Multilink PPP (MMP).

Cisco 10000 Series Router

You can configure up to 4095 total virtual template interfaces on the Cisco 10000 series router.

To ensure proper scaling and to minimize CPU utilization, we recommend the following virtual template interface settings:

- A keepalive timer of 30 seconds or greater using the **keepalive** command. The default is 10 seconds.
- Do not enable the Cisco Discovery Protocol (CDP). CDP is disabled by default. Use the **no cdp enable** command to disable CDP, if necessary.
- Disable link-status event messaging using the **no logging event link-status**command.
- To prevent the virtual-access subinterfaces from being registered with the SNMP functionality of the router and using memory, do not use the router's SNMP management tools to monitor PPP sessions. Use the **no virtual-template snmp** command to disable the SNMP management tools.

When a virtual template interface is applied dynamically to an incoming user session, a virtual access interface (VAI) is created.

If you configure a virtual template interface with interface-specific commands, the Cisco 10000 series router does not achieve the highest possible scaling. To verify that the router does not have interface-specific commands within the virtual template interface configuration, use the **test virtual-template** *number* **subinterface** command.

In Cisco IOS Release 12.2(33)SB, the default configuration for the **virtual-template snmp** command was changed to **no virtual-template snmp**. This prevents large numbers of entries into the MIB ifTable, thereby avoiding CPU Hog messages as SNMP uses the interfaces MIB and other related MIBs. If you configure the **no virtual-template snmp** command, the router no longer accepts the **s nmp trap link-status** command under a virtual-template interface. Instead, the router displays a configuration error message such as the following:

```
Router(config)# interface virtual-template 1
Router(config-if)# snmp trap link-status
%Unable set link-status enable/disable for interface
```

If your configuration already has the **snmp trap link-status** command configured under a virtual-template interface and you upgrade to Cisco IOS Release 12.2(33)SB, the configuration error occurs when the router reloads even though the virtual template interface is already registered in the interfaces MIB.

Examples

Examples

The following example creates a virtual template interface called Virtual-Template1:

```
Router(config)# interface Virtual-Template1
Router(config-if)# ip unnumbered Loopback1
Router(config-if)# keepalive 60
Router(config-if)# no peer default ip address
Router(config-if)# ppp authentication pap
Router(config-if)# ppp authorization vpn1
Router(config-if)# ppp accounting vpn1
Router(config-if)# no logging event link-status
Router(config-if)# no virtual-template snmp
```

Examples

The following example creates and configures virtual template interface 1:

```
interface virtual-template 1 type ethernet
 ip unnumbered ethernet 0
 ppp multilink
 ppp authentication chap
```

Examples

The following example shows how to configure a virtual template for an IPsec virtual tunnel interface.

```
interface virtual-template1 type tunnel
 ip unnumbered Loopback1
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile virtualtunnelinterface
```

Related Commands

Command	Description
cdp enable	Enables Cisco Discovery Protocol (CDP) on an interface.
clear interface virtual-access	Tears down the live sessions and frees the memory for other client uses.
keepalive	Enables keepalive packets and to specify the number of times that the Cisco IOS software tries to send keepalive packets without a response before bringing down the interface.
show interface virtual-access	Displays the configuration of the active VAI that was created using a virtual template interface.
tunnel protection	Associates a tunnel interface with an IPsec profile.
virtual interface	Sets the zone name for the connected AppleTalk network.
virtual-profile	Enables virtual profiles.
virtual template	Specifies the destination for a tunnel interface.

ip (webvpn url rewrite)

To configure the IP address of the site to be mangled on a Secure Socket Layer virtual private network (SSL VPN) gateway, use the **ip** command in webvpn url rewrite configuration mode. To deselect the IP address, use the **no** form of this command.

ip *ip-address*

no ip *ip-address*

Syntax Description

ip-address	IP address of the site to be mangled.

Command Default

A site is not selected for mangling.

Command Modes

Webvpn url rewrite (config-webvpn-url-rewrite)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Examples

The following example shows that the IP address 10.1.0.0 255.255.0.0 has been selected for mangling:

```
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 host name 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.

ip access-group

To apply an IP access list or object group access control list (OGACL) to an interface or a service policy map, use the **ip access-group** command in the appropriate configuration mode. To remove an IP access list or OGACL, use the **no** form of this command.

ip access-group {*access-list-name*| *access-list-number*} {**in**| **out**}

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

Syntax Description

access-list-name	Name of the existing IP access list or OGACL as specified by an **ip access-list** command.
access-list-number	Number of the existing access list. • Integer from 1 to 199 for a standard or extended IP access list. • Integer from 1300 to 2699 for a standard or extended IP expanded access list.
in	Filters on inbound packets.
out	Filters on outbound packets.

Command Default

An access list is not applied.

Command Modes

Interface configuration (config-if) Service policy-map configuration (config-service-policymap)

Command History

Release	Modification
10.0	This command was introduced.
11.2	The *access-list-name* argument was added.
12.2(28)SB	This command was made available in service policy-map configuration mode.
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(20)T	The *access-list-name* keyword was modified to accept the name of an OGACL.

Release	Modification
Cisco IOS XE 3.3S	This command was integrated into Cisco IOS XE Release 3.3S.
15.2(02)SA	This command was implemented on the Cisco ME 2600X Series Ethernet Access Switches.

Usage Guidelines

If the specified access list does not exist, all packets are passed (no warning message is issued).

Applying Access Lists to Interfaces

Acc ess lists or OGACLs are applied on either outbound or inbound interfaces. For standard inbound access lists, after an interface receives a packet, the Cisco IOS software checks the source address of the packet against the access list. For extended access lists or OGACLs, the networking device also checks the destination access list or OGACL. If the access list or OGACL permits the address, the software continues to process the packet. If the access list or OGACL rejects the address, the software discards the packet and returns an Internet Control Management Protocol (ICMP) host unreachable message.

For standard outbound access lists, after a device receives and routes a packet to a controlled interface, the software checks the source address of the packet against the access list. For extended access lists or OGACLs, the networking device also checks the destination access list or OGACL. If the access list or OGACL permits the address, the software sends the packet. If the access list or OGACL rejects the address, the software discards the packet and returns an ICMP host unreachable message.

When you enable outbound access lists or OGACLs, you automatically disable autonomous switching for that interface. When you enable inbound access lists or OGACLs on any CBus or CxBus interface, you automatically disable autonomous switching for all interfaces (with one exception--a Storage Services Enabler (SSE) configured with simple access lists can still switch packets, on output only).

Applying Access Lists or OGACLs to Service Policy Maps

You can use the **ip access-group** command to configure Intelligent Services Gateway (ISG) per-subscriber firewalls. Per-subscriber firewalls are Cisco IOS IP access lists or OGACLs that are used to prevent subscribers, services, and pass-through traffic from accessing specific IP addresses and ports.

ACLs and OGACLs can be configured in user profiles or service profiles on an authentication, authorization, and accounting (AAA) server or in service policy maps on an ISG. OGACLS or numbered or named IP access lists can be configured on the ISG, or the ACL or OGACL statements can be included in the profile configuration.

When an ACL or OGACL is added to a service, all subscribers of that service are prevented from accessing the specified IP address, subnet mask, and port combinations through the service.

Examples

The following example applies list 101 on packets outbound from Ethernet interface 0:

```
Router> enable
Router# configure terminal
Router(config)# interface ethernet 0
Router(config-if)# ip access-group 101 out
```

Related Commands

Command	Description
deny	Sets conditions in a named IP access list or OGACL that will deny packets.
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.
show ip access-list	Displays the contents of IP access lists or OGACLs.
show object-group	Displays information about object groups that are configured.

ip access-list

To define an IP access list or object-group access control list (ACL) by name or number or to enable filtering for packets with IP helper-address destinations, use the **ip access-list** command in global configuration mode. To remove the IP access list or object-group ACL or to disable filtering for packets with IP helper-address destinations, use the **no** form of this command.

ip access-list {{**standard**| **extended**} {*access-list-name*| *access-list-number*}| **helper egress check**}

no ip access-list {{**standard**| **extended**} {*access-list-name*| *access-list-number*}| **helper egress check**}

Syntax Description

standard	Specifies a standard IP access list.
extended	Specifies an extended IP access list. Required for object-group ACLs.
access-list-name	Name of the IP access list or object-group ACL. Names cannot contain a space or quotation mark, and must begin with an alphabetic character to prevent ambiguity with numbered access lists.
access-list-number	Number of the access list. • A standard IP access list is in the ranges 1-99 or 1300-1999. • An extended IP access list is in the ranges 100-199 or 2000-2699.
helper egress check	Enables permit or deny matching capability for an outbound access list that is applied to an interface, for traffic that is relayed via the IP helper feature to a destination server address.

Command Default

No IP access list or object-group ACL is defined, and outbound ACLs do not match and filter IP helper relayed traffic.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.2	This command was introduced.
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.
12.4(20)T	This command was modified. Object-group ACLs are now accepted when the **deny** and **permit** commands are used in standard IP access-list configuration mode or extended IP access-list configuration mode.
Cisco IOS XE Release 3.2S	This command was implemented on Cisco ASR 1000 series routers.
15.0(1)M5	This command was modified. The **helper**, **egress**, and **check** keywords were added.
15.1(1)SY	This command was modified. The **helper**, **egress**, and **check** keywords were added.
15.1(3)T3	This command was modified. The **helper**, **egress**, and **check** keywords were added.
15.1(2)SNG	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.

Usage Guidelines

Use this command to configure a named or numbered IP access list or an object-group ACL. This command places the router in access-list configuration mode, where you must define the denied or permitted access conditions by using the **deny**and **permit** commands.

Specifying the **standard** or **extended** keyword with the **ip access-list** command determines the prompt that appears when you enter access-list configuration mode. You must use the **extended** keyword when defining object-group ACLs.

You can create object groups and IP access lists or object-group ACLs independently, which means that you can use object-group names that do not yet exist.

Named access lists are not compatible with Cisco IOS software releases prior to Release 11.2.

Use the **ip access-group** command to apply the access list to an interface.

The **ip access-list helper egress check** command enables outbound ACL matching for permit or deny capability on packets with IP helper-address destinations. When you use an outbound extended ACL with this command, you can permit or deny IP helper relayed traffic based on source or destination User Datagram Protocol (UDP) ports. The **ip access-list helper egress check** command is disabled by default; outbound ACLs will not match and filter IP helper relayed traffic.

Examples

The following example defines a standard access list named Internetfilter:

```
Router> enable
Router# configure terminal
Router(config)# ip access-list standard Internetfilter
Router(config-std-nacl)# permit 192.168.255.0 0.0.0.255
Router(config-std-nacl)# permit 10.88.0.0 0.0.255.255
Router(config-std-nacl)# permit 10.0.0.0 0.255.255.255
```

The following example shows how to create an object-group ACL that permits packets from the users in my_network_object_group if the protocol ports match the ports specified in my_service_object_group:

```
Router> enable
Router# configure terminal
Router(config)# ip access-list extended my_ogacl_policy
Router(config-ext-nacl)# permit tcp object-group my_network_object_group portgroup
 my_service_object_group any
Router(config-ext-nacl)# deny tcp any any
```

The following example shows how to enable outbound ACL filtering on packets with helper-address destinations:

```
Router> enable
Router# configure terminal
Router(config)# ip access-list helper egress check
```

Related Commands

Command	Description
deny	Sets conditions in a named IP access list or in an object-group ACL that will deny packets.
ip access-group	Applies an ACL or an object-group ACL to an interface or a service policy map.
object-group network	Defines network object groups for use in object-group ACLs.
object-group service	Defines service object groups for use in object-group ACLs.
permit	Sets conditions in a named IP access list or in an object-group ACL that will permit packets.
show ip access-list	Displays the contents of IP access lists or object-group ACLs.
show object-group	Displays information about object groups that are configured.

ip access-list hardware permit fragments

To permit all noninitial fragments in the hardware, use the **ip access-list hardware permit fragments** command in global configuration mode. To return to the default settings, use the **no** form of this command.

ip access-list hardware permit fragments

no ip access-list hardware permit fragments

Syntax Description

This command has no arguments or keywords.

Command Default

All fragments from flows that are received from an ACE with Layer 4 ports and permit action are permitted. All other fragments are dropped in the hardware. This action also applies to flows that are handled in the software regardless of this command setting.

Command Modes

Global 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 Cisco IOS Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(18)SXF5	This command was changed to affect all ACLs currently applied to interfaces and not just newly-applied ACLs. See the "Usage Guidelines" section for more information.

Usage Guidelines

Flow fragments that match ACEs with Layer 4 ports and permit results are permitted in the hardware, and all other fragments are dropped. An entry is added in the TCAM for each ACE with Layer 4 ports and permit action. This action could cause large ACLs to not fit in the TCAM. If this is the case, use the **ip access-list hardware permit fragments** command to permit all noninitial fragments in the hardware.

Note Configurations that you modify after you entered the **ip access-list hardware permit fragments** command will permit all noninitial fragments in the hardware. Hardware configurations that you modified before you entered the **ip access-list hardware permit fragments** command will not be changed.

Note Hardware configurations that you modify after you entered the **no ip access-list hardware permit fragments** command will return to the default settings. Hardware configurations that you modified before you entered the **no ip access-list hardware permit fragments** command do not change.

The initial flow fragments that match the ACEs with Layer 4 ports and permit results are permitted in the hardware. All other initial fragments are dropped in the hardware.

Catalyst 6500 Series Switches

The following restrictions apply to Cisco IOS releases before Cisco IOS Release 12.2(18)SX5:

Note Configurations that you modify after you entered the **ip access-list hardware permit fragments** command will permit all noninitial fragments in the hardware. Hardware configurations that you modified before you entered the **ip access-list hardware permit fragments** command will not be changed.

Note Hardware configurations that you modify after you entered the **no ip access-list hardware permit fragments** command will return to the default settings. Hardware configurations that you modified before you entered the **no ip access-list hardware permit fragments** command do not change.

In Cisco IOS releases after Cisco IOS Release 12.2(18)SX5, this command affects all ACLs currently applied to interfaces and not just newly-applied ACLs.

Examples

This example shows how to permit all noninitial fragments in the hardware:

```
Router(config)# ip access-list hardware permit fragments
```

This example shows how to return to the default settings:

```
Router(config)# no ip access-list hardware permit fragments
```

Related Commands

Command	Description
show ip interface	Displays the usability status of interfaces that are configured for IP.

ip access-list logging interval

To configure the logging interval for access list entries, use the **ip access-list logging interval** command in global configuration mode. To disable the configuration, use the **no** form of this command.

ip access-list logging interval *interval*

no ip access-list logging interval

Syntax Description

interval	Access list logging interval, in milliseconds. The range is from 0 to 2147483647.

Command Default

Access list logging intervals are not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
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 and implemented on the Cisco ASR 1000 Series Aggregation Services Routers.

Examples

The following example shows how to set the access list logging interval to 100 milliseconds:

```
Router# configure terminal
Router(config)# ip access-list logging interval 100
```

Related Commands

Command	Description
ip access-list logging hash-generation	Enables hash-value generation for ACE syslog entries.

ip access-list log-update

To set the threshold number of packets that generate a log message if they match an access list, use the **ip access-list log-update**command in global configuration mode. To remove the threshold, use the **no** form of this command.

ip access-list log-update threshold *number-of-matches*

no ip access-list log-update

Syntax Description

number-of-matches	Threshold number of packets necessary to match an access list before a log message is generated. The range is 0 to 2147483647. There is no default number of matches.

Command Default

Log messages are sent at the first matching packet and at 5-minute intervals after that.

Command Modes

Global configuration

Command History

Release	Modification
12.0(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 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

Log messages are generated if you have specified the **log** keyword in the **access-list (IP standard)**, **access-list (IP extended)**, **deny (IP)**, **dynamic**, or **permit** command.

Log messages provide information about the packets that are permitted or denied by an access list. By default, log messages appear at the console. (The level of messages logged to the console is controlled by the **logging console** command.) The log message includes the access list number, whether the packet was permitted or denied, and other information.

By default, the log messages are sent at the first matching packet and after that, identical messages are accumulated for 5-minute intervals, with a single message being sent with the number of packets permitted and denied during that interval. However, you can use the **ip access-list log-update** command to set the number of packets that, when match an access list (and are permitted or denied), cause the system to generate a log message. You might want to do this to receive log messages more frequently than at 5-minute intervals.

⚠

Caution If you set the *number-of-matches* argument to 1, a log message is sent right away, rather than caching it; every packet that matches an access list causes a log message. A setting of 1 is not recommended because the volume of log messages could overwhelm the system.

Even if you use the **ip access-list log-update** command, the 5-minute timer remains in effect, so the cache is emptied at the end of 5 minutes, regardless of the count of messages in the cache. Regardless of when the log message is sent, the cache is flushed and the count reset to 0 for that message the same way it is when a threshold is not specified.

If the syslog server is not directly connected to a LAN that the router shares, any intermediate router might drop the log messages because they are UDP (unreliable) messages.

Examples

The following example enables logging whenever the 1000th packet matches an access list entry:

```
ip access-list log-update threshold 1000
```

Related Commands

Command	Description
access-list (IP extended)	Defines an extended IP access list.
access-list (IP standard)	Defines a standard IP access list.
deny (IP)	Sets conditions under which a packet is denied by a named IP access list.
dynamic	Defines a named dynamic IP access list.
logging console	Limits messages logged to the console, based on severity.
permit	Sets conditions under which a packet passes a named IP access list.

ip access-list resequence

To apply sequence numbers to the access list entries in an access list, use the **ip access-list resequence** command in global configuration mode.

ip access-list resequence *access-list-name* **starting-sequence-number** *increment*

Syntax Description

access-list-name	Name of the access list. Names cannot contain a space or quotation mark.
starting-sequence-number	Access list entries will be resequenced using this initial value. The default value is 10. The range of possible sequence numbers is 1 through 2147483647.
increment	The number by which the sequence numbers change. The default value is 10. For example, if the increment value is 5 and the beginning sequence number is 20, the subsequent sequence numbers are 25, 30, 35, 40, and so on.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.2(14)S	This command was introduced.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)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 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 allows the **permit** and **deny** entries of a specified access list to be resequenced with an initial sequence number value determined by the *starting-sequence-number* argument, and continuing in increments determined by the *increment* argument. If the highest sequence number exceeds the maximum possible sequence number, then no sequencing occurs.

For backward compatibility with previous releases, if entries with no sequence numbers are applied, the first entry is assigned a sequence number of 10, and successive entries are incremented by 10. The maximum sequence number is 2147483647. If the generated sequence number exceeds this maximum number, the following message is displayed:

```
Exceeded maximum sequence number.
```

If the user enters an entry without a sequence number, it is assigned a sequence number that is 10 greater than the last sequence number in that access list and is placed at the end of the list.

If the user enters an entry that matches an already existing entry (except for the sequence number), then no changes are made.

If the user enters a sequence number that is already present, the following error message is generated:

```
Duplicate sequence number.
```

If a new access list is entered from global configuration mode, then sequence numbers for that access list are generated automatically.

Distributed support is provided so that the sequence numbers of entries in the Route Processor (RP) and line card (LC) are in synchronization at all times.

Sequence numbers are not saved in NVRAM. That is, the sequence numbers themselves are not saved. In the event that the system is reloaded, the configured sequence numbers revert to the default sequence starting number and increment.

This command works with named standard and extended IP access lists. Because the name of an access list can be designated as a number, numbers are acceptable as names as long as they are entered in named access list configuration mode.

Examples

The following example resequences an access list named kmd1. The starting sequence number is 100, and the increment value is 5:

```
ip access-list resequence kmd1 100 5
```

Related Commands

Command	Description
deny (IP)	Sets conditions under which a packet does not pass a named IP access list.
permit (IP)	Sets conditions under which a packet passes a named IP access list.

ip access-list logging hash-generation

To enable hash-value generation for access control entry (ACE) syslog entries, use the **ip access-list logging hash-generation** command in global configuration mode. To disable hash value generation, use the **no** form of this command.

ip access-list logging hash-generation

no ip access-list logging hash-generation

Syntax Description

This command has no arguments or keywords.

Command Default

Hash value generation is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(22)T	This command was introduced.

Usage Guidelin

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.

Cisco IOS routers generate syslog entries for log-enabled ACEs. The system appends a tag (either a user-defined cookie or a router-generated MD5 hash value) to ACE syslog entries. This tag uniquely identifies the ACE, within an access control list (ACL), that generated the syslog entry.

Use this command to generate an MD5 hash value for all the log enabled ACEs in the system that do not have a user-defined cookie. The system attaches the router-generated hash value to the corresponding ACE. The hash value is stored locally in the router's NVRAM and persists through router reloads.

Examples

The following example shows how to enable hash value generation on the router, for IP access list syslog entries:

```
Router(config)# ip access-list logging hash-generation
Router(config)#
*Aug 7 01:10:12.077: %IPACL-HASHGEN: ACL: 101 seq no : 20 Hash code is 0x75F079
```

Related Commands

Command	Description
access-list (IP extended)	Defines an extended IP access list.
access-list (IP standard)	Defines a standard IP access list.
debug ip access-list hash-generation	Displays debugging information about ACL hash generation.
show ip access-list	Displays the contents of all current access lists.

ip-address (ca-trustpoint)

To specify an IPv4 or IPv6 address, or the interface that is included as “unstructuredAddress” in the certificate request, use the **ip-address** command in ca-trustpoint configuration mode. To restore the default behavior, use the **no** form of this command.

ip-address {*ip-address*| *interface*| **none**}

no ip-address

Syntax Description

ip-address	Specifies the IPv4 or IPv6 address that is included as “unstructuredAddress” in the certificate request.
interface	Specifies an interface, from which the router can get an IP address, that is included as “unstructuredAddress” in the certificate request.
none	Specifies that an IP address is not to be included in the certificate request.

Command Default

An IP address is not configured. You are prompted for the IP address during certificate enrollment.

Command Modes

Ca-trustpoint configuration (config-ca-trustpoint)

Command History

Release	Modification
12.2(8)T	This command was introduced.
15.2(1)T	This command was modified. Support for specifying the IPv6 address that is included as “unstructuredAddress” in the certificate request was added.

Usage Guidelines

Before you can issue this command, you must enable the **crypto ca pki trustpoint** command, which declares the certification authority (CA) that your router should use and enters ca-trustpoint configuration mode. The **ip-address** command allows a certificate enrollment parameter to be specified.

Use the **ip-address** command to include the IP address of the specified interface in the certificate request or to specify that an IP address should not be included in the certificate request.

If this command is enabled, you are not prompted for an IP address during certificate enrollment.

Examples

The following example shows how to include the IP address of the Ethernet-0 interface in the certificate request for the trustpoint “my_trustpoint”:

```
crypto ca trustpoint my_trustpoint
 enrollment url http://my_trustpoint.cisco.com/
 subject-name OU=Spiral Dept., O=tiedye.com
 ip-address ethernet-0
```

The following example shows how to include the IPv6 address that is included as “unstructuredAddress” in the certificate request for the trustpoint “my_trustpoint”:

```
crypto ca trustpoint my_trustpoint
 enrollment url http://[2001:DB8:1:1::1]:80/
 subject-name OU=Spiral Dept., O=tiedye.com
 ip-address 2001:DB8:1:1::1
```

The following example shows that an IPv4 address is not to be included in the certificate request:

```
crypto ca trustpoint my_trustpoint
 enrollment url http://10.3.0.7:80
 fqdn none
 ip-address none
 subject-name CN=subject1, OU=PKI, O=Cisco Systems, C=US
```

Related Commands

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

ip address dhcp

To acquire an IP address on an interface from the DHCP, use the **ip address dhcp**command in interface configuration mode. To remove any address that was acquired, use the **no** form of this command.

ip address dhcp [**client-id** *interface-type number*] [**hostname** *hostname*]

no ip address dhcp [**client-id** *interface-type number*] [**hostname** *hostname*]

Syntax Description

client-id	(Optional) Specifies the client identifier. By default, the client identifier is an ASCII value. The **client-id** *interface-type number*option sets the client identifier to the hexadecimal MAC address of the named interface.
interface-type	(Optional) Interface type. For more information, use the question mark (?) online help function.
number	(Optional) Interface or subinterface number. For more information about the numbering syntax for your networking device, use the question mark (?) online help function.
hostname	(Optional) Specifies the hostname.
hostname	(Optional) Name of the host to be placed in the DHCP option 12 field. This name need not be the same as the hostname entered in global configuration mode.

Command Default

The hostname is the globally configured hostname of the router. The client identifier is an ASCII value.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.1(2)T	This command was introduced.
12.1(3)T	This command was modified. The **client-id**keyword and *interface-type number*argument were added.
12.2(3)	This command was modified. The **hostname**keyword and *hostname*argument were added. The behavior of the **client-id** *interface-type number*option changed. See the “Usage Guidelines” section for details.

Release	Modification
12.2(8)T	This command was modified. The command was expanded for use on PPP over ATM (PPPoA) interfaces and certain ATM interfaces.
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.
15.1(3)T	This command was modified. Support was provided on the tunnel interface.

Usage Guidelin

Note Prior to Cisco IOS Release 12.2(8)T, the **ip address dhcp** command could be used only on Ethernet interfaces.

The **ip address dhcp** command allows any interface to dynamically learn its IP address by using the DHCP protocol. It is especially useful on Ethernet interfaces that dynamically connect to an Internet service provider (ISP). Once assigned a dynamic address, the interface can be used with the Port Address Translation (PAT) of Cisco IOS Network Address Translation (NAT) to provide Internet access to a privately addressed network attached to the router.

The **ip address dhcp** command also works with ATM point-to-point interfaces and will accept any encapsulation type. However, for ATM multipoint interfaces you must specify Inverse ARP via the **protocol ip inarp** interface configuration command and use only the aa15snap encapsulation type.

Some ISPs require that the DHCPDISCOVER message have a specific hostname and client identifier that is the MAC address of the interface. The most typical usage of the **ip address dhcp client-id** *interface-type number* **hostname** *hostname* command is when *interface-type*is the Ethernet interface where the command is configured and *interface-type number*is the hostname provided by the ISP.

A client identifier (DHCP option 61) can be a hexadecimal or an ASCII value. By default, the client identifier is an ASCII value. The **client-id** *interface-type number*option overrides the default and forces the use of the hexadecimal MAC address of the named interface.

Note Between Cisco IOS Releases 12.1(3)T and 12.2(3), the **client-id** optional keyword allows the change of the fixed ASCII value for the client identifier. After Release 12.2(3), the optional **client-id** keyword forces the use of the hexadecimal MAC address of the named interface as the client identifier.

If a Cisco router is configured to obtain its IP address from a DHCP server, it sends a DHCPDISCOVER message to provide information about itself to the DHCP server on the network.

If you use the **ip address dhcp** command with or without any of the optional keywords, the DHCP option 12 field (hostname option) is included in the DISCOVER message. By default, the hostname specified in option 12 will be the globally configured hostname of the router. However, you can use the **ip address dhcp hostname** *hostname* command to place a different name in the DHCP option 12 field than the globally configured hostname of the router.

The **no ip address dhcp** command removes any IP address that was acquired, thus sending a DHCPRELEASE message.

You might need to experiment with different configurations to determine the one required by your DHCP server. The table below shows the possible configuration methods and the information placed in the DISCOVER message for each method.

Table 7: Configuration Method and Resulting Contents of the DISCOVER Message

Configuration Method	Contents of DISCOVER Messages
ip address dhcp	The DISCOVER message contains "cisco- *mac-address* -Eth1" in the client ID field. The *mac-address* is the MAC address of the Ethernet 1 interface and contains the default hostname of the router in the option 12 field.
ip address dhcp hostname *hostname*	The DISCOVER message contains "cisco- *mac-address* -Eth1" in the client ID field. The *mac-address* is the MAC address of the Ethernet 1 interface, and contains *hostname* in the option 12 field.
ip address dhcp client-id ethernet 1	The DISCOVER message contains the MAC address of the Ethernet 1 interface in the client ID field and contains the default hostname of the router in the option 12 field.
ip address dhcp client-id ethernet 1 hostname *hostname*	The DISCOVER message contains the MAC address of the Ethernet 1 interface in the client ID field and contains *hostname* in the option 12 field.

Examples

In the examples that follow, the command **ip address dhcp** is entered for Ethernet interface 1. The DISCOVER message sent by a router configured as shown in the following example would contain "cisco- *mac-address* -Eth1" in the client-ID field, and the value abc in the option 12 field.

```
hostname abc
!
interface Ethernet 1
 ip address dhcp
```

The DISCOVER message sent by a router configured as shown in the following example would contain "cisco- mac-address -Eth1" in the client-ID field, and the value def in the option 12 field.

```
hostname abc
!
interface Ethernet 1
 ip address dhcp hostname def
```

The DISCOVER message sent by a router configured as shown in the following example would contain the MAC address of Ethernet interface 1 in the client-id field, and the value abc in the option 12 field.

```
hostname abc
!
```

```
interface Ethernet 1
 ip address dhcp client-id Ethernet 1
```

The DISCOVER message sent by a router configured as shown in the following example would contain the MAC address of Ethernet interface 1 in the client-id field, and the value def in the option 12 field.

```
hostname abc
!
interface Ethernet 1
 ip address dhcp client-id Ethernet 1 hostname def
```

Related Commands

Command	Description
ip dhcp pool	Configures a DHCP address pool on a Cisco IOS DHCP server and enters DHCP pool configuration mode.

ip address (WebVPN)

To configure a proxy IP address on a Secure Socket Layer virtual private network (SSL VPN) gateway, use the **ip address**command in webvpn gateway configuration mode. To remove the proxy IP address from the SSL VPN gateway, use the **no** form of this command.

ip address *ip-address* [**port** *port-number*] [**standby** *name*]

no ip address

Syntax Description

ip-address	IPv4 address.
port *port-number*	(Optional) Specifies the port number for proxy traffic. A number from 1 to 65535 can be entered for this argument. The default port number 443 is used if this command is configured without entering the **port** keyword.
standby *name*	• (Optional) Indicates that the IP address is a virtual address configured on one of the router interfaces using Hot StandbyRouting Protocol (HSRP). • *name* --Must be the same as the HSRP group name that was configured on the router interface. **Note** Note that the *name* argument is not an optional parameter when the **standby** keyword is used.

Command Default

A proxy IP address is not configured.

Command Modes

Webvpn gateway configuration (config-webvpn-gateway)

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.4(20)T	The **standby** keyword and *name*arguments were added.

Usage Guidelines

The **ip address** command is used to configure a proxy IP address for an SSL VPN gateway. The IP address is the termination point for all SSL VPN client connections. This IP address can be any routable IP address assigned to a valid interface.

Examples

The following example configures 192.168.1.1 as a proxy address on an SSL VPN gateway. Proxy traffic is directed over port 443.

```
Router(config)# webvpn gateway SSL_GATEWAY
```

```
Router(config-webvpn-gateway)# ip address 192.168.1.1 port 443
```

The following example shows that Router 1 and Router 2 are configured for HSRP on Gateway Webvpn:

Examples

```
Router# configure terminal
Router config)# interface g0/1
Router (config-if)# standby 0 ip 10.1.1.1
Router (config-if)# standby 0 name SSLVPN
Router (config-if)# exit
Router (config)# webvpn gateway Webvpn
Router (config-webvpn-gateway)# ip address 10.1.1.1 port 443 standby SSLVPN
```

Examples

```
Router# configure terminal
Router (config)# interface g0/0
Router (config-if)# standby 0 ip 10.1.1.1
Router (config-if)# standby 0 name SSLVPN2
Router (config-if)# exit
Router (config)# webvpn gateway Webvpn
Router (config-webvpn-gateway)# ip address 10.1.1.1 port 443 standby SSLVPN2
```

Related Commands

Command	Description
standby name	Configures the name of the standby group.
webvpn gateway	Defines an SSL VPN gateway and enters webvpn gateway configuration mode.

ip admission

To create a Layer 3 network admission control rule to be applied to the interface, or to create a policy that can be applied on an interface when the authentication, authorization and accounting (AAA) server is unreachable, use the **ip admission**command in interface configuration mode. To create a global policy that can be applied on a network access device, use the **ip admission command with the optional keywords**and argument in global configuration mode. To remove the admission control rule, use the **no** form of this command.

ip admission *admission-name* [**event timeout aaa policy identity** *identity-policy-name*]

no ip admission *admission-name* [**event timeout aaa policy identity** *identity-policy-name*]

Syntax Description

admission-name	Authentication or admission rule name.
event timeout aaa policy identity	Specifies an authentication policy to be applied when the AAA server is unreachable.
identity-policy-name	Authentication or admission rule name to be applied when the AAA server is unreachable.

Command Default

A network admission control rule is not applied to the interface.

Command Modes

Interface configuration (config-if) Global configuration (config)

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.4(11)T	This command was modified to include the **event timeout aaa policy identity** keywords and the *identity-policy-name* argument.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

The admission rule defines how you apply admission control.

The optional keywords and argument define the network admission policy to be applied to a network access device or an interface when no AAA server is reachable. The command can be used to associate a default identity policy with Extensible Authentication Protocol over User Datagram Protocol (EAPoUDP) sessions.

Examples

The following example shows how to apply a network admission control rule named "nacrule1" to the interface:

```
Router (config-if)# ip admission nacrule1
```

The following example shows how to apply an identity policy named "example" to the device when the AAA server is unreachable:

```
Router (config)# ip admission nacrule1 event timeout aaa policy identity example
```

Related Commands

Command	Description
interface	Defines an interface.

ip admission consent banner

To display a banner on the authentication proxy consent webpage, use the **ip admission consent banner** command in global configuration mode. To disable a display of the banner, use the **no** form of this command.

ip admission consent banner {**file** *file-name*| **text** *banner-text*}

no ip admission consent banner

Syntax Description

file *file-name*	Specifies a file that is to be shown as the consent webpage.
text *banner-text*	Specifies a text string to replace the default banner, which is the name of the router. The text string should be written in the following format: "C *banner-text* C," where "C" is a delimiting character.

Command Default

A banner is not displayed on the authentication proxy consent webpage.

Command Modes

Global configuration

Command History

Release	Modification
12.4(15)T	This command was introduced.

Usage Guidelines

The ip admission consent banner command allows users to configure one of two possible scenarios:

- The ip admission consent banner command with a filename is enabled.

In this scenario, the administrator supplies the location and name of the file that is to be used for the consent webpage.

- The ip admission consent banner command with the banner text is enabled.

In this scenario, the administrator can supply multiline text that will be converted to HTML by the auth-proxy parser code. Thus, only the multiline text is displayed on the authentication proxy login page.

Note If the **ip admission consent banner**command is not enabled, nothing will be displayed to the user on a consent login page except a text box to enter the username and a text box to enter the password.

Note When HTTP authentication proxy is configured together with the Consent feature, any HTTP authentication proxy-related configurations or policies will override the Consent Page-related configurations or policies. For example, if the **ip admission name** *admission-name* **consent**command is configured, the **ip admission consent banner** command is ignored, and only the banner that is configured by the **ip admission auth-proxy-banner** command is shown.

Examples

The following example shows how to display the file "consent_page.html" located in flash:

```
ip admission consent-banner file flash:consent_page.html
```

The following example shows how to specify the custom banner "Consent-Page-Banner-Text" to be displayed in the authentication proxy consent webpage:

```
ip admission consent-banner text ^C Consent-Page-Banner-Text ^C
```

Related Commands

Command	Description
ip auth-proxy auth-proxy-banner	Displays a banner, such as the router name, in the authentication proxy login page.

ip admission name

To create an IP network admission control rule, use the **ip admission name**command in global configuration mode. To remove the network admission control rule, use the **no** form of this command.

ip admission name *admission-name* [**eapoudp [bypass]**| **proxy** {**ftp**| **http**| **telnet**}| **service-policy type tag** *service-policy-name*] [**list** {*acl*| *acl-name*}] **[event]** [**timeout aaa**] [**policy identity identity-policy-name**]

no ip admission name *admission-name* [**eapoudp [bypass]**| **proxy** {**ftp**| **http**| **telnet**}| **service-policy type tag** *service-policy-name*] [**list** {*acl*| *acl-name*}] **[event]** [**timeout aaa**] [**policy identity identity-policy-name**]

Syntax for Authentication Proxy Consent Webpage

ip admission name *admission-name* **consent** [[**absolute-timer** *minutes*] **[event]** [**inactivity-time** *minutes*] [**list** {*acl*| *acl-name*}] [**parameter-map** *consent-parameter-map-name*]]

no ip admission name *admission-name* **consent** [[**absolute-timer** *minutes*] **[event]** [**inactivity-time** *minutes*] [**list** {*acl*| *acl-name*}] [**parameter-map** *consent-parameter-map-name*]]

Syntax Description

admission-name	Name of network admission control rule.
eapoudp	(Optional) Specifies IP network admission control using Extensible Authentication Protocol over UDP (EAPoUDP).
bypass	(Optional) Admission rule bypasses EAPoUDP communication.
proxy	(Optional) Specifies authentication proxy.
ftp	Specifies that FTP is to be used to trigger the authentication proxy.
http	Specifies that HTTP is to be used to trigger authentication proxy.
telnet	Specified that Telnet is to be used to trigger authentication proxy.
service-policy type tag	(Optional) A control plane service policy is to be configured.
service-policy-name	Control plane tag service policy that is configured using the **policy-map type control tag** {*policy name*} command, keyword, and argument. This policy map is used to apply the actions on the host when a tag is received.

list	(Optional) Associates the named rule with an access control list (ACL).
acl	Applies a standard, extended list to a named admission control rule. The value ranges from 1 through 199.
acl-name	Applies a named access list to a named admission control rule.
event	(Optional) Identifies the condition that triggered the application of the policy.
timeout aaa	(Optional) Specifies that the AAA server is unreachable.
policy identity	Configures the application of an identity policy to be used while the AAA server is unreachable.
identity -policy -name	Specifies the identity policy to apply.
consent	Associates an authentication proxy consent webpage with the IP admission rule specified via the *admission-name* argument.
absolute-timer *minutes*	(Optional) Elapsed time, in minutes, before the external server times out.
inactivity-time *minutes*	(Optional) Elapsed time, in minutes, before the external file server is deemed unreachable.
parameter-map	(Optional) A parameter map policy is to be associated with consent profile.
consent-parameter-map-name	Specifies the consent profile parameters to apply.

Command Default

An IP network admission control rule is not created.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.4(6)T	The **bypass** and **service-policy type tag** keywords and *service-policy-name* argument were added.

Release	Modification
12.4(11)T	The **event**, **timeout aaa**, and **policy identity** keywords and the *identity -policy -name argument were added.*
12.4(15)T	The following keywords and arguments were added: **consent**, **absolute-timer ,** *minutes*, **inactivity-time**, *minutes,* **parameter-map**, and *consent-parameter-map-name*.
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 admission rule defines how you apply admission control.

You can associate the named rule with an ACL, providing control over which hosts use the admission control feature. If no standard access list is defined, the named admission rule intercepts IP traffic from all hosts whose connection-initiating packets are received at the configured interface.

The **bypass** keyword allows an administrator the choice of not having to use the EAPoUDP-based posture validation for the hosts that are trying to connect on the port. The bypass can be used if an administrator knows that the hosts that are connected on the port do not have the Cisco Trust Agent client installed.

The **service-policy type tag** {*service-policy-name*} keywords and argument allow you to associate the service policy of the type tag with the IP admission rule. On the network access device (NAD), a set of policies can be associated with an arbitrary tag string, and if the AAA server sends the same tag in response to the posture validation or authentication response, the policies that are associated with the tag can be applied on the host. The **service policy** keyword is an optional keyword, and if the service policy is not associated with the IP admission name, the policies that are received from the AAA server are applied on the host.

The **list** keyword option allows you to apply a standard, extended (1 through 199) or named access list to a named admission control rule. IP connections that are initiated by hosts in the access list are intercepted by the admission control feature.

The **event** keyword option allows you to specify the condition that triggered application of an identity policy.

The **timeout aaa** keyword option specifies that the AAA server is unreachable, and this condition is triggering the application of an identity policy.

The **policy identity** keyword and the *identity -policy -name argument* allow you to configure application of an identity policy and specify the policy type to be applied while the AAA server is unreachable.

The **consent** keyword and the **parameter-map** *consent-parameter-map-name* keyword and argument allow you to associate the authentication proxy consent feature with an IP admission rule. The consent feature enables customers to display a consent webpage to an end user, providing access to wireless services only after the end user accepts the agreement.

Examples

Examples

The following example shows that an IP admission control rule is named "greentree" and that it is associated with ACL "101." Any IP traffic that is destined to a previously configured network (using the **access-list** command) will be subjected to antivirus state validation using EAPoUDP.

```
Router (config)# ip admission name greentree eapoudp list 101
```

The following example shows that EAPoUDP bypass has been configured:

```
Router (config)# ip admission name greentree eapoudp bypass list 101
```

In the following service policy example, tags named "healthy" and "non_healthy" can be received from an AAA server, the policy map is defined on the NAD, and the tag policy type is associated with the IP admission name "greentree."

Examples

```
Router (config)# class-map type tag healthy_class
Router(config-cmap)# match tag healthy
Router(config-cmap)# end
```

Examples

```
Router (config)# class-map type tag non_healthy_class
Router (config-cmap)# match tag non_healthy
Router (config-cmap)# end
```

Examples

```
! The following line will be associated with the IP admission name.
Router (config)# policy-map type control tag global_class
! The following line refers to the healthy class map that was defined above.
Router (config-pmap)# class healthy_class
Router (config-pmap-c)# identity policy healthy_policy
Router(config-pmap-c)# exit
The following line refers to the non_healthy class that was defined above.
Router (config-pmap)# class non_healthy_class
Router(config-pmap-c)# identity policy non_healthy_policy
Router (config-pmap-c)# end
```

Examples

```
Router (config)# identity policy healthy_policy
! The following line is the IP access list for healthy users.
Router (config-identity-policy)# access-group healthy
Router (config-identity-policy)# end
Router (config)# identity policy non_healthy_policy
Router (config-identity-policy)# access-group non_healthy

Router (config-identity-policy)# end
```

Examples

```
Router (config)# ip access-list extended healthy_class
! The following line can be anything, but as an example, traffic is being allowed.
Router (config-ext-nacl)# permit ip any any
Router (config-ext-nac)# end
Router (config)# ip access-list extended non_healthy_class
! The following line is only an example. In practical cases, you could prevent a user from
 accessing specific networks.
Router (config-ext-nacl)# deny ip any any
Router (config-ext-nac)# end
```

Examples

```
Router (config)# ip admission name greentree service-policy type tag global_class

! In the next line, the admission name can be associated with the interface.
Router (config)# interface fastethernet 1/0
Router (config-if)# ip admission greentree
```

In the above configuration, if the AAA server sends a tag named "healthy" or "non_healthy" for any host, the policies that are associated with the appropriate identity policy will be applied on the host.

Examples

The following example shows how to define an IP admission control rule named "samplerule" and attach it to a specific interface:

```
Router (config)# ip admission name samplerule eapoudp list 101 event timeout aaa policy
identity aaa_fail_policy
```

Router (config)# **interface fastethernet 1/1**

Router (config-if)# **ip admission samplerule**

Router (config-if)# **end**

In the above configuration, if the specified interface is not already authorized when the AAA server becomes unreachable, it will operate under the specified policy until revalidation is possible.

Examples

The following example shows how to configure an IP admission consent rule and associate the consent rule with the definitions of the parameter map "consent_parameter_map":

```
ip admission name consent-rule consent inactivity-time 204 absolute-timer 304 parameter-map
 consent_parameter_map list 103
ip admission consent-banner file flash:consent_page.html
ip admission consent-banner text ^C Consen-Page-Banner-Text ^C
ip admission max-login-attempts 5
ip admission init-state-timer 15
ip admission auth-proxy-audit
ip admission inactivity-timer 205
ip admission absolute-timer 305
ip admission ratelimit 100
ip http server
ip http secure-server
!
interface FastEthernet 0/0
 description ### CLIENT-N/W ###
 ip address 192.168.100.170 255.255.255.0
 ip access-group 102 in
 ip admission consent-rule
 no shut
 exit
!
interface FastEthernet 0/1
 description ### AAA-DHCP-AUDIT-SERVER-N/W ###
 ip address 192.168.104.170 255.255.255.0
 no shut
 exit
!
line con 0
 exec-timeout 0 0
 login authentication noAAA
 exit
!
line vty 0 15
 exec-timeout 0 0
 login authentication noAAA
 exit
!
```

Related Commands

Command	Description
ip address	Sets a primary or secondary IP address for an interface.
ip admission event timeout aaa policy identity	Defines a policy to be applied when the AAA server is unreachable.

ip admission name bypass regex

To configure browser-based authentication bypass on a Network Admission Control (NAC) rule, use the **ip admission name bypass regex** command in global configuration mode. To remove browser-based authentication bypass, use the **no** form of this command.

ip admission name *admission-name* **bypass regex** *regex-map* [**absolute-timer** *minutes*]

no ip admission name *admission-name* **bypass**

Syntax Description

admission-name	Name of a NAC rule.
regex-map	Regular expression (regex) parameter map with a regex pattern to enable bypass authentication for a web browser.
absolute-timer *minutes*	(Optional) Specifies the maximum time, in minutes, before a browser session times out. The maximum time ranges from 0 to 35791. Default value for an authentication session is 0. Default value for an authentication bypass session is 60.

Command Default

Authentication is required for all browsers.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.3(3)M	This command was introduced.

Usage Guidelines

The **bypass regex** *regex-map* keyword and argument configures a regex pattern that can be compared to the user-agent field in the HTTP Get request to bypass authentication for a configured browser. This command defines the NAC policy to be applied to a network access device to bypass browser authentication.

Examples

The following example shows how to bypass browser authentication:

```
Device> enable
Device# configure terminal
Device(config)# ip admission name rule1 bypass regex regex-map1 absolute-timer 10
```

ip admission name http-basic

To create a basic HTTP authentication network admission control rule, use the **ip admission name http-basic** command in global configuration mode. To remove the network admission control rule, use the **no** form of this command.

ip admission name *admission-name* **http-basic** [**passive**] [**absolute-timer** *minutes*] [**event timeout aaa policy identity** *identity-policy-name*] [**inactivity-time** *minutes*] [**list** {*acl-list* | *extended-acl-list* | *acl-name*}] [**service-policy type tag** *service-policy-name*]

no ip admission name *admission-name* **http-basic**

Syntax Description

admission-name	Name of the network admission control rule.
passive	(Optional) Specifies passive mode.
absolute-timer *minutes*	(Optional) Specifies the elapsed time, in minutes, before the external server time out. Valid values are from 0 to 35791. The default is 0.
event	(Optional) Specifies the event to be associated with a policy.
timeout	(Optional) Specifies timeout-based events.
aaa	(Optional) Specifies that the authentication, authorization, and accounting (AAA) server is unreachable.
policy identity	(Optional) Applies an identity policy to be used while the AAA server is unreachable.
identity-policy-name	(Optional) Name of the identity policy to be applied.
inactivity-time *minutes*	(Optional) Specifies the lapsed time, in minutes, before the external file server is deemed unreachable. Valid values are from 1 to 35791.
list	(Optional) Specifies an access control list (ACL) to apply to an authentication proxy.
acl-list	(Optional) Standard ACL number. Valid values are from 1 to 199.
extended-acl-list	(Optional) Expanded range of ACL numbers. Valid values are from 1300 to 2699.
acl-name	(Optional) ACL name.

service-policy	(Optional) Specifies a control plane service policy is to be configured.
type	(Optional) Specifies the type of the service policy.
tag	(Optional) Specifies the tag-based service policy type.
service-policy-name	(Optional) Name of the control plane service policy. This service policy is used to apply actions on the host when a tag is received.

Command Default

A basic HTTP authentication network admission control rule is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(1)T1	This command was introduced.

Usage Guidelines

When you configure the **ip admission name http-basic** command, client applications always prompt users to enter their credentials.

The absolute timeout value allows you to configure a time duration during which the authentication proxy on the enabled interface is active. After the absolute timer expires, the authentication proxy is disabled regardless of any activity. The absolute timeout value can be configured per protocol or globally. The default value of the absolute timeout is zero. Hence the absolute timer is disabled by default and the authentication proxy is enabled indefinitely.

The **timeout aaa** keywords specify that the AAA server is unreachable, and this condition triggers the application of an identity policy.

The **service-policy type tag** *service-policy-name* keywords and argument allow you to associate a service policy of the type tag with the IP admission rule. On the network access device (NAD), a set of policies can be associated with an arbitrary tag string, and if the AAA server sends the same tag in response to the posture validation or authentication response, the policies that are associated with the tag can be applied on the host. The **service policy** keyword is an optional keyword, and if the service policy is not associated with the IP admission name, the policies that are received from the AAA server are applied on the host.

Examples

The following example shows how to configure a basic HTTP network admission control rule:

```
Router(config)# ip admission name admission1 http-basic
```

Related Commands

Command	Description
ip address	Sets a primary or secondary IP address for an interface.
ip admission event timeout aaa policy identity	Defines a policy to be applied when the AAA server is unreachable.

ip admission name method-list

To create a list of authentication, authorization, and accounting(AAA) method network admission control rules, use the **ip admission name method-list** command in global configuration mode. To remove the network admission control rules, use the **no** form of this command.

ip admission name *admission-name* **method-list** [**accounting**] [**authentication**] [**authorization**] {*list-name*| **default**}

no ip admission name *admission-name* **method-list**

Syntax Description

admission-name	Name of the network admission control rule.
accounting	(Optional) Specifies the accounting method.
authentication	(Optional) Specifies the authentication method.
authorization	(Optional) Specifies the authorization method.
list-name	Method list name.
default	Specifies the default method list.

Command Default

A list of AAA method network admission control rules is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(1)T1	This command was introduced.

Usage Guidelines

The **ip admission name method-list accounting** command defines the reference to the accounting method list of service type auth-proxy or the network that is configured using the **aaa accounting auth-proxy** and **aaa accounting network** commands respectively.

The **ip admission name method-list authentication** command defines the reference to the authentication method list of service type login that is configured using the **aaa authentication login** command.

The **ip admission name method-list authorization** command defines the reference to the authorization method list of service type auth-proxy or the network that is configured using the **aaa authorization auth-proxy** and **aaa authorization network** commands respectively.

Examples

The following example shows how to create an accounting method network admission control rule:

```
Router(config)# ip admission name admission1 method-list accounting accounting-method
```

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 login	Sets AAA authentication at login.
aaa authorization network	Sets the parameters that restrict user access to a network.
ip address	Sets a primary or secondary IP address for an interface.
ip admission event timeout aaa policy identity	Defines a policy to be applied when the AAA server is unreachable.

ip admission name ntlm

To create a Windows network, NT LAN Manager (NTLM) authentication network admission control rule, use the **ip admission name ntlm** command in global configuration mode. To remove the network admission control rule, use the **no** form of this command.

ip admission name *admission-name* **ntlm** [**absolute-timer** *minutes*] [**event timeout aaa policy identity** *identity-policy-name*] [**list** {*acl-list* | *extended-acl-list* | *acl-name*}] [**service-policy type tag** *service-policy-name*]

no ip admission name *admission-name* **ntlm**

Syntax Description

admission-name	Name of the network admission control rule.
absolute-timer *minutes*	(Optional) Specifies the elapsed time, in minutes, before the external server times out. Valid values are from 0 to 35791.
event	(Optional) Specifies the event to be associated with a policy.
timeout	(Optional) Specifies timeout-based events.
aaa	(Optional) Specifies that the authentication, authorization, and accounting (AAA) server is unreachable.
policy identity	(Optional) Applies an identity policy to be used while the AAA server is unreachable.
identity-policy-name	(Optional) Name of the identity policy to be applied.
list	(Optional) Specifies an access control list (ACL) to apply to an authentication proxy.
acl-list	(Optional) Standard ACL number. Valid values are from 1 to 199.
extended-acl-list	(Optional) Expanded range of ACL numbers. Valid values are from 1300 to 2699.
acl-name	(Optional) ACL name.
service-policy	(Optional) Specifies a control plane service policy is to be configured.
type	(Optional) Specifies the type of the service policy.

tag	(Optional) Specifies the tag-based service policy type.
service-policy-name	(Optional) Name of the control plane service policy. This service policy is used to apply actions on the host when a tag is received.

Command Default

An NTLM Authentication network admission control rule is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(1)T1	This command was introduced.

Usage Guidelines

When you use the NTLM authentication method, the router tries to retrieve the user credentials transparently from the client application without prompting end users. If the client application cannot send user credentials transparently, it prompts users to enter their username and password.

The absolute timeout value allows you to configure a time duration during which the authentication proxy on the enabled interface is active. After the absolute timer expires, the authentication proxy is disabled regardless of any activity. The absolute timeout value can be configured per protocol or globally. The default value of the absolute timeout is zero. Hence the absolute timer is disabled by default and the authentication proxy is enabled indefinitely.

The **timeout aaa** keyword specifies that the AAA server is unreachable, and this condition triggers the application of an identity policy.

The **service-policy type tag** *service-policy-name* keywords and argument allow you to associate a service policy of the type tag with the IP admission rule. On the network access device (NAD), a set of policies can be associated with an arbitrary tag string, and if the AAA server sends the same tag in response to the posture validation or authentication response, the policies that are associated with the tag can be applied on the host. The **service policy** keyword is an optional keyword, and if the service policy is not associated with the IP admission name, the policies that are received from the AAA server are applied on the host.

Examples

The following example shows how to create an NTLM network admission control rule:

```
Router(config)# ip admission name admission1 ntlm
```

Related Commands

Command	Description
ip address	Sets a primary or secondary IP address for an interface.

Command	Description
ip admission event timeout aaa policy identity	Defines a policy to be applied when the AAA server is unreachable.

ip admission name order

To create a fallback authentication order for the network admission control rule, use the **ip admission name order** command in global configuration mode. To remove the authentication order for the network admission control rule, use the **no** form of this command.

ip admission name *admission-name* **order** [**http-basic**] [**ntlm**] [**proxy-http**]

ip admission name *admission-name* **order**

Syntax Description

admission-name	Name of the network admission control rule.
http-basic	(Optional) Specifies HTTP basic authentication.
ntlm	(Optional) Specifies Windows network, NT LAN Manager (NTLM) authentication.
proxy-http	(Optional) Specifies proxy HTTP authentication.

Command Default

A fallback authentication order for the network admission control rule is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(1)T1	This command was introduced.

Examples

The following example shows how to create an authentication order for a network admission control rule:

```
Router(config)# ip admission name admission1 order http-basic
```

Related Commands

Command	Description
ip admission name	Creates an authentication network admission control rule.
ip admission name http-basic	Creates a basic HTTP authentication network admission control rule.

Command	Description
ip admission name ntlm	Creates an NTLM authentication network admission control rule.

ip admission proxy http

To specify the display of custom authentication proxy web pages during web-based authentication, use the **ip admission proxy http** command in global configuration mode. To specify the use of the default web page, use the **no** form of this command.

ip admission proxy http {{**login**| **success**| **failure**| **login expired**} **page file** *device:file-name*| **success redirect** *url*}

no ip admission proxy http {{**login**| **success**| **failure**| **login expired**} **page file** *device:file-name*| **success redirect** *url*}

Syntax Description

login	Specifies a locally stored web page to be displayed during login.
success	Specifies a locally stored web page to be displayed when the login is successful.
failure	Specifies a locally stored web page to be displayed when the login has failed.
login expired	Specifies a locally stored web page to be displayed when the login has expired.
device	Specifies a disk or flash memory in the switch memory file system where the custom HTML file is stored.
file-name	Specifies the name of the custom HTML file to be used in place of the default HTML file for the specified condition.
success redirect *url*	Specifies an external web page to be displayed when the login is successful.

Command Default

The internal default authentication proxy web pages are displayed during web-based authentication.

Command Modes

Global configuration

Command History

Release	Modification
12.2(33)SXI	This command was introduced.

Usage Guidelines

When configuring the use of customized authentication proxy web pages, consider the following guidelines:

- To enable the custom web pages feature, you must specify all four custom HTML files. If fewer than four files are specified, the internal default HTML pages will be used.
- The four custom HTML files must be present on the disk or flash of the switch. The maximum size of each HTML file is 8 KB.
- Any images on the custom pages must be located on an accessible HTTP server. An intercept ACL must be configured within the admission rule to allow access to the HTTP server.
- Any external link from a custom page will require configuration of an intercept ACL within the admission rule.
- Any name resolution required for external links or images will require configuration of an intercept ACL within the admission rule to access a valid DNS server.
- If the custom web pages feature is enabled, a configured auth-proxy-banner will not be used.
- If the custom web pages feature is enabled, the redirection URL for successful login feature will not be available.
- Because the custom login page is a public web form, consider the following guidelines for this page:
    - The login form must accept user input for the username and password and must POST the data as uname and pwd.
    - The custom login page should follow best practices for a web form, such as page timeout, hidden password, and prevention of redundant submissions.
- When configuring a redirection URL for successful login, consider the following guidelines:
    - If the custom authentication proxy web pages feature is enabled, the redirection URL feature is disabled and will not be available in the CLI. You can perform redirection in the custom login success page.
    - If the redirection URL feature is enabled, a configured auth-proxy-banner will not be used.

Examples

The following example shows how to configure custom authentication proxy web pages:

```
Router(config)# ip admission proxy http login page file disk1:login.htm
Router(config)# ip admission proxy http success page file disk1:success.htm
Router(config)# ip admission proxy http fail page file disk1:fail.htm
Router(config)# ip admission proxy http login expired page file disk1:expired.htm
```

The following example shows how to verify the configuration of custom authentication proxy web pages:

```
Router# show ip admission configuration
Authentication proxy webpage
 Login page         : disk1:login.htm
 Success page       : disk1:success.htm
 Fail Page          : disk1:fail.htm
 Login expired Page : disk1:expired.htm
Authentication global cache time is 60 minutes
Authentication global absolute time is 0 minutes
Authentication global init state time is 2 minutes
Authentication Proxy Session ratelimit is 100
Authentication Proxy Watch-list is disabled
Authentication Proxy Auditing is disabled
Max Login attempts per user is 5
```

The following example shows how to configure a redirection URL for successful login:

```
Router(config)# ip admission proxy http success redirect www.example.com
```

The following example shows how to verify the redirection URL for successful login:

```
Router# show ip admission configuration
Authentication Proxy Banner not configured
Customizable Authentication Proxy webpage not configured
HTTP Authentication success redirect to URL: http://www.example.com
Authentication global cache time is 60 minutes
Authentication global absolute time is 0 minutes
Authentication global init state time is 2 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
```

Related Commands

Command	Description
ip http server ip https server	Enables the HTTP server within the switch.
show ip admission configuration	Displays the configuration of web-based authentication ip admission.

ip admission virtual-ip

To configure a web-based proxy authentication virtual IP address, use the **ip admission virtual-ip** command in global configuration mode. To remove the address, use the **no** form of this command.

ip admission virtual-ip *ip-address*

no ip admission virtual-ip *ip-address*

Syntax Description

ip-address	Virtual IP address.

Command Default

A web-based proxy authentication virtual IP address is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.2(1)T1	This command was introduced.

Usage Guidelines

A virtual IP address is used only in communication between the Cisco IOS HTTP authentication and clients. For the web-based proxy authentication to operate you must set the virtual IP address, and no other device on the network can have the same IP address as the virtual IP address.

Examples

The following example shows how to configure the web-based proxy authentication virtual IP address:

```
Router(config)# ip admission virtual-ip 10.1.1.1
```

Related Commands

Command	Description
content-scan out	Enables content scanning on an egress interface.

ip audit

To apply an audit specification created with the **ip audit**command to a specific interface and for a specific direction, use the **ip audit**command in interface configuration mode. To disable auditing of the interface for the specified direction, use the **no** version of this command.

ip audit *audit-name* {**in**| **out**}

no ip audit *audit-name* {**in**| **out**}

Syntax Description

audit-name	Name of an audit specification.
in	Inbound traffic.
out	Outbound traffic.

Command Default

No audit specifications are applied to an interface or direction.

Command Modes

Interface 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.(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 **ip audit**interface configuration command to apply an audit specification created with the **ip audit**command to a specific interface and for a specific direction.

Examples

In the following example, the audit specification MARCUS is applied to an interface and direction:

```
interface e0
 ip audit MARCUS in
```

In the following example, the audit specification MARCUS is removed from the interface on which it was previously added:

```
interface e0
 no ip audit MARCUS in
```

ip audit attack

To specify the default actions for attack signatures, use the **ip audit attack** command in global configuration mode. To set the default action for attack signatures, use the **no** form of this command.

ip audit attack action [alarm] [drop] [reset]

no ip audit attack

Syntax Description

action	Specifies an action for the attack signature to take in response to a match.
alarm	(Optional) Sends an alarm to the console, NetRanger Director, or to a syslog server. Used with the **action** keyword.
drop	(Optional) Drops the packet. Used with the **action** keyword.
reset	(Optional) Resets the TCP session. Used with the **action** keyword.

Command Default

The default action is **alarm**.

Command Modes

Global 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.(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 **ip audit attack** global configuration command to specify the default actions for attack signatures.

Examples

In the following example, the default action for attack signatures is set to all three actions:

```
ip audit attack action alarm drop reset
```

ip audit info

To specify the default actions for info signatures, use the **ip audit info** command in global configuration mode. To set the default action for info signatures, use the **no** form of this command.

ip audit info action [alarm] [drop] [reset]

no ip audit info

Syntax Description

action	Sets an action for the info signature to take in response to a match.
alarm	(Optional) Sends an alarm to the console, NetRanger Director, or to a syslog server. Used with the **action** keyword.
drop	(Optional) Drops the packet. Used with the **action** keyword.
reset	(Optional) Resets the TCP session. Used with the **action** keyword.

Command Default

The default action is **alarm**.

Command Modes

Global 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.(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 **ip audit info** global configuration command to specify the default actions for info signatures.

Examples

In the following example, the default action for info signatures is set to all three actions:

```
ip audit info action alarm drop reset
```

ip audit name

To create audit rules for info and attack signature types, use the **ip audit name** command in global configuration mode. To delete an audit rule, use the **no** form of this command.

ip audit name *audit-name* {**info**| **attack**} [**list** *standard-acl*] [**action [alarm] [drop] [reset]**]

no ip audit name *audit-name* {**info**| **attack**}

Syntax Description

audit-name	Name for an audit specification.
info	Specifies that the audit rule is for info signatures.
attack	Specifies that the audit rule is for attack signatures.
list	(Optional) Specifies an ACL to attach to the audit rule.
standard-acl	(Optional) Integer representing an access control list. Use with the **list** keyword.
action	(Optional) Specifies an action or actions to take in response to a match.
alarm	(Optional) Sends an alarm to the console, NetRanger Director, or to a syslog server. Use with the **action** keyword.
drop	(Optional) Drops the packet. Use with the **action** keyword.
reset	(Optional) Resets the TCP session. Use with the **action** keyword.

Command Default

If an action is not specified, the default action is **alarm**.

Command Modes

Global 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.(33)SRA.

Release	Modification
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

Any signatures disabled with the **ip audit signature** command do not become a part of the audit rule created with the **ip audit name** command.

Examples

In the following example, an audit rule called INFO.2 is created, and configured with all three actions:

```
ip audit name INFO.2 info action alarm drop reset
```

In the following example, an info signature is disabled and an audit rule called INFO.3 is created:

```
ip audit signature 1000 disable
ip audit name INFO.3 info action alarm drop reset
```

In the following example, an audit rule called ATTACK.2 is created with an attached ACL 91, and the ACL is created:

```
ip audit name ATTACK.2 list 91
access-list 91 deny 10.1.0.0 0.0.255.255
access-list 91 permit any
```

ip audit notify

To specify the method of event notification, use the **ip audit notify** command in global configuration mode. To disable event notifications, use the **no** form of this command.

ip audit notify {**nr-director**| **log**}

no ip audit notify {**nr-director**| **log**}

Syntax Description

nr-director	Send messages in NetRanger format to the NetRanger Director or Sensor.
log	Send messages in syslog format.

Command Default

The default is to send messages in syslog format.

Command Modes

Global 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.(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

If messages are sent to the NetRanger Director, then you must also configure the NetRanger Director's Post Office transport parameters using the **ip audit po remote** command.

Examples

In the following example, event notifications are specified to be sent in NetRanger format:

```
ip audit notify nr-director
```

Related Commands

Command	Description
ip audit po local	Specifies the local Post Office parameters used when sending event notifications to the NetRanger Director.

Command	Description
ip audit po remote	Specifies one or more sets of Post Office parameters for NetRanger Directors receiving event notifications from the router.

ip audit po local

To specify the local Post Office parameters used when sending event notifications to the NetRanger Director, use the **ip audit po local** command in global configuration mode. To set the local Post Office parameters to their default settings, use the **no** form of this command.

ip audit po local hostid *id-number* **orgid** *id-number*

no ip audit po local [**hostid** *id-number* **orgid** *id-number*]

Syntax Description

hostid	Specifies a NetRanger host ID.
id-number	Unique integer in the range 1 to 65535 used in NetRanger communications to identify the local host. The default host ID is 1.
orgid	Specifies a NetRanger organization ID.
id-number	Unique integer in the range 1 to 65535 used in NetRanger communications to identify the group to which the local host belongs. The default organization ID is 1.

Command Default

The default organization ID is 1. The default host ID is 1.

Command Modes

Global 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.(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 **ip audit po local** global configuration command to specify the local Post Office parameters used when sending event notifications to the NetRanger Director.

Examples

In the following example, the local host is assigned a host ID of 10 and an organization ID of 500:

```
ip audit po local hostid 10 orgid 500
```

ip audit po max-events

To specify the maximum number of event notifications that are placed in the router's event queue, use the **ip audit po max-events**command inglobal configuration mode. To set the number of recipients to the default setting, use the **no** version of this command.

ip audit po max-events *number-of-events*

no ip audit po max-events

Syntax Description

number-of-events	Integer in the range from 1 to 65535 that designates the maximum number of events allowable in the event queue. The default is 100 events.

Command Default

The default number of events is 100.

Command Modes

Global 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.(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

Raising the number of events past 100 may cause memory and performance impacts because each event in the event queue requires 32 KB of memory.

Examples

In the following example, the number of events in the event queue is set to 250:

```
ip audit po max-events 250
```

ip audit po protected

To specify whether an address is on a protected network, use the **ip audit po protected** command in global configuration mode. To remove network addresses from the protected network list, use the **no** form of this command.

ip audit po protected *ip-addr* [**to** *ip-addr*]

no ip audit po protected [*ip-addr*]

Syntax Description

ip-addr	IP address of a network host.
to *ip-addr*	(Optional) Specifies a range of IP addresses.

Command Default

If no addresses are defined as protected, then all addresses are considered outside the protected network.

Command Modes

Global 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.(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 can enter a single address at a time or a range of addresses at a time. You can also make as many entries to the protected networks list as you want. When an attack is detected, the corresponding event contains a flag that denotes whether the source or destination of the packet belongs to a protected network or not.

If you specify an IP address for removal, that address is removed from the list. If you do not specify an address, then all IP addresses are removed from the list.

Examples

In the following example, a range of addresses is added to the protected network list:

```
ip audit po protected 10.1.1.0 to 10.1.1.255
```

In the following example, three individual addresses are added to the protected network list:

```
ip audit po protected 10.4.1.1
ip audit po protected 10.4.1.8
ip audit po protected 10.4.1.25
```

In the following example, an address is removed from the protected network list:

```
no ip audit po protected 10.4.1.1
```

ip audit po remote

To specify one or more set of Post Office parameters for NetRanger Directors receiving event notifications from the router, use the **ip audit po remote** global configuration command. To remove a NetRanger Director's Post Office parameters as defined by host ID, organization ID, and IP address, use the **no** form of this command.

ip audit po remote hostid *host-id* **orgid** *org-id* **rmtaddress** *ip-address* **localaddress** *ip-address* [**port** *port-number*] [**preference** *preference-number*] [**timeout** *seconds*] [**application** {**director**| **logger**}]

no ip audit po remote hostid *host-id* **orgid** *org-id* **rmtaddress** *ip-address*

Syntax Description

host-id	Unique integer in the range from 1 to 65535 used in NetRanger communications to identify the local host. Use with the **hostid** keyword.
hostid	Specifies a NetRanger host ID.
org-id	Unique integer in the range from 1 to 65535 used in NetRanger communications to identify the group in which the local host belongs. Use with the **orgid** keyword.
orgid	Specifies a NetRanger organization ID.
rmtaddress	Specifies the IP address of the NetRanger Director.
localaddress	Specifies the IP address of the Cisco IOS Firewall IDS router.
ip-address	IP address of the NetRanger Director or Cisco IOS Firewall IDS router's interface. Use with the **rmtaddress**and **localaddress**keywords.
port-number	(Optional) Integer representing the UDP port on which the NetRanger Director is listening for event notifications. Use with the **port** keyword.
port	(Optional) Specifies a User Datagram Protocol port through which to send messages.
preference	(Optional) Specifies a route preference for communication.
preference-number	(Optional) Integer representing the relative priority of a route to a NetRanger Director, if more than one route exists. Use with the **preference** keyword.

seconds	(Optional) Integer representing the heartbeat timeout value for Post Office communications. Use with the **timeout** keyword.
timeout	(Optional) Specifies a timeout value for Post Office communications.
application	(Optional) Specifies the type of application that is receiving the Cisco IOS Firewall IDS messages.
director	(Optional) Specifies that the receiving application is the NetRanger Director interface.
logger	(Optional) Specifies that the receiving application is a NetRanger Sensor.

Command Default

The default organization ID is 1.

The default host ID is 1.

The default UDP port number is 45000.

The default preference is 1.

The default heartbeat timeout is 5 seconds.

The default application is **director**.

Command Modes

Global 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.(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

A router can report to more than one NetRanger Director. In this case, use the **ip audit po remote** command to add each NetRanger Director to which the router sends notifications.

More than one route can be established to the same NetRanger Director. In this case, you must give each route a preference number that establishes the relative priority of routes. The router always attempts to use the lowest numbered route, switching automatically to the next higher number when a route fails, and then switching back when the route begins functioning again.

A router can also report to a NetRanger Sensor. In this case, use the **ip audit po remote** command and specify **logger** as the application.

Examples

In the following example, two communication routes for the same dual-homed NetRanger Director are defined:

```
ip audit po remote hostid 30 orgid 500 rmtaddress 10.1.99.100 localaddress 10.1.99.1
preference 1
ip audit po remote hostid 30 orgid 500 rmtaddress 10.1.4.30 localaddress 10.1.4.1 preference
 2
```

The router uses the first entry to establish communication with the NetRanger Director defined with host ID 30 and organization ID 500. If this route fails, then the router will switch to the secondary communications route. As soon as the first route begins functioning again, the router switches back to the primary route and closes the secondary route.

In the following example, a different Director is assigned a longer heartbeat timeout value because of network congestion, and is designated as a logger application:

```
ip audit po remote hostid 70 orgid 500 rmtaddress 10.1.8.1 localaddress 10.1.8.100 timeout
 10 application director
```

ip audit signature

To attach a policy to a signature, use the **ip audit signature** command in global configuration mode. To remove the policy, use the **no** form of this command. If the policy disabled a signature, then the **no** form of this command reenables the signature. If the policy attached an access list to the signature, the **no** form of this command removes the access list.

ip audit signature *signature-id* {**disable**| **list** *acl-list*}

no ip audit signature *signature-id*

Syntax Description

signature-id	Unique integer specifying a signature as defined in the NetRanger Network Security Database.
disable	Disables the ACL associated with the signature.
list	Specifies an ACL to associate with the signature.
acl-list	Unique integer specifying a configured ACL on the router. Use with the **list** keyword.

Command Default

No policy is attached to a signature.

Command Modes

Global 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.(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 allow you to set two policies: disable the audit of a signature or qualify the audit of a signature with an access list.

If you are attaching an access control list to a signature, then you also need to create an audit rule with the **ip audit name**command and apply it to an interface with the **ip audit** command.

Examples

In the following example, a signature is disabled, another signature has ACL 99 attached to it, and ACL 99 is defined:

```
ip audit signature 6150 disable
ip audit signature 1000 list 99
access-list 99 deny 10.1.10.0 0.0.0.255
access-list 99 permit any
```

ip audit smtp

To specify the number of recipients in a mail message over which a s pam attack is suspected, use the **ip audit smtp** command in global configuration mode. To set the number of recipients to the default setting, use the **no** form of this command.

ip audit smtp spam *number-of-recipients*

no ip audit smtp spam

Syntax Description

spam	Specifies a threshold beyond which the Cisco IOS Firewall IDS alarms on spam e-mail.
number-of-recipients	Integer in the range of 1 to 65535 that designates the maximum number of recipients in a mail message before a spam attack is suspected. Use with the **spam** keyword. The default is 250 recipients.

Command Default

The default number of recipients is 250.

Command Modes

Global 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.(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 **ip audit smtp** global configuration command to specify the number of recipients in a mail message over which a spam attack is suspected.

Examples

In the following example, the number of recipients is set to 300:

```
ip audit smtp spam 300
```

ip auth-proxy (global configuration)

To set the the authenticatio proxy idle timeout or maximum number of idle connections, use the **ip auth-proxy**command in global configuration mode. To return the idle timeout or maximum number of idle connections to their default values, use the **no** form of this command.

ip auth-proxy {**absolute-timer** *min*| **inactivity-timer** *min*| **init-state-timer** *min*| **max-nodata-conns** *number*}

no ip auth-proxy [absolute-timer] [inactivity-timer] [init-state-timer] [max-nodata-conns]

Syntax Description

absolute-timer *min*	Length of time in minutes that an ingress IP authentication proxy session can remain active. After this timer expires, each session must go through the entire process of establishing its connection as if it was a new request. The range is 0 to 35,791. The default is 0.
inactivity-timer *min*	L ength of time in minutes that an active ingress session can be present with no activity or data from the end client. If this timer expires without activity or data, the session is cleared. The range is 1 to 2,147,483,647. The default is 60. **Note** This keyword and argument pair replaces the auth-cache-time *min* keyword and argument pair.
init-state-timer *min*	Length of time in minutes that an ingress authentication proxy session can stay in the INIT state. An ingress session is first registered in the INIT state until the user enters their username and password credentials. If the timer expires before the credentials are entered, the session is removed. The range is 1 to 15. The default is 2.
max-nodata-conns *number*	Maximum number of idle ("no data") TCP connections that can exist globally for the IP authentication feature. The range is 1 to 1,000. The default is 3.

Command Default

The absolute timer is enabled indefinitely. The inactivity timer, and the INIT state timer are enabled. The limit on the number of global idle TCP connections is enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.3(1)	The **inactivity-timer**and **absolute-timer** keywords were added .
12.4(6)T	The **init-state-timer**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.

Usage Guidelines

You use the **ip auth-proxy**command to set the global idle timeout value for the authentication proxy. The idle timeout value is the length of time an authentication cache entry, along with its associated dynamic user access control list, is cleared after a period of inactivity.

You use the **absolute-timer** keyword to configure the length of time during which the authentication proxy on the enabled interface is active. After the absolute timer expires, the authentication proxy is disabled regardless of any activity. You can override the global absolute timeout value with the local (per protocol) value, which you can enable by using the **ip auth-proxy name** command. The absolute timer is turned off by default, and the authentication proxy is enabled indefinitely.

You must set the value of the **inactivity-timer**keyword to a higher value than the idle timeout of any Context-Based Access Control (CBAC) protocols. Otherwise, when the authentication proxy removes the user profile (and its associated dynamic user ACLs), there might be idle connections monitored by CBAC. Removing these user-specific ACLs could cause those idle connections to hang. If the CBAC idle timeout value is shorter, CBAC resets these connections when the CBAC idle timeout expires, which is before the authentication proxy removes the user profile.

You use the **init-state-timer** keyword to configure the amount of time that the authentication proxy is allowed to clear connections that are in the INIT state. Authentication attempts can remain in the INIT state when the router is loaded heavily and the authentication is not completed in two minutes. This problem is more likely if HTTPS is used for authenticating users. The default value of two minutes is usually sufficient to handle most cases, but if not, you should use the **init-state-timer** keyword to increase this value.

You use the **max-nodata-conns** keyword to limit the number of idle TCP connections (TCP sessions that are active but do not transmit data for a long period of time). There is no timer associated with this number.

Examples

The following example sets the inactivity timer to 30 minutes:

```
Router> enable
Router# configure terminal
Router(config)# ip auth-proxy inactivity-timer 30
```

The following example sets the INIT state timer to 15 minutes:

```
Router> enable
Router# configure terminal
Router(config)# ip auth-proxy init-state-timer 15
```

Related Commands

Command	Description
ip auth-proxy name	Creates an authentication proxy rule.
show ip auth-proxy configuration	Displays the authentication proxy entries or the running authentication proxy configuration.

ip auth-proxy (interface configuration)

To apply an authentication proxy rule at a firewall interface, use the **ip auth-proxy**command in interface configuration mode. To remove the authentication proxy rules, use the **no** form of this command.

ip auth-proxy *auth-proxy-name*

no ip auth-proxy *auth-proxy-name*

Syntax Description

auth-proxy-name	Specifies the name of the authentication proxy rule to apply to the interface configuration. The authentication proxy rule is established with the **ip auth-proxy name** command.

Command Default

No default behavior or values.

Command Modes

Interface 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.(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 **ip auth-proxy** command to enable the named authentication proxy rule at the firewall interface. Traffic passing through the interface from hosts with an IP address matching the standard access list and protocol type (HTTP) is intercepted for authentication if no corresponding authentication cache entry exists. If no access list is defined, the authentication proxy intercepts traffic from all hosts whose connection initiating packets are received at the configured interface.

Use the no form of this command with a rule name to disable the authentication proxy for a given rule on a specific interface. If a rule is not specified, the **no** form of this command disables the authentication proxy on the interface.

Examples

The following example configures interface Ethernet0 with the HQ_users rule:

```
interface e0
 ip address 172.21.127.210 255.255.255.0
 ip access-group 111 in
 ip auth-proxy HQ_users
 ip nat inside
```

Related Commands

Command	Description
ip auth-proxy name	Creates an authentication proxy rule.

ip auth-proxy auth-proxy-banner

To display a banner, such as the router name, in the authentication proxy login page, use the **ip auth-proxy auth-proxy-banner** command in global configuration mode. To disable display of the banner, use the **no** form of this command.

ip auth-proxy auth-proxy-banner {**ftp**| **http**| **telnet**} [*banner-text*]

no ip auth-proxy auth-proxy-banner {**ftp**| **http**| **telnet**}

Syntax Description

ftp	Specifies the FTP protocol.
http	Specifies the HTTP protocol.
telnet	Specifies the Telnet protocol.
banner-text	(Optional) Specifies a text string to replace the default banner, which is the name of the router. The text string should be written in the following format: “C banner-text C,” where “C” is a delimiting character.

Command Default

This command is not enabled, and a banner is not displayed on the authentication proxy login page.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.3(1)	The following keywords were added: **ftp**, **http**, and **telnet**.
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 **ip auth-proxy auth-proxy-banner** command allows users to configure one of two possible scenarios:

- The **ip auth-proxy auth-proxy-banner** command is enabled.

In this scenario, the administrator has not supplied any text. Thus, a default banner that states the following: “Cisco Systems, <router’s hostname> Authentication” will be displayed in the authentication proxy login page. This scenario is most commonly used.

- The **ip auth-proxy auth-proxy-banner** command with the *banner-text* argument is enabled.

In this scenario, the administrator can supply multiline text that will be converted to HTML by the auth-proxy parser code. Thus, only the multiline text will displayed in the authentication proxy login page. You will not see the default banner, “Cisco Systems, <router’s hostname> Authentication.”

Note If the **ip auth-proxy auth-proxy-banner** command is not enabled, there will not be any banner configuration. Thus, nothing will be displayed to the user on authentication proxy login page except a text box to enter the username and a text box to enter the password.

Examples

The following example causes the router name to be displayed in the authentication proxy login page:

```
ip auth-proxy auth-proxy-banner ftp
```

The following example shows how to specify the custom banner “whozat” to be displayed in the authentication proxy login page:

```
ip auth-proxy auth-proxy-banner telnet CwhozatC
```

Related Commands

Command	Description
ip auth-proxy name	Creates an authentication proxy rule.

ip auth-proxy max-login-attempts

To limit the number of login attempts at a firewall interface in the interface configuration command mode, use the **ip auth-proxy max-login-attempts** command. Use the **no** form of this command to return to the default settings.

ip auth-proxy max-login-attempts *number*

no ip auth-proxy max-login-attempts

Syntax Description

number	Maximum number of login attempts. The range is 1 to 100. The default value depends on the authentication mechanism: • FTP: 5 • HTTP: 30 • Telnet: 3

Command Default

Enabled

Command Modes

Interface configuration

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.
12.2SE	This command was modified. The maximum number of login attempts was changed to 100.

Usage Guidelines

This command is supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2 only.

This command is supported on the firewall interfaces only.

The maximum login attempt functionality is independent of the watch-list feature (you create a watch list with the **ip access-list hardware permit fragments** command). If you do not configure a watch list, the existing authentication proxy behavior occurs, but it displays the new number for retries. If you configure a watch list, when the maximum is reached, the session is blocked and the IP address is put in the watch list.

Examples

This example shows how to set a limit to the number of login attempts at a firewall interface:

```
Router> enable
Router# configure terminal
Router(config)# interface FastEthernet 0/0
Router(config-if)# ip auth-proxy max-login-attempts 4
Router(config-if)# end
```

Related Commands

Command	Description
clear ip auth-proxy watch-list	Deletes a single watch-list entry or all watch-list entries.
ip auth-proxy watch-list	Enables and configures an authentication proxy watch list.
show ip auth-proxy watch-list	Displays the information about the authentication proxy watch list.

ip auth-proxy name

To create an authentication proxy rule, use the **ip auth-proxy name**command in global configuration mode. To remove the authentication proxy rules, use the **no** form of this command.

Cisco IOS 12.4(6)T and Later Releases

ip auth-proxy name *auth-proxy-name* {**ftp| http| telnet**} [**event timeout aaa policy identity** *id-policy-name*] [**absolute-timer** *timeout*] [**auth-cache-time** *timeout*] [**inactivity-time** *timeout*] [**list** {*list-num* [**service-policy type tag** *policy-name*]| *std-list-num*| *list-name*}] [**service-policy type tag** *service-policy-name*]

no ip auth-proxy name *auth-proxy-name* {**ftp| http| telnet**}

Cisco IOS Release 12.2(33)SRA, 12.2SX, and Later Releases

ip auth-proxy name *auth-proxy-name* {**ftp| http| telnet**} [**event timeout aaa policy identity** *id-policy-name*] [**absolute-timer** *timeout*] [**auth-cache-time** *timeout*] [**inactivity-time** *timeout*] [**list** {*list-num*| *std-list-num*| *list-name*}]

no ip auth-proxy name *auth-proxy-name* {**ftp| http| telnet**}

Syntax Description

auth-proxy-name	A name of up to 16 alphanumeric characters to be associated with an authentication proxy rule.
ftp	Specifies FTP to trigger the authentication proxy.
http	Specifies HTTP to trigger the authentication proxy.
telnet	Specifies Telnet to trigger the authentication proxy.
event timeout aaa policy identity *id-policy-name*	(Optional) Specifies the event to be associated with the policy, timeout of the based event, AAA fail policy to be applied, Identity fail policy to be applied, and Identity policy name.
absolute-timer *timeout*	(Optional) Specifies a window in which the authentication proxy on the enabled interface is active. Enter a value in the range 0 to 35791 minutes. The default value is 0 minutes.
auth-cache-time *timeout*	(Optional) Alias of inactivity timeout in minutes. Enter a value in the range 1 to 35791 minutes.

inactivity-time *min*	(Optional) Overrides the global authentication proxy cache timer for a specific authentication proxy name, offering more control over timeout values. Enter a value in the range 1 to 35791 minutes. The default value is equal to the value set with the ip auth-proxy command. **Note** This option deprecates the **auth-cache-time** *timeout*option.
list {*list-num* | *std-list-num* | *list-name*	(Optional) Specifies a standard (1 to 99), extended (1 to 199), or named IP access list to use with the authentication proxy. With this option, the authentication proxy is applied only to those hosts in the access list. If no list is specified, all connections initiating HTTP, FTP, or Telnet traffic arriving at the interface are subject to authentication.
service-policy type tag	(Optional) A control plane service policy is to be configured.
service-policy-name	(Optional) Control plane tag service policy that is configured using the **policy-map type control tag** *policy-map-name* command. This policy map is used to apply the actions on the host when a tag is received.

Command Default

The default value is equal to the value set with the **ip auth-proxy auth-cache-time** command.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.2	Support for named and extend access lists was introduced.
12.3(1)	The following keywords were introduced: • **ftp** • **telnet** • **inactivity-time** *timeout* • **absolute-timer** *timeout*
12.4(6)T	The **service-policy type tag** keywords and *service-policy-name*argumentwere added.

Release	Modification
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.
15.0(1)M	This command was modified in a release earlier than Cisco IOS Release 15.0(1)M. The **event**, **timeout**, **aaa**, **policy**, **identity**keywords and the *id-policy-name*argument were added.

Usage Guidelines

This command creates a named authentication proxy rule, and it allows you to associate that rule with an access control list (ACL), providing control over which hosts use the authentication proxy. The rule is applied to an interface on a router using the **ip auth-proxy**command.

Use the **inactivity-time** *timeout*option to override the global the authentication proxy cache timer. This option provides control over timeout values for specific authentication proxy rules. The authentication proxy cache timer monitors the length of time (in minutes) that an authentication cache entry, along with its associated dynamic user access control list, is managed after a period of inactivity. When that period of inactivity (idle time) expires, the authentication entry and the associated dynamic access lists are deleted.

Use the **list** option to associate a set of specific IP addresses or a named ACL with the **ip auth-proxy name**command.

Use the **no** form of this command with a rule name to remove the authentication proxy rules. If no rule is specified, the **no** form of this command removes all the authentication rules on the router, and disables the proxy at all interfaces.

Note You must use the **aaa authorization auth-proxy** command with the **ip auth-proxy name**command. Together these commands set up the authorization policy to be retrieved by the firewall. Refer to the **aaa authorization auth-proxy** command for more information.

Examples

The following example shows how to create the HQ_users authentication proxy rule. Because an access list is not specified in the rule, all connection-initiating HTTP traffic is subjected to authentication.

```
ip auth-proxy name HQ_users http
```

The following example shows how to create the Mfg_users authentication proxy rule and apply it to hosts specified in ACL 10:

```
access-list 10 192.168.7.0 0.0.0.255
ip auth-proxy name Mfg_users http list 10
```

The following example shows how to set the timeout value for Mfg_users to 30 minutes:

```
access-list 15 any
ip auth-proxy name Mfg_users http inactivity-timer 30 list 15
```

The following example shows how to disable the Mfg_users rule:

```
no ip auth-proxy name Mfg_users
```

The following example shows how to disable the authentication proxy at all interfaces and remove all the rules from the router configuration:

```
no ip auth-proxy xyz ftp
```

Related Commands

Command	Description
aaa authorization	Sets parameters that restrict network access to a user.
ip auth-proxy (global)	Sets the authentication proxy idle timeout value (that is, 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)	Applies an authentication proxy rule at a firewall interface.
show ip auth-proxy configuration	Displays the authentication proxy entries or the running authentication proxy configuration.

ip auth-proxy watch-list

To enable and configure an authentication proxy watch list in the interface configuration command mode, use the **ip auth-proxy watch-list** command. To disable the watch-list functionality, remove an IP address from the watch list. Or, to return to the default setting, use the **no** form of this command.

ip auth-proxy watch-list {**add-item** *ip-addr*| **enable**| **expiry-time** *minutes*}

no ip auth-proxy watch-list [**add-item** *ip-addr*| **expiry-time**]

Syntax Description

add-item *ip-addr*	Adds an IP address to the watch list.
enable	Enables a watch list.
expiry-time *minutes*	Specifies the duration of time that an entry is in the watch list; see the "Usage Guidelines" section for valid values.

Command Default

The defaults are as follows:

- *minutes* is **30** minutes.
- The watch-list functionality is disabled.

Command Modes

Interface configuration

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 supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2 only.

The valid values for minutes are from 0 to the largest 32-bit positive number (0x7FFFFFFF or 2147483647 in decimal). Setting the *minutes* to 0 (zero) places the entries in the list permanently.

This command is supported on the firewall interfaces only.

Use the **no** form of this command to do the following:

- **no ip auth-proxy watch-list** --Disables the watch-list functionality .
- no **ip auth-proxy watch-list add-item** *ip-addr*--Removes the IP address from the watch list.

- **no ip auth-proxy watch-list expiry-time** --Returns to the default setting.

A watch list consists of IP addresses that have opened TCP connections to port 80 and have not sent any data. No new connections are accepted from this type of IP address (to port 80) and the packet is dropped.

An entry remains in the watch list for the time that is specified by **expiry-time** *minutes*.

When you disable a watch list, no new entries are put into the watch list, but the sessions are put in SERVICE_DENIED state. The timer deletes sessions after 2 minutes.

Examples

This example shows how to enable an authentication proxy watch list:

```
Router(config-if)# ip auth-proxy watch-list enable
Router(config-if)#
```

This example shows how to disable an authentication proxy watch list:

```
Router(config-if)# no ip auth-proxy watch-list
Router(config-if)#
```

This example shows how to add an IP address to a watch list:

```
Router(config-if)# ip auth-proxy watch-list add-item 10.0.0.2
Router(config-if)#
```

This example shows how to set the duration of time that an entry is in a watch list:

```
Router(config-if)# ip auth-proxy watch-list expiry-time 29
Router(config-if)#
```

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.
show ip auth-proxy watch-list	Displays the information about the authentication proxy watch list.

ip device tracking probe

To enable the tracking of device probes, use the **ip device tracking probe** command in configuration mode. To disable device probes, use the **no** form of this command.

ip device tracking probe {**count** *count*| **delay** *delay*| **interval** *interval*}

Syntax Description

count *count*	Specifies the number of IP tracking probes from 1 to 5.
delay *delay*	Specifies the delay time of IP tracking probes from 1 to 120 seconds.
interval *interval*	Specifies the time between IP tracking probes from 30 to 300 minutes.

Command Default

Device probe tracking is disabled.

Command Modes

Config mode (config #)

Command History

Release	Modification
12.2(33)SXI7	This command was introduced.

Examples

The following example shows how to set the probe count to 5:

```
Router(config)# ip device tracking probe count 5
```

The following example shows how to set the delay time to 60:

```
Router(config)# ip device tracking probe delay 60
```

The following example shows how to set the interval time to 35:

```
Router(config)# ip device tracking probe interval 35
```

Related Commands

Command	Description
show ip device tracking	Displays information about entries in the IP device tracking table.

ip dhcp client broadcast-flag (interface)

To configure a DHCP client to set or clear the broadcast flag, use the **ip dhcp client broadcast-flag** command in interface configuration mode. To disable the configuration, use the **no** form of this command.

ip dhcp client broadcast-flag {**clear**| **set**}

no ip dhcp client broadcast-flag

Syntax Description

clear	Clears the broadcast flag.
set	Sets the broadcast flag.

Command Default

The broadcast flag is set.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.1(3)T	This command was introduced.

Usage Guidelines

For a DHCP server to work on a Dynamic Multipoint VPN (DMVPN) network, the DHCP client available on the spoke must unicast the DHCP messages from the server to the client. By default, the DHCP client on the spoke broadcasts the DHCP messages. The broadcast flag is set during broadcast. Hence, the DHCP client on the spoke must have an option to clear the DHCP broadcast flag. You can use the **ip dhcp client broadcast-flag** command to configure the DHCP client to set or clear the broadcast flag.

Examples

The following example shows how to configure a DHCP client to clear the broadcast flag:

```
Router(config)# tunnel 1
Router(config-if)# ip dhcp client broadcast-flag clear
```

Related Commands

Command	Description
ip address dhcp	Acquires an IP address on an interface from the DHCP.
ip dhcp support tunnel unicast	Configures a spoke-to-hub tunnel to unicast the DHCP replies over the DMVPN network.

ip dhcp support tunnel unicast

To configure a spoke-to-hub tunnel to unicast DHCP replies over a Dynamic Multipoint VPN (DMVPN) network, use the **ip dhcp support tunnel unicast** command in global configuration mode. To disable the configuration, use the **no** form of this command.

ip dhcp support tunnel unicast

no ip dhcp support tunnel unicast

Syntax Description

This command has no arguments or keywords.

Command Default

A spoke-to-hub tunnel broadcasts the replies over the DMVPN network.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(3)T	This command was introduced.

Usage Guidelines

By default, the DHCP replies are broadcast from the DMVPN hub to the spoke. The DHCP relay agent must unicast the DHCP messages for a DHCP server to be functional in the DMVPN environment. Hence for the DHCP to be functional in DMVPN environment, you must configure the DHCP relay agent to unicast the DHCP messages.

Use the **ip dhcp support tunnel unicast** command to configure the DHCP relay agent to unicast the DHCP protocol messages from the server (hub) to the client (spoke). The relay agent uses the nonbroadcast multiaccess (NBMA) address to create temporary routes in Next Hop Resolution Protocol (NHRP) to help unicast the DHCPOFFER and DHCPACK messages to the spoke.

Examples

The following example shows how to configure a spoke-to-hub tunnel to unicast the replies over a DMVPN network:

```
Router(config)# ip dhcp support tunnel unicast
```

Related Commands

Command	Description
ip address dhcp	Configures an IP address on an interface acquired through DHCP.
ip dhcp client broadcast-flag	Configures the DHCP client to set or clear the broadcast flag.

ip-extension

To specify that IP extensions are included in a certificate request either for enrollment or generation of a certificate authority (CA) certificate for the Cisco IOS CA, use the **ip-extension** command in ca-trustpoint configuration mode. To remove a previously specified IP extension, use the **no** form of this command.

ip-extension [**multicast**| **unicast**] {**inherit** [**ipv4**| **ipv6**]| **prefix** *ipaddress*| **range** *min-ipaddress max-ipaddress*}

no ip-extension [**multicast**| **unicast**] {**inherit** [**ipv4**| **ipv6**]| **prefix** *ipaddress*| **range** *min-ipaddress max-ipaddress*}

Syntax Description

multicast	(Optional) Specifies that only multicast traffic, a subsequent address family identifier (SAFI), will be included in certificate requests. **Note** If neither multicast nor unicast traffic is specified, both will be included in a certificate request.
unicast	(Optional) Specifies that only unicast traffic, a SAFI, will be included in certificate requests. **Note** If neither multicast nor unicast traffic is specified, both will be included in a certificate request.
inherit	Specifies that IP addresses will be inherited from an issuer certificate. The issuer's certificate is first checked to find a certificate containing the address range or prefix. If no match is found, the certificate from the next issuer in the chain is checked, and so forth, up the certificate chain, recursively, until a match is located.
ipv4	(Optional) Specifies that only IPv4 addresses are inherited. **Note** If neither an **ipv4** nor an **ipv6** address is specified, both address families are inherited.
ipv6	(Optional) Specifies that only IPv6 addresses are inherited. **Note** If neither an **ipv4** nor an **ipv6** address is specified, both address families are inherited.

prefix *ipaddress*	Specifies the IP address prefix or a single IP address for either an IPv4 or IPv6 address. The IP address formats are: • A.B.C.D IPv4 address • A.B.C.D/nn IPv4 prefix • X:X:X:X::X IPv6 address • X:X:X:X::X/<0-128> IPv6 prefix
range	Specifies that there is a range of IP addresses.
min-ipaddress	The beginning IP address in the IP address range, in either IPv4 or IPv6 address format. The IP address formats are: • A.B.C.D Beginning IPv4 address in the range • X:X:X:X::X Beginning IPv6 address in the range
max-ipaddress	The ending IP address in the IP address range, in either IPv4 or IPv6 address format. The IP address formats are: • A.B.C.D Ending IPv4 address in the range • X:X:X:X::X Ending IPv6 address in the range

Command Default

No IP extensions will be included in a certificate request.

Command Modes

Ca-trustpoint configuration (ca-trustpoint)

Command History

Release	Modification
12.4(22)T	This command was introduced.
12.4(24)T	Support for IPv6 Secure Neighbor Discovery (SeND) was added.

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.

The **ip-extension** command may be used to specify IP extensions for a public key infrastructure (PKI) server or client and may be issued one or more times, including multiple issuances with the **inherit**, **prefix**, and **range**keywords. For the inherit option, if the address family is not specified, both IPv4 and IPv6 addresses will be inherited. When the IPv4 or IPv6 address family is not specified for prefix or range, the address family will be determined from the address format.

Note It is recommended that you validate each **ip-extension** command line against your existing IP-extension configuration according to RFC 3779, verifying that IP address ranges do not overlap. The issue's certificate may not be available to validate the issuer's certificate for subsets of addresses.

Examples

The following example shows how to specify that multiple IP extensions are included in the server certificate request:

```
Router(ca-trustpoint)# ip-extension multicast prefix 10.64.0.0/11
! Only multicast traffic with the IPv4 prefix 10.64.0.0/11 will be included in certificate
 requests.
```

Router(ca-trustpoint)# **ip-extension prefix 2001:100:1::/48**

! Multicast and unicast traffic with the IPv6 prefix 2001:100:1::/48 will be included in certificate requests.

Router(ca-trustpoint)# **ip-extension inherit**

! Multicast and unicast traffic with IPv4 and IPv6 addresses will be inherited from the issuer's certificate.

Router(ca-trustpoint)# **ip-extension inherit ipv6**

! Multicast and unicast traffic with IPv6 addresses only will be inherited from the issuer's certificate.

Router(ca-trustpoint)# **ip-extension unicast range 209.165.200.225 143.255.55.255**

```
! Unicast traffic within the specified IPv4 address range will be included in the certificate
 request.
Router(ca-trustpoint)# ip-extension range 2001:1:1::1 2001:1:2:ffff:ffff:ffff:ffff:ffff
! Multicast and unicast traffic within the specified IPv6 address range will be included
in the certificate request.
```

The following is sample output from the **show crypto pki certificates verbose** command. The output displays X.509 certificate IP address extension information where the IPv4 multicast prefix has been set to 10.64.0.0/11, and the IPv4 unicast range has been set to 209.165.201.1 209.165.201.30.

```
CA Certificate
   Status: Available
   Version: 3
   Certificate Serial Number (hex): 01
   Certificate Usage: Signature
   Issuer:
     cn=srtr1
   Subject:
```

```
  cn=srtr1
Validity Date:
  start date: 21:50:11 PST Sep 29 2008
  end   date: 21:50:11 PST Sep 29 2011
Subject Key Info:
  Public Key Algorithm: rsaEncryption
  RSA Public Key: (1024 bit)
Signature Algorithm: MD5 with RSA Encryption
Fingerprint MD5: 30C1C9B6 BC17815F DF6095CD EDE2A5F3
Fingerprint SHA1: A67C451E 49E94E87 8EB0F71D 5BE642CF C68901EF
X509v3 extensions:
  X509v3 Key Usage: 86000000
    Digital Signature
    Key Cert Sign
    CRL Signature
  X509v3 Subject Key ID: B593E52F F711094F 1CCAA4AE 683049AE 4ACE8E8C
  X509v3 Basic Constraints:
      CA: TRUE
  X509v3 Authority Key ID: B593E52F F711094F 1CCAA4AE 683049AE 4ACE8E8C
  Authority Info Access:
  X509v3 IP Extension:
      IPv4 (Unicast):
        209.165.202.129-209.165.202.158
      IPv4 (Multicast):
        10.64.0.0/11
Associated Trustpoints: srtr1
```

Related Commands

Command	Description
show crypto pki certificates	Displays information about the CA certificate.
show crypto pki trustpoints	Displays information about trustpoints that are configured on the router.

ip http ezvpn

To enable the Cisco Easy VPN remote web server interface, use the **ip http ezvpn** command in global configuration mode. To disable the Cisco Easy VPN remote web server interface, use the **no** form of this command.

Cisco uBR905 and Cisco BR925 cable access routers

ip http ezvpn

no ip http ezvpn

Syntax Description

This command has no arguments or keywords.

Command Default

The Cisco Easy VPN Remote web server interface is disabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(8)YJ	This command was introduced for the Cisco uBR905 and Cisco uBR925 cable access routers.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)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.

Usage Guidelines

This command enables the Cisco Easy VPN Remote web server, an onboard web server that allows users to connect an IPSec Easy VPN tunnel and to provide the required authentication information. The Cisco Easy VPN Remote web server allows the user to perform these functions without having to use the Cisco command-line interface (CLI).

Before using this command, you must first enable the Cisco web server that is onboard the cable access router by entering the **ip http server** command. Then use the **ip http ezvpn** command to enable the Cisco Easy VPN remote web server. You can then access the web server by entering the IP address for the Ethernet interface of the router in your web browser.

Note The Cisco Easy VPN Remote web interface does not work with the cable monitor web interface in Cisco IOS Release 12.2(8)YJ. To access the cable monitor web interface, you must first disable the Cisco Easy VPN remote web interface with the **no ip http ezvpn** command, and then enable the cable monitor with the **ip http cable-monitor** command.

Examples

The following example shows how to enable the Cisco Easy VPN remote web server interface:

```
Router# configure terminal
Router(config)# ip http server
Router(config)# ip http ezvpn
Router(config)# exit
Router# copy running-config startup-config
```

Related Commands

Command	Description
ip http cable-monitor	Enables and disables the Cable Monitor Web Server feature.
ip http port	Configures the TCP port number for the HTTP web server of the router.
ip http server	Enables and disables the HTTP web server of the router.

ip inspect through ip security strip

ip inspect

To apply a set of inspection rules to an interface, use the ip inspect command in interface configuration mode. There are two different modes for this command, configuration mode and interface configuration mode. To remove the set of rules from the interface, use the **no** form of this command.

Global Configuation Mode

ip inspect *inspection-name* {**in**| **out**} [**redundancy**| **stateful hsrp-group-name**| **update seconds***seconds*]

no ip inspect *inspection-name* {**in**| **out**} [**redundancy**| **stateful hsrp-group-name**| **update seconds***seconds*]

Interface Configuration Mode

ip inspect *inspection-name* {**in**| **out**} [**redundancy**| **stateful hsrp-group-name**]

no ip inspect *inspection-name* {**in**| **out**} [**redundancy**| **stateful hsrp-group-name**]

Syntax Description

Interface Configuration Mode	
inspection-name	Identifies which set of inspection rules to apply.
in	Applies the inspection rules to inbound interface.
out	Applies the inspection rules to outbound interface.
redunancy	Enables reduncany.
stateful	Enables stateful redundancy.
hsrp-group-name	The hsrp-group name that is used to configure box-to-box HA
Global Configuration Mode	
redundancy	Redundancy settings for firewall sessions
update	Update settings for firewall HA sessions
seconds <*10-60*>	The time interval between consecutive updates. The default is 10 seconds.

Command Default

If no set of inspection rules is applied to an interface, no traffic will be inspected by CBAC. If **redundancy stateful <hsrp-grp-name>** is not used, there will be no stateful firewall high-availability.

Command Modes

Interface configuration mode(conf-if)

Command History

Release	Modification
11.2	This command was introduced.
12.4(6)T	Added support for **redunancy, update**, **seconds**, and **stateful** keywords.
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 apply a set of inspection rules to an interface.

Typically, if the interface connects to the external network, you apply the inspection rules to outbound traffic; alternately, if the interface connects to the internal network, you apply the inspection rules to inbound traffic.

In the Interface Configuration mode, use **ip inspect<name> in/out redundancy stateful <hsrp-group>**command. Use the redundancy stateful <hsrp-grp> option to turn on stateful high availability for all session that come up on this inspect rule. The incoming IP traffic is the return traffic of an existing session. It not necessary to have redundancy stateful HSRP group name if you do not require IOS Firewall High availability.

In the Global Configuration mode, use **ip inspect redundancy update seconds <10-60>**. Use the redundancy update seconds option to configure the time interval between the synchronization of the active and standby firewall HA sessions.

Examples

The following example applies a set of inspection rules named MY-INSPECT_RULE to serial0 interface's outbound traffic. This causes the inbound IP traffic to be permitted only if the traffic is part of an existing session, and to be denied if the traffic is not part of an existing session.

```
interface serial0
ip inspect MY-INSPECT_RULE out redundancy stateful B2B-HA-HSRP-GRP
```

Related Commands

Command	Description
ip inspect name	Defines a set of inspection rules.

ip inspect alert-off

To disable Context-based Access Control (CBAC) alert messages, which are displayed on the console, use the **ip inspect alert-off**command in global configuration mode. To enable CBAC alert messages, use the **no** form of this command.

ip inspect alert-off [**vrf** *vrf-name*]

no ip inspect alert-off [**vrf** *vrf-name*]

Syntax Description

vrf *vrf-name*	(Optional) Disables CBAC alert messages only for the specified Virtual Routing and Forwarding (VRF) interface.

Command Default

Alert messages are displayed.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.3(14)T	The **vrf** *vrf-name*keyword/argument pair 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.

Examples

The following example disables CBAC alert messages:

```
ip inspect alert-off
```

ip inspect audit-trail

To turn on Context-based Access Control (CBAC) audit trail messages, which will be displayed on the console after each CBAC session closes, use the **ip inspect audit-trail** command in global configuration mode. To turn off CBAC audit trail messages, use the **no** form of this command.

ip inspect audit-trail [**vrf** *vrf-name*]

no ip inspect audit-trail [**vrf** *vrf-name*]

Syntax Description

vrf *vrf-name*	(Optional) Turns on CBAC audit trail messages only for the specified Virtual Routing and Forwarding (VRF) interface.

Command Default

Audit trail messages are not displayed.

Command Modes

Global configuration

Command History

Release	Modification
11.2 P	This command was introduced.
12.3(14)T	The **vrf** *vrf-name*keyword/argument pair 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.

Usage Guidelines

Use this command to turn on CBAC audit trail messages.

Examples

The following example turns on CBAC audit trail messages:

```
ip inspect audit-trail
```

Afterward, audit trail messages such as the following are displayed. These messages are examples of audit trail messages. To determine which protocol was inspected, see the port number of the responder. The port number follows the IP address of the responder.

```
%FW-6-SESS_AUDIT_TRAIL: tcp session initiator (192.168.1.13:33192) sent 22 bytes -- responder
 (192.168.129.11:25) sent 208 bytes
```

```
%FW-6-SESS_AUDIT_TRAIL: ftp session initiator 192.168.1.13:33194) sent 336 bytes -- responder
 (192.168.129.11:21) sent 325 bytes
```

The following example disables CBAC audit trail messages for VRF interface vrf1:

```
no ip inspect audit-trail vrf vrf1
```

Following are examples of audit trail messages:

```
00:10:15: %FW-6-SESS_AUDIT_TRAIL: VRF-vrf1:Stop udp session: initiator (192.168.14.1:40801)
 sent 54 bytes -- responder (192.168.114.1:7) sent 54 bytes
00:10:47: %FW-6-SESS_AUDIT_TRAIL: VRF-vrf1:Stop ftp-data session: initiator (192.168.114.1:20)
 sent 80000 bytes -- responder (192.168.14.1:38766) sent 0 bytes
00:10:47: %FW-6-SESS_AUDIT_TRAIL: VRF-vrf1:Stop ftp session: initiator (192.168.14.1:38765)
 sent 80 bytes -- responder (192.168.114.1:21) sent 265 bytes
00:10:57: %FW-6-SESS_AUDIT_TRAIL: VRF-vrf1:Stop rcmd session: initiator (192.168.14.1:531)
 sent 31 bytes -- responder (192.168.114.1:514) sent 12 bytes
00:10:57: %FW-6-SESS_AUDIT_TRAIL: VRF-vrf1:Stop rcmd-data session: initiator
(192.168.114.1:594) sent 0 bytes -- responder (192.168.14.1:530) sent 0 bytes
```

ip inspect dns-timeout

To specify the Domain Name System (DNS) idle timeout (the length of time during which a DNS name lookup session will still be managed while there is no activity), use the **ip inspect dns-timeout**command in global configuration mode. To reset the timeout to the default of 5 seconds, use the **no** form of this command.

ip inspect dns-timeout *seconds* [**vrf** *vrf-name*]

no ip inspect dns-timeout *seconds* [**vrf** *vrf-name*]

Syntax Description

seconds	Specifies the length of time in seconds, for which a DNS name lookup session will still be managed while there is no activity. The default is 5 seconds.
vrf *vrf-name*	(Optional) Specifies the DNS idle timeout only for the specified Virtual Routing and Forwarding (VRF) interface.

Command Default

5 seconds

Command Modes

Global configuration

Command History

Release	Modification
11.2 P	This command was introduced.
12.3(14)T	The **vrf** *vrf-name*keyword/argument pair 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.

Usage Guidelines

When the software detects a valid User Datagram Protocol (UDP) packet for a new DNS name lookup session, if Context-based Access Control (CBAC) inspection is configured for UDP, the software establishes state information for the new DNS session.

If the software detects no packets for the DNS session for a time period defined by the DNS idle timeout, the software will not continue to manage state information for the session.

The DNS idle timeout applies to all DNS name lookup sessions inspected by CBAC.

The DNS idle timeout value overrides the global UDP timeout. The DNS idle timeout value also enters aggressive mode and overrides any timeouts specified for specific interfaces when you define a set of inspection rules with the **ip inspect name** command.

Examples

The following example sets the DNS idle timeout to 30 seconds:

```
ip inspect dns-timeout 30
```

The following example sets the DNS idle timeout back to the default (5 seconds):

```
no ip inspect dns-timeout
```

ip inspect hashtable

To change the size of the session hash table, use the **ip inspect hashtable** command in global configuration mode. To restore the size of the session hash table to the default, use the **no** form of this command.

ip inspect hashtable *number*

no ip inspect hashtable *number*

Syntax Description

number	Size of the hash table in terms of buckets. Possible values for the hash table are 1024, 2048, 4096, and 8192; the default value is 1024.

Command Default

1024 buckets

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

Use the **ip inspect hashtable** command to increase the size of the hash table when the number of concurrent sessions increases or to reduce the search time for the session. Collisions in a hash table result in poor hash function distribution because many entries are hashed into the same bucket for certain patterns of addresses. Even if a hash function distribution evenly dispenses the input across all of the buckets, a small hash table size will not scale well if there are a large number of sessions. As the number of sessions increase, the collisions increase, which increases the length of the linked lists, thereby, deteriorating the throughput performance.

Note You should increase the hash table size when the total number of sessions running through the context-based access control (CBAC) router is approximately twice the current hash size; decrease the hash table size when the total number of sessions is reduced to approximately half the current hash size. Essentially, try to maintain a 1:1 ratio between the number of sessions and the size of the hash table.

Examples

The following example shows how to change the size of the session hash table to 2048 buckets:

```
ip inspect hashtable 2048
```

ip inspect L2-transparent dhcp-passthrough

To allow a transparent firewall to forward Dynamic Host Control Protocol (DHCP) pass-through traffic, use the **ip inspect L2-transparent dhcp-passthrough**command in global configuration mode. To return to the default functionality, use the **no** form of this command.

ip inspect L2-transparent dhcp-passthrough

no ip inspect L2-transparent dhcp-passthrough

Syntax Description

This command has no arguments or keywords.

Command Default

This command is not enabled; thus, DHCP packets are forwarded or denied according to the configured access control list (ACL).

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

A transparent firewall allows a Cisco IOS Firewall (a Layer 3 device) to operate as a Layer 2 firewall in bridging mode. Thus, the firewall can exist “transparently” to a network, no longer requiring users to reconfigure their statically defined network devices.

The **ip inspect L2-transparent dhcp-passthrough** command overrides the ACL for DHCP packets; that is, DHCP packets are forwarded even if the ACL is configured to deny all IP packets. Thus, this command can be used to enable a transparent firewall to forward DHCP packets across the bridge without inspection so clients on one side of the bridge can get an IP address from a DHCP server on the opposite side of the bridge.

Examples

Examples

In this example, the static IP address of the client is removed, and the address is acquired via DHCP using the **ip address dhcp** command on the interface that is connected to the transparent firewall.

```
Router# show debug
ARP:
  ARP packet debugging is on
L2 Inspection:
  INSPECT L2 firewall debugging is on
  INSPECT L2 firewall DHCP debugging is on
Router#
Router#
! Configure DHCP passthrough
Router(config)# ip insp L2-transparent dhcp-passthrough
! The DHCP discover broadcast packet arrives from the client. Since this packet is a !
broadcast (255.255.255.255), it arrives in the flood path
```

```
*Mar  1 00:35:01.299:L2FW:insp_l2_flood:input is Ethernet0 output is Ethernet1
*Mar  1 00:35:01.299:L2FW*:Src 0.0.0.0 dst 255.255.255.255 protocol udp
*Mar  1 00:35:01.299:L2FW:udp ports src 68 dst 67
*Mar  1 00:35:01.299:L2FW:src 0.0.0.0 dst 255.255.255.255
! The DHCP pass through flag is checked and the packet is allowed
*Mar  1 00:35:01.299:L2FW:DHCP packet seen. Pass-through flag allows the packet
! The packet is a broadcast packet and therefore not sent to CBAC
*Mar  1 00:35:01.299:L2FW*:Packet is broadcast or multicast.PASS
! The DHCP server 97.0.0.23 responds to the client's request
*Mar  1 00:35:01.303:L2FW:insp_l2_flood:input is Ethernet1 output is Ethernet0
*Mar  1 00:35:01.303:L2FW*:Src 172.16.0.23 dst 255.255.255.255 protocol udp
*Mar  1 00:35:01.307:L2FW:udp ports src 67 dst 68
*Mar  1 00:35:01.307:L2FW:src 172.16.0.23 dst 255.255.255.255
*Mar  1 00:35:01.307:L2FW:DHCP packet seen. Pass-through flag allows the packet
*Mar  1 00:35:01.307:L2FW*:Packet is broadcast or multicast.PASS
*Mar  1 00:35:01.311:L2FW:insp_l2_flood:input is Ethernet0 output is Ethernet1
*Mar  1 00:35:01.311:L2FW*:Src 0.0.0.0 dst 255.255.255.255 protocol udp
*Mar  1 00:35:01.311:L2FW:udp ports src 68 dst 67
*Mar  1 00:35:01.311:L2FW:src 0.0.0.0 dst 255.255.255.255
*Mar  1 00:35:01.315:L2FW:DHCP packet seen. Pass-through flag allows the packet
*Mar  1 00:35:01.315:L2FW*:Packet is broadcast or multicast.PASS
*Mar  1 00:35:01.315:L2FW:insp_l2_flood:input is Ethernet1 output is Ethernet0
*Mar  1 00:35:01.323:L2FW*:Src 172.16.0.23 dst 255.255.255.255 protocol udp
*Mar  1 00:35:01.323:L2FW:udp ports src 67 dst 68
*Mar  1 00:35:01.323:L2FW:src 172.16.0.23 dst 255.255.255.255
*Mar  1 00:35:01.323:L2FW:DHCP packet seen. Pass-through flag allows the packet
*Mar  1 00:35:01.323:L2FW*:Packet is broadcast or multicast.PASS
! The client has an IP address (172.16.0.5) and has issued a G-ARP to let everyone know it's
 address
*Mar  1 00:35:01.327:IP ARP:rcvd rep src 172.16.0.5 0008.a3b6.b603, dst 172.16.0.5 BVI1
Router#
```

Examples

In this example, DHCP pass-through traffic is not allowed (via the **no ip inspect L2-transparent dhcp-passthrough**command). The client is denied when it attempts to acquire a DHCP address from the server.

```
! Deny DHCP pass-through traffic
Router(config)# no ip inspect L2-transparent dhcp-passthrough
```

```
! The DHCP discover broadcast packet arrives from the client
*Mar  1 00:36:40.003:L2FW:insp_l2_flood:input is Ethernet0 output is Ethernet1
*Mar  1 00:36:40.003:L2FW*:Src 0.0.0.0 dst 255.255.255.255 protocol udp
*Mar  1 00:36:40.003:L2FW:udp ports src 68 dst 67
*Mar  1 00:36:40.007:L2FW:src 0.0.0.0 dst 255.255.255.255
! The pass-through flag is checked
*Mar  1 00:36:40.007:L2FW:DHCP packet seen. Pass-through flag denies the packet
! The packet is dropped because the flag does not allow DHCP passthrough traffic. Thus, !
the client cannot acquire an address, and it times out
*Mar  1 00:36:40.007:L2FW:FLOOD Dropping the packet after ACL check.
```

Related Commands

Command	Description
debug ip inspect L2-transparent	Enables debugging messages for transparent firewall events.
show ip inspect	Displays Cisco IOS Firewall configuration and session information.

ip inspect log drop-pkt

To log all packets dropped by the firewall, use the **ip inspect log drop-pkt** command in global configuration mode. To return to the default state, use the **no** form of this command.

ip inspect log drop-pkt

no ip inspect log drop-pkt

Syntax Description

This command has no arguments or keywords.

Command Default

Packets dropped by the firewall are not logged.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(7)T1	This command was introduced.
12.3(8)T	This command was integrated into Release 12.3(8)T.

Usage Guidelines

To see the packets that are dropped by the firewall, the ip inspect log drop-pkt command must be enabled.

Examples

The following example shows how to enable the logging of packets dropped by the firewall:

```
Router> enable
Router# configure terminal
Router(config
)# ip inspect log drop-pkt
```

The following example shows a possible message that can be displayed when packets are dropped:

```
*Sep 9 19:56:28.699: %FW-6-DROP_PKT: Dropping tcp pkt 17.2.2.1:0 => 19.2.2.1:0 with ip ident
 229 due to Invalid Header length
*Sep 9 20:30:47.839: %FW-6-DROP_TCP_PKT: Dropping tcp pkt 17.2.2.1:42829 => 19.2.2.1:80 due
 to SYN pkt with illegal flags -- ip ident 23915 tcpflags 40962 seq.no 3928613134 ack 0
*Sep 10 00:30:24.931: %FW-6-DROP_TCP_PKT: Dropping tcp pkt 17.2.2.1:45771 =>
19.2.2.1:80 due to SYN with data or with PSH/URG flags -- ip ident 55001 tcpflags 40962
seq.no 2232798685 ack 0
*Aug 29 21:57:16.895: %FW-6-DROP_PKT: Dropping tcp pkt 17.2.2.1:51613 => 19.2.2.1:80 due
to Out-Of-Order Segment
```

The table below describes messages that occur when packets are dropped.

Table 8: ip inspect log drop-pkt Messages

Field	Description
Invalid Header length	The datagram is so small that it could not contain the layer 4 TCP, Universal Computer Protocol (UCP), or Internet Control Message Protocol (ICMP) header.
Police rate limiting	Rate limiting is enabled, and the packet in question has exceeded the rate limit.
Session limiting	Session limiting is on, and the session count exceeds the configured session threshold.
Bidirectional traffic disabled	Session is unidirectional and the firewall is seeing packets in the other direction and dropping the session.
SYN with data or with PSH/URG flags	TCP SYN packet is seen with data.
Segment matching no TCP connection	Non-initial TCP segment is received without a valid session.
Invalid Segment	There is an invalid TCP segment.
Invalid Seq#	The packet contains an invalid TCP sequence number.
Invalid Ack (or no Ack)	The packet contains an invalid TCP acknowledgement number.
Invalid Flags	Flags in a TCP segment are invalid.
Invalid Checksum	There is an invalid TCP checksum.
SYN inside current window	A synchronization packet is seen within the window of an already established TCP connection.
RST inside current window	A reset (RST) packet is observed within the window of an already established TCP connection.
Out-Of-Order Segment	The packets in a segment are out of order.
Retransmitted Segment with Invalid Flags	A retransmitted packet was already acknowledged by the receiver.
Stray Segment	A TCP segment is received that should not have been received through the TCP state machine such as a TCP SYN packet being received in the listen state.
Internal Error	The TCP state machine that is maintained by the firewall encounters an internal error.

Field	Description
Invalid Window scale option	The responder on one side of a firewall proposes an illegal window scale option. The window scale option is illegal in this case because the initiating side did not propose the option first.
Invalid TCP options	The options in the TCP header are not TCP protocol compliant.

Related Commands

Command	Description
ip inspect tcp block-non-session	Blocks packets that do not belong to the existing firewall TCP sessions in the inbound and outbound directions.
ip inspect tcp finwait-time	Defines how long a TCP session will still be managed after the firewall detects a FIN-exchange.
ip inspect tcp idle-time	Specifies the TCP idle timeout (the length of time a TCP session will still be managed while there is no activity).
ip inspect tcp max-incomplete host	Specifies threshold and blocking time values for TCP host-specific DoS detection and prevention.
ip inspect tcp reassembly	Sets parameters that define how Cisco IOS Firewall application inspection and Cisco IOS IPS will handle out-of-order TCP packets.
ip inspect tcp synwait-time	Defines how long the software will wait for a TCP session to reach the established state before dropping the session.
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).

ip inspect max-incomplete high

To define the number of existing half-open sessions that will cause the software to start deleting half-open sessions, use the **ip inspect max-incomplete high**command in global configuration mode. To reset the threshold to the default of 500 half-open sessions, use the **no** form of this command.

ip inspect max-incomplete high *number* [**vrf** *vrf-name*]

no ip inspect max-incomplete high

Syntax Description

number	Specifies the number of existing half-open sessions that will cause the software to start deleting half-open sessions . The default is 500 half-open sessions.
vrf *vrf-name*	(Optional) Defines the number of existing half-open sessions only for the specified Virtual Routing and Forwarding (VRF) interface.

Command Default

500 half-open sessions

Command Modes

Global configuration

Command History

Release	Modification
11.2 P	This command was introduced.
12.3(14)T	The **vrf** *vrf-name*keyword/argument pair 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.

Usage Guidelines

An unusually high number of half-open sessions (either absolute or measured as the arrival rate) could indicate that a denial-of-service attack is occurring. For TCP, “half-open” means that the session has not reached the established state. For User Datagram Protocol (UDP), “half-open” means that the firewall has detected traffic from one direction only.

Context-based Access Control (CBAC) measures both the total number of existing half-open sessions and the rate of session establishment attempts. Both TCP and UDP half-open sessions are counted in the total number and rate measurements. Measurements are made once a minute.

When the number of existing half-open sessions rises above a threshold (the **max-incomplete high** number), the software will delete half-open sessions as required to accommodate new connection requests. The software will continue to delete half-open requests as necessary, until the number of existing half-open sessions drops below another threshold (the **max-incomplete low** number).

The global value specified for this threshold applies to all TCP and UDP connections inspected by CBAC.

Examples

The following example causes the software to start deleting half-open sessions when the number of existing half-open sessions rises above 900, and to stop deleting half-open sessions when the number drops below 800:

```
ip inspect max-incomplete high 900
ip inspect max-incomplete low 800
```

The following example shows an ALERT_ON message generated for the **ip inspect max-incomplete high** command:

```
ip inspect max-incomplete high 20 vrf vrf1
show log / include ALERT_ON
00:59:00:%FW-4-ALERT_ON: VRF-vrf1:getting aggressive, count (21/20) current 1-min rate: 21
```

Related Commands

Command	Description
ip inspect max-incomplete low	Defines the number of existing half-open sessions that will cause the software to stop deleting half-open sessions.
ip inspect one-minute high	Defines the rate of new unestablished sessions that will cause the software to start deleting half-open sessions.
ip inspect one-minute low	Defines the rate of new unestablished TCP sessions that will cause the software to stop deleting half-open sessions.
ip inspect tcp max-incomplete host	Specifies the threshold and blocking time values for TCP host-specific DoS detection and prevention.

ip inspect max-incomplete low

To define the number of existing half-open sessions that will cause the software to stop deleting half-open sessions, use the **ip inspect max-incomplete low**command in global configuration mode. To reset the threshold to the default of 400 half-open sessions, use the **no** form of this command.

ip inspect max-incomplete low *number* [**vrf** *vrf-name*]

no ip inspect max-incomplete low

Syntax Description

number	Specifies the number of existing half-open sessions that will cause the software to stop deleting half-open sessions . The default is 400 half-open sessions.
vrf *vrf-name*	(Optional) Defines the number of existing half-open sessions only for the specified Virtual Routing and Forwarding (VRF) interface.

Command Default

400 half-open sessions

Command Modes

Global configuration

Command History

Release	Modification
11.2 P	This command was introduced.
12.3(14)T	The **vrf** *vrf-name*keyword/argument pair 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.

Usage Guidelines

An unusually high number of half-open sessions (either absolute or measured as the arrival rate) could indicate that a denial-of-service attack is occurring. For TCP, “half-open” means that the session has not reached the established state. For User Datagram Protocol (UDP), “half-open” means that the firewall has detected traffic from one direction only.

Context-based Access Control (CBAC) measures both the total number of existing half-open sessions and the rate of session establishment attempts. Both TCP and UDP half-open sessions are counted in the total number and rate measurements. Measurements are made once a minute.

When the number of existing half-open sessions rises above a threshold (the **max-incomplete high** number), the software will delete half-open sessions as required to accommodate new connection requests. The software will continue to delete half-open requests as necessary, until the number of existing half-open sessions drops below another threshold (the **max-incomplete low** number).

The global value specified for this threshold applies to all TCP and UDP connections inspected by CBAC.

Examples

The following example causes the software to start deleting half-open sessions when the number of existing half-open sessions rises above 900, and to stop deleting half-open sessions when the number drops below 800:

```
ip inspect max-incomplete high 900
ip inspect max-incomplete low 800
```

The following example shows an ALERT_OFF message generated for the **ip inspect max-incomplete low**command:

```
ip inspect max-incomplete low 10 vrf vrf1
show log / include ALERT_OFF
00:59:31: %FW-4-ALERT_OFF: VRF-vrf1:calming down, count (9/10) current 1-min rate: 100
```

Related Commands

Command	Description
ip inspect max-incomplete high	Defines the number of existing half-open sessions that will cause the software to start deleting half-open sessions.
ip inspect one-minute high	Defines the rate of new unestablished sessions that will cause the software to start deleting half-open sessions.
ip inspect one-minute low	Defines the rate of new unestablished TCP sessions that will cause the software to stop deleting half-open sessions.
ip inspect tcp max-incomplete host	Specifies the threshold and blocking time values for TCP host-specific DoS detection and prevention.

ip inspect name

To define a set of inspection rules, use the **ip inspect name**command in global configuration mode. To remove the inspection rule for a protocol or to remove the entire set of inspection rules, use the **no** form of this command.

ip inspect name *inspection-name* [**parameter max-sessions** *number*] *protocol* [**alert** {**on**| **off**}] [**audit-trail** {**on**| **off**}] [**timeout** *seconds*]

no ip inspect name *inspection-name* [**parameter max-sessions** *number*] *protocol* [**alert** {**on**| **off**}] [**audit-trail** {**on**| **off**}] [**timeout** *seconds*]

HTTP Inspection Syntax

ip inspect name *inspection-name* **http** [**java-list** *access-list*] **[urlfilter]** [**alert** {**on**| **off**}] [**audit-trail** {**on**| **off**}] [**timeout** *seconds*]

no ip inspect name *inspection-name protocol*

Simple Mail Transfer Protocol (SMTP) and Extended SMTP Inspection (ESMTP) Syntax

ip inspect name *inspection-name* {**smtp**| **esmtp**} [**alert** {**on**| **off**}] [**audit-trail** {**on**| **off**}] [**max-data** *number*] [**timeout** *seconds*]

remote-procedure call (RPC) Inspection Syntax

ip inspect name *inspection-name* [**parameter max-sessions** *number*] **rpc program-number** *number* [**wait-time** *minutes*] [**alert** {**on**| **off**}] [**audit-trail** {**on**| **off**}] [**timeout** *seconds*]

no ip inspect name *inspection-name protocol*

Post Office Protocol 3(POP3)/ Internet Message Access Protocol(IMAP) Inspection Syntax

ip inspect name *inspection-name* **imap** [**alert** {**on**| **off**}] [**audit-trail** {**on**| **off**}] **[reset]** **[secure-login]** [**timeout** *number*]

ip inspect name *inspection-name* **pop3** [**alert** {**on**| **off**}] [**audit-trail** {**on**| **off**}] **[reset]** **[secure-login]** [**timeout** *number*]

Fragment Inspection Syntax

ip inspect name *inspection-name* [**parameter max-sessions** *number*] **fragment** [**max** *number* **timeout** *seconds*]

no ip inspect name *inspection-name* [**parameter max-sessions** *number*] **fragment** [**max** *number* **timeout** *seconds*]

Application Firewall Provisioning Syntax

ip inspect name *inspection-name* [**parameter max-sessions** *number*] **appfw** *policy-name*

no ip inspect name *inspection-name* [**parameter max-sessions** *number*] **appfw** *policy-name*

User-Defined Application Syntax

ip inspect *inspection-name user-10* [**alert** {**on**| **off**}] [**audit-trail** {**on**| **off**}] [**timeout** *seconds*]

noip inspect *inspection-name user-10* [**alert** {**on**| **off**}] [**audit-trail** {**on**| **off**}] [**timeout** *seconds*]

Session Limiting Syntax

no ip inspect name *inspection-name* [**parameter max-sessions** *number*]

Syntax Description

inspection-name	N ame the set of inspection rules. If you want to add a protocol to an existing set of rules, use the same *inspection-name* as the existing set of rules. **Note** The *inspection-name* cannot exceed 16 characters; otherwise, the name will be truncated to the 16-character limit.
parameter max-sessions *number*	(Optional) Limits the number of established firewall sessions that a firewall rule creates. By default, there is no limit to the number of firewall sessions.
protocol	A protocol keyword listed in the tables below.
alert {**on** | **off**}	(Optional) For each inspected protocol, the generation of alert messages can be set be **on** or **off**. If no option is selected, alerts are generated on the basis of the setting of the **ip inspect alert-off** command.
audit-trail {**on** | **off**}	(Optional) For each inspected protocol, **audit trail**can be set **on** or **off**. If no option is selected, an audit trail message is generated depending on the configuration of the **ip inspect audit-trail**command.
timeout *seconds*	(Optional) To override the global TCP or UDP, or Internet Control Message Protocol (ICMP) idle timeouts for the specified protocol, specify the number of seconds for a different idle timeout. This timeout overrides the global TCP, UDP, or ICMP timeouts but will not override the global Domain Name System (DNS) timeout.
http	Specifies the HTTP protocol for Java applet blocking.
java-list *access-list*	(Optional) Specifies the numbered standard access list to use to determine "friendly" sites. This keyword is available only for the HTTP protocol, for Java applet blocking. Java blocking works only with numbered standard access lists.

urlfilter	(Optional) Associates URL filtering with HTTP inspection.
smtp | **esmtp**	Specifies the protocol being used to inspect the traffic.
max-data *number*	(Optional) Specifies the maximum amount of data, in bytes,that can be transferred in a single Simple Mail Transport Protocol (SMTP) session. After the maximum value is exceeded, the firewall logs an alert message and closes the session. The default value is 20MB.
rpc program-number *number*	Specifies the program number to permit. This keyword is available only for the remote-procedure call (RPC) protocol.
wait-time *minutes*	(Optional) Specifies the number of minutes to keep a small gap in the firewall to allow subsequent connections from the same source address and to the same destination address and port. The default wait-time is zero minutes. This keyword is available only for the RPC protocol.
imap	Specifies that the Internet Message Access Protocol (IMAP) is being used.
reset	(Optional) Resets the TCP connection if the client enters a nonprotocol command before authentication is complete.
secure-login	(Optional) Causes a user at a nonsecure location to use encryption for authentication.
pop3	Specifies that the Post Office Protocol, Version 3 (POP3) is being used.
fragment	Specifies fragment inspection for the named rule.
max *number*	(Optional) Specifies the maximum number of unassembled packets for which state information (structures) is allocated by Cisco IOS software. Unassembled packets are packets that arrive at the router interface before the initial packet for a session. The acceptable range is 50 through 10000. The default is 256 state entries. • Memory is allocated for the state structures, and setting this value to a larger number may cause memory resources to be exhausted.

timeout *seconds* (fragmentation)	(Optional) Configures the number of seconds that a packet state structure remains active. When the timeout value expires, the router drops the unassembled packet, freeing that structure for use by another packet. The default timeout value is 1 second. • If this number is set to a value greater that 1 second, it is automatically adjusted by the Cisco IOS software when the number of free state structures goes below certain thresholds: when the number of free states is fewer than 32, the timeout is divided by 2. When the number of free states is fewer than 16, the timeout is set to 1 second.
appfw	Specifies application firewall provisioning.
policy-name	Application firewall policy name. **Note** This name must match the name specified via the **appfw policy-name** command.

Command Default

No inspection rules are defined.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.2P	This command was introduced.
12.0(5)T	This command was modified. Support was added for configurable alert and audit trail, IP fragmentation checking, and NetShow protocol.
12.2(11)YU	This command was modified. Support was added for ICMP and Session Initiation Protocol (SIP) protocols. The urlfilter keyword was added to the HTTP inspection syntax.
12.2(15)T	This command was modified. Support was added for ICMP, SIP, and the urlfilter keyword was added.
12.3(1)	This command was modified. Skinny protocol support was added.
12.3(7)T	This command was modified. Extended Simple Mail Transfer Protocol (ESMTP) protocol support was added.

Release	Modification
12.3(14)T	This command was modified.The **appfw** keyword and the *policy-name* argument were added to support application firewall provisioning. The **parameter max-sessions**, **reset**, **router-traffic,**and **secure-login**, and keywordswere added. Support for a larger list of protocols including user-defined applications 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.
15.1(1)T	This command was modified. Support for the CU-SeeMe protocol and the **cuseeme** keyword was removed.

Usage Guidelines

To define a set of inspection rules, enter the **ip inspect name**command for each protocol that you want the Cisco IOS firewall to inspect, using the same *inspection-name*. Give each set of inspection rules a unique *inspection-name*, which should not exceed the 16-character length limit. Define either one or two sets of rules per interface--you can define one set to examine both inbound and outbound traffic, or you can define two sets: one for outbound traffic and one for inbound traffic. The **no ip inspect-name** *protocol* removes the inspection rule for the specified protocol.

no ip inspect name command removes the entire set of inspection rules.

To define a single set of inspection rules, configure inspection for all the desired application-layer protocols, and for ICMP, TCP, and UDP, or as desired. This combination of TCP, UDP, and application-layer protocols join together to form a single set of inspection rules with a unique name. (There are no application-layer protocols associated with ICMP.)

To remove the inspection rule for a protocol, use the **no** form of this command with the specified inspection name and protocol; To remove the entire set of inspection rules, use the **no** form of this command only; that is, do not list any inspection names or protocols.

In general, when inspection is configured for a protocol, return traffic entering the internal network will be permitted only if the packets are part of a valid, existing session for which state information is being maintained.

Table 9: Protocol Keywords--Transport-Layer and Network-Layer Protocols

Protocol	Keyword
ICMP	icmp
TCP	**tcp**
UDP	**udp**

Note The TCP, UDP, and H.323 protocols support the **router-traffic** keyword, which enables inspection of traffic destined to or originated from a router. The command format is as follows: **ip inspect name** *inspection-nam*e {**tcp** | **udp** | **H323**} [**alert** {**on** | **off**}] [**audit-trail** {**on** | **off**}] [**router-traffic**][**timeout** *seconds*]

TCP and UDP Inspection

You can configure TCP and UDP inspection to permit TCP and UDP packets to enter the internal network through the firewall, even if the application-layer protocol is not configured to be inspected. However, TCP and UDP inspection do not recognize application-specific commands, and therefore might not permit all return packets for an application, particularly if the return packets have a different port number from the previous exiting packet.

Any application-layer protocol that is inspected will take precedence over the TCP or UDP packet inspection. For example, if inspection is configured for FTP, all control channel information will be recorded in the state table, and all FTP traffic will be permitted back through the firewall if the control channel information is valid for the state of the FTP session. The fact that TCP inspection is configured is irrelevant.

With TCP and UDP inspection, packets entering the network must exactly match an existing session. The entering packets must have the same source or destination addresses and source or destination port numbers as the exiting packet (but reversed). Otherwise, the entering packets will be blocked at the interface.

Granular protocol inspection allows you to specify TCP or UDP ports by using the port-to-application mapping (PAM) table. This eliminates having to inspect all applications running under TCP or UDP and the need for multiple ACLs to filter the traffic.

Using the PAM table, you can pick an existing application or define a new one for inspection, thereby simplifying Access Control List (ACL) configuration.

ICMP Inspection

ICMP inspection sessions are done on the basis of the source address of the inside host that originates the ICMP packet. Dynamic ACLs are created for return ICMP packets of the allowed types (echo-reply,destination unreachable, time-exceeded, and timestamp reply) for each session. No port numbers associated with an ICMP session, and the permitted IP address of the return packet is a wild-card in the ACL. The wildcard address is because the IP address of the return packet cannot be known in advance for time-exceeded and destination-unreachable replies. These replies can come from intermediate devices rather than the intended destination.

Application-Layer Protocol Inspection

In general, if you configure inspection for an application-layer protocol, packets for that protocol should be permitted to exit the firewall (by configuring the correct ACL), and packets for that protocol will be allowed back in through the firewall only if they belong to a valid existing session. Each protocol packet is inspected to maintain information about the session state.

Java, H.323, RPC, SIP, and SMTP inspection have additional information, described in the next five sections. The table below lists the supported application-layer protocols.

Table 10: Protocol Keywords--Application-Layer Protocols

Protocol	Keyword
Application Firewall	**appfw**

Protocol	Keyword
CU-SeeMe	**cuseeme**
ESMTP	**smtp**
FTP	**ftp**
IMAP	**imap**
Java	**http**
H.323	**h323**
Microsoft NetShow	**netshow**
POP3	**pop3**
RealAudio	**realaudio**
RPC	**rpc**
SIP	**sip**
Simple Mail Transfer Protocol (SMTP)	**smtp**
Skinny Client Control Protocol (SCCP)	**skinny**
StreamWorks	**streamworks**
Structured Query Language*Net (SQL*Net)	**sqlnet**
TFTP	**tftp**
UNIX R commands (rlogin, rexec, rsh)	**rcmd**
VDOLive	**vdolive**
WORD	**user-defined application name** ; **use prefix -user** **Note** All applications that appear under the **show ip port-map** command are supported.

Java Inspection

Java inspection enables Java applet filtering at the firewall. Java applet filtering distinguishes between trusted and untrusted applets by relying on a list of external sites that you designate as "friendly." If an applet is from a friendly site, the firewall allows the applet through. If the applet is not from a friendly site, the applet will be blocked. Alternately, you could permit applets from all sites except sites specifically designated as "hostile."

Note Before you configure Java inspection, you must configure a numbered standard access list that defines "friendly" and "hostile" external sites. You configure this numbered standard access list to permit traffic from friendly sites, and to deny traffic from hostile sites. If you do not configure a numbered standard access list, but use a "placeholder" access list in the **ip inspect name** *inspection-name* **http** command, all Java applets will be blocked.

Note Java blocking forces a strict order on TCP packets. To properly verify that Java applets are not in the response, a firewall will drop any TCP packet that is out of order. Because the network--not the firewall--determines how packets are routed, the firewall cannot control the order of the packets; the firewall can only drop and retransmit all TCP packets that are not in order.

Caution Context-Based Access Control (CBAC) does not detect or block encapsulated Java applets. Therefore, Java applets that are wrapped or encapsulated, such as applets in .zip or .jar format, are *not* blocked at the firewall. CBAC also does not detect or block applets loaded via FTP, gopher, or HTTP on a nonstandard port.

H.323 Inspection

If you want CBAC inspection to work with NetMeeting 2.0 traffic (an H.323 application-layer protocol), you must also configure inspection for TCP, as described in the chapter "Configuring Context-Based Access Control" in the *Cisco IOS Security Configuration Guide* . This requirement exists because NetMeeting 2.0 uses an additional TCP channel not defined in the H.323 specification.

RPC Inspection

RPC inspection allows the specification of various program numbers. You can define multiple program numbers by creating multiple entries for RPC inspection, each with a different program number. If a program number is specified, all traffic for that program number will be permitted. If a program number is not specified, all traffic for that program number will be blocked. For example, if you created an RPC entry with the NFS program number, all NFS traffic will be allowed through the firewall.

SIP Inspection

You can configure SIP inspection to permit media sessions associated with SIP-signaled calls to traverse the firewall. Because SIP is frequently used to signal both incoming and outgoing calls, it is often necessary to configure SIP inspection in both directions on a firewall (both from the protected internal network and from the external network). Because inspection of traffic from the external network is not done with most protocols, it may be necessary to create an additional inspection rule to cause only SIP inspection to be performed on traffic coming from the external network.

SMTP Inspection

SMTP inspection causes SMTP commands to be inspected for illegal commands. Packets with illegal commands are modified to a "xxxx" pattern and forwarded to the server. This process causes the server to send a negative reply, forcing the client to issue a valid command. An illegal SMTP command is any command except the following:

- DATA
- HELO

- HELP
- MAIL
- NOOP
- QUIT
- RCPT
- RSET
- SAML
- SEND
- SOML
- VRFY

ESMTP Inspection

Like SMTP, ESMTP inspection also causes the commands to be inspected for illegal commands. Packets with illegal commands are modified to a "xxxx" pattern and forwarded to the server. This process causes the server to send a negative reply, forcing the client to issue a valid command. An illegal ESMTP command is any command except the following:

- AUTH
- DATA
- EHLO
- ETRN
- HELO
- HELP
- MAIL
- NOOP
- QUIT
- RCPT
- RSET
- SAML
- SEND
- SOML
- VRFY

In addition to inspecting commands, the ESMTP firewall also inspects the following extensions via deeper command inspection:

- Message Size Declaration (SIZE)
- Remote Queue Processing Declaration (ETRN)

- Binary MIME (BINARYMIME)
- Command Pipelining
- Authentication
- Delivery Status Notification (DSN)
- Enhanced Status Code (ENHANCEDSTATUSCODE)
- 8bit-MIMEtransport (8BITMIME)

Note SMTP and ESMTP cannot exist simultaneously. An attempt to configure both protocols will result in an error message.

Use of the urlfilter Keyword

If you specify the **urlfilter** keyword, the Cisco IOS Firewall will interact with a URL filtering software to control web traffic for a given host or user on the basis of a specified security policy.

Note Enabling HTTP inspection with or without any option triggers the Java applet scanner, which is CPU intensive. The only way to stop the Java applet scanner is to specify the **java-list** *access-list* option. Configuring URL filtering without enabling the **java-list** *access-list*option will severely impact performance.

Use of the timeout Keyword

If you specify a timeout for any of the transport-layer or application-layer protocols, the timeout will override the global idle timeout for the interface to which the set of inspection rules is applied.

If the protocol is TCP or a TCP application-layer protocol, the timeout will override the global TCP idle timeout. If the protocol is UDP or a UDP application-layer protocol, the timeout will override the global UDP idle timeout.

If you do not specify a timeout for a protocol, the timeout value applied to a new session of that protocol will be taken from the corresponding TCP or UDP global timeout value valid at the time of session creation.

The default ICMP timeout is deliberately short (10 seconds) due to the security hole that is opened by allowing ICMP packets with a wild-card source address back into the inside network. The timeout will occur 10 seconds after the last outgoing packet from the originating host. For example, if you send a set of 10 ping packets spaced one second apart, the timeout will expire in 20 seconds or 10 seconds after the last outgoing packet. However, the timeout is not extended for return packets. If a return packet is not seen within the timeout window, the gap will be closed and the return packet will not be allowed in. Although the default timeout can be made longer if desired, it is recommended that this value be kept relatively short.

IP Fragmentation Inspection

CBAC inspection rules can help protect hosts against certain denial-of-service attacks involving fragmented IP packets. Even though the firewall keeps an attacker from making actual connections to a given host, the attacker may still be able to disrupt services provided by that host. This is done by sending many noninitial IP fragments or by sending complete fragmented packets through a router with an ACL that filters the first fragment of a fragmented packet. These fragments can tie up resources on the target host as it tries to reassemble the incomplete packets.

Using fragmentation inspection, the firewall maintains an *interfragment state* (structure) for IP traffic. Noninitial fragments are discarded unless the corresponding initial fragment was permitted to pass through the firewall. Noninitial fragments received before the corresponding initial fragments are discarded.

Note Fragmentation inspection can have undesirable effects in certain cases, because it can result in the firewall discarding any packet whose fragments arrive out of order. There are many circumstances that can cause out-of-order delivery of legitimate fragments. Apply fragmentation inspection in situations where legitimate fragments, which are likely to arrive out of order, might have a severe performance impact.

Because routers running Cisco IOS software are used in a very large variety of networks, and because the CBAC feature is often used to isolate parts of internal networks from one another, the fragmentation inspection feature is not enabled by default. Fragmentation detection must be explicitly enabled for an inspection rule using the **ip inspect name** command. Unfragmented traffic is never discarded because it lacks a fragment state. Even when the system is under heavy attack with fragmented packets, legitimate fragmented traffic, if any, will still get some fraction of the firewall's fragment state resources, and legitimate, unfragmented traffic can flow through the firewall unimpeded.

Application Firewall Provisioning

Application firewall provisioning allows you to configure your Cisco IOS Firewall to detect and prohibit a specific protocol type of traffic.

Most firewalls provide packet filtering capabilities that simply permit or deny traffic without inspecting the data stream; the Cisco IOS application firewall can detect whether a packet is in compliance with a given HTTP protocol. If the packet is determined to be unauthorized, it will be dropped, the connection will be reset, and a syslog message will be generated, as appropriate.

User-Defined Applications

You can define your own applications and enter them into the PAM table using the **ip port-map** command. Then you set up your inspection rules by inserting your user-defined application as a value for the *protocol* argument in the **ip inspect name** command.

Session Limiting

Users can limit the number of established firewall sessions that a firewall rule creates by setting the "max-sessions" threshold. A session counter is maintained for each firewall interface. When a session count exceeds the specified threshold, an alert FW-4-SESSION_THRESHOLD_EXCEEDED message is logged to the syslog server and no new sessions can be created.

Examples

The following example causes the software to inspect TCP sessions and UDP sessions, and to specifically allow CU-SeeMe, FTP, and RPC traffic back through the firewall for existing sessions only. For UDP traffic, audit-trail is on. For FTP traffic, the idle timeout is set to override the global TCP idle timeout. For RPC traffic, program numbers 100003, 100005, and 100021 are permitted.

```
ip inspect name myrules tcp
ip inspect name myrules udp audit-trail on
ip inspect name myrules cuseeme
ip inspect name myrules ftp timeout 120
ip inspect name myrules rpc program-number 100003
ip inspect name myrules rpc program-number 100005
ip inspect name myrules rpc program-number 100021
```

The following example adds fragment checking to software inspection of TCP and UDP sessions for the rule named *"myrules*." In this example, the firewall software will allocate 100 state structures, and the timeout value for dropping unassembled packets is set to 4 seconds. If 100 initial fragments for 100 different packets are sent through the router, all of the state structures will be used up. The initial fragment for packet 101 will be dropped. Additionally, if the number of free state structures (structures available for use by unassembled packets) drops below the threshold values, 32 or 16, the timeout value is automatically reduced to 2 or 1, respectively. Changing the timeout value frees up packet state structures more quickly.

```
ip inspect name myrules tcp
ip inspect name myrules udp audit-trail on
ip inspect name myrules cuseeme
ip inspect name myrules ftp timeout 120
ip inspect name myrules rpc program-number 100003
ip inspect name myrules rpc program-number 100005
ip inspect name myrules rpc program-number 100021
ip inspect name myrules fragment max 100 timeout 4
```

The following firewall and SIP example shows how to allow outside-initiated calls and internal calls. For outside-initiated calls, an ACL needs to be accessed to allow for the traffic from the initial signaling packet from outside. Subsequent signaling and media channels will be allowed by the inspection module.

```
ip inspect name voip sip
interface FastEthernet0/0
 ip inspect voip in
!
!
interface FastEthernet0/1
 ip inspect voip in
 ip access-group 100 in
!
!
access-list 100 permit udp host <gw ip> any eq 5060
access-list 100 permit udp host <proxy ip> any eq 5060
access-list deny ip any any
```

The following example shows two configured inspections named fw_only and fw_urlf; URL filtering will work only on the traffic that is inspected by fw_urlf. Note that the **java-list** *access-list*option has been enabled, which disables java scanning.

```
ip inspect name fw_only http java-list 51 timeout 30
interface e0
 ip inspect fw_only in
!
ip inspect name fw_urlf  http java-list 51 urlfilter timeout 30
interface e1
 ip inspect fw_urlf in
```

The following example shows how to define the HTTP application firewall policy mypolicy. This policy includes all supported HTTP policy rules. This example also includes sample output from the **show appfw configuration** and **show ip inspect config** commands, which allow you to verify the configured setting for the application policy.

```
! 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
!
!
! Issue the show appfw configuration
 command and the show ip inspect config
command after the inspection rule "mypolicy" is applied to all incoming HTTP traffic on the
 FastEthernet0/0 interface.
!
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
Router# show ip inspect config

Session audit trail is disabled
Session alert is enabled
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 firewall
http alert is on audit-trail is off timeout 3600
```

Related Commands

Command	Description
ip inspect	Applies a set of inspection rules to an interface.
ip inspect alert-off	Disables CBAC alert messages.
ip inspect audit trail	Turns on CBAC audit trail messages, which will be displayed on the console after each CBAC session close.

ip inspect one-minute high

To define the rate of new unestablished sessions that will cause the software to start deleting half-open sessions, use the **ip inspect one-minute high**command in global configuration mode. To reset the threshold to the default of 500 half-open sessions, use the **no** form of this command.

ip inspect one-minute high *number* [**vrf** *vrf-name*]

no ip inspect one-minute high

Syntax Description

number	Specifies the rate of new unestablished TCP sessions that will cause the software to start deleting half-open sessions . The default is 500 half-open sessions.
vrf *vrf-name*	(Optional) Defines the information only for the specified Virtual Routing and Forwarding (VRF) interface.

Command Default

500 half-open sessions

Command Modes

Global configuration

Command History

Release	Modification
11.2 P	This command was introduced.
12.3(14)T	The **vrf** *vrf-name*keyword/argument pair 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.

Usage Guidelines

An unusually high number of half-open sessions (either absolute or measured as the arrival rate) could indicate that a denial-of-service attack is occurring. For TCP, “half-open” means that the session has not reached the established state. For User Datagram Protocol (UDP), “half-open” means that the firewall has detected traffic from one direction only.

Context-based Access Control (CBAC) measures both the total number of existing half-open sessions and the rate of session establishment attempts. Both TCP and UDP half-open sessions are included in the total number and rate measurements. Measurements are made once a minute.

When the rate of new connection attempts rises above a threshold (the **one-minute high** number), the software will delete half-open sessions as required to accommodate new connection attempts. The software will continue to delete half-open sessions as necessary, until the rate of new connection attempts drops below another threshold (the **one-minute low** number). The rate thresholds are measured as the number of new session connection attempts detected in the last one-minute sample period. (The rate is calculated as an exponentially decayed rate.)

The global value specified for this threshold applies to all TCP and UDP connections inspected by CBAC.

Examples

The following example causes the software to start deleting half-open sessions when more than 1000 session establishment attempts have been detected in the last minute, and to stop deleting half-open sessions when fewer than 950 session establishment attempts have been detected in the last minute:

```
ip inspect one-minute high 1000
ip inspect one-minute low 950
```

Related Commands

Command	Description
ip inspect one-minute low	Defines the rate of new unestablished TCP sessions that will cause the software to stop deleting half-open sessions.
ip inspect max-incomplete high	Defines the number of existing half-open sessions that will cause the software to start deleting half-open sessions.
ip inspect max-incomplete low	Defines the number of existing half-open sessions that will cause the software to stop deleting half-open sessions.
ip inspect tcp max-incomplete host	Specifies the threshold and blocking time values for TCP host-specific DoS detection and prevention.

ip inspect one-minute low

To define the rate of new unestablished TCP sessions that will cause the software to stop deleting half-open sessions, use the **ip inspect one-minute low**command in global configuration mode. To reset the threshold to the default of 400 half-open sessions, use the **no** form of this command.

ip inspect one-minute low *number* [**vrf** *vrf-name*]

no ip inspect one-minute low

Syntax Description

number	Specifies the rate of new unestablished TCP sessions that will cause the software to stop deleting half-open sessions . The default is 400 half-open sessions.
vrf *vrf-name*	(Optional) Defines the information only for the specified Virtual Routing and Forwarding (VRF) interface.

Command Default

400 half-open sessions

Command Modes

Global configuration

Command History

Release	Modification
11.2 P	This command was introduced.
12.3(14)T	The **vrf** *vrf-name*keyword/argument pair 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.

Usage Guidelines

An unusually high number of half-open sessions (either absolute or measured as the arrival rate) could indicate that a denial-of-service attack is occurring. For TCP, "half-open" means that the session has not reached the established state. For User Datagram Protocol (UDP), "half-open" means that the firewall has detected traffic from one direction only.

Context-based Access Control (CBAC) measures both the total number of existing half-open sessions and the rate of session establishment attempts. Both TCP and UDP half-open sessions are included in the total number and rate measurements. Measurements are made once a minute.

When the rate of new connection attempts rises above a threshold (the **one-minute high** number), the software will delete half-open sessions as required to accommodate new connection attempts. The software will continue to delete half-open sessions as necessary, until the rate of new connection attempts drops below another threshold (the **one-minute low** number). The rate thresholds are measured as the number of new session connection attempts detected in the last one-minute sample period. (The rate is calculated as an exponentially decayed rate.)

The global value specified for this threshold applies to all TCP and UDP connections inspected by CBAC.

Examples

The following example causes the software to start deleting half-open sessions when more than 1000 session establishment attempts have been detected in the last minute, and to stop deleting half-open sessions when fewer than 950 session establishment attempts have been detected in the last minute:

```
ip inspect one-minute high 1000
ip inspect one-minute low 950
```

Related Commands

Command	Description
ip inspect max-incomplete high	Defines the number of existing half-open sessions that will cause the software to start deleting half-open sessions.
ip inspect max-incomplete low	Defines the number of existing half-open sessions that will cause the software to stop deleting half-open sessions.
ip inspect one-minute high	Defines the rate of new unestablished sessions that will cause the software to start deleting half-open sessions.
ip inspect tcp max-incomplete host	Specifies the threshold and blocking time values for TCP host-specific DoS detection and prevention.

ip inspect tcp block-non-session

To block packets that do not belong to the existing firewall TCP sessions in the inbound and outbound directions, use the **ip inspect tcp block-non-session** command in global configuration mode. To return to the default state, use the **no** form of this command.

ip inspect tcp block-non-session [**vrf vrf-name**]

no inspect tcp block-non-session [**vrf vrf-name**]

Syntax Description

vrf	(Optional) Declares a specific VPN routing/forwarding instance (VRF).
vrf-name	(Optional) Name of the VRF.

Command Default

TCP packets that do not belong to an existing TCP session on the firewall are allowed through the firewall.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(6)	This command was introduced.
12.3(7)T	This command was integrated into Release 12.3(6)T.
12.3(7)XI	This command was integrated into the Release 12.3(7)XI.
12.3(14)T	The vrf keyword and vrf-name argument were added.

Usage Guidelines

This command will deny TCP packets that do not belong to an existing TCP session the firewall knows about. To be applicable, the following conditions must be met:

- The TCP packets should traverse interfaces where a firewall rule is applicable.
- The TCP packets should be non-connection initiating (that is, packets without the SYN bit set in them). For connection initiating packets, the existing rules of session creation would apply.

Examples

The following example shows how to configure the firewall to block any externally initiated TCP sessions:

```
Router> enable
Router# config terminal
```

```
Router(config
)# ip inspect tcp block-non-session
```

Related Commands

Command	Description
ip inspect log drop-pkt	Logs all packets dropped by the firewall.
ip inspect tcp finwait-time	Defines how long a TCP session will still be managed after the firewall detects a FIN-exchange.
ip inspect tcp idle-time	Specifies the TCP idle timeout (the length of time a TCP session will still be managed while there is no activity).
ip inspect tcp max-incomplete host	Specifies threshold and blocking time values for TCP host-specific (DoS) detection and prevention.
ip inspect tcp reassembly	Sets parameters that define how Cisco IOS Firewall application inspection and Cisco IOS IPS will handle out-of-order TCP packets.
ip inspect tcp synwait-time	Defines how long the software will wait for a TCP session to reach the established state before dropping the session.
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).

ip inspect tcp finwait-time

To define how long a TCP session will be managed after the firewall detects a finish (FIN)-exchange, use the **ip inspect tcp finwait-time** command in global configuration mode. To reset the timeout to the default of 5 seconds, use the **no** form of this command.

ip inspect tcp finwait-time *seconds* [**vrf** *vrf-name*]

no ip inspect tcp finwait-time

Syntax Description

seconds	Specifies how long a TCP session will be managed after the firewall detects a FIN-exchange. The default is 5 seconds. Valid values are from 1 to 2147483. If the FIN-exchange completes within the configured finwait time, the connection is closed normally.
vrf *vrf-name*	(Optional) Defines the information only for the specified VPN routing and forwarding (VRF) interface.

Command Default

The default management time is 5 seconds.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.2 P	This command was introduced.
12.3(14)T	This command was modified. The **vrf** *vrf-name* keyword and argument pair 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.

Usage Guidelines

When the software detects a valid TCP packet that is the first in a session, and if Context-Based Access Control (CBAC) inspection is configured for the protocol of the packet, the software establishes state information for the new session.

Use this command to define how long a 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. In a TCP connection, the client and the server terminate their end of the connection by sending a FIN message. The time that the client and the server wait for their FIN message to be acknowledged by each other 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.

The global value specified for the finwait timeout applies to all TCP sessions inspected by CBAC.

Examples

The following example shows how to change the finwait timeout to 10 seconds:

```
ip inspect tcp finwait-time 10
```

The following example shows how to change the finwait timeout back to the default (5 seconds):

```
no ip inspect tcp finwait-time
```

Related Commands

Command	Description
show ip inspect	Displays CBAC configuration and session information.

ip inspect tcp idle-time

To specify the TCP idle timeout (the length of time a TCP session will still be managed while there is no activity), use the **ip inspect tcp idle-time**command in global configuration mode. To reset the timeout to the default of 3600 seconds (1 hour), use the **no** form of this command.

ip inspect tcp idle-time *seconds* [**vrf** *vrf-name*]

no ip inspect tcp idle-time

Syntax Description

seconds	Specifies the length of time, in seconds, for which a TCP session will still be managed while there is no activity. The default is 3600 seconds (1 hour).
vrf *vrf-name*	(Optional) Specifies the TCP idle timer only for the specified Virtual Routing and Forwarding (VRF) interface.

Command Default

3600 seconds (1 hour)

Command Modes

Global configuration

Command History

Release	Modification
11.2 P	This command was introduced.
12.3(14)T	The **vrf** *vrf-name*keyword/argument pair 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.

Usage Guidelines

When the software detects a valid TCP packet that is the first in a session, and if Context-based Access Control (CBAC) inspection is configured for the packet's protocol, 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 continue to manage state information for the session.

The global value specified for this timeout applies to all TCP sessions inspected by CBAC. This global value can be overridden for specific interfaces when you define a set of inspection rules with the **ip inspect name**(global configuration) command.

Note This command does not affect any of the currently defined inspection rules that have explicitly defined timeouts. Sessions created based on these rules still inherit the explicitly defined timeout value. If you change the TCP idle timeout with this command, the new timeout will apply to any new inspection rules you define or to any existing inspection rules that do not have an explicitly defined timeout. That is, new sessions based on these rules (having no explicitly defined timeout) will inherit the global timeout value.

Examples

The following example sets the global TCP idle timeout to 1800 seconds (30 minutes):

```
ip inspect tcp idle-time 1800
```

The following example sets the global TCP idle timeout back to the default of 3600 seconds (one hour):

```
no ip inspect tcp idle-time
```

ip inspect tcp max-incomplete host

To specify threshold and blocking time values for TCP host-specific denial-of-service (DoS) detection and prevention, use the **ip inspect tcp max-incomplete host**command in global configuration mode. To reset the threshold and blocking time to the default values, use the **no** form of this command.

ip inspect tcp max-incomplete host *number* **block-time** *minutes* [**vrf** *vrf-name*]

no ip inspect tcp max-incomplete host

Syntax Description

number	Specifies how many half-open TCP sessions with the same host destination address can exist at a time, before the software starts deleting half-open sessions to the host. Use a number from 1 to 250. The default is 50 half-open sessions.
block-time	Specifies blocking of connection initiation to a host.
minutes	Specifies how long the software will continue to delete new connection requests to the host. The default is 0 minutes.
vrf *vrf-name*	(Optional) Specifies the information only for the specified Virtual Routing and Forwarding (VRF) interface.

Command Default

50 half-open sessions and 0 minutes

Command Modes

Global configuration

Command History

Release	Modification
11.2 P	This command was introduced.
12.3(14)T	The **vrf** *vrf-name*keyword/argument pair 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.

Usage Guidelines

An unusually high number of half-open sessions with the same destination host address could indicate that a denial-of-service attack is being launched against the host. For TCP, “half-open” means that the session has not reached the established state.

Whenever the number of half-open sessions with the same destination host address rises above a threshold (the **max-incomplete host** number), the software will delete half-open sessions according to one of the following methods:

- If the **block-time** *minutes* timeout is 0 (the default):

The software will delete 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 will never exceed the threshold.

- If the **block-time** *minutes* timeout is greater than 0:

The software will delete all existing half-open sessions for the host, and then block all new connection requests to the host. The software will continue to block all new connection requests until the **block-time** expires.

The software also sends syslog messages whenever the **max-incomplete host** number 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 inspected by Context-based Access Control (CBAC).

Examples

The following example changes the max-incomplete host number to 40 half-open sessions, and changes the block-time timeout to 2 minutes:

```
ip inspect tcp max-incomplete host 40 block-time 2
```

The following example resets the defaults (50 half-open sessions and 0 minutes):

```
no ip inspect tcp max-incomplete host
```

Related Commands

Command	Description
ip inspect max-incomplete high	Defines the number of existing half-open sessions that will cause the software to start deleting half-open sessions.
ip inspect max-incomplete low	Defines the number of existing half-open sessions that will cause the software to stop deleting half-open sessions.
ip inspect one-minute high	Defines the rate of new unestablished sessions that will cause the software to start deleting half-open sessions.
ip inspect one-minute low	Defines the rate of new unestablished TCP sessions that will cause the software to stop deleting half-open sessions.

ip inspect tcp reassembly

To set parameters that define how Cisco IOS Firewall application inspection and Cisco IOS Intrusion Prevention System (IPS) will handle out-of-order TCP packets, use the **ip inspect tcp reassembly** command in global configuration mode. To disable at least one defined parameter, use the **no** form of this command.

ip inspect tcp reassembly {**alarm** {**on**| **off**}| **memory limit** *size-in-kb*| **queue length** *number-of-packets*| **timeout** *seconds*} [**vrf** *vrf-name*]

no ip inspect tcp reassembly {**alarm**| **queue length**| **timeout**| **memory limit**} [**vrf** *vrf-name*]

Syntax Description

alarm {**on** | **off**	Specifies the alert message configuration. If enabled, a syslog message is generated when an out-of-order packet is dropped. Default value: **on**
memory	Specifies the memory use allowed by the TCP reassembly module.
limit *size-in-kb*	Specifies the limit of out of order queue size.
queue	Specifies the out of order queue parameters.
length *number-of-packets*	Maximum number of out-of-order packets that can be held per queue (buffer). (There are two queues per session.) Available value range: 0 to 1024. Default value: 16. **Note** If the queue length is set to 0, all out-of-order packets are dropped; that is, TCP out-of-order packet buffering and reassembly is disabled.
timeout *seconds*	Number of seconds the TCP reassembly module will hold out-of-order segments that are waiting for the first segment missing in the sequence. After the timeout timer has expired, a retry timer is started. The value for the retry timer is four times the configured timeout value.
vrf *vrf-name*	Specifies the VPN routing and forwarding (VRF) parameter and name.

Command Default

Queue length: 16

Memory Limit: 1024 kilobytes

Alarm: on

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(11)T	This command was introduced.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Usage Guidelines

The queue length Value

The value specified for the queue length is applicable for two queues per session: one queue is for the initiator traffic and the other queue is for the responder traffic. For example, the default queue size is 16. Thus, up to 16 packets can be held per queue, so 16 packets per queue results in a maximum of 32 packets per session.

When the maximum queue length value is reached, the packet being switched is dropped unless it is the packet that will be processed by a firewall or IPS. If the packet is dropped, a syslog message, which explains why the packet was dropped, will be generated. (To generate syslog messages, you must have the alarm option set to "on.")

The timeout Value

When a timer expires for the first time, the packets in the queue are not deleted. However, after the retry timer expires, the session is deleted, a syslog message is generated, and all unprocessed, out-of-order packets still in the queue are deleted.

The memory limit Value

When the limit for TCP reassembly memory is reached, packets from the reassembly queue of the current session are released so incoming packets can be accepted. Packets from the end of the queue are released to ensure that they are farthest away from the hole that is to be filled. However, if the queue is empty and the maximum memory has been reached, the incoming packet is dropped.

The alarm Value

If an alarm value is not configured, the value is set to "on," unless the **ip inspect alarm** command is enabled and set to off; thus, syslog messages related to TCP connections will not be generated. However, if the alarm value for this command is set to "on" and the **ip inspect alarm** command is set to "off," the value of the **ip inspect alarm** command is ignored and syslog messages are generated.

The alarm value is independent of and in addition to the syslog messages that can be enabled for a Cisco IOS Firewall or Cisco IOS IPS.

Examples

The following example shows how to instruct Cisco IOS IPS how to handle out-of-order packets for TCP connections:

```
Router(config)#
ip inspect tcp reassembly queue length 18
Router(config)#
ip inspect tcp reassembly memory limit 200
```

Related Commands

Command	Description
ip inspect tcp block-non-session	Blocks packets that do not belong to the existing firewall TCP sessions in the inbound and outbound directions.

ip inspect tcp synwait-time

To define how long the software will wait for a TCP session to reach the established state before dropping the session, use the **ip inspect tcp synwait-time**command in global configuration mode. To reset the timeout to the default of 30 seconds, use the **no** form of this command.

ip inspect tcp synwait-time *seconds* [**vrf** *vrf-name*]

no ip inspect tcp synwait-time

Syntax Description

seconds	Specifies how long, in seconds, the software will wait for a TCP session to reach the established state before dropping the session . The default is 30 seconds.
vrf *vrf-name*	(Optional) Defines the information only for the specified Virtual Routing and Forwarding (VRF) interface.

Command Default

30 seconds

Command Modes

Global configuration

Command History

Release	Modification
11.2 P	This command was introduced.
12.3(14)T	The **vrf** *vrf-name*keyword/argument pair 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.

Usage Guidelines

Use this command to define how long Cisco IOS software will wait for a TCP session to reach the established state before dropping the session. The session is considered to have reached the established state after the first synchronize sequence number (SYN) bit of the session is detected.

The global value specified for this timeout applies to all TCP sessions inspected by Context-based Access Control (CBAC).

Examples

The following example changes the synwait timeout to 20 seconds:

```
ip inspect tcp synwait-time 20
```

The following example changes the synwait timeout back to the default (30 seconds):

```
no ip inspect tcp synwait-time
```

ip inspect tcp window-scale-enforcement loose

To configure Cisco IOS software to disable the window scale option check for a TCP packet that has an invalid window scale option under the Context-Based Access Control (CBAC) firewall, use the **ip inspect tcp window-scale-enforcement loose** command in global configuration mode. To return to the command default, use the **no** form of this command.

ip inspect tcp window-scale-enforcement loose

no ip inspect tcp window-scale-enforcement loose

Command Default

The strict window scale option check is enabled in the firewall by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(20)T	This command was introduced.

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. Cisco IOS software enforces strict checking of the TCP window scale option. See section 2 of RFC1323, “TCP Window Scale Option,” for more information on this function.

There are occasions when a server may be using a non-RFC compliant TCP/IP protocol stack. In this case, the initiator does not offer the window scale option, but the responder has the option enabled with a window scale factor that is not zero.

Cisco IOS administrators who experience issues with a noncompliant server may not have control over the client to which they need to connect. Disabling the Cisco IOS firewall to connect to the 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.

The **ip inspect tcp window-scale-enforcement loose** command is used in global configuration mode to allow noncompliant window scale negotiation and works without the firewall being disabled to access the noncompliant servers. This command works under the CBAC firewall, which intelligently filters TCP and UDP packets based on application-layer protocol session information. CBAC inspects traffic that travels through the firewall to discover and manage state information for TCP and UDP sessions. CBAC is configured using an inspect rule only on interfaces. This state information is used to create temporary openings in the firewall's access lists to allow return traffic and additional data connections for permissible sessions. Traffic entering or leaving the configured interface is inspected based on the direction that the inspect rule was applied.

Examples

The following example configures the IOS to disable the window scale option check in the CBAC firewall for a TCP packet that has an invalid window scale option:

```
Router# config
Router(config)# ip inspect tcp window-scale-enforcement loose
```

Related Commands

Command	Description
ip inspect tcp synwait-time	Configures the length of time the software waits for a TCP session to reach the established state before dropping the session.

ip inspect udp idle-time

To specify the User Datagram Protocol (UDP) idle timeout (the length of time for which a UDP “session” will still be managed while there is no activity), use the **ip inspect udp idle-time** command in global configuration mode. To reset the timeout to the default of 30 seconds, use the **no** form of this command.

ip inspect udp idle-time *seconds* [**vrf** *vrf-name*]

no ip inspect udp idle-time

Syntax Description

seconds	Specifies the length of time a UDP “session” will still be managed while there is no activity . The default is 30 seconds.
vrf *vrf-name*	(Optional) Specifies the UDP idle timeout only for the specified Virtual Routing and Forwarding (VRF) interface.

Command Default

30 seconds

Command Modes

Global configuration

Command History

Release	Modification
11.2 P	This command was introduced.
12.3(14)T	The **vrf** *vrf-name*keyword/argument pair 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.

Usage Guidelines

When the software detects a valid UDP packet, if Context-based Access Control (CBAC) inspection is configured for the packet’s protocol, the software establishes state information for a new UDP “session.” Because UDP is a connectionless service, there are no actual sessions, so the software approximates sessions by examining the information in the packet and determining 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 a period of time defined by the UDP idle timeout, the software will not continue to manage state information for the session.

The global value specified for this timeout applies to all UDP sessions inspected by CBAC. This global value can be overridden for specific interfaces when you define a set of inspection rules with the **ip inspect name**command.

Note This command does not affect any of the currently defined inspection rules that have explicitly defined timeouts. Sessions created based on these rules still inherit the explicitly defined timeout value. If you change the UDP idle timeout with this command, the new timeout will apply to any new inspection rules you define or to any existing inspection rules that do not have an explicitly defined timeout. That is, new sessions based on these rules (having no explicitly defined timeout) will inherit the global timeout value.

Examples

The following example sets the global UDP idle timeout to 120 seconds (2 minutes):

```
ip inspect udp idle-time 120
```

The following example sets the global UDP idle timeout back to the default of 30 seconds:

```
no ip inspect udp idle-time
```

integrity

To specify one or more integrity algorithms for an Internet Key Exchange Version 2 (IKEv2) proposal, use the **integrity**command in IKEv2 proposal configuration mode. To remove the configuration of the hash algorithm, us e the **no** form of this command.

integrity sha1 sha256 sha384 sha512 md5

no integrity

Syntax Description

sha1	Specifies Secure Hash Algorithm (SHA-1 - HMAC variant) as the hash algorithm.
sha256	Specifies SHA-2 family 256-bit (HMAC variant) as the hash algorithm.
sha384	Specifies SHA-2 family 384-bit (HMAC variant) as the hash algorithm.
sha512	Specifies SHA-2 family 512-bit (HMAC variant) as the hash algorithm.
md5	Specifies Message-Digest algorithm 5 (MD5 - HMAC variant) as the hash algorithm.

Command Default

The default integrity algorithm is used.

Command Modes

IKEv2 proposal configuration (config-ikev2-proposal)

Command History

Release	Modification
15.1(1)T	This command was introduced.
15.1(2)T	This command was modified. The **sha256** and **sha384** keywords were added.
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

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.

Use this command to specify the integrity algorithm to be used in an IKEv2 proposal. The default integrity algorithms in the default proposal are SHA-1 and MD5.

Note You cannot selectively remove an integrity algorithm when multiple integrity algorithms are configured.

Suite-B adds support for the SHA-2 family (HMAC variant) hash algorithm used to authenticate packet data and verify the integrity verification mechanisms for the IKEv2 proposal configuration. HMAC is a variant that provides an additional level of hashing.

Examples

The following example configures an IKEv2 proposal with the MD5 integrity algorithm:

```
Router(config)#
crypto ikev2 proposal proposal1
Router(config-ikev2-proposal)#
integrity md5
```

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 Diffie-Hellman group identifier in an IKEv2 proposal.
show crypto ikev2 proposal	Displays the parameters for each IKEv2 proposal.

ip interface

To configure a virtual gateway IP interface on a Secure Socket Layer Virtual Private Network (SSL VPN) gateway, use the **ip interface** command in webvpn gateway configuration mode. To disable the configuration, use the **no** form of this command.

ip interface *type number* [**port** {**443**| *port-number*}]

no ip interface

Syntax Description

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.
port	(Optional) Configures a specific port on the gateway.
443	(Optional) Configures the default secure port.
port-number	(Optional) Port number to be configured on the SSL VPN gateway. Range: 1025 to 65535. Default: 443.

Command Default

The command is disabled. The virtual gateway IP address is not configured.

Command Modes

Webvpn gateway configuration (config-webvpn-gateway)

Command History

Release	Modification
12.4(24)T	This command was introduced.

Usage Guidelines

The **ip interface** command is used to configure a interface on a SSL VPN gateway. You can use this command to configure the WebVPN gateway to retrieve the IP address from an interface, and if you do not want to configure the IP address manually. This command is useful when the public interface is Dynamic Host Configuration Protocol (DHCP) and you do not know the IP address or when the IP address gets changed.

If the **ip interface** command is not configured then the WebVPN will use the IP address configured using the **ip address** command.

Examples

The following example shows how to configure a virtual gateway IP interface on port 1036 of an SSL VPN gateway:

```
Router# configure terminal
Router(config)# webvpn gateway gateway1
Router(config-webvpn-gateway)# ip interface FastEthernet 0/1 port 1036
```

Related Commands

Command	Description
ip address	Configures a proxy IP address on an SSL VPN gateway.
webvpn gateway	Defines an SSL VPN gateway and enters WebVPN gateway configuration mode.

ip ips

To apply an Intrusion Prevention System (IPS) rule to an interface, use the **ip ips**command in interface configuration mode. To remove an IPS rule from an interface direction, use the **no** form of this command.

ip ips *ips-name* {**in**| **out**}

no ip ips *ips-name* {**in**| **out**}

Syntax Description

ips-name	Name of IPS signature definition file (SDF).
in	Applies IPS to inbound traffic.
out	Applies IPS to outbound traffic.

Command Default

By default, IPS signatures are not applied to an interface or direction.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.3(8)T	The command name was changed from the **ip audit**command to the **ip ips**command.

Usage Guidelines

The **ip ips** command loads the SDF onto the router and builds the signature engines when IPS is applied to the first interface.

Note The router prompt disappears while the signatures are loading and the signature engines are building. It will reappear after these tasks are complete. Depending on your platform and how many signatures are being loaded, building the signature engine can take several of minutes. It is recommended that you enable logging messages so you can monitor the engine building status.

The **ip ips** command replaces the **ip audit** command. If the **ip audit**command is part of an existing configuration, IPS will interpret it as the **ip ips**command.

Examples

The following example shows the basic configuration necessary to load the attack-drop.sdf file onto a router running Cisco IOS IPS. Note that the configuration is almost the same as when you load the default signatures onto a router, except for the **ip ips sdf location** command, which specifies the attack-drop.sdf file.

```
!
ip ips sdf location disk2:attack-drop.sdf
ip ips name MYIPS
!
interface GigabitEthernet0/1
 ip address 10.1.1.16 255.255.255.0
 ip ips MYIPS in
 duplex full
 speed 100
 media-type rj45
 no negotiation auto
!
```

The following example shows how to configure the router to load and merge the attack-drop.sdf file with the default signatures. After you have merged the two files, it is recommended to copy the newly merged signatures to a separate file. The router can then be reloaded (via the reload command) or reinitalized to so as to recognize the newly merged file (as shown the following example)

```
!
ip ips name MYIPS
!
interface GigabitEthernet0/1
 ip address 10.1.1.16 255.255.255.0
 ip ips MYIPS in
 duplex full
 speed 100
 media-type rj45
 no negotiation auto
!
!
! Merge the flash-based SDF (attack-drop.sdf) with the built-in signatures.
copy disk2:attack-drop.sdf ips-sdf
! Save the newly merged signatures to a separate file.
copy ips-sdf disk2:my-signatures.sdf
!
! Configure the router to use the new file, my-signatures.sdf
configure terminal
ip ips sdf location disk2:my-signatures.sdf
! Reinitialize the IPS by removing the IPS rule set and reapplying the rule set.
interface gig 0/1
 no ip ips MYIPS in
!
*Apr 8 14:05:38.243:%IPS-2-DISABLED:IPS removed from all interfaces - IPS disabled
!
 ip ips MYIPS in
!
 exit
```

Related Commands

Command	Description
copy ips-sdf	Loads or saves the SDF in the router.
ip ips sdf location	Specifies the location in which the router should load the SDF.

ip ips auto-update

To enable automatic signature updates for Cisco IOS Intrusion Prevention System (IPS), use the **ip ips auto-update** command in global configuration mode. To revert back to the default value, use the **no** form of this command.

ip ips auto-update

no ip ips auto-update

Syntax Description

This command has no arguments or keywords.

Command Default

The default value is defined in the signature definition XML.

Command Modes

Global configuration (config)

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.

Use the **ip ips auto-update** command to enable Cisco IOS IPS to automatically update the signature file on the system. When enabling automatic signature updates, it is recommended that you ensure the following configuration guidelines have been met:

- The router's clock is set up with the proper relative time.
- The frequency for Cisco IOS IPS to obtain updated signature information has been defined (through the **occur-at** command).
- Automatic signature updates can be enabled from Cisco.com by using the **cisco** command. This command cannot be used in conjunction with the **url** command.
- The URL in which to retrieve the Cisco IOS IPS signature configuration files has been specified (through the **url** command).
- Optionally, the username and password in which to access the files from the server has been specified (through the **username** command). The **username** command would be optional in this case if the username and password command were previously configured through the **ips signature update cisco**command in Priviledged EXEC mode. The user name and password must be configured for updating signatures directly from Cisco.com.

The Default Value

A user or a management station can override the default value through the **category** command or the **signature** command; a value set with either of these commands will be saved as the delta value. The no form of the ip ips auto-update command will remove the delta value and revert back to the default value in the definition XML.

Setting Time for Auto Updates

Cisco IOS time can be updated through the hardware clock or the software configurable clock (which ever option is available on your system). Although Network Time Protocol (NTP) is typically used for automated time synchronization, Cisco IOS IPS updates use the local clock resources as a reference for update intervals. Thus, NTP should be configured to update the local time server of the router, as appropriate.

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 third hour of the 5 day of the month, at the 56th minute of this hour. (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 monthly 5 56 3
Router#
*May 4 2006 15:50:28 MST: IPS Auto Update: setting update timer for next update: 5 days 56
 min 3 hrs
*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) : 56
  hours (0-23) : 3
  days of month (1-31) : 5
  days of week: (0-6) :
```

Related Commands

Command	Description
occur-at	Defines the frequency in which Cisco IOS IPS obtains updated signature information.
cisco	Enables automatic signature updates from Cisco.com.
url (ips-autoupdate)	Defines a location in which to retrieve the Cisco IOS IPS signature configuration files.
username (ips-autoupdate)	Defines a username and password in which to access signature files from the server.

ip ips config location

To specify the location in which the router will save signature information, use the **ip ips config location**command in global configuration mode. To remove the specified location, use the **no** form of this command.

ip ips config location *url*

no ip ips config location

Syntax Description

url	Location where the signature file is saved. Available URL options: • Local flash, such as flash:sig.xml • FTP server, such as ftp://myuser:mypass@ftp_server.sig.xml • rcp, such as rcp://myuser@rcp_server/sig.xml • TFTP server, such as tftp://tftp_server/sig.xml **Note** If the specified location is a URL, such as an FTP server, the user must have writer privileges.

Command Default

No configuration files are saved.

Command Modes

Global configuration

Command History

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

Usage Guidelines

Before configuring the **ip ips config location**command, you must create a directory for the config location via the **mkdir** command.

The **ip ips config location**command configures a Cisco IOS Intrusion Prevention System (IPS) signature location, which tells Cisco IOS IPS where to save signature information.

The configuration location is used to restore the IPS configuration in cases such as router reboots or IPS becoming disabled or reenabled. Files, such as signature definitions, signature-type definitions, and signature category information, are written in XML format, compressed, and saved to the specified IPS signature location.

Note If a location is not specified, or if a location is removed via the **no** form, no files will be saved.

Note The **ip ips config location** command replaces the **ip ips sdf location**command.

Examples

The following example shows how to instruct the router to save all signature information to the directory “flash:/ips5”:

```
Router# mkdir
flash:/ips5
Create directory filename [ips5]?
Created dir flash:/ips5
Router#
Router#
Router#
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ip ips name MYIPS
Router(config)# ip ips config location
flash:/ips5
Router(config)# ip ips signature-category
Router(config-ips-category)# category all
Router(config-ips-category-action)# retired true
Router(config-ips-category-action)# exit
Router(config-ips-category)# category ios_ips advanced
Router(config-ips-category-action)# retired false
Router(config-ips-category-action)# exit

Router(config-ips-category)# exit
Do you want to accept these changes? [confirm]
Router(config)# d
*Nov 14 2006 17:16:42 MST: Applying Category configuration to signatures ..
Router(config)#
```

ip ips deny-action ips-interface

To create an access control list (ACL) filter for the deny actions (“denyFlowInline” and “denyConnectionInline”) on the intrusion prevention system (IPS) interface rather than ingress interface, use the **ip ips deny-action ips-interface**command in global configuration mode. To return to the default, use the **no** form of this command.

ip ips deny-action ips-interface

no ip ips deny-action ips-interface

Syntax Description

This command has no arguments or keywords.

Command Default

ACLs filter for the deny actions are applied to the ingress interface.

Command Modes

Global configuration

Command History

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

Usage Guidelines

Use the **ip ips deny-action ips-interface** command to change the default behavior of the ACL filters that are created for the deny actions.

Note You should configure this command only if at least one signature is configured to use the supported deny actions (denyFlowInline and denyConnectionInline, if the input interface is configured to for load balancing, and if IPS is configured on the output interface.

Default ACL Filter Approach

By default, ACL filters for the deny actions are created on the ingress interfaces of the offending packet. Thus, if Cisco IOS IPS is configured in outbound direction on the egress interface and the “deny” ACLs are created on the ingress interface, Cisco IOS IPS will drop the matching traffic before it goes through much processing. Unfortunately, this approach does not work in load balancing scenarios for which there is more than one ingress interface performing load-balancing.

Alternative ACL Filter Approach

T he **ip ips deny-action ips-interface** command enables ACLs to be created on the same interface and in the same direction as Cisco IOS IPS is configured. This alternative approach supports load-balancing scenarios--assuming that the load-balancing interfaces have the same Cisco IOS IPS configuration. However, all outbound Cisco IOS IPS traffic will go through substantial packet path processing before it is eventually dropped by the ACLs.

Examples

The following example shows how to configure load-balancing between interface e0 and interface e1:

```
ip ips name test
ip ips deny-action ips-interface
! Enables load balancing with e1
interface e0
 ip address 10.1.1.14 255.255.255.0
 no shut
!
! Enables load balancing with e0
interface e1
 ip address 10.1.1.16 255.255.255.0
 no shut
!
interface e2
 ip address 10.1.1.18 255.255.255.0
 ip ips test in
 no shut
```

ip ips enable-clidelta

To enable the signature tuning settings in the clidelta.xmz file on the router to take precedence over the signature settings in the intrusion prevention system (IPS) iosips-sig-delta.xmz file, use the **ip ips enable-clidelta** command in global configuration mode. To restore precedence to the iosips-sig-delta.xmz file settings, use the no form of this command.

ip ips enable-clidelta

no ip ips enable-clidelta

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

Most IPS devices and applications provide either a single default configuration or multiple default configurations. Using one of these default configurations is an ideal starting point for deploying IPS. When IOS IPS is deployed, parameters such as severity, active status, or event actions of certain signatures need to be tuned to meet the requirements of an enterprise network traffic profile.

Once the **ip ips enable-clidelta**commandis enabled, a local cli-delta.xmz file is generated containing the local tuning signatures configured through the CLI. The settings in the clidelta.xmz file take precedence when a globally administered delta signature update, contained in the iosips-sig-delta.xmz file, is sent from a central repository and applied to the configuration of the local router.

Examples

The following example shows how to enable the clidelta functionality:

```
Router(config)# ip ips enable-clidelta
```

Related Commands

Command	Description
show ip ips sig-clidelta	Displays information about the IPS iosips-sig-clidelta.xmz file on the router to verify signature tuning settings.

ip ips event-action-rules

To enter config-rule configuration mode, which allows users to change the target value rating, use the **ip ips event-action-rules** command in global configuration mode.

ip ips event-action-rules

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration

Command History

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

Usage Guidelines

You must issue the **ip ips event-action-rules** command to define the target value rating via the **target-value** 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
```

Related Commands

Command	Description
target-value	Defines the target value rating for a host.

ip ips fail closed

To instruct the router to drop all packets until the signature engine is built and ready to scan traffic, use the **ip ips fail closed** command in global configuration mode. To return to the default functionality, use the **no** form of this command.

ip ips fail closed

no ip ips fail closed

Syntax Description

This command has no arguments or keywords.

Command Default

All packets are passed without being scanned while the signature engine is being built or if the signature engine fails to build.

Command Modes

Global configuration

Command History

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

Usage Guidelines

Cisco IOS IPS Fails to Load the SDF

By default, the router running Intrusion Prevention System (IPS) will load the built-in signatures if it fails to load the signature definition file (SDF). If this command is issued, the router will drop all packets--unless the user specifies an access control list (ACL) for packets to send to IPS.

IPS Loads the SDF but Fails to Build a Signature Engine

If the router running IPS loads the SDF but fails to build a signature engine, the router will mark the engine “not ready.” If an available engine is previously loaded, the IPS will keep the available engine and discard the engine that is not ready for use. If no previous engines have been loaded or “not ready,” the router will install the engine that is not ready and rely on the configuration of the **ip ips fail closed**command.

By default, packets destined for an engine marked “not ready” will be passed without being scanned. If this command is issued, the router will drop all packets that are destined for that signature engine.

Examples

The following example shows how to instruct the router to drop all packets if the SME is not yet available:

```
Router(config)# ip ips fail closed
```

ip ips inherit-obsolete-tunings

Note Effective with Cisco IOS Release 15.2T, the **ip ips inherit-obsolete tunings** command is deprecated because the Cisco IOS IPS Signature Scanning with Lightweight Signatures feature is discontinued.

To enable Cisco IOS Intrusion Prevention System (IPS) signatures to inherit tunings from obsoleted signatures in a Cisco IOS IPS, use the **ip ips inherit-obsolete tunings** command in global configuration mode. To disable this function, use the **no** form of this command.

ip ips inherit-obsolete-tunings

no ip ips inherit-obsolete-tunings

Syntax Description

This command has no arguments or keywords.

Command Default

Tunings from obsoleted signatures in Cisco IOS IPS are not inherited.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced.
15.2T	This command was deprecated.

Usage Guidelines

The ip ips inherit-obsolete-tunings command enables new signatures to obsolete older signatures and inherit the event-action and enabled parameters of the obsolete tuning values without the need to manually tune the new signatures. All other parameter changes, including the "Retire" parameter saved in the old signatures, will be ignored.

After you enter the command, the screen displays a warning message asking you to clarify the intended usage and then asks whether you accept the configuration, By default, old signatures tunings are not inherited by new signatures.

Note The tunings of old signatures will be lost if they are not migrated to new signatures.

Note To enable inheritance of tunings, configure the ip ips inherit-obsolete-tunings command before a signature file is loaded.

Note Users of management devices should use those devices and not enable the ip ips inherit-obsolete-tunings command.

Examples

The following example shows how to configure a router running Cisco IOS IPS to allow new signatures to inherit the tuning values from the obsoleted signatures, without having to manually tune the new signatures:

```
Router(config)# ip ips inherit-obsolete-tunings
```

Related Commands

Command	Description
ip ips	Applies a IPS rule to an interface.
ip ips memory regex chaining	Enables an Cisco IOS IPS to chain multiple regex tables together and load additional signatures.
ip ips memory threshold	Specifies an Cisco IOS IPS memory threshold.
show ip ips	Displays Cisco IOS IPS information such as configured sessions and signatures.

ip ips memory regex chaining

Note Effective with Cisco IOS Release 15.2T, the **ip ips memory regex chaining** command is deprecated because the Cisco IOS IPS Signature Scanning with Lightweight Signatures feature is discontinued.

To enable a Cisco IOS Intrusion Prevention System (IPS) to chain multiple regex tables together and load additional signatures, use the **ip ips memory regex chaining** command in global configuration mode. To disable this function, use the **no** form of this command.

ip ips memory regex chaining

no ip ips memory regex chaining

Syntax Description

This command has no arguments or keywords.

Command Default

Multiple regex table chaining is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced.
15.2T	This command was deprecated.

Usage Guidelines

Multiple regex table chaining is used to load additional signatures when a Cisco IOS IPS is supporting a large signature set. The default is three chained tables when the ip ips memory regex chaining command is enabled. This results in slower performance of Cisco IOS IPS scanning due to scanning packets across more than a single regex table.

When a user tries to load a specific set of signatures that does not fit using a single table, compilation errors will result. A compiler failure error message looks like this:

```
*Sep  9 17:27:46.907: %IPS-4-SIGNATURE_COMPILE_FAILURE: string-tcp 3730:0 - compiles
discontinued for this engine
```

Examples

The following example shows how to enable the ip ips memory regex chaining command:

```
Router(config)# ip ips memory regex chaining
```

Related Commands

Command	Description
ip ips	Applies an IPS rule to an interface.
ip ips inherit-obsolete-tunings	Applies tunings from obsoleted signatures to the new versions of the signatures.
ip ips memory threshold	Specifies a Cisco IOS IPS memory threshold.
show ip ips	Displays Cisco IOS IPS information such as configured sessions and signatures.

ip ips memory threshold

Note Effective with Cisco IOS Release 15.2T, the **ip ips memory threshold** command is deprecated because the Cisco IOS IPS Signature Scanning with Lightweight Signatures feature is discontinued.

To specify a memory threshold when using a Cisco IOS Intrusion Prevention System (IPS), use the **ip ips memory threshold** command in global configuration mode. To disable this function, use the no form of this command.

ip ips memory threshold megabytes

no ip ips memory threshold

Syntax Description

megabytes	The IPS memory threshold, in megabytes. The valid range is from 0-1024.

Command Default

The default IPS memory threshold is 10 percent of free memory--this is available for router operations other than Cisco IOS IPS.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced.
15.2T	This command was deprecated.

Usage Guidelines

The IPS memory threshold defines the amount of free memory unavailable to the IPS.

When you are loading signatures, the default state is that Cisco IOS IPS cannot consume any more memory if the remaining (free) memory becomes less than 10 percent of the size of the total DRAM installed on the router (for example, less than 25.6 MB free memory left on routers with 256 MB DRAM). The 10 percent of free memory unavailable to IPS defines the IPS memory threshold. The IPS memory threshold can be changed using the ip ips memory threshold command to force IPS to use less memory, so that other features get access to more memory if they need it.

Setting a memory threshold for Cisco IOS IPS is recommended especially when an arbitrary number of signatures may be added on top of the recommended sets in Cisco IOS IPS Basic or Advanced/Default categories, or when a fully customized signature set is created and loaded.

Examples

The following example shows how to configure a router running Cisco IOS IPS to set the IPS memory threshold to a value of 50 MB:

```
Router(config)# ip ips memory threshold 50
```

Related Commands

Command	Description
ip ips	Applies an IPS rule to an interface.
ip ips inherit-obsolete-tunings	Applies tunings from obsoleted signatures to the newer versions of the signatures.
ip ips memory regex chaining	Enables a Cisco IOS IPS to chain multiple regex tables together and load additional signatures.
show ip ips	Displays Cisco IOS IPS information such as configured sessions and signatures.

ip ips name

To specify an intrusion prevention system (IPS) rule, use the **ip ips name**command in global configuration mode. To delete an IPS rule, use the **no** form of this command.

ip ips name *ips-name* [**list** *acl*]

no ip ips name *ips-name* [**list** *acl*]

Syntax Description

ips-name	Name for IPS rule.
list *acl*	(Optional) Specifies an extended or standard access control list (ACL) to filter the traffic that will be scanned. **Note** All traffic that is permitted by the ACL is subject to inspection by the IPS. Traffic that is denied by the ACL is not inspected by the IPS.

Command Default

An IPS rule does not exist.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.3(8)T	The command name was changed from the **ip audit name**command to the **ip ips name**command.

Usage Guidelines

The IPS does not load the signatures until the rule is applied to an interface via the **ip ips**command.

Note This command replaces the **ip audit name** global configuration command. If the **ip audit name** command has been issued in an existing configuration and an access control list (ACL) has been defined, IPS will apply the **ip ips name** command and the ACL parameter on all interfaces that applied the rule.

Examples

The following example shows how to configure a router running Cisco IOS IPS to load the default, built-in signatures. Note that a configuration option for specifying an SDF location is not necessary; built-in signatures reside statically in Cisco IOS.

```
!
ip ips po max-events 100
ip ips name MYIPS
!
interface GigabitEthernet0/1
 ip address 10.1.1.16 255.255.255.0
 ip ips MYIPS in
 duplex full
 speed 100
 media-type rj45
 no negotiation auto
!
```

Related Commands

Command	Description
ip ips	Applies an IPS rule to an interface.
show ip ips	Displays IPS information such as configured sessions and signatures.

ip ips notify

To specify the method of event notification, use the **ip ips notify** command in global configuration mode. To disable event notification, use the **no** form of this command.

ip ips notify [**log**| **sdee**]

no ip ips notify [**log**| **sdee**]

Syntax Description

log	(Optional) Send messages in syslog format. **Note** If an option is not specified, alert messages are sent in syslog format.
sdee	(Optional) Send messages in Security Device Event Exchange (SDEE) format.

Command Default

Disabled (alert messages are not sent).

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.3(8)T	The command name was changed from the **ip audit notify**command to the **ip ips notify**command. Also, support for SDEE was introduced, and the **sdee** keyword was added.
12.3(14)T	The Post Office protocol was deprecated, and the **nr-director** keyword was removed.

Usage Guidelines

SDEE is always running, but it does not receive and process events from Intrusion Prevention System (IPS) unless SDEE notification is enabled. If it is not enabled and a client sends a request, SDEE will respond with a fault response message, indicating that notification is not enabled.

To use SDEE, the HTTP server must be enabled (via the **ip http server** command). If the HTTP server is not enabled, the router cannot respond to the SDEE clients because it cannot not see the requests.

Note The **ip ips notify** command replaces the **ip audit notify** command. If the **ip audit notify**command is part of an existing configuration, the IPS will interpret it as the **ip ips notify**command .

Examples

In the following example, event notifications are specified to be sent in SDEE format:

```
ip ips notify sdee
```

Related Commands

Command	Description
ip http server	Enables the HTTP server on your system.

ip ips sdf location

Note

In Cisco IOS Release 12.4(11)T, the **ip ips sdf location** command was replaced with the **ip ips config location** command. For more information, see the **ip ips config location** command.

To specify the location in which the router will load the signature definition file (SDF), use the **ip ips sdf location** command in global configuration mode. To remove an SDF location from the configuration, use the **no** form of this command.

ip ips sdf location *url* [**retries** *number* **wait-time** *seconds*] **[autosave]**

no ip ips sdf location *url* [**retries** *number* **wait-time** *seconds*] **[autosave]**

Syntax Description

url	Location of the SDF. Available URL options: • local flash, such as flash:sig.xml • FTP server, such as ftp://myuser:mypass@ftp_server.sig.xml • rcp, such as rcp://myuser@rcp_server/sig.xml • TFTP server, such as tftp://tftp_server/sig.xml
retries *number*	(Optional) Number of times the router will try to load the SDF after the first attempt fails.
wait-time *seconds*	(Optional) Duration, in seconds, between retry attempts.
autosave	(Optional) Specifies that the router will save a new SDF to the specified location.

Command Default

If an SDF location is not specified, the router will load the default built-in signatures.

Command Modes

Global configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.
12.4(4)T	The **autosave** keyword was added.

Release	Modification
12.4(7.20)T	The **retries** *number* and the **wait-time** *seconds* options were added.
12.4(11)T	This command was replaced with the **ip ips config location** command.

Usage Guidelines

When you specify the **ip ips sdf location** command, the signatures are not loaded until the router is rebooted or until the Intrusion Prevention System (IPS) is applied to an interface (via the **ip ips** command). If IPS is already applied to an interface, the signatures are not loaded. If IPS cannot load the SDF, an error message is issued and the router uses the built-in IPS signatures.

You can also specify the **copy ips-sdf** command to load an SDF from a specified location. Unlike the **ip ips sdf location** command, the signatures are loaded immediately after the **copy ips-sdf** command is entered.

When you specify the **autosave** keyword, the router saves a new SDF to the specified location when signatures are loaded using either the **copy** command or an external management platform such as Security Device Manager (SDM), IPS Management Center (IPSMC) or Cisco Incident Control Server (Cisco ICS). You can specify multiple autosave locations. The router will attempt to save to all autosave locations. The URL must have proper write access permissions.

Examples

The following example shows how to configure the router to load and merge the attack-drop.sdf file with the default signatures. After the files are merged, it is recommended that you copy the merged signatures to a separate file. You can then reload the router (by entering the **reload** command) or reinitialize the router so that it recognizes the newly merged file (as shown the following example).

```
!
ip ips name MYIPS
!
interface GigabitEthernet0/1
 ip address 10.1.1.16 255.255.255.0
 ip ips MYIPS in
 duplex full
 speed 100
 media-type rj45
 no negotiation auto
!
!
! Merge the flash-based SDF (attack-drop.sdf) with the built-in signatures.
copy disk2:attack-drop.sdf ips-sdf
! Save the newly merged signatures to a separate file.
copy ips-sdf disk2:my-signatures.sdf
!
! Configure the router to use the new file, my-signatures.sdf
configure terminal
ip ips sdf location disk2:my-signatures.sdf
! Reinitialize the IPS by removing the IPS rule set and reapplying the rule set.
interface gig 0/1
no ip ips MYIPS in
!
*Apr 8 14:05:38.243:%IPS-2-DISABLED:IPS removed from all interfaces - IPS disabled
!
 ip ips MYIPS in
!
exit
```

Related Commands

Command	Description
copy ips-sdf	Loads or saves the SDF in the router.
ip ips	Applies the IPS rule to an interface.

ip ips signature

Note In Cisco IOS Release 12.4(11)T, the **ip ips signature** command was deprecated.

To attach a policy to a signature, use the **ip ips signature** command in global configuration mode. If the policy disabled a signature, use the **no** form of this command to reenable the signature. If the policy attached an access list to the signature, use the **no** form of this command to remove the access list.

ip ips signature *signature-id* {**delete| disable|** **list** *acl-list*}

no ip ips signature *signature-id*

Syntax Description

signature-id	Signature within the signature detection file (SDF).
delete	Deleted a specified signature.
disable	Disables a specified signature.
list *acl-list*	A named, standard, or ACL that is associated with the signature.

Command Default

No policy is attached to a signature.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.3(8)T	The command name was changed from the **ip audit signature** command to the **ip ips signature** command to support SDFs.
12.4(11)T	This command and support for SDFs were removed.

Usage Guidelines

This command allow you to set three policies: delete a signature, disable the audit of a signature, or qualify the audit of a signature with an access list.

If you are attaching an ACL to a signature, then you also need to create an Intrusion Prevention System (IPS) rule with the **ip ips name**command and apply it to an interface with the **ip ips** command.

Note The **ip ips signature**command replaces the **ip audit signature** command. If the **ip audit signature** command is found in an existing configuration, Cisco IOS IPS will interpret it as the **ip ips signature** command.

Examples

In the following example, a signature is disabled, another signature has ACL 99 attached to it, and ACL 99 is defined:

```
ip ips signature 6150 disable
ip ips signature 1000 list 99
access-list 99 deny 10.1.10.0 0.0.0.255
access-list 99 permit any
```

ip ips signature-category

To enter IPS category (config-ips-category) configuration mode, which allows you to tune Cisco IOS Intrusion Prevention System (IPS) signature parameters on the basis of a signature category, use the **ip ips signature-category** command in global configuration mode.

ip ips signature-category

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Global configuration

Command History

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

Usage Guidelines

Use the **ip ips signature-category** command if you want to tune signature parameters per category.

Examples

The following example shows how to tune event-action parameters for the signature category “adware/spyware.” All tuning information will be applied to all signatures that belong to the adware/spyware category.

```
Router(config)# ip ips signature-category
Router(config-ips-category)# category attack adware/spyware
Router(config-ips-category-action)# event-action produce-alert
Router(config-ips-category-action)# event-action deny-packet-inline
Router(config-ips-category-action)# event-action reset-tcp-connection
Router(config-ips-category-action)# retired false
Router(config-ips-category-action)# ^Z
Do you want to accept these changes? [confirm]y
```

Related Commands

Command	Description
category	Specifies a signature category that is to be used for multiple signature actions or conditions.

ip ips signature-definition

To enter signature-definition-signature configuration mode, which allows you to define a signature for command-line interface (CLI) user tunings, use the **ip ips signature-definition**command in global configuration mode. To revert back to the default value, use the **no** form of this command.

ip ips signature-definition

no ip ips signature-definition

Syntax Description

This command has no arguments or keywords.

Command Default

Signature parameters cannot be defined and default values are used.

Command Modes

Global configuration

Command History

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

Usage Guidelines

Use the **ip ips signature-definition** command to enter signature-definition-signature configuration mode, which allows you to issue the **signature** command. The **signature** command is used to specify a signature whose CLI user tunings are to be customized. After you issue the **signature** command, 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
signature	Specifies a signature for which the CLI user tunings will be changed.

ip ips signature disable

To instruct the router to scan for a given signature but not take any action if the signature is detected , use the **ip ips signature**command in global configuration mode. To reenable a signature, use the **no** form of this command.

ip ips signature *signature-id* [*sub-signature-id*] **disable** [**list** *acl-list*]

no ip ips signature *signature-id* [*sub-signature-id*] **disable** [**list** *acl-list*]

Syntax Description

signature-id *sub-signature-id*	Signature that is disabled.
list *acl-list*	(Optional) A named, standard, or extended access control list (ACL) to filter the traffic that will be scanned. If the packet is permitted by the ACL, the signature will be scanned and reported; if the packet is denied by the ACL, the signature is deemed disabled.

Command Default

All signatures within the signature definition file (SDF) are reported, if detected.

Command Modes

Global configuration

Command History

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

Usage Guidelines

You may want to disable a signature (or set of signatures) if your deployment scenario deems the signatures unnecessary.

Examples

The following example shows how to instructs the router not to report on signature 1000, if detected:

```
Router(config) ip ips signature 1000 disable
```

Related Commands

Command	Description
ip ips	Applies the IPS rule to an interface.

Command	Description
ip ips name	Specifies an IPS rule.

ip kerberos source-interface

To specify an interface for the source address of the kerberos packets, use the **ip kerberos source-interface** command in global configuration mode. To disable the configuration, use the **no** form of this command.

ip kerberos source-interface *interface-type number*

no ip kerberos source-interface

Syntax Description

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

An interface for the source address of Kerberos packets is not set.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
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 and implemented on the Cisco ASR 1000 Series Aggregation Services Routers.

Examples

The following example shows how to specify an interface for the source address of the Kerberos packets:

```
Router# configure terminal
Router(config)# ip kerberos source-interface FastEthernet 0/0
```

Related Commands

Command	Description
clear kerberos creds	Deletes the contents of the credentials cache.
debug kerberos	Displays information associated with the Kerberos Authentication Subsystem.

ip msdp border

To configure a router that borders a Protocol Independent Multicast (PIM) sparse mode region and dense mode region to use Multicast Source Discovery Protocol (MSDP), use the **ip msdp border**command in global configuration mode. To prevent this action, use the **no** form of this command.

ip msdp [**vrf** *vrf-name*] **border sa-address** *interface-type interface-number*

no ip msdp [**vrf** *vrf-name*] **border sa-address** *interface-type interface-number*

Syntax Description

vrf	(Optional) Supports the multicast VPN routing and forwarding (VRF) instance.
vrf-name	(Optional) Name assigned to the VRF.
sa-address	Specifies the active source IP address.
interface-type interface-number	Interface type and number from which the IP address is derived and used as the rendezvous point (RP) address in Source-Active (SA) messages. Thus, MSDP peers can forward SA messages away from this border. The IP address of the interface is used as the originator ID, which is the RP field in the MSDP SA message. No space is needed between the values.

Command Default

The active sources in the dense mode region will not participate in MSDP.

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)T	This command was introduced.
12.0(23)S	The **vrf** keyword and *vrf-name* argument were added.
12.2(13)T	The **vrf** keyword and *vrf-name* argument were added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
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.

Usage Guidelines

Use this command if you want the router to send SA messages for sources active in the PIM dense mode region to MSDP peers.

Specifying the interface-type and interface-number values allow the MSDP peers to forward source-active messages away from this border. The IP address of the interface is used as the originator ID, which is the rendezvous point field in the MSDP source-active message.

Note We recommend configuring the border router in the sparse mode domain to proxy-register sources in the dense mode domain, and have the sparse mode domain use standard MSDP procedures to advertise these sources.

Note If you use this command, you must constrain the sources advertised by using the **ip msdp redistribute** command. Configure the **ip msdp redistribute** command to apply to only local sources. Be aware that this configuration can result in (S, G) state remaining long after a source in the dense mode domain has stopped sending.

Note The **ip msdp originator-id**command also identifies an interface type and number to be used as the RP address. If both the **ip msdp border**and **ip msdp originator-id**commands are configured, the address derived from the **ip msdp originator-id**command determines the address of the RP.

Examples

In the following example, the local router is not an RP. It borders a PIM sparse mode region with a dense mode region. It uses the IP address of Ethernet interface 0 as the “RP” address in SA messages.

```
ip msdp border sa-address ethernet0
```

Related Commands

Command	Description
ip msdp originator-id	Allows an MSDP speaker that originates an SA message to use the IP address of its interface as the RP address in the SA message.
ip msdp redistribute	Configures which (S, G) entries from the multicast routing table are advertised in SA messages originated to MSDP peers.

ip mtu

To set the maximum transmission unit (MTU) size of IP packets that are sent on an interface, use the **ip mtu** command in interface configuration mode. To restore the default MTU size, use the **no** form of this command.

ip mtu *bytes*

no ip mtu

Syntax Description

bytes	MTU size, in bytes.

Command Default

The default MTU value depends on the interface type.

Table 11: Default MTU Values by Interface Type

Interface Type	Default MTU (Bytes)
ATM	4470
Ethernet	1500
FDDI	4470
High-Speed Serial Interface High Speed Access (HSSI HSA)	4470
Serial	1500
Token Ring	4464
VRF-Aware Service Infrastructure (VASI)	9216

Command Modes

Interface configuration (config-if)

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.

Release	Modification
Cisco IOS XE Release 2.4	This command was integrated into Cisco IOS XE Release 2.4.

Usage Guidelines

If an IP packet exceeds the MTU size that is set for the interface, the Cisco software fragments the IP packet.

When an IPsec MTU is less than 256 bytes, the crypto engine MTU is set to 256 bytes and packets greater than 256 bytes are fragmented.

For VASI interfaces that involve Ethernet type interfaces (Ethernet, Fast Ethernet, or Gigabit Ethernet), the IP MTU size of a VASI interface must be set to the same value as the lower default setting of the Ethernet type interface of 1500 bytes. If this adjustment is not made, OSPF reconvergence on the VASI interface requires a long time.

Note Changing the MTU value (by using the **mtu** interface configuration command) can affect the IP MTU value. If the current IP MTU value is the same as the MTU value and you change the MTU value, then the IP MTU value is modified automatically to match the new MTU value. However, the reverse is not true; changing the IP MTU value has no effect on the MTU value.

If a dynamic virtual tunnel interface (VTI) configured with an IP MTU causes encapsulating security payload (ESP) fragmentation, clear and re-establish the encryption session.

When a loopback interface is used as the VTI tunnel source, you must manually configure the **ip mtu** command. This is because the IPsec encapsulation bytes are calculated based on the outgoing physical interface.

MTU Size in an IPsec Configuration

In an IPsec configuration, such as in a crypto environment, an MTU value that is less than 256 bytes is not accepted. If you configure an MTU value less than 256 bytes, the MTU value is automatically overwritten and given a value of 256 bytes.

MTU Size in Cisco ME 3600X Series Ethernet Access Switches

In Cisco ME 3600X Series Ethernet Access Switches, you can configure seven unique MTU sizes on router and switchport interfaces and eight unique sizes on VLAN interfaces. This does not include the default size of 1500.

Examples

The following example shows how to set the maximum IP packet size for the first serial interface to 300 bytes:

```
Device(config)# interface serial 0
Device(config-if)# ip mtu 300
```

Related Commands

Command	Description
mtu	Adjusts the MTU size.

ip nhrp cache non-authoritative

To turn off authoritative flags on NHRP cache entries, use the **ip nhrp cache non-authoritative** command in interface configuration mode. To turn authoritative flags on again, use the no form of this command.

ip nhrp cache non-authoritative

no ip nhrp cache non-authoritative

Syntax Description

This command has no arguments or keywords.

Command Default

Authoritative flags are turned on.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

By default the next hop server (NHS) replies to authoritative Next Hop Resolution Protocol (NHRP) resolution requests if it has a cache entry that is marked as authoritative. The **ip nhrp cache non-authoritative** comand turns off the “authoritative” flag on the cache entries. Thus, the request is forwarded to the next hop client (NHC), which responds to the resolution.

Configuring the **ip nhrp cache non-authoritative**command offloads the resolution replies from the hub to the spokes. It also helps the spokes complete NHRP mapping entries when a spoke-to-spoke tunnel is built, thus alleviating flap conditions in which the IP security (IPsec) tunnel is built but for which there are no corresponding NHRP mappings.

Examples

The following example shows that the authoritative flags have been turned off:

```
interface Tunnel0
 ip nhrp cache non-authoritative
```

ip nhrp nhs

To specify the address of one or more Next Hop Resolution Protocol (NHRP) servers, use the **ip nhrp nhs**command ininterface configuration mode. To remove the address, use the **no** form of this command.

Cisco IOS Release 12.2(33)SRA, 12.2SX, and Later Releases

ip nhrp nhs *nhs-address* [*net-address* [*netmask*]]

no ip nhrp nhs *nhs-address* [*net-address* [*netmask*]]

Cisco IOS Release 15.1(2)T and Later Releases

ip nhrp nhs {*nhs-address* [**nbma** {*nbma-address*| *FQDN-string*}] **[multicast]** [**priority** *value*] [**cluster** *value*]| **cluster** *value* **max-connections** *value*| **dynamic nbma** {*nbma-address*| *FQDN-string*} **[multicast]** [**priority** *value*] [**cluster** *value*]| **fallback** *seconds*}

no ip nhrp nhs {*nhs-address* [**nbma** {*nbma-address*| *FQDN-string*}] **[multicast]** [**priority** *value*] [**cluster** *value*]| **cluster** *value* **max-connections** *value*| **dynamic nbma** {*nbma-address*| *FQDN-string*} **[multicast]** [**priority** *value*] [**cluster** *value*]| **fallback** *seconds*}

Syntax Description

nhs-address	Address of the next-hop server being specified.
net-address	(Optional) IP address of a network served by the next-hop server.
netmask	(Optional) IP network mask to be associated with the IP address. The IP address is logically ANDed with the mask.
nbma	(Optional) Specifies the nonbroadcast multiple access (NBMA) address or FQDN.
nbma-address	NBMA address.
FQDN-string	Next hop server (NHS) fully qualified domain name (FQDN) string.
multicast	(Optional) Specifies to use NBMA mapping for broadcasts and multicasts.
priority *value*	(Optional) Assigns a priority to hubs to control the order in which spokes select hubs to establish tunnels. The range is from 0 to 255; 0 is the highest and 255 is the lowest priority.
cluster *value*	(Optional) Specifies NHS groups. The range is from 0 to 10; 0 is the highest and 10 is the lowest. The default value is 0.

max-connections *value*	Specifies the number of NHS elements from each NHS group that needs to be active. The range is from 0 to 255.
dynamic	Configures the spoke to learn the NHS protocol address dynamically.
fallback *seconds*	Specifies the duration, in seconds, for which the spoke must wait before falling back to an NHS of higher priority upon recovery.

Command Default

No next-hop servers are explicitly configured, so normal network layer routing decisions are used to forward NHRP traffic.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
10.3	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.
15.1(2)T	This command was modified. The *net-address* and *mask* arguments were removed and the **nbma**, *nbma-address*, *FQDN-string*, **multicast**, **priority** *value*, **cluster** *value*, **max-connections** *value*, **dynamic**, and **fallback** *seconds* keywords and arguments were added.
15.2(1)T	This command was modified. The NBMA address was modified to support IPv6 address.

Usage Guidelines

Use the **ip nhrp nhs** command to specify the address of a next hop server and the networks it serves. Normally, NHRP consults the network layer forwarding table to determine how to forward NHRP packets. When next hop servers are configured, these next hop addresses override the forwarding path that would otherwise be used for NHRP traffic.

For any next hop server that is configured, you can specify multiple networks by repeating this command with the same *nhs-address*argument, but with different IP network addresses.

Examples

The following example shows how to register a hub to a spoke using NBMA and FQDN:

```
Router# configure terminal
Router(config)# interface tunnel 1
Router(config-if)# ip nhrp nhs 192.0.2.1 nbma examplehub.example1.com
```

The following example shows how to configure the desired **max-connections** value:

```
Router# configure terminal
Router(config)# interface tunnel 1
Router(config-if)# ip nhrp nhs cluster 5 max-connections 100
```

The following example shows how to configure the NHS fallback time:

```
Router# configure terminal
Router(config)# interface tunnel 1
Router(config-if)# ip nhrp nhs fallback 25
```

The following example shows how to configure NHS priority and group values:

```
Router# configure terminal
Router(config)# interface tunnel 1
Router(config-if)# ip nhrp nhs 192.0.2.1 priority 1 cluster 2
```

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.

ip port-map

To establish port-to-application mapping (PAM), use the **ip port-map** command in global configuration mode. To delete user-defined PAM entries, use the **no** form of this command.

ip port-map *appl-name* **port** [**tcp**| **udp**] [*port-num*| **from** *begin-port-num* **to** *end-port-num*] [**list** {*standard-acl-number*| *extended-acl-number* | *ipv6-acl*}] [**description** *description-string*]

no ip port-map *appl-name* **port** [**tcp**| **udp**] [*port-num*| **from** *begin-port-num* **to** *end-port-num*] [**list** {*standard-acl-number*| *extended-acl-number* | *ipv6-acl*}] [**description** *description-string*]

Syntax Description

appl-name	The application used to apply the port mapping. An application name can contain an underscore or a hyphen. An application can also be system or user-defined. However, a user-defined application must have the prefix *user-* in it; for example, *user-payroll*, *user-sales*, or *user-10*. Otherwise, the following error message appears: "Unable to add port-map entry. Names for user-defined applications must start with 'user-'."
port	Indicates that a port number maps to the application. You can specify up to five port numbers for each port.
tcp | **udp**	(Optional) Specifies the protocol for the application. For well-known applications (and those existing under PAM), you can omit these keywords, and the system configures the standard protocol for that application. However, for user-defined applications, you must specify either **tcp** or **udp**.
port-num	(Optional) The port number. The range is from 1 to 65535.
from *begin-port-num* **to** *end-port-num*	(Optional) Specifies a range of port numbers. You must use the **from** and **to** keywords together.
list	(Optional) Indicates that the port mapping information applies to a specific host or subnet by associating the port or subnet to an access control list (ACL) number used with PAM.
standard-acl-number	(Optional) The standard ACL number. The range is from 1 to 99.
extended-acl-number	(Optional) The extended ACL number. The range is from 1300 to 1999.
ipv6-acl	(Optional) Name of the IPv6 ACL.
description *description-string*	(Optional) Specifies a description of up to 40 characters in length.

Command Default

PAM does not get established by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.3(1)	This command was modified. Support for the Skinny Client Control Protocol (SCCP) was added.
12.3(14)T	This command was modified. Support was added for the following: • User-defined application names • User-specified descriptions • Port ranges • **tcp** and **udp** keywords • **from** *begin-port-num* **to** *end-port-num* keyword-argument pairs • **description** *description-string* keyword-argument pair
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 3.6S Release	This command was modified. The *ipv6-acl* argument was added.

Usage Guidelines

The **ip port-map** command associates TCP or UDP port numbers with applications or services, establishing a table of default port mapping information at the firewall. The port mapping information is used to support network environments that run services using ports that are different from the registered or well-known ports associated with a service or application.

When you configure the **no** form of the command, include all the parameters needed to remove the entry matching that specific set of parameters. For example, when you configure the **no ip port-map** *appl-name* command, all entries for that application are removed.

The port mapping information in the PAM table can be one of the following three types:

- System-defined

- User-defined
- Host-specific

System-Defined Port Mapping

Initially, PAM creates a set of system-defined entries in the mapping table by using well-known or registered port mapping information set up during system startup. The Context-Based Access Control (CBAC) firewall requires the system-defined port mapping information to function.

You can delete or modify system-defined port mapping information. Use the **no** form of the command to delete a port mapping and the regular form of the command to remap the system-defined port mapping information to another application.

You can also add new port numbers to system-defined applications. However, for some system-defined applications like HTTP and Simple Mail Transfer Protocol (SMTP), in which the firewall inspects deeper into packets, the protocol (UDP or TCP) cannot be changed from that defined in the system. In these instances, error messages are displayed.

The table below lists some default system-defined services and applications in the PAM table. (Use the **show ip port-map** command to display the complete list.)

Table 12: System-Defined Port Mapping

Application Name	Well-Known or Registered Port Number	Protocol Description
cuseeme	7648	CU-SeeMe Protocol
exec	512	Remote Process Execution
ftp	21	File Transfer Protocol (control port)
h323	1720	H.323 Protocol (for example, MS NetMeeting, Intel Video Phone)
http	80	Hypertext Transfer Protocol
login	513	Remote login
msrpc	135	Microsoft Remote Procedure Call
netshow	1755	Microsoft NetShow
real-audio-video	7070	RealAudio and RealVideo
sccp	2000	Skinny Client Control Protocol
smtp	25	Simple Mail Transfer Protocol
sql-net	1521	SQL-NET
streamworks	1558	StreamWorks Protocol

Application Name	Well-Known or Registered Port Number	Protocol Description
sunrpc	111	SUN Remote Procedure Call
tftp	69	Trivial File Transfer Protocol
vdolive	7000	VDOLive Protocol

Note You can override system-defined entries for a specific host or a subnet using the **ip port-map** *appl-name* **port list** command.

User-Defined Port Mapping

Network applications that use nonstandard ports require user-defined entries in the mapping table. Use the **ip port-map** command to create default user-defined entries in the PAM table. These entries automatically appear as an option for the **ip inspect name** command to facilitate the creation of inspection rules.

You can specify up to five separate port numbers for each port map in a single entry. You can also specify a port range in a single entry. However, you cannot specify both single port numbers and port ranges in the same entry.

Note If you try to map an application to a system-defined port, a message appears warning you of a mapping conflict. Delete the system-defined entry before mapping it to another application. Deleted system-defined mappings appear in the running configuration in their **no ip port-map** form.

Use the **no** form of the **ip port-map** command to delete user-defined entries from the PAM table. To remove a single mapping, use the **no** form of the command with all its parameters.

To overwrite an existing user-defined port mapping, use the **ip port-map** command to associate another service or application with the specific port.

Multiple commands for the same application name are cumulative.

If you assign the same port number to a new application, the new entry replaces the existing entry. The entry no longer appears in the running configuration and you receive a message about the remapping.

You cannot specify a port number that is in a range assigned to another application. You cannot specify overlapping port ranges.

Host-Specific Port Mapping

User-defined entries in the mapping table can include host-specific mapping information, which establishes port mapping information for specific hosts or subnets. In some environments, it might be necessary to override the default port mapping information for a specific host or a subnet, including system-defined default port mapping information. Use the **ip port-map** *appl-name* **port list** command to specify an ACL for a host or a subnet that uses PAM.

Note If the host-specific port mapping information is the same as the existing system-defined or user-defined default entries, host-specific port changes have no effect.

Examples

The following examples show how to add and remove user-defined PAM configuration entries at the firewall.

The following example shows how to establish the nonstandard port 8000 as the user-defined default port for HTTP services:

```
Device(config)# ip port-map http port 8000
```

The following example shows how to configure PAM entries that establish a range of nonstandard ports for HTTP services:

```
Device(config)# ip port-map http port 8001
Device(config)# ip port-map http port 8002
Device(config)# ip port-map http port 8003
Device(config)# ip port-map http port 8004
```

The following example shows how to configure port 8000 for FTP services. ACL 10 identifies the server address (192.168.32.43), and port 8000 is mapped with FTP services:

```
Device(config)# access-list 10 permit 192.168.32.43
Device(config)# ip port-map ftp port 8000 list 10
```

The following example shows how to configure port 21, which is usually reserved for FTP services, to the RealAudio application for hosts in the ACL list 10. In this configuration, hosts in list 10 do not recognize FTP activity on port 21.

```
Device(config)# ip port-map realaudio port 21 list 10
```

The following example shows that the **ip port-map** command has failed and an error message is generated:

```
Device(config)# ip port-map netshow port 21

Command fail: the port 21 has already been defined for ftp by the system.
              No change can be made to the system defined port mappings.
```

The following example shows how the **no** form of this command deletes user-defined entries from the PAM table. The **no** command has no effect on the system-defined port mappings. This command deletes the host-specific port mapping of FTP.

```
Device(config)# no ip port-map ftp port 1022 list 10
```

Note All **no** forms of the **ip port-map** command appear before other entries in the running configuration.

The following example shows how to configure a specific host to use port 8000 for FTP services. ACL 10 identifies the server address (192.168.32.43), and port 8000 is mapped with FTP services.

```
Device(config)# access-list 10 permit 192.168.32.43
Device(config)# ip port-map ftp port 8000 list 10
```

The following example shows how to configure a specific subnet to run HTTP services on port 8080. ACL 50 identifies the subnet, and the PAM entry maps port 8080 with HTTP services.

```
Device(config)# access-list 50 permit 192.168.92.0
Device(config)# ip port-map http port 8080 list 50
```

The following example shows how to configure a specific host to run HTTP services on port 25, which is the system-defined port number for SMTP services. This requires a host-specific PAM entry that overrides the system-defined default port mapping for HTTP, which is port 80. ACL 15 identifies the host address (192.168.33.43), and port 25 is mapped with HTTP services.

```
Device(config)# access-list 15 permit 192.168.33.43
Device(config)# ip port-map http port 25 list 15
```

The following example shows how to configure the same port number for different services running on different hosts. Port 8000 is required for HTTP services by host 192.168.3.4, and also required for FTP services by host 192.168.5.6. ACL 10 and ACL 20 identify the specific hosts, and PAM maps the ports with the services for each ACL.

```
Device(config)# access-list 10 permit 192.168.3.4
Device(config)# access-list 20 permit 192.168.5.6
Device(config)# ip port-map http port 8000 list 10
Device(config)# ip port-map http port 8000 list 20
```

The following example shows how to configure five separate port numbers:

```
Device(config)# ip port-map user-my-app port tcp 8085 8087 8092 8093 8094
```

The following example shows how to configure multiple commands for the same application name and both ports map to the myapp application:

```
Device(config)# ip port-map user-myapp port tcp 3400
Device(config)# ip port-map user-myapp port tcp 3500
```

The following example shows how to configure the same port number for a new application. The new entry replaces the existing entry, meaning that port 5670 gets mapped to user-my-new-app and its mapping to myapp is removed. As a result, the first command no longer appears in the running configuration and you receive a message about the remapping.

```
Device(config)# ip port-map user-myapp port tcp 5670
Device(config)# ip port-map user-my-new-app port tcp 5670
```

In the following example, the second command assigns port 8085 to user-my-new-app because you cannot specify a port number that is in a range assigned to another application. As a result, the first command no longer appears in the running configuration, and you receive a message about the port being moved from one application to another.

```
Device(config)# ip port-map user-my-app port tcp 8085
Device(config)# ip port-map user-my-new-app port tcp from 8080 to 8090
```

Similarly, in the following example the second command assigns port range 8080 to 8085 to user-my-new-app and the first command no longer appears in the running configuration. You receive a message about the remapping.

```
Device(config)# ip port-map user-my-app port tcp from 8080 to 8085
Device(config)# ip port-map user-my-new-app port tcp from 8080 to 8090
```

Related Commands

Command	Description
show ip port-map	Displays PAM information.

ip radius source-interface

To force RADIUS to use the IP address of a specified interface for all outgoing RADIUS packets, use the **ip radius source-interface**command in global configuration mode. To prevent RADIUS from using the IP address of a specified interface for all outgoing RADIUS packets, use the no form of this command.

ip radius source-interface *subinterface-name* [**vrf** *vrf-name*]

no ip radius source-interface

Syntax Description

subinterface-name	Name of the interface that RADIUS uses for all of its outgoing packets.
vrf *vrf-name*	(Optional) Per virtual route forwarding (VRF) configuration.

Command Default

No default behavior or values.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.3	This command was introduced.
12.2(1)DX	The vrf keyword and *vrf-name* argument were implemented 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.
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)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)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.

Usage Guidelines

Use this command to set the IP address of a subinterface to be used as the source address for all outgoing RADIUS packets. The IP address is used as long as the subinterface is in the *up* state. The RADIUS server can use one IP address entry for every network access client instead of maintaining a list of IP addresses. Radius uses the IP address of the interface that it is associated to, regardless of whether the interface is in the *up* or *down* state.

The **ip radius source-interface**command is especially useful in cases where the router has many subinterfaces and you want to ensure that all RADIUS packets from a particular router have the same IP address.

The specified sub-interface should have a valid IP address and should be in the *up* state for a valid configuration. If the specified sub-interface does not have a valid IP address or is in the *down* state, RADIUS enforces the source-interface configuration. In case the interface has no IP address, RADIUS configures the best available local IP address. To avoid this, add a valid IP address to the sub-interface or bring the sub-interface to the *up* state.

Use the **vrf** *vrf-name* keyword and argument to configure this command per VRF, which allows multiple disjoined routing or forwarding tables, where the routes of one user have no correlation with the routes of another user.

Examples

The following example shows how to configure RADIUS to use the IP address of subinterface s2 for all outgoing RADIUS packets:

```
ip radius source-interface s2
```

The following example shows how to configure RADIUS to use the IP address of subinterface Ethernet0 for VRF definition:

```
ip radius source-interface Ethernet0 vrf vrf1
```

Related Commands

Command	Description
ip tacacs source-interface	Uses the IP address of a specified interface for all outgoing TACACS packets.
ip telnet source-interface	Allows a user to select an address of an interface as the source address for Telnet connections.
ip tftp source-interface	Allows a user to select the interface whose address will be used as the source address for TFTP connections.

ip reflexive-list timeout

To specify the length of time that reflexive access list entries will continue to exist when no packets in the session are detected, use the **ip reflexive-list timeout** command in global configuration mode. To reset the timeout period to the default timeout, use the **no** form of this command.

ip reflexive-list timeout seconds

no ip reflexive-list timeout

Syntax Description

seconds	Specifies the number of seconds to wait (when no session traffic is being detected) before temporary access list entries expire. Use a positive integer from 0 to 2,147,483. The default is 300 seconds.

Command Default

300 seconds

Command Modes

Global 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.

Usage Guidelines

This command is used with reflexive filtering, a form of session filtering.

This command specifies when a reflexive access list entry will be removed after a period of no traffic for the session (the timeout period).

With reflexive filtering, when an IP upper-layer session begins from within your network, a temporary entry is created within the reflexive access list, and a timer is set. Whenever a packet belonging to this session is forwarded (inbound or outbound) the timer is reset. When this timer counts down to zero without being reset, the temporary reflexive access list entry is removed.

The timer is set to the *timeout period*. Individual timeout periods can be defined for specific reflexive access lists, but for reflexive access lists that do not have individually defined timeout periods, the global timeout period is used. The global timeout value is 300 seconds by default; however, you can change the global timeout to a different value at any time using this command.

This command does not take effect for reflexive access list entries that were already created when the command is entered; this command only changes the timeout period for entries created after the command is entered.

Examples

The following example sets the global timeout period for reflexive access list entries to 120 seconds:

```
ip reflexive-list timeout 120
```

The following example returns the global timeout period to the default of 300 seconds:

```
no ip reflexive-list timeout
```

Related Commands

Command	Description
evaluate	Nests a reflexive access list within an access list.
ip access-list	Defines an IP access list by name.
permit (reflexive)	Creates a reflexive access list and enables its temporary entries to be automatically generated.

ip route (vasi)

To establish a static route on the VRF-Aware Service Infrastructure (VASI) interface, use the **ip route vrf**command in global configuration mode. To remove the static route connection, use the **no** form of this command.

ip route [**vrf** *vrf-name*] *destination-prefix detination-prefix-mask* {**vasileft| vasiright**} *number*

no ip route [**vrf** *vrf-name*] *destination-prefix detination-prefix-mask* {**vasileft| vasiright**} *number*

Syntax Description

vrf *vrf-name*	Specifies the Virtual Routing and Forwarding (VRF) instance for the static route.
destination-prefix	IP route prefix for the destination, in dotted decimal format.
destination-prefix -mask	Prefix mask for the destination, in dotted decimal format.
vasileft	Configures the vasileft interface.
vasiright	Configures the vasiright interface.
number	Identifier of the VASI interface. The range is from 1 to 256.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Release 2.6	This command was introduced.

Examples

The following example shows how to configure static route on a VASI interface:

```
router(config)# ip route vrf red 0.0.0.0 0.0.0.0 vasileft 100
```

Related Commands

Command	Description
interface (vasi)	Configures the VASI interface.

debug interface (vasi)	Displays debugging information of VASI interface descriptor block.
debug vasi	Displays debugging information of VASI.
show vasi pair	Displays the status of a VASI pair.

ip scp server enable

To enable the router to securely copy files from a remote workstation, use the **ip scp server enable** command in global configuration mode. To disable secure copy functionality (the default), use the **no** form of this command.

ip scp server enable

no ip scp server enable

Syntax Description

This command has no arguments or keywords.

Command Default

The secure copy function is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.0(21)S	This command was integrated into Cisco IOS Release 12.0(21)S and support for the Cisco 7500 series and Cisco 12000 series routers was added.
12.2(18)SXD	This command was integrated into Cisco IOS Release 12.2(18)SXD.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(15)S.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.

Usage Guidelines

Use this command to enable secure copying of files from systems using the Secure Shell (SSH) application. This secure copy function is accomplished by an addition to the **copy** command in the Cisco IOS software, which takes care of using the secure copy protocol (scp) to copy to and from a router while logged in to the router itself. Because copying files is generally a restricted operation in the Cisco IOS software, a user attempting to copy such files needs to be at the correct enable level.

The Cisco IOS software must also allow files to be copied to or from itself from a remote workstation running the SSH application (which is supported by both the Microsoft Windows and UNIX operating systems). To get this information, the Cisco IOS software must have authentication and authorization configured in the authentication, authorization, and accounting (AAA) feature. SSH already relies on AAA authentication to authenticate the user username and password. Scp adds the requirement that AAA authorization be turned on so that the operating system can determine whether or not the user is at the correct privilege level.

Examples

The following example shows a typical configuration that allows the router to securely copy files from a remote workstation. Because scp relies on AAA authentication and authorization to function properly, AAA must be configured.

```
aaa new-model
aaa authentication login default tac-group tacacs+
aaa authorization exec default local
username user1 privilege 15 password 0 lab
ip scp server enable
```

The following example shows how to use scp to copy a system image from Flash memory to a server that supports SSH:

```
Router# copy flash:c4500-ik2s-mz.scp scp://user1@host1/
Address or name of remote host [host1]?
Destination username [user1]?
Destination filename [c4500-ik2s-mz.scp]?
Writing c4500-ik2s-mz.scp
Password:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

Note When using scp, you cannot enter the password into the **copy** command; enter the password when prompted.

Related Commands

Command	Description
aaa authentication login	Sets AAA authentication at login.
aaa authorization	Sets parameters that restrict user access to a network.
copy	Copies any file from a source to a destination.
debug ip scp	Troubleshoots scp authentication problems.
ip ssh port	Enables secure network access to the tty lines.
username	Establishes a username-based authentication system.

ip sdee

To set the Security Device Event Exchange (SDEE) attribute values, use the **ip sdee** command in global configuration mode. To change the current selection or return to the default, use the **no** form of this command.

ip sdee {**alerts** *alert-number*| **messages** *message-number*| **subscriptions** *subscription-number*}

no ip sdee {**alerts**| **messages**| **subscriptions**}

Syntax Description

alerts *alert-number*	Specifies the maximum number of alerts the router must store. The range is from 10 to 2000. The default value is 200. **Note** Storing more alerts uses more router memory.
messages *message-number*	Specifies the maximum number of messages the router must store. The range is from 10 to 500. The default value is 200. **Note** Storing more messages uses more router memory.
subscriptions *subscription -number*	Specifies the maximum number of subscriptions. The range is from 1 to 3. The default value is 1.

Command Default

The default subscription is 1. The default message is 200. The default alert is 200.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(8)T	This command was introduced.
15.0(1)M	This command was modified in a release earlier than Cisco IOS Release 15.0(1)M. The **alerts** *alert-number* and **messages** *message-number* keywords and arguments were added.

Usage Guidelines

The SDEE messages report on the progress of Cisco IOS Intrusion Prevention System (IPS) initialization and operation. After you have enabled SDEE to receive and process events from IPS, you can issue the **ip sdee subscriptions** command to modify the number of allowed open SDEE subscriptions.

Examples

The following example shows how to change the number of allowed open subscriptions to 2:

```
Router# configure terminal
Router(config)# ip ips notify sdee
Router(config)# ip sdee events 500
Router(config)# ip sdee subscriptions 2
```

The following example shows how to change the number of alerts that must be stored on the router to 10:

```
Router# configure terminal
Router(config)# ip ips notify sdee
Router(config)# ip sdee events 500
Router(config)# ip sdee alerts 10
```

The following example shows how to change the number of messages that must be stored on the router to 10:

```
Router# configure terminal
Router(config)# ip ips notify sdee
Router(config)# ip sdee events 500
Router(config)# ip sdee messages 10
```

Related Commands

Command	Description
ip ips notify	Specifies the method of event notification.

ip sdee events

To set the maximum number of Security Device Event Exchange (SDEE) events that can be stored in the event buffer, use the **ip sdee events** command in global configuration mode. To change the buffer size or return to the default buffer size, use the **no** form of this command.

ip sdee events *events*

no ip sdee events *events*

Syntax Description

events	Maximum number of events; maximum number of allowable events: 1000.

Command Default

200 events

Command Modes

Global configuration

Command History

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

Usage Guidelines

When SDEE notification is enabled (via the **ip ips notify sdee** command), 200 hundred events can automatically be stored in the buffer. When SDEE notification is disabled, all stored events are lost. A new buffer is allocated when the notifications are reenabled.

When specifying the size of an events buffer, note the following functionality:

- It is circular. When the end of the buffer is reached, the buffer will start overwriting the earliest stored events. (If overwritten events have not yet been reported, you will receive a buffer overflow notice.)
- If a new, smaller buffer is requested, all events that are stored in the previous buffer will be lost.
- If a new, larger buffer is requested, all existing events will be saved.

Examples

The following example shows how to set the maximum buffer events size to 500:

```
configure terminal
 ip ips notify sdee
 ip sdee events 500
```

Related Commands

Command	Description
ip ips notify	Specifies the method of event notification.

ip security add

To a dd a basic security option to all outgoing packets, use the **ip security add** command in interface configuration mode. To disable the adding of a basic security option to all outgoing packets, use the **no** form of this command.

ip security add

no ip security add

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled, when the security level of the interface is “Unclassified Genser” (or unconfigured). Otherwise, the default is enabled.

Command Modes

Interface configuration

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.

Usage Guidelines

If an outgoing packet does not have a security option present, this interface configuration command will add one as the first IP option. The security label added to the option field is the label that was computed for this packet when it first entered the router. Because this action is performed after all the security tests have been passed, this label will either be the same or will fall within the range of the interface.

Examples

The following example adds a basic security option to each packet leaving Ethernet interface 0:

```
interface ethernet 0
 ip security add
```

Related Commands

Command	Description
ip security dedicated	Sets the level of classification and authority on the interface.

Command	Description
ip security extended-allowed	Accepts packets on an interface that has an Extended Security Option present.
ip security first	Prioritizes the presence of security options on a packet.
ip security ignore-authorities	Causes the Cisco IOS software to ignore the authorities field of all incoming packets.
ip security implicit-labelling	Forces the Cisco IOS software to accept packets on the interface, even if they do not include a security option.
ip security multilevel	Sets the range of classifications and authorities on an interface.
ip security reserved-allowed	Treats as valid any packets that have Reserved1 through Reserved4 security levels.
ip security strip	Removes any basic security option on outgoing packets on an interface.

ip security aeso

To atta ch Auxiliary Extended Security Options (AESOs) to an interface, use the **ip security aeso** command in interface configuration mode. To disable AESO on an interface, use the **no** form of this command.

ip security aeso *source compartment-bits*

no ip security aeso *source compartment-bits*

Syntax Description

source	Extended Security Option (ESO) source. This can be an integer from 0 to 255.
compartment-bits	Number of compartment bits in hexadecimal.

Command Default

Disabled

Command Modes

Interface configuration

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.

Usage Guidelines

Compartment bits are specified only if this AESO is to be inserted in a packet. On every incoming packet at this level on this interface, these AESOs should be present.

Beyond being recognized, no further processing of AESO information is performed. AESO contents are not checked and are assumed to be valid if the source is listed in the configurable AESO table.

Configuring any per-interface extended IP Security Option (IPSO) information automatically enables **ip security extended-allowed** (disabled by default).

Examples

The following example defines the Extended Security Option source as 5 and sets the compartments bits to 5:

```
interface ethernet 0
 ip security aeso 5 5
```

Related Commands

Command	Description
ip security eso-info	Configures system-wide defaults for extended IPSO information.
ip security eso-max	Specifies the maximum sensitivity level for an interface.
ip security eso-min	Configures the minimum sensitivity level for an interface.
ip security extended-allowed	Accepts packets on an interface that has an Extended Security Option present.

ip security dedicated

To set the level of classification and authority on the interface, use the **ip security dedicated** command in interface configuration mode. To reset the interface to the default classification and authorities, use the **no** form of this command.

ip security dedicated *level authority* [*authority* ...]

no ip security dedicated *level authority* [*authority* ...]

Syntax Description

level	Degree of sensitivity of information. The *level* keywords are listed in the first table below.
authority	Organization that defines the set of security levels that will be used in a network. The authority keywords are listed in the second table below.

Command Default

Disabled

Command Modes

Interface configuration

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.

Usage Guidelines

All traffic entering the system on this interface must have a security option that exactly matches this label. Any traffic leaving via this interface will have this label attached to it.

The following definitions apply to the descriptions of the IP Security Option (IPSO) in this section:

- level -- The degree of sensitivity of information. For example, data marked TOPSECRET is more sensitive than data marked SECRET. The level keywords and their corresponding bit patterns are shown in the table below.

Table 13: IPSO Level Keywords and Bit Patterns

Level Keyword	Bit Pattern
Reserved4	0000 0001
TopSecret	0011 1101
Secret	0101 1010
Confidential	1001 0110
Reserved3	0110 0110
Reserved2	1100 1100
Unclassified	1010 1011
Reserved1	1111 0001

- authority -- An organization that defines the set of security levels that will be used in a network. For example, the Genser authority consists of level names defined by the U.S. Defense Communications Agency (DCA). The authority keywords and their corresponding bit patterns are shown in the table below.

Table 14: IPSO Authority Keywords and Bit Patterns

Authority Keyword	Bit Pattern
Genser	1000 0000
Siop-Esi	0100 0000
DIA	0010 0000
NSA	0001 0000
DOE	0000 1000

- label -- A combination of a security level and an authority or authorities.

Examples

The following example sets a confidential level with Genser authority:

```
ip security dedicated confidential Genser
```

Related Commands

Command	Description
ip security add	Adds a basic security option to all outgoing packets.
ip security extended-allowed	Accepts packets on an interface that has an Extended Security Option present.
ip security first	Prioritizes the presence of security options on a packet.
ip security ignore-authorities	Causes the Cisco IOS software to ignore the authorities field of all incoming packets.
ip security implicit-labelling	Forces the Cisco IOS software to accept packets on the interface, even if they do not include a security option.
ip security multilevel	Sets the range of classifications and authorities on an interface.
ip security reserved-allowed	Treats as valid any packets that have Reserved1 through Reserved4 security levels.
ip security strip	Removes any basic security option on outgoing packets on an interface.

ip security eso-info

To confi gure system-wide defaults for extended IP Security Option (IPSO) information, use the **ip security eso-info** command in global configuration mode. To return to the default settings, use the **no** form of this command.

ip security eso-info *source compartment-size default-bit*

no ip security eso-info *source compartment-size default-bit*

Syntax Description

source	Hexadecimal or decimal value representing the extended IPSO source. This is an integer from 0 to 255.
compartment-size	Maximum number of bytes of compartment information allowed for a particular extended IPSO source. This is an integer from 1 to 16.
default-bit	Default bit value for any unsent compartment bits.

Command Default

Disabled

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.(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 configures Extended Security Option (ESO) information, including Auxiliary Extended Security Option (AESO). Transmitted compartment information is padded to the size specified by the *compartment-size* argument.

Examples

The following example sets system-wide defaults for source, compartment size, and the default bit value:

```
ip security eso-info 100 5 1
```

Related Commands

Command	Description
ip security eso-max	Specifies the maximum sensitivity level for an interface.
ip security eso-min	Configures the minimum sensitivity level for an interface.

ip security eso-max

To sp ecify the maximum sensitivity level for an interface, use the **ip security eso-max**command in interface configuration mode. To return to the default, use the **no** form of this command.

ip security eso-max *source compartment-bits*

no ip security eso-max *source compartment-bits*

Syntax Description

source	Extended Security Option (ESO) source. This is an integer from 1 to 255.
compartment-bits	Number of compartment bits in hexadecimal.

Command Default

Disabled

Command Modes

Interface configuration

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.

Usage Guidelines

The command is used to specify the maximum sensitivity level for a particular interface. Before the per-interface compartment information for a particular Network-Level Extended Security Option (NLESO) source can be configured, the **ip security eso-info** global configuration command must be used to specify the default information.

On every incoming packet on the interface, these Extended Security Options should be present at the minimum level and should match the configured compartment bits. Every outgoing packet must have these ESOs.

On every packet transmitted or received on this interface, any NLESO sources present in the IP header should be bounded by the minimum sensitivity level and bounded by the maximum sensitivity level configured for the interface.

When transmitting locally generated traffic out this interface, or adding security information (with the **ip security add** command), the maximum compartment bit information can be used to construct the NLESO sources placed in the IP header.

A maximum of 16 NLESO sources can be configured per interface. Due to IP header length restrictions, a maximum of 9 of these NLESO sources appear in the IP header of a packet.

Examples

In the following example, the specified ESO source is 240 and the compartment bits are specified as 500:

```
interface ethernet 0
 ip security eso-max 240 500
```

Related Commands

Command	Description
ip security eso-info	Configures system-wide defaults for extended IPSO information.
ip security eso-min	Configures the minimum sensitivity level for an interface.

ip security eso-min

To confi gure the minimum sensitivity for an interface, use the **ip security eso-min**command in interface configuration mode. To return to the default, use the **no** form of this command.

ip security eso-min *source compartment-bits*

no ip security eso-min *source compartment-bits*

Syntax Description

source	Extended Security Option (ESO) source. This is an integer from 1 to 255.
compartment-bits	Number of compartment bits in hexadecimal.

Command Default

Disabled

Command Modes

Interface configuration

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.

Usage Guidelines

The command is used to specify the minimum sensitivity level for a particular interface. Before the per-interface compartment information for a particular Network Level Extended Security Option (NLESO) source can be configured, the **ip security eso-info** global configuration command must be used to specify the default information.

On every incoming packet on this interface, these Extended Security Options should be present at the minimum level and should match the configured compartment bits. Every outgoing packet must have these ESOs.

On every packet transmitted or received on this interface, any NLESO sources present in the IP header should be bounded by the minimum sensitivity level and bounded by the maximum sensitivity level configured for the interface.

When transmitting locally generated traffic out this interface, or adding security information (with the **ip security add** command), the maximum compartment bit information can be used to construct the NLESO sources placed in the IP header.

A maximum of 16 NLESO sources can be configured per interface. Due to IP header length restrictions, a maximum of 9 of these NLESO sources appear in the IP header of a packet.

Examples

In the following example, the specified ESO source is 5, and the compartment bits are specified as 5:

```
interface ethernet 0
 ip security eso-min 5 5
```

Related Commands

Command	Description
ip security eso-info	Configures system-wide defaults for extended IPSO information.
ip security eso-max	Specifies the maximum sensitivity level for an interface.

ip security extended-allowed

To accept packets on an interface that has an extended security option present, use the **ip security extended-allowed** command in interface configuration mode. To restore the default, use the **no** form of this command.

ip security extended-allowed

no ip security extended-allowed

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Interface configuration

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.

Usage Guidelines

Packets containing extended security options are rejected.

Examples

The following example allows interface Ethernet 0 to accept packets that have an extended security option present:

```
interface ethernet 0
 ip security extended-allowed
```

Related Commands

Command	Description
ip security add	Adds a basic security option to all outgoing packets.
ip security dedicated	Sets the level of classification and authority on the interface.

Command	Description
ip security first	Prioritizes the presence of security options on a packet.
ip security ignore-authorities	Causes the Cisco IOS software to ignore the authorities field of all incoming packets.
ip security implicit-labelling	Forces the Cisco IOS software to accept packets on the interface, even if they do not include a security option.
ip security multilevel	Sets the range of classifications and authorities on an interface.
ip security reserved-allowed	Treats as valid any packets that have Reserved1 through Reserved4 security levels.
ip security strip	Removes any basic security option on outgoing packets on an interface.

ip security first

To prioritize the presence of security options on a packet, use the **ip security first** command in interface configuration mode. To prevent packets that include security options from moving to the front of the options field, use the **no**form of this command.

ip security first

no ip security first

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Interface configuration

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.

Usage Guidelines

If a basic security option is present on an outgoing packet, but it is not the first IP option, then the packet is moved to the front of the options field when this interface configuration command is used.

Examples

The following example ensures that, if a basic security option is present in the options field of a packet exiting interface Ethernet 0, the packet is moved to the front of the options field:

```
interface ethernet 0
 ip security first
```

Related Commands

Command	Description
ip security add	Adds a basic security option to all outgoing packets.
ip security dedicated	Sets the level of classification and authority on the interface.

Command	Description
ip security extended-allowed	Accepts packets on an interface that has an Extended Security Option present.
ip security ignore-authorities	Causes the Cisco IOS software to ignore the authorities field of all incoming packets.
ip security implicit-labelling	Forces the Cisco IOS software to accept packets on the interface, even if they do not include a security option.
ip security multilevel	Sets the range of classifications and authorities on an interface.
ip security reserved-allowed	Treats as valid any packets that have Reserved1 through Reserved4 security levels.
ip security strip	Removes any basic security option on outgoing packets on an interface.

ip security ignore-authorities

To have the Cisco IOS software ignore the authorities field of all incoming packets, use the **ip security ignore-authorities** command in interface configuration mode. To disable this function, use the **no** form of this command.

ip security ignore-authorities

no ip security ignore-authorities

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Interface configuration

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.

Usage Guidelines

When the packet’s authority field is ignored, the value used in place of this field is the authority value declared for the specified interface. The **ip security ignore-authorities** can be configured only on interfaces that have dedicated security levels.

Examples

The following example causes interface Ethernet 0 to ignore the authorities field on all incoming packets:

```
interface ethernet 0
 ip security ignore-authorities
```

Related Commands

Command	Description
ip security add	Adds a basic security option to all outgoing packets.
ip security dedicated	Sets the level of classification and authority on the interface.

Command	Description
ip security extended-allowed	Accepts packets on an interface that has an Extended Security Option present.
ip security first	Prioritizes the presence of security options on a packet.
ip security implicit-labelling	Forces the Cisco IOS software to accept packets on the interface, even if they do not include a security option.
ip security multilevel	Sets the range of classifications and authorities on an interface.
ip security reserved-allowed	Treats as valid any packets that have Reserved1 through Reserved4 security levels.
ip security strip	Removes any basic security option on outgoing packets on an interface.

ip security ignore-cipso

To enable Cisco IOS software to ignore the Commercial IP Security Option (CIPSO) field of all incoming packets at the interface, use the **ip security ignore-cipso** command in interface configuration mode. To disable this function, use the **no** form of this command.

ip security ignore-cipso

no ip security ignore-cipso

Syntax Description

This command has no arguments or keywords.

Command Default

Cisco IOS software cannot ignore the CIPSO field.

Command Modes

Interface configuration

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **ip security ignore-cipso** command allows a router running Cisco IOS software to ignore the CIPSO field in the IP packet and forward the packet as if the field was not present.

Examples

The following example shows how to enable Cisco IOS software to ignore the CIPSO field for all incoming packets at the Ethernet interface:

```
interface ethernet 0
 ip security ignore-cipso
```

The following sample output from the **show ip interface** command can be used to verify that the **ip security ignore-cipso** option has been enabled. If this option is enabled, the output will display the text “Commercial security options are ignored.”

```
Router# show ip interface ethernet 0
Ethernet0 is up, line protocol is up
Internet address is 172.16.0.0/28
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 enabled
Secondary address 172.19.56.31/24
Outgoing access list is not set
Inbound access list is not set
Proxy ARP is enabled
Security level is default
```

```
Commercial security options are ignored
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 multicast fast switching is disabled
Router Discovery is disabled
IP output packet accounting is disabled
IP access violation accounting is disabled
TCP/IP header compression is disabled
Probe proxy name replies are disabled
Gateway Discovery is disabled
Policy routing is disabled
Network address translation is disabled
```

The following sample outputs from the **show ip traffic** command can be used to verify that the **ip security ignore-cipso** command has been enabled:

Examples

```
Router# show ip traffic
IP statistics:
Rcvd: 153 total, 129 local destination
0 format errors, 0 checksum errors, 0 bad hop count
0 unknown protocol, 0 not a gateway
0 security failures, 34 bad options, 44 with options
Opts: 10 end, 0 nop, 0 basic security, 0 loose source route
0 timestamp, 0 extended security, 0 record route
0 stream ID, 0 strict source route, 0 alert, 0 other
Frags: 0 reassembled, 0 timeouts, 0 couldn't reassemble
0 fragmented, 0 couldn't fragment
Bcast: 108 received, 1 sent
Mcast: 0 received, 4 sent
Sent: 30 generated, 0 forwarded
2 encapsulation failed, 0 no route
Sample Output with the ip security ignore-cipso Command Enabled
Router# show ip traffic
IP statistics:
Rcvd: 153 total, 129 local destination
0 format errors, 0 checksum errors, 0 bad hop count
0 unknown protocol, 0 not a gateway
0 security failures, 34 bad options, 44 with options
Opts: 10 end, 0 nop, 0 basic security, 0 loose source route
0 timestamp, 0 extended security, 0 record route
0 stream ID, 0 strict source route, 0 alert, 44 cipso
0 other
Frags: 0 reas
sembled, 0 timeouts, 0 couldn't reassemble
0 fragmented, 0 couldn't fragment
Bcast: 108 received, 1 sent
Mcast: 0 received, 4 sent
Sent: 30 generated, 0 forwarded
2 encapsulation failed, 0 no route
```

Related Commands

Command	Description
show ip interfaces	Displays the usability status of interfaces configured for IP.
show ip traffic	Displays statistics about IP traffic.

ip security implicit-labelling

To force the Cisco IOS software to accept packets on the interface, even if they do not include a security option, use the **ip security implicit-labelling** command in interface configuration mode. To require security options, use the **no** form of this command.

Application Firewall Provisioning Syntax

ip security implicit-labelling [*level authority* [*authority...*]]

no ip security implicit-labelling [*level authority* [*authority...*]]

Syntax Description

level	(Optional) Degree of sensitivity of information. If your interface has multilevel security set, you must specify this argument. (See the *level* keywords listed in the first table in the **ip security dedicated** command section.)
authority	(Optional) Organization that defines the set of security levels that will be used in a network. If your interface has multilevel security set, you must specify this argument. You can specify more than one. (See the *authority* keywords listed in the second table in the **ip security dedicated** command section.)

Command Default

Enabled, when the security level of the interface is “Unclassified Genser” (or unconfigured). Otherwise, the default is disabled.

Command Modes

Interface configuration

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.

Usage Guidelines

If your interface has multilevel security set, you must use the expanded form of the command (with the optional arguments as noted in brackets) because the arguments are used to specify the precise level and authority to use when labeling the packet. If your interface has dedicated security set, the additional arguments are ignored.

Examples

In the following example, an interface is set for security and will accept unlabeled packets:

```
ip security dedicated confidential genser
ip security implicit-labelling
```

Related Commands

Command	Description
ip security add	Adds a basic security option to all outgoing packets.
ip security dedicated	Sets the level of classification and authority on the interface.
ip security extended-allowed	Accepts packets on an interface that has an Extended Security Option present.
ip security first	Prioritizes the presence of security options on a packet.
ip security ignore-authorities	Causes the Cisco IOS software to ignore the authorities field of all incoming packets.
ip security multilevel	Sets the range of classifications and authorities on an interface.
ip security reserved-allowed	Treats as valid any packets that have Reserved1 through Reserved4 security levels.
ip security strip	Removes any basic security option on outgoing packets on an interface.

ip security multilevel

To set the range of classifications and authorities on an interface, use the **ip security multilevel** command in interface configuration mode. To remove security classifications and authorities, use the **no** form of this command.

ip security multilevel *level1* [*authority1...*] **to** *level2* [*authority2...*]

no ip security multilevel

Syntax Description

level1	Degree of sensitivity of information. The classification level of incoming packets must be equal to or greater than this value for processing to occur. (See the *level* keywords found in the first table in the **ip security dedicated** command section.)
authority1	(Optional) Organization that defines the set of security levels that will be used in a network. The authority bits must be a superset of this value. (See the *authority* keywords listed in the second table in the **ip security dedicated**command section.)
to	Separates the range of classifications and authorities.
level2	Degree of sensitivity of information. The classification level of incoming packets must be equal to or less than this value for processing to occur. (See the *level* keywords found in the first table in the **ip security dedicated** command section.)
authority2	Organization that defines the set of security levels that will be used in a network. The authority bits must be a proper subset of this value. (See the *authority* keywords listed in the second table in the **ip security dedicated** command section.)

Command Default

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
10.0	This command was introduced.

Release	Modification
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

All traffic entering or leaving the system must have a security option that falls within this range. Being within range requires that the following two conditions be met:

- The classification level must be greater than or equal to *level1* and less than or equal to *level2.*
- The authority bits must be a superset of *authority1* and a proper subset of *authority2.*That is, *authority1* specifies those authority bits that are required on a packet, and *authority2* specifies the required bits plus any optional authorities that also can be included. If the *authority1* field is the empty set, then a packet is required to specify any one or more of the authority bits in *authority*2.

Examples

The following example specifies levels Unclassified to Secret and NSA authority:

```
ip security multilevel unclassified to secret nsa
```

Related Commands

Command	Description
ip security add	Adds a basic security option to all outgoing packets.
ip security dedicated	Sets the level of classification and authority on the interface.
ip security extended-allowed	Accepts packets on an interface that has an Extended Security Option present.
ip security first	Prioritizes the presence of security options on a packet.
ip security ignore-authorities	Causes the Cisco IOS software to ignore the authorities field of all incoming packets.
ip security implicit-labelling	Forces the Cisco IOS software to accept packets on the interface, even if they do not include a security option.
ip security reserved-allowed	Treats as valid any packets that have Reserved1 through Reserved4 security levels.
ip security strip	Removes any basic security option on outgoing packets on an interface.

ip security reserved-allowed

To treat as valid any packets that have Reserved1 through Reserved4 security levels, use the **ip security reserved-allowed** command in interface configuration mode. To disallow packets that have security levels of Reserved3 and Reserved2, use the **no** form of this command.

ip security reserved-allowed

no ip security reserved-allowed

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Interface configuration

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.

Usage Guidelines

When you set multilevel security on an interface, and indicate, for example, that the highest range allowed is Confidential, and the lowest is Unclassified, the Cisco IOS software neither allows nor operates on packets that have security levels of Reserved3 and Reserved2 because they are undefined.

If you use the IP Security Option (IPSO) to block transmission out of unclassified interfaces, and you use one of the Reserved security levels, you *must* enable this feature to preserve network security.

Examples

The following example allows a security level of Reserved through Ethernet interface 0:

```
interface ethernet 0
 ip security reserved-allowed
```

Related Commands

Command	Description
ip security add	Adds a basic security option to all outgoing packets.

Command	Description
ip security dedicated	Sets the level of classification and authority on the interface.
ip security extended-allowed	Accepts packets on an interface that has an Extended Security Option present.
ip security first	Prioritizes the presence of security options on a packet.
ip security ignore-authorities	Causes the Cisco IOS software to ignore the authorities field of all incoming packets.
ip security implicit-labelling	Forces the Cisco IOS software to accept packets on the interface, even if they do not include a security option.
ip security multilevel	Sets the range of classifications and authorities on an interface.
ip security strip	Removes any basic security option on outgoing packets on an interface.

ip security strip

To remove any basic security option on outgoing packets on an interface, use the **ip security strip** command in interface configuration mode. To restore security options, use the **no** form of this command.

ip security strip

no ip security strip

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Interface configuration

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.

Usage Guidelines

The removal procedure is performed after all security tests in the router have been passed. This command is not allowed for multilevel interfaces.

Examples

The following example removes any basic security options on outgoing packets on Ethernet interface 0:

```
interface ethernet 0
 ip security strip
```

Related Commands

Command	Description
ip security add	Adds a basic security option to all outgoing packets.
ip security dedicated	Sets the level of classification and authority on the interface.
ip security extended-allowed	Accepts packets on an interface that has an Extended Security Option present.

Command	Description
ip security first	Prioritizes the presence of security options on a packet.
ip security ignore-authorities	Causes the Cisco IOS software to ignore the authorities field of all incoming packets.
ip security implicit-labelling	Forces the Cisco IOS software to accept packets on the interface, even if they do not include a security option.
ip security multilevel	Sets the range of classifications and authorities on an interface.
ip security reserved-allowed	Treats as valid any packets that have Reserved1 through Reserved4 security levels.

ip source-track through ivrf

ip source-track

To enable IP source tracking for a specified host, use the **ip source-track**command in global configuration mode. To disable IP source tracking, use the **no** form of this command.

ip source-track *ip-address*

no ip source-track *ip-address*

Syntax Description

ip-address	Destination IP address of the host that is to be tracked.

Command Default

IP address tracking is not enabled.

Command Modes

Global configuration

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

IP source tracking allows you to gather information about the traffic that is flowing to a host that is suspected of being under attack. It also allows you to easily trace a denial-of-service (DoS) attack to its entry point into the network.

After you have identified the destination that is being attacked, enable tracking for the destination address on the whole router by entering the ip source-track command.

Examples

The following example shows how to configure IP source tracking on all line cards and port adapters in the router. In this example, each line card or port adapter collects traffic flow data to host address 100.10.0.1 for

2 minutes before creating an internal system log entry; packet and flow information recorded in the system log is exported for viewing to the route processor or switch processor every 60 seconds.

```
Router# configure interface
Router(config)# ip source-track 10.10.0.1
Router(config)# ip source-track syslog-interval 2
Router(config)# ip source-track export-interval 60
```

Related Commands

Command	Description
ip source-track address-limit	Configures the maximum number of destination hosts that can be simultaneously tracked at any given moment.
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.
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	Displays traffic flow statistics for tracked IP host addresses.
show ip source-track export flows	Displays the last 10 packet flows that were exported from the line card to the route processor.

ip source-track address-limit

To configure the maximum number of destination hosts that can be simultaneously tracked at any given moment, use the **ip source-track address-limit**command in global configuration mode. To cancel this administrative limit and return to the default, use the **no** form of this command.

ip source-track address-limit *number*

no ip source-track address-limit *number*

Syntax Description

number	Maximum number of hosts that can be tracked.

Command Default

An unlimited number of hosts can be tracked.

Command Modes

Global configuration

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

After you have configured at least one destination IP address for source tracking (via the **ip source-track** command), you can limit the number of destination IP addresses that can be tracked via the **ip source-track address-limit** command.

Examples

The following example shows how to configure IP source tracking for data that flows to host 100.10.1.1 and limit IP source tracking to 10 IP addresses:

```
Router(config)# ip source-track 100.10.0.1
Router(config)# ip source-track address-limit 10
```

Related Commands

Command	Description
ip source-track	Enables IP source tracking for a specified host.
show ip source-track	Displays traffic flow statistics for tracked IP host addresses.

ip source-track export-interval

To set the time interval (in seconds) in which IP source tracking statistics are exported from the line card to the route processor (RP), use the **ip source-track export-interval**command in global configuration mode. To return to default functionality, use the **no** form of this command.

ip source-track export-interval *number*

no ip source-track export-interval *number*

Syntax Description

number	Number of seconds that pass before IP source tracking statistics are exported.

Command Default

Traffic flow information is exported from the line card to the RP every 30 seconds.

Command Modes

Global configuration

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

Use the **ip source-track export-interval** command to specify the frequency in which IP source tracking information is sent to the RP for viewing.

Note This command can be issued only on distributed platforms such as the gigabit route processor (GRP) and the route switch processor (RSP).

Examples

The following example shows how to configure IP source tracking on all line cards and port adapters in the router. In this example, each line card or port adapter collects traffic flow data to host address 100.10.0.1 for 2 minutes before creating an internal system log entry; packet and flow information recorded in the system log is exported for viewing to the route processor or switch processor every 60 seconds.

```
Router# configure interface
Router(config)# ip source-track 10.10.0.1
Router(config)# ip source-track syslog-interval 2
Router(config)# ip source-track export-interval 60
```

Related Commands

Command	Description
ip source-track	Enables IP source tracking for a specified host.
show ip source-track export flows	Displays the last 10 packet flows that were exported from the line card to the route processor.

ip source-track syslog-interval

To set the time interval (in minutes) in which syslog messages are generated if IP source tracking is enabled on a device, use the **ip source-track syslog-interval**command in global configuration mode. To cancel this setting and disable syslog generation, use the **no** form of this command.

ip source-track syslog-interval *number*

no ip source-track syslog-interval *number*

Syntax Description

number	IP address of the destination that is to be tracked.

Command Default

Syslog messages are not generated.

Command Modes

Global configuration

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

Use the **ip source-track syslog-interval** command to track the source interfaces of traffic that are destined to a particular address.

Examples

The following example shows how to configure IP source tracking on all line cards and port adapters in the router. In this example, each line card or port adapter collects traffic flow data to host address 100.10.0.1 for

2 minutes before creating an internal system log entry; packet and flow information recorded in the system log is exported for viewing to the route processor or switch processor every 60 seconds.

```
Router# configure interface
Router(config)# ip source-track 10.10.0.1
Router(config)# ip source-track syslog-interval 2
Router(config)# ip source-track export-interval 60
```

Related Commands

Command	Description
ip source-track	Enables IP source tracking for a specified host.
show ip source-track	Displays traffic flow statistics for tracked IP host addresses.

ip ssh

To configure Secure Shell (SSH) control parameters on your router, use the **ip ssh** command in global configuration mode. To restore the default value, use the **no** form of this command.

ip ssh [**timeout** *seconds*| **authentication-retries** *integer*]

no ip ssh [**timeout** *seconds*| **authentication-retries** *integer*]

Syntax Description

timeout	(Optional) The time interval that the router waits for the SSH client to respond. This setting applies to the SSH negotiation phase. Once the EXEC session starts, the standard timeouts configured for the vty apply. By default, there are 5 vtys defined (0-4), therefore 5 terminal sessions are possible. After the SSH executes a shell, the vty timeout starts. The vty timeout defaults to 10 minutes.
seconds	(Optional) The number of seconds until timeout disconnects, with a maximum of 120 seconds. The default is 120 seconds.
authentication- retries	(Optional) The number of attempts after which the interface is reset.
integer	(Optional) The number of retries, with a maximum of 5 authentication retries. The default is 3.

Command Default

SSH control parameters are set to default router values.

Command Modes

Global configuration (config)

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(1) T.
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.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 series routers.

Usage Guidelines

Before you configure SSH on your router, you must enable the SSH server using the **crypto key generate rsa**command.

Examples

The following examples configure SSH control parameters on your router:

```
ip ssh timeout 120
ip ssh authentication-retries 3
```

ip ssh break-string

To configure a string that, when received from a Secure Shell (SSH) client, will cause the Cisco IOS SSH server to transmit a break signal out an asynchronous line, use the **ip ssh break-string** command in global configuration mode. To remove the string, use the **no** form of this command.

ip ssh break-string *string*

no ip ssh break-string *string*

Syntax Description

string	Any sequence of characters not including embedded whitespace. Include control characters by prefixing them with ^V (control/V) *or denote them using the \000 notation (that is, a backslash followed by the the ASCII value of the character in three octal digits.)*

Command Default

Break signal is not enabled

Command Modes

Global configuration

Command History

Release	Modification
12.3(2)	This command was introduced.
12.3(2)T	This command was integrated into Cisco IOS Release 12.3(2)T.

Usage Guidelines

Note This break string is used only for SSH sessions that are outbound on physical lines using the SSH Terminal-Line Access feature. This break string is not used by the Cisco IOS SSH client, nor is it used by the Cisco IOS SSH server when the server uses a virtual terminal (VTY) line. This break string does not provide any interoperability with the method that is described in the Internet Engineering Task Force (IETF) Internet-Draft “Session Channel Break Extension” (draft-ietf-secsh-break-02.txt).

Note In some versions of Cisco IOS, if the SSH break string is set to a single character, the Cisco IOS server will not immediately process that character as a break signal on receipt of that character but will delay until it has received a subsequent character. A break string of two or more characters will be immediately processed as a break signal after the last character in the string has been received from the SSH client.

Examples

The following example shows that the control-B character (ASCII 2) has been set as the SSH break string:

```
Router (config)# ip ssh break-string \002
```

Related Commands

Command	Description
ip ssh port	Enables SSH access to TTY lines.

ip ssh dh min size

To configure the modulus size on the Secure Shell (SSH) server, use the **ip ssh dh min size** command in privileged EXEC mode. To disable the configuration, use the **no** form of this command.

ip ssh dh min size [*number*]

no ip ssh dh min size

Syntax Description

number	(Optional) Minimum number of bits in the key size. The default is 1024.

Command Default

Bit key support is disabled.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.
15.1(2)S	This command was integrated into Cisco IOS Release 15.1(2)S.

Usage Guidelines

Use the **ip ssh dh min size**command to ensure that the CLI is successfully parsed from either the client side or the server side.

Examples

The following example shows how to set the minimum modulus size to 2048 bits:

```
Router> enable
Router# ip ssh dh min size 2048
```

Related Commands

Command	Description
show ip ssh	Displays the status of SSH server connections.

ip ssh dscp

To specify the IP differentiated services code point (DSCP) value that can be set for a Secure Shell (SSH) configuration, use the **ip ssh dscp**command in global configuration mode. To restore the default value, use the **no** form of this command.

ip ssh dscp *number*

no ip ssh dscp *number*

Syntax Description

number	Value that can be set. The default value is 0 (zero). - *number* --0 through 63.

Command Default

The IP DSCP value is not specified.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(20)S	This command was introduced.
12.2SR	This command is supported in the Cisco IOS Release 12.2SR train. Support in a specific 12.2SR train depends on your feature set, platform, and platform hardware.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX train depends on your feature set, platform, and platform hardware.
12.4(22)T	This command was integrated into Cisco IOS Release 12.4(22)T.

Usage Guidelines

IP DSCP values can be configured on both the SSH client and the SSH server for SSH traffic that is generated on either end.

Examples

The following example shows that the DSCP value is set to 35:

```
Router(config)# ip ssh dscp 35
```

Related Commands

Command	Description
ip ssh precedence	Specifies the IP precedence value that may be set.

ip ssh maxstartups

To set the maximum concurrent sessions allowed on a Secure Shell (SSH), use the **ip ssh maxstartups** command in global configuration mode. To disable the configuration, use the **no** form of this command.

ip ssh maxstartups [*number*]

no ip ssh maxstartups [*number*]

Syntax Description

number	(Optional) Number of connections to be accepted concurrently. The range is from 2 to 128. The default is 128.

Command Default

The number of maximum concurrent sessions is 128.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
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.

Usage Guidelines

You must create RSA keys to enable SSH. The RSA key must be at least 768 bits for SSHv2.

Examples

The following example shows how to set the maximum concurrent sessions allowed on a SSH to 100:

```
Router# configure terminal
Router(config)# ip ssh maxstartups 100
```

Related Commands

Command	Description
debug ip ssh	Displays debugging messages for SSH.
ip ssh	Configures SSH control parameters on your router.

ip ssh port

To enable secure access to tty (asynchronous) lines, use the **ip ssh port**command in global configuration mode. To disable this functionality, use the **no** form of this command.

ip ssh port *por-tnum* **rotary** *group*

no ip ssh port *por-tnum* **rotary** *group*

Syntax Description

port-num	Specifies the port, such as 2001, to which Secure Shell (SSH) needs to connect.
rotary *group*	Specifies the defined rotary that should search for a valid name.

Command Default

This command is disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.2(2)T	This command was introduced.

Usage Guidelines

The ip ssh port co mmand supports a functionality that replaces reverse Telnet with SSH. Use this command to securely access the devices attached to the serial ports of a router and to perform the following tasks:

- Connect to a router with multiple terminal lines that are connected to consoles of other devices.
- Allow network available modems to be securely accessed for dial-out.

Examples

The following example shows how to configure the SSH Terminal-Line Access feature on a modem that is used for dial-out on lines 1 through 200:

```
line 1 200
 no exec
 login authentication default
 rotary 1
 transport input ssh
ip ssh port 2000 rotary 1
```

The following example shows how to configure the SSH Terminal-Line Access feature to access the console ports of various devices that are attached to the serial ports of the router. For this type of access, each line is put into its own rotary, and each rotary is used for a single port. In this example, lines 1 through 3 are used, and the port (line) mappings of the configuration are as follows: Port 2001 = Line 1, Port 2002 = Line 2, and Port 2003 = Line 3.

```
line 1
 no exec
 login authentication default
 rotary 1
 transport input ssh
line 2
 no exec
 login authentication default
 rotary 2
 transport input ssh
line 3
 no exec
 login authentication default
 rotary 3
 transport input ssh
ip ssh port 2001 rotary 1 3
```

From any UNIX or UNIX-like device, the following command is typically used to form an S SH session:

```
ssh -c 3des -p 2002 router.example.com
```

This command will initiate an SSH session using the Triple DES cipher to the device known as “router.example.com,” which uses port 2002. This device will connect to the device on Line 2, which was associated with port 2002. Similarly, many Windows SSH packages have related methods of selecting the cipher and the port for this access.

Related Commands

Command	Description
crypto key generate rsa	Enables the SSH server.
debug ip ssh	Displays debugging messages for SSH.
ip ssh	Configures SSH control variables on your router.
line	Identifies a specific line for configuration and begins the command in line configuration mode.
rotary	Defines a group of lines consisting of one or more lines.
ssh	Starts an encrypted session with a remote networking device.
transport input	Defines which protocols to use to connect to a specific line of the router.

ip ssh precedence

To specify the IP precedence value that can be set for a Secure Shell (SSH) configuration, use the **ip ssh precedence**command in global configuration mode. To restore the default value, use the **no** form of this command.

ip ssh precedence *number*

no ip ssh precedence *number*

Syntax Description

number	Value that can be set. The default value is 0 (zero). • *number* --0 through 7.

Command Default

The IP precedence value is not specified.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(20)S	This command was introduced.
12.2SR	This command is supported in the Cisco IOS Release 12.2SR train. Support in a specific 12.2SR train depends on your feature set, platform, and platform hardware.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX train depends on your feature set, platform, and platform hardware.
12.4(22)T	This command was integrated into Cisco IOS Release 12.4(22)T.

Usage Guidelines

IP precedence values can be configured on both the SSH client and the SSH server for SSH traffic that is generated on either end.

Examples

The following example shows that up to six IP precedence values can be set:

```
Router(config)# ip precedence value 6
```

Related Commands

Command	Description
ip ssh dscp	Specifies the IP DSCP value that can be set for an SSH configuration.

ip ssh pubkey-chain

To configure Secure Shell RSA (SSH-RSA) keys for user and server authentication on the SSH server, use the **ip ssh pubkey-chain** command in global configuration mode. To remove SSH-RSA keys for user and server authentication on the SSH server, use the **no** form of this command.

ip ssh pubkey-chain

no ip ssh pubkey-chain

Syntax Description

This command has no arguments or keywords.

Command Default

SSH-RSA keys are not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced.
15.1(1)S	This command was integrated into Cisco IOS Release 15.1(1)S.

Usage Guidelines

Use the **ip ssh pubkey-chain**command to ensure SSH server and user public key authentication.

Examples

The following example shows how to enable public key generation:

```
Router(config)# ip ssh pubkey-chain
```

Related Commands

Command	Description
ip ssh stricthostkeycheck	Enables strict host key checking on the SSH server.

ip ssh rekey

To configure a time-based rekey or a volume-based rekey for a secure shell (SSH) session, use the **ip ssh rekey** command in global configuration mode. To disable the rekey, use the **no** form of this command.

ip ssh rekey{**time** *time* | **volume** *volume*}

no ip ssh rekey

Syntax Description

time *time*	Rekey time, in minutes. The range is from 10 minutes to 1440 minutes.
volume *volume*	Amount of rekeyed data, in kilobytes. The range is from 100 KB to 4194303 KB.

Command Default

The rekey time or volume is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(2)SE	This command was introduced.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

SSH rekey initiation occurs when the session key negotiated at connection startup is used for an unusually long time. A server or a client initiates a new key exchange based on the maximum number of packets transmitted or based on a specified time. The **ip ssh rekey time** command enables you to specify a time for the rekey initiation. The **ip ssh rekey volume**command enables you to specify a volume that is based on the maximum number of packets transmitted for the rekey initiation. When you use the **no ip ssh rekey**command, the configured time-based rekey or volume-based rekey is disabled.

Examples

The following example shows how to configure a time-based rekey for an SSH session:

```
Device(config)# ip ssh rekey time 108
```

The following example shows how to configure a volume-based rekey for an SSH session:

```
Device(config)# ip ssh rekey volume 500
```

Related Commands

Command	Description
ip ssh	Configures SSH control parameters on a device.

ip ssh rsa keypair-name

To specify which Rivest, Shimar, and Adelman (RSA) key pair to use for a Secure Shell (SSH) connection, use the **ip ssh rsa keypair-name**command in global configuration mode. To disable the key pair that was configured, use the **no** form of this command.

ip ssh rsa keypair-name *keypair-name*

no ip ssh rsa keypair-name *keypair-name*

Syntax Description

keypair-name	Name of the key pair.

Command Default

If this command is not configured, SSH will use the first RSA key pair that is enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.3(2)XE	This command was integrated into Cisco IOS Release 12.3(2)XE.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.3(7)JA	This command was integrated into Cisco IOS Release 12.3(7)JA.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.2(33)SXI4	This command was integrated into Cisco IOS Release 12.2(33)SXI4.

Usage Guidelines

Using the **ip ssh rsa keypair-name** command, you can enable an SSH connection using RSA keys that you have configured using the *keypair-name* argument. Previously, SSH was tied to the first RSA keys that were generated (that is, SSH was enabled when the first RSA key pair was generated). The previous behavior still exists, but by using the **ip ssh rsa keypair-name** command, you can overcome that behavior. If you configure the **ip ssh rsa keypair-name** command with a key pair name, SSH is enabled if the key pair exists, or SSH will be enabled if the key pair is generated later. If you use this command, you are not forced to configure a hostname and a domain name.

Note A Cisco IOS router can have many RSA key pairs.

Examples

The following example shows how to specify the RSA key pair “sshkeys” for an SSH connection:

```
Router# configure terminal
Router(config)# ip ssh rsa keypair-name sshkeys
```

Related Commands

Command	Description
debug ip ssh	Displays debug messages for SSH.
disconnect ssh	Terminates a SSH connection on your router.
ip ssh	Configures SSH control parameters on your router.
ip ssh version	Specifies the version of SSH to be run on a router.
show ip ssh	Displays the SSH connections of your router.

ip ssh server authenticate user

To enable the user authentication methods available in the Secure Shell (SSH) server, use the **ip ssh server authenticate user** command in global configuration mode. To disable the user authentication methods available in the SSH server, use the **no** form of this command. To return to the default behavior in which all user authentication methods are enabled in the predefined order, use the **default** form of this command.

ip ssh server authenticate user {**publickey** | **keyboard** | **password**}

no ip ssh server authenticate user {**publickey** | **keyboard** | **password**}

default ip ssh server authenticate user

Syntax Description

publickey	Enables the public-key-based authentication method.
keyboard	Enables the keyboard-interactive-based authentication method.
password	Enables the password-based authentication method.

Command Default

All three user authentication methods are enabled in the following predefined order:

- Public-key authentication method
- Keyboard-interactive authentication method
- Password authentication method

Command Modes

Global configuration (config)

Command History

Release	Modification
15.3(3)M	This command was introduced.
Cisco IOS XE Release 3.10S	This command was integrated into Cisco IOS XE Release 3.10S.

Usage Guidelines

The **no ip ssh authenticate user** {**publickey** | **keyboard** | **pasword**} command enables the SSH server to choose a preferred user authentication method by disabling any of the other supported user authentication methods. By default, all user authentication methods are enabled on the SSH server in the following predefined order:

- Public-key authentication method

- Keyboard-interactive authentication method
- Password authentication method

The following messages are displayed during specific scenarios:

- If the public-key-based authentication method is disabled using the **no ip ssh server authenticate user publickey** command, the RFC 4252 (The Secure Shell (SSH) Authentication Protocol) behavior in which public-key authentication is mandatory is overridden and the following warning message is displayed:

  ```
  %SSH: Publickey disabled. Overriding RFC
  ```

- If all three authentication methods are disabled, the following warning message is displayed:

  ```
  %SSH: No auth method configured. Incoming connection will be dropped
  ```

- In the event of an incoming SSH session request from the SSH client when all three user authentication methods are disabled on the SSH server, the connection request is dropped at the SSH server and a system log message is available in the following format:

  ```
  %SSH-3-NO_USERAUTH: No auth method configured for SSH Server. Incoming connection from
   <ip address> (tty = <ttynum>) dropped
  ```

Examples

The following example shows how to disable the public-key-based authentication and keyboard-interactive-based authentication methods, allowing the SSH client to connect to the SSH server using password-based authentication:

```
Device> enable
Device# configure terminal
Device(config)# no ip ssh server authenticate user publickey
%SSH: Publickey disabled. Overriding RFC
Device(config)# no ip ssh server authenticate user keyboard
Device(config)# exit
```

The following example shows how to enable the public-key-based authentication and keyboard-interactive-based authentication methods:

```
Device> enable
Device# configure terminal
Device(config)# ip ssh server authenticate user publickey
Device(config)# ip ssh server authenticate user keyboard
Device(config)# exit
```

The following example shows how to return to the default behavior in which all user authentication methods are enabled in the predefined order:

```
Device> enable
Device# configure terminal
Device(config)# default ip ssh server authenticate user
Device(config)# exit
```

Related Commands

Command	Description
show ip ssh	Displays the version and configuration data for SSH.

ip ssh source-interface

To specify the IP address of an interface as the source address for a Secure Shell (SSH) client device, use the **ip ssh source-interface**command in global configuration mode. To remove the IP address as the source address, use the **no** form of this command.

ip ssh source-interface *interface*

no ip ssh source-interface *interface*

Syntax Description

interface	The interface whose address is used as the source address for the SSH client.

Command Default

The address of the closest interface to the destination is used as the source address (the closest interface is the output interface through which the SSH packet is sent).

Command Modes

Global configuration

Command History

Release	Modification
12.2(8)T	This command was introduced.

Usage Guidelines

By specifying this command, you can force the SSH client to use the IP address of the source interface as the source address.

Examples

In the following example, the IP address assigned to Ethernet interface 0 will be used as the source address for the SSH client:

```
ip ssh source-interface ethernet0
```

ip ssh stricthostkeycheck

To enable strict host key checking on the Secure Shell (SSH) server, use the **ip ssh stricthostcheck** command in global configuration mode. To disable strict host key checking, use the **no** form of this command.

ip ssh stricthostkeycheck

no ip ssh stricthostkeycheck

Syntax Description

This command has no arguments or keywords.

Command Default

Strict host key checking on the SSH server is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced.
15.1(1)S	This command was integrated into Cisco IOS Release 15.1(1)S.

Usage Guidelines

Use the **ip ssh stricthostkeycheck**command to ensure SSH server side strict checking. Configuring the **ip ssh stricthostkeycheck** command authenticates all servers.

Note This command is not available on SSH Version 1.

- If the **ip ssh pubkey-chain** command is not configured, the **ip ssh stricthostkeycheck** command will lead to connection failure in SSH Version 2.

Examples

The following example shows how to enable strict host key checking:

```
Router(config)# ip ssh stricthostkeycheck
```

Related Commands

Command	Description
ip ssh pubkey-chain	Configures SSH-RSA keys for user and server authentication on the SSH server.

ip ssh version

To specify the version of Secure Shell (SSH) to be run on a router, use the **ip ssh version**command in global configuration mode. To disable the version of SSH that was configured and to return to compatibility mode, use the **no** form of this command.

ip ssh version [**1**| **2**]

no ip ssh version [**1**| **2**]

Syntax Description

1	(Optional) Router runs only SSH Version 1.
2	(Optional) Router runs only SSH Version 2.

Command Default

If this command is not configured, SSH operates in compatibility mode, that is, Version 1 and Version 2 are both supported.

Command Modes

Global configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.3(2)XE	This command was integrated into Cisco IOS Release 12.3(2)XE.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.3(7)JA	This command was integrated into Cisco IOS Release 12.3(7)JA.
12.0(32)SY	This command was integrated into Cisco IOS Release 12.0(32)SY.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
15.2(2)SA2	This command was implemented on the Cisco ME 2600X Series Ethernet Access Switches.

Usage Guidelines

You can use this command with the **2** keyword to ensure that your router will not inadvertently establish a weaker SSH Version 1 connection.

Examples

The following example shows that only SSH Version 1 support is configured:

```
Router (config)# ip ssh version 1
```

The following example shows that only SSH Version 2 is configured:

```
Router (config)# ip ssh version 2
```

The following example shows that SSH Versions 1 and 2 are configured:

```
Router (config)# no ip ssh version
```

Related Commands

Command	Description
debug ip ssh	Displays debug messages for SSH.
disconnect ssh	Terminates a SSH connection on your router.
ip ssh	Configures SSH control parameters on your router.
ip ssh rsa keypair-name	Specifies which RSA key pair to use for a SSH connection.
show ip ssh	Displays the SSH connections of your router.

ip tacacs source-interface

To use the IP address of a specified interface for all outgoing TACACS+ packets, use the **ip tacacs source-interface** command in global configuration or server-group configuration mode. To disable use of the specified interface IP address, use the **no** form of this command.

ip tacacs source-interface *subinterface-name*

no ip tacacs source-interface

Syntax Description

subinterface-name	Name of the interface that TACACS+ uses for all of its outgoing packets.

Command Default

None

Command Modes

Global configuration (config)

Server-group configuration (server-group)

Command History

Release	Modification
10.0	This command was introduced.
12.3(7)T	This command was introduced in server-group configuration mode.
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)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.

Usage Guidelines

Use this command to set the IP address of a subinterface for all outgoing TACACS+ packets. This address is used as long as the interface is in the *up* state. In this way, the TACACS+ server can use one IP address entry associated with the network access client instead of maintaining a list of all IP addresses.

This command is especially useful in cases where the router has many interfaces and you want to ensure that all TACACS+ packets from a particular router have the same IP address.

The specified sub-interface should have a valid IP address and should be in the *up* state for a valid configuration. If the specified sub-interface does not have a valid IP address or is in the *down* state, TACACS+ enforces the source-interface configuration. In case the interface has no IP address, a null IP address is sent. To avoid this, add a valid IP address to the sub-interface or bring the sub-interface to the *up* state.

Note This command can be configured globally or in server-group configuration mode. If this command is configured in the server-group configuration mode, the IP address of the specified interface is used for packets that are going only to servers that are defined in that server group. If this command is not configured in server-group configuration mode, the global configuration applies.

Examples

The following example makes TACACS+ use the IP address of subinterface “s2” for all outgoing TACACS+ packets:

```
ip tacacs source-interface s2
```

In the following example, TACACS+ is to use the IP address of Loopback0 for packets that are going only to server 10.1.1.1:

```
aaa group server tacacs+ tacacs1
    server-private 10.1.1.1 port 19 key cisco
    ip vrf forwarding cisco
    ip tacacs source-interface Loopback0
  ip vrf cisco
   rd 100:1
  interface Loopback0
   ip address 10.0.0.2 255.0.0.0
   ip vrf forwarding cisco
```

Related Commands

Command	Description
ip radius source-interface	Forces RADIUS to use the IP address of a specified interface for all outgoing RADIUS packets.
ip telnet source-interface	Allows a user to select an address of an interface as the source address for Telnet connections.
ip tftp source-interface	Allows a user to select the interface whose address will be used as the source address for TFTP connections.
ip vrf forwarding (server-group)	Configures the VRF reference of an AAA RADIUS or TACACS+ server group.
server-private	Configures the IP address of the private RADIUS or TACACS+ server for the group server.

ip tcp intercept connection-timeout

To change how long a TCP connection will be managed by the TCP intercept after no activity, use the **ip tcp intercept connection-timeout** command in global configuration mode. To restore the default, use the **no** form of this command.

ip tcp intercept connection-timeout *seconds*

no ip tcp intercept connection-timeout [*seconds*]

Syntax Description

seconds	Time (in seconds) that the software will still manage the connection after no activity. The minimum value is 1 second. The default is 86,400 seconds (24 hours).

Command Default

86,400 seconds (24 hours)

Command Modes

Global configuration

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 **ip tcp intercept connection-timeout**command to change how long a TCP connection will be managed by the TCP intercept after a period of inactivity.

Examples

The following example sets the software to manage the connection for 12 hours (43,200 seconds) after no activity:

```
ip tcp intercept connection-timeout 43200
```

ip tcp intercept drop-mode

To set the TCP intercept drop mode, use the **ip tcp intercept drop-mode** command in g lobal configuration mode . To restore the default, use the **no** form of this command.

ip tcp intercept drop-mode [**oldest**| **random**]

no ip tcp intercept drop-mode [**oldest**| **random**]

Syntax Description

oldest	(Optional) S oftware drops the oldest partial connection. This is the default.
random	(Optional) Software drops a randomly selected partial connection.

Command Default

oldest

Command Modes

Global configuration

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

If the number of incomplete connections exceeds 1100 or the number of connections arriving in the last 1 minute exceeds 1100, the TCP intercept feature becomes more aggressive. When this happens, each new arriving connection causes the oldest partial connection to be deleted, and the initial retransmission timeout is reduced by half to 0.5 seconds (and so the total time trying to establish the connection will be cut in half).

Note that the 1100 thresholds can be configured with the **ip tcp intercept max-incomplete high** and **ip tcp intercept one-minute high** commands.

Use the **ip tcp intercept drop-mode** command to change the dropping strategy from oldest to a random drop.

Examples

The following example sets the drop mode to random:

```
ip tcp intercept drop-mode random
```

Related Commands

Command	Description
ip tcp intercept max-incomplete high	Defines the maximum number of incomplete connections allowed before the software enters aggressive mode.
ip tcp intercept max-incomplete low	Defines the number of incomplete connections below which the software leaves aggressive mode.
ip tcp intercept one-minute high	Defines the number of connection requests received in the last one-minute sample period before the software enters aggressive mode.
ip tcp intercept one-minute low	Defines the number of connection requests below which the software leaves aggressive mode.

ip tcp intercept finrst-timeout

To chang e how long after receipt of a reset or FIN-exchange the software ceases to manage the connection, use the **ip tcp intercept finrst-timeout** command in global configuration mode. To restore the default, use the **no**form of this command.

ip tcp intercept finrst-timeout *seconds*

no ip tcp intercept finrst-timeout [*seconds*]

Syntax Description

seconds	Time (in seconds) after receiving a reset or FIN-exchange that the software ceases to manage the connection. The minimum value is 1 second. The default is 5 seconds.

Command Default

5 seconds

Command Modes

Global configuration

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

Even after the two ends of the connection are joined, the software intercepts packets being sent back and forth. Use this command if you need to adjust how soon after receiving a reset or FIN-exchange the software stops intercepting packets.

Examples

The following example sets the software to wait for 10 seconds before it leaves intercept mode:

```
ip tcp intercept finrst-timeout 10
```

ip tcp intercept list

To e nable TCP intercept, use the **ip tcp intercept list** command in globa l configuration mode . To disable TCP intercept, use the **no** form of this command.

ip tcp intercept list *access-list-number*

no ip tcp intercept list *access-list-number*

Syntax Description

access-list-number	E xtended access list number in the range from 100 to 199.

Command Default

Disabled

Command Modes

Global configuration

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

The TCP intercept feature intercepts TCP connection attempts and shields servers from TCP SYN-flood attacks, also known as denial-of-service attacks.

TCP packets matching the access list are presented to the TCP intercept code for processing, as determined by the **ip tcp intercept mode**command. The TCP intercept code either intercepts or watches the connections.

To have all TCP connection attempts submitted to the TCP intercept code, have the access list match everything.

Examples

The following example configuration defines access list 101, causing the software to intercept packets for all TCP servers on the 192.168.1.0/24 subnet:

```
ip tcp intercept list 101
!
access-list 101 permit tcp any 192.168.1.0 0.0.0.255
```

Related Commands

Command	Description
access-list (IP extended)	Defines an extended IP access list.
ip tcp intercept mode	Changes the TCP intercept mode.
show tcp intercept connections	Displays TCP incomplete and established connections.
show tcp intercept statistics	Displays TCP intercept statistics.

ip tcp intercept max-incomplete

To define either the number of incomplete connections below which the software leaves aggressive mode or the maximum number of incomplete connections allowed before the software enters aggressive mode, use the **ip tcp intercept max-incomplete**command in global configuration mode . To restore the default, use the **no** form of this command.

ip tcp intercept max-incomplete low *number* **high** *number*

no ip tcp intercept max-incomplete [**low** *number* **high** *number*]

Syntax Description

low *number*	Defines the number of incomplete connections below which the software leaves aggressive mode. The range is 1 to 2147483647. The default is 900
high *number*	Defines the number of incomplete connections allowed, above which the software enters aggressive mode. The range is from 1 to 2147483647. The default is 1100.

Command Default

The number of incomplete connections below which the software leaves aggressive mode is 900.

The maximum number of incomplete connections allowed before the software enters aggressive mode is 1100.

Command Modes

Global configuration

Command History

Release	Modification
12.4(15)T	This command was introduced in Cisco IOS Release 12.4(15)T. This command replaces the **ip tcp intercept max-incomplete low** and the **ip tcp intercept max-incomplete high** commands.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

There are two factors that determine aggressive mode: connection requests and incomplete connections.

By default, if both the number of connection requests and the number of incomplete connections is 900 or lower, aggressive mode ends.

By default, if either the number of connection requests or the number of incomplete connections is 1100 or greater, aggressive mode begins.

The number of connection requests may be defined by the **ip tcp intercept one-minute** command and the number of incomplete connections may be defined by the **ip tcp intercept max-incomplete**command.

Characteristics of Aggressive Mode

The following are the characteristics of aggressive mode:

- Each new arriving connection causes the oldest partial connection to be deleted.
- The initial retransmission timeout, the total time the router attempts to establish the connection, is reduced from 1 second to 0.5 seconds.
- The watch-timeout period is reduced from 30 seconds to 15 seconds.

Examples

The following example sets the software to leave aggressive mode when the number of incomplete connections falls below 1000 and allows 1500 incomplete connections before the software enters aggressive mode. The running configuration is also shown.

```
Router(config)# ip tcp intercept max-incomplete low 1000 high 1500
Router(config)# show running config | i ip tcp
     ip tcp intercept one-minute low 1000 high 1400
```

Related Commands

Command	Description
ip tcp intercept drop-mode	Sets the TCP intercept drop mode.
ip tcp intercept one-minute	Defines the number of connection requests below which the software leaves aggressive mode and the number of connection requests received before the software enters aggressive mode.

ip tcp intercept max-incomplete high

Note Effective with Cisco IOS Release 12.2(33)SXH and Cisco IOS Release 12.4(15)T, the **ip tcp intercept max-incomplete high** command is replaced by the **ip tcp intercept max-incomplete**command. See the **ip tcp intercept max-incomplete** command for more information.

To define the maximum number of incomplete connections allowed before the software enters aggressive mode, use the **ip tcp intercept max-incomplete high**command in global configuration mode . To restore the default, use the **no** form of this command.

ip tcp intercept max-incomplete high *number*

no ip tcp intercept max-incomplete high [*number*]

Syntax Description

number	Defines the number of incomplete connections allowed, above which the software enters aggressive mode. The range is from 1 to 2147483647. The default is 1100.

Command Default

1100 incomplete connections

Command Modes

Global configuration

Command History

Release	Modification
11.2 F	This command was introduced.
12.4(15)T	This command was replaced by the **ip tcp intercept max-incomplete** command.
12.2(33)SXH	This command was replaced by the **ip tcp intercept max-incomplete** command.

Usage Guidelin

Note If you are running Cisco IOS Release 12.2(33)SXH or Cisco IOS Release 12.4(15)T and issue the **ip tcp intercept max-incomplete high** command, it will be accepted by the router, but a message will be displayed stating that the **ip tcp intercept max-incomplete high** command has been replaced by the **ip tcp intercept max-incomplete** command.

If the number of incomplete connections exceeds the *number* configured, the TCP intercept feature becomes aggressive. The following are the characteristics of aggressive mode:

- Each new arriving connection causes the oldest partial connection to be deleted.
- The initial retransmission timeout is reduced by half to 0.5 seconds (and so the total time trying to establish the connection is cut in half).
- The watch-timeout is cut in half (from 30 seconds to 15 seconds).

You can change the drop strategy from the oldest connection to a random connection with the **ip tcp intercept drop-mode** command.

Note The two factors that determine aggressive mode (connection requests and incomplete connections) are related and work together. When the value of *either***ip tcp intercept one-minute high** or **ip tcp intercept max-incomplete high** is exceeded, aggressive mode begins. When *both* connection requests and incomplete connections fall below the values of ip tcp intercept one-minute low and **ip tcp intercept max-incomplete low**, aggressive mode ends.

The software will back off from its aggressive mode when the number of incomplete connections falls below the number specified by the **ip tcp intercept max-incomplete low** command.

Examples

The following example allows 1500 incomplete connections before the software enters aggressive mode:

```
ip tcp intercept max-incomplete high 1500
```

Related Commands

Command	Description
ip tcp intercept drop-mode	Sets the TCP intercept drop mode.
ip tcp intercept max-incomplete low	Defines the number of incomplete connections below which the software leaves aggressive mode.
ip tcp intercept one-minute high	Defines the number of connection requests received in the last one-minutes sample period before the software enters aggressive mode.
ip tcp intercept one-minute low	Defines the number of connection requests below which the software leaves aggressive mode.

ip tcp intercept max-incomplete low

Note Effective with Cisco IOS Release 12.2(33)SXH and Cisco IOS Release 12.4(15)T, the **ip tcp intercept max-incomplete low** command is replaced by the **ip tcp intercept max-incomplete**command. See the **ip tcp intercept max-incomplete** command for more information.

To define the number of incomplete connections below which the software leaves aggressive mode, use the **ip tcp intercept max-incomplete low**command in global configuration mode . To restore the default, use the **no** form of this command.

ip tcp intercept max-incomplete low *number*

no ip tcp intercept max-incomplete low [*number*]

Syntax Description

number	Defines the number of incomplete connections below which the software leaves aggressive mode. The range is 1 to 2147483647. The default is 900.

Command Default

900 incomplete connections

Command Modes

Global configuration

Command History

Release	Modification
11.2 F	This command was introduced.
12.4(15)T	This command was replaced by the **ip tcp intercept max-incomplete** command.
12.2(33)SXH	This command was replaced by the **ip tcp intercept max-incomplete** command.

Usage Guidelin

Note If you are running Cisco IOS Release 12.2(33)SXH, or Cisco IOS Release 12.4(15)T and issue the **ip tcp intercept max-incomplete low** command, it will be accepted by the router, but a message will be displayed stating that the **ip tcp intercept max-incomplete high**command has been replaced by the **ip tcp intercept max-incomplete** command.

When *both* connection requests and incomplete connections fall below the values of **ip tcp intercept one-minute low** and **ip tcp intercept max-incomplete low**, the TCP intercept feature leaves aggressive mode.

Note The two factors that determine aggressive mode (connection requests and incomplete connections) are related and work together. When the value of *either***ip tcp intercept one-minute high**or **ip tcp intercept max-incomplete high** is exceeded, aggressive mode begins. When *both* connection requests and incomplete connections fall below the values of **ip tcp intercept one-minute low**and **ip tcp intercept max-incomplete low**, aggressive mode ends.

See the **ip tcp intercept max-incomplete high** command for a description of aggressive mode.

Examples

The following example sets the software to leave aggressive mode when the number of incomplete connections falls below 1000:

```
ip tcp intercept max-incomplete low 1000
```

Related Commands

Command	Description
ip tcp intercept drop-mode	Sets the TCP intercept drop mode.
ip tcp intercept max-incomplete high	Defines the maximum number of incomplete connections allowed before the software enters aggressive mode.
ip tcp intercept one-minute high	Defines the number of connection requests received in the last one-minutes sample period before the software enters aggressive mode.
ip tcp intercept one-minute low	Defines the number of connection requests below which the software leaves aggressive mode.

ip tcp intercept mode

To c hange the TCP intercept mode, use the **ip tcp intercept mode**command in global configuration mode. To restore the default, use the **no** form of this command.

ip tcp intercept mode {**intercept**| **watch**}

no ip tcp intercept mode [**intercept**| **watch**]

Syntax Description

intercept	Active mode in which the TCP intercept software intercepts TCP packets from clients to servers that match the configured access list and performs intercept duties. This is the default.
watch	Monitoring mode in which the software allows connection attempts to pass through the router and watches them until they are established.

Command Default

intercept

Command Modes

Global configuration

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

When TCP intercept is enabled, it operates in intercept mode by default. In intercept mode, the software actively intercepts TCP SYN packets from clients to servers that match the specified access list. For each SYN, the software responds on behalf of the server with an ACK and SYN, and waits for an ACK of the SYN from the client. When that ACK is received, the original SYN is sent to the server, and the code then performs a three-way handshake with the server. Then the two half-connections are joined.

In watch mode, the software allows connection attempts to pass through the router, but watches them until they become established. If they fail to become established in 30 seconds (or the value set by the **ip tcp intercept watch-timeout** command), a Reset is sent to the server to clear its state.

Examples

The following example sets the mode to watch mode:

```
ip tcp intercept mode watch
```

Related Commands

Command	Description
ip tcp intercept watch-timeout	Defines how long the software will wait for a watched TCP intercept connection to reach established state before sending a reset to the server.

ip tcp intercept one-minute

To define both the number of connection requests below which the software leaves aggressive mode and the number of connection requests that can be received before the software enters aggressive mode, use the **ip tcp intercept one-minute**command in gl obal configuration mode . To restore the default connection request settings, use the **no** form of this command.

ip tcp intercept one-minute low *number* **high** *number*

no ip tcp intercept one-minute [**low** *number* **high** *number*]

Syntax Description

low *number*	Specifies the number of connection requests in the last one-minute sample period below which the software leaves aggressive mode. The range is from 1 to 2147483647. The default is 900.
high *number*	Specifies the number of connection requests that can be received in the last one-minute sample period before the software enters aggressive mode. The range is 1 to 2147483647. The default is 1100.

Command Default

The default number of connection requests below which the software leaves aggressive mode is 900.

The default number of connection requests received before the software enters aggressive mode is 1100.

Command Modes

Global configuration

Command History

Release	Modification
12.4(15)T	This command was introduced in Cisco IOS Release 12.4(15)T. This command replaces the **ip tcp intercept one-minute low** and the **ip tcp intercept one-minute high** commands.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

There are two factors that determine aggressive mode: connection requests and incomplete connections.

By default, if both the number of connection requests and the number of incomplete connections is 900 or lower, aggressive mode ends.

By default, if either the number of connection requests or the number of incomplete connections is 1100 or greater, aggressive mode begins.

The number of connection requests may be defined by the **ip tcp intercept one-minute** command and the number of incomplete connections may be defined by the **ip tcp intercept max-incomplete**command. The default number of connection requests

Characteristics of Aggressive Mode

The following are the characteristics of aggressive mode:

- Each new arriving connection causes the oldest partial connection to be deleted.
- The initial retransmission timeout, the total time the router attempts to establish the connection, is reduced from 1 second to 0.5 seconds.
- The watch-timeout period is reduced from 30 seconds to 15 seconds.

Examples

The following example sets the software to leave aggressive mode when the number of connection requests falls below 1000 and allows 1400 connection requests before the software enters aggressive mode. The the running configuration is then shown.

```
Router(config)# ip tcp intercept one-minute low 1000 high 1400
Router(config)# show running configuration | i ip tcp
     ip tcp intercept one-minute low 1000 high 1400
```

Related Commands

Command	Description
ip tcp intercept drop-mode	Sets the TCP intercept drop mode.
ip tcp intercept max-incomplete	Defines the number of incomplete connections below which the software leaves aggressive mode or the maximum number of incomplete connections allowed before the software enters aggressive mode.

ip tcp intercept one-minute high

Note Effective with Cisco IOS Release 12.2(33)SXH and Cisco IOS Release 12.4(15)T the **ip tcp intercept one-minute high** command is replaced by the **ip tcp intercept one-minute**command. See the **ip tcp intercept one-minute**command for more information.

To define the number of connection requests received in the last one-minutes sample period before the software enters aggressive mode, use the **ip tcp intercept one-minute high**command in global configuration mode. To restore the default, use the **no** form of this command.

ip tcp intercept one-minute high *number*

no ip tcp intercept one-minute high [*number*]

Syntax Description

number	Specifies the number of connection requests that can be received in the last one-minute sample period before the software enters aggressive mode. The range is 1 to 2147483647. The default is 1100.

Command Default

1100 connection requests

Command Modes

Global configuration

Command History

Release	Modification
11.2 F	This command was introduced.
12.4(15)T	This command was replaced by the **ip tcp intercept one-minute** command.
12.2(33)SXH	This command was replaced by the **ip tcp intercept one-minute** command.

Usage Guidelines

Note If you are running Cisco IOS Release 12.2(33)SXH or Cisco IOS Release 12.4(15)T and issue the **ip tcp intercept one-minute high** command, it will be accepted by the router, but a message will be displayed stating that the **ip tcp intercept one-minute high** command has been replaced by the **ip tcp intercept one-minute**command.

If the number of connection requests exceeds the *number* value configured, the TCP intercept feature becomes aggressive. The following are the characteristics of aggressive mode:

- Each new arriving connection causes the oldest partial connection to be deleted.
- The initial retransmission timeout is reduced by half to 0.5 seconds (and so the total time trying to establish the connection is cut in half).
- The watch-timeout is cut in half (from 30 seconds to 15 seconds).

You can change the drop strategy from the oldest connection to a random connection with the **ip tcp intercept drop-mode** command.

Note The two factors that determine aggressive mode (connection requests and incomplete connections) are related and work together. When the value of *either***ip tcp intercept one-minute high**or **ip tcp intercept max-incomplete high** is exceeded, aggressive mode begins. When *both* connection requests and incomplete connections fall below the values of **ip tcp intercept one-minute low**and **ip tcp intercept max-incomplete low**, aggressive mode ends.

Examples

The following example allows 1400 connection requests before the software enters aggressive mode:

```
ip tcp intercept one-minute high 1400
```

Related Commands

Command	Description
ip tcp intercept drop-mode	Sets the TCP intercept drop mode.
ip tcp intercept max-incomplete high	Defines the maximum number of incomplete connections allowed before the software enters aggressive mode.
ip tcp intercept max-incomplete low	Defines the number of incomplete connections below which the software leaves aggressive mode.
ip tcp intercept one-minute low	Defines the number of connection requests below which the software leaves aggressive mode.

ip tcp intercept one-minute low

Note Effective with Cisco IOS Release 12.2(33)SXH and Cisco IOS Release 12.4(15)T, the **ip tcp intercept one-minute low**command is replaced by the **ip tcp intercept one-minute**command. See the **ip tcp intercept one-minute**command for more information.

To define the number of connection requests below which the software leaves aggressive mode, use the **ip tcp intercept one-minute low**command in gl obal configuration mode . To restore the default, use the **no** form of this command.

ip tcp intercept one-minute low *number*

no ip tcp intercept one-minute low [*number*]

Syntax Description

number	Defines the number of connection requests in the last one-minute sample period below which the software leaves aggressive mode. The range is from 1 to 2147483647. The default is 900.

Command Default

900 connection requests

Command Modes

Global configuration

Command History

Release	Modification
11.2 F	This command was introduced.
12.4(15)T	This command was replaced by the **ip tcp intercept one-minute** command.
12.2(33)SXH	This command was replaced by the **ip tcp intercept one-minute** command.

Usage Guidelin

Note If you are running Cisco IOS Release 12.2(33)SXH or Cisco IOS Release 12.4(15)T and issue the **ip tcp intercept one-minute low** command, it will be accepted by the router, but a message will be displayed stating that the **ip tcp intercept one-minute low** command has been replaced by the **ip tcp intercept one-minute**command.

When *both* connection requests and incomplete connections fall below the values of **ip tcp intercept one-minute low**and **ip tcp intercept max-incomplete low**, the TCP intercept feature leaves aggressive mode.

Note The two factors that determine aggressive mode (connection requests and incomplete connections) are related and work together. When the value of *either* **ip tcp intercept one-minute high**or **ip tcp intercept max-incomplete high** is exceeded, aggressive mode begins. When *both* connection requests and incomplete connections fall below the values of **ip tcp intercept one-minute low**and **ip tcp intercept max-incomplete low**, aggressive mode ends.

See the **ip tcp intercept one-minute high** command for a description of aggressive mode.

Examples

The following example sets the software to leave aggressive mode when the number of connection requests falls below 1000:

```
ip tcp intercept one-minute low 1000
```

Related Commands

Command	Description
ip tcp intercept drop-mode	Sets the TCP intercept drop mode.
ip tcp intercept max-incomplete high	Defines the maximum number of incomplete connections allowed before the software enters aggressive mode.
ip tcp intercept max-incomplete low	Defines the number of incomplete connections below which the software leaves aggressive mode.
ip tcp intercept one-minute high	Defines the number of connection requests received in the last one-minutes sample period before the software enters aggressive mode.

ip tcp intercept watch-timeout

To define how long the software will wait for a watched TCP intercept connection to reach established state before sending a reset to the server, use the **ip tcp intercept watch-timeout**command in global configuration mode. To restore the default, use the **no** form of this command.

ip tcp intercept watch-timeout *seconds*

no ip tcp intercept watch-timeout [*seconds*]

Syntax Description

seconds	Time (in seconds) that the software waits for a watched connection to reach established state before sending a Reset to the server. The minimum value is 1 second. The default is 30 seconds.

Command Default

30 seconds

Command Modes

Global configuration

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 this command if you have set the TCP intercept to passive watch mode and you want to change the default time the connection is watched. During aggressive mode, the watch timeout time is cut in half.

Examples

The following example sets the software to wait 60 seconds for a watched connection to reach established state before sending a Reset to the server:

```
ip tcp intercept watch-timeout 60
```

Related Commands

Command	Description
ip tcp intercept mode	Changes the TCP intercept mode.

ip traffic-export apply

To apply an IP traffic export profile or an IP traffic capture profile to a specific interface, use the **ip traffic-export apply**command in interface configuration mode. To remove an IP traffic export profile or an IP traffic capture profile from an interface, use the **no** form of this command.

ip traffic-export apply *profile-name*

no ip traffic-export apply *profile-name*

Cisco 1841, Cisco 2800 Series, and Cisco 3800 Series

ip traffic-export apply *profile-name* **size** *size*

no ip traffic-export apply *profile-name*

Syntax Description

profile-name	Name of the profile that is to be applied to a specified interface. The *profile-name* argument must match a name that was specified in the **ip traffic-export profile** command.
size	Optional. Used in IP traffic capture mode to set up a local capture buffer.
size	Optional. Specifies the size of the local capture buffer, in bytes.

Command Default

If you do not use this command, a sucessfully configured profile is not active.

Command Modes

Interface configuration

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.
12.4(11)T	This command was updated to incorporate the **size** keyword and *size* argument for IP traffic capture mode on the Cisco 1841, Cisco 2800 series, and Cisco 3800 series routers.

Usage Guidelines

After you configure at least one export profile, use the **ip traffic-export apply**command to activate IP traffic export on the specified ingress interface.

After you configure a capture profile, use the **ip traffic-export apply**command to activate IP traffic capture on the specified ingress interface, and to specify the size of the local capture buffer.

Examples

The following example shows how to apply the export profile “corp1” to interface Fast Ethernet 0/0.

```
Router(config)# ip traffic-export profile corp1
Router(config-rite)# interface FastEthernet 0/1
Router(config-rite)# bidirectional
Router(config-rite)# mac-address 00a.8aab.90a0
Router(config-rite)# outgoing sample one-in-every 50
Router(config-rite)# incoming access-list spam_acl
Router(config-rite)# exit
Router(config)# interface FastEthernet 0/0
Router(config-if)# ip traffic-export apply corp1
```

The following example shows how to apply the capture profile “corp2” to interface Fast Ethernet 0/0, and specify a capture buffer of 10,000,000 bytes.

```
Router(config)# ip traffic-export profile corp2 mode_capture
Router(config-rite)# bidirectional
Router(config-rite)# outgoing sample one-in-every 50
Router(config-rite)# incoming access-list ham_acl
Router(config-rite)# length 512
Router(config-rite)# exit
Router(config)# interface FastEthernet 0/0
Router(config-if)# ip traffic-export apply corp2 size 10000000
```

After a profile is activated on the interface, a logging message such as the following will appear:

```
%RITE-5-ACTIVATE: Activated IP traffic export on interface FastEthernet 0/0.
```

After a profile is removed from the interface, a logging message such as the following will appear:

```
%RITE-5-DEACTIVATE: Deactivated IP traffic export on interface FastEthernet 0/0.
```

If you attempt to apply an incomplete profile to an interface, you will receive the following message:

```
Router(config-if)# ip traffic-export apply newone
RITE: profile newone has missing outgoing interface
```

Related Commands

Command	Description
ip traffic-export profile	Creates or edits an IP traffic export profile and enables the profile on an ingress interface.
traffic-export	Controls the operation of IP traffic capture mode.

ip traffic-export profile

To create or edit an IP traffic export profile or an IP traffic capture profile and enable the profile on an ingress interface, use the **ip traffic-export profile** command in global configuration mode. To remove an IP traffic export profile from your router configuration, use the **no** form of this command.

ip traffic-export profile *profile-name*

no ip traffic-export profile *profile-name*

Cisco 1841, Cisco 2800 Series, and Cisco 3800 Series Routers

ip traffic-export profile *profile-name* **mode** {**capture**| **export**}

no ip traffic-export profile *profile-name*

Syntax Description

profile-name	IP traffic export profile name.
mode {**capture**| **export}**	Specifies either capture or export mode. • **capture** --Captures data to memory. • **export** --Exports data to an interface.

Command Default

A profile does not exist.

Command Modes

Global configuration

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.
12.4(11)T	This command was updated to incorporate the **mode, capture, and export**keywords on the Cisco 1841, Cisco 2800 series, and Cisco 3800 series routers.

Usage Guidelines

The **ip traffic-export profile** command allows you to begin a profile that can be configured to capture or export IP packets as they arrive on or leave from a selected router ingress interface.

When exporting IP packets, a designated egress interface exports IP packets out of the router. So, the router can export unaltered IP packets to a directly connected device.

When capturing IP packets, the packets are stored in local router memory. They may then be dumped to an external device.

IP Traffic Export Profiles

All exported IP traffic configurations are specified by profiles, which consist of RITE-related command-line interface (CLI) commands that control various attributes of both incoming and outgoing IP traffic. You can configure a router with multiple profiles. (Each profile must have a different name.) You can apply different profiles on different interfaces.

The two profiles to configure are:

- Global configuration profile, which you configure using the **ip traffic-export profile**command.
- Submode configuration profile, which you configure using any of the following RITE commands--**bidirectional**, **incoming**, **interface**, **mac-address**, and **outgoing**.

Use **interface** and **mac-address** commands to successfully create a profile. If you do not issue these commands, the user will receive a profile incomplete messages such as the following:

```
ip traffic-export profile newone
! No outgoing interface configured
! No destination mac-address configured
```

After you configure your profiles, you can apply the profiles to an interface with the **ip traffic-export apply profile**command, which will activate it.

IP Traffic Capture Profiles

On the Cisco 1841, Cisco 2800 series, and Cisco 3800 series routers, you can also configure IP traffic capture. A captured IP traffic configuration is specified by a profile, which consists of RITE-related command-line interface (CLI) commands that control various attributes of both incoming and outgoing IP traffic.

The two profiles that you should configure are:

- Global configuration profile, which you configure using the **ip traffic-export profile mode capture** command.
- Submode configuration profile, which you configure using any of the following RITE commands--**bidirectional**, **incoming**, **length**, and **outgoing**.

After you configure your profiles, you can apply the profiles to an interface with the **ip traffic-export apply profile**command, which will activate it.

When the IP traffic capture profile is applied to an interface, use the **traffic-export** command to control the capture of the traffic.

Note Cisco IOS Release 12.4(9)T and 12.4(15)T cannot capture outgoing router-generated Internet Control Message Protocol (ICMP) or IPsec traffic.

Examples

The following example shows how to configure the profile "corp1," which sends captured IP traffic to host "00a.8aab.90a0" at the interface "FastEthernet 0/1." This profile is also configured to export 1 in every 50 packets and to allow incoming traffic only from the access control list (ACL) "ham_ACL."

```
Router(config)# ip traffic-export profile corp1
Router(config-rite)# interface FastEthernet 0/1
Router(config-rite)# bidirectional
Router(config-rite)# mac-address 00a.8aab.90a0
Router(config-rite)# outgoing sample one-in-every 50
Router(config-rite)# incoming access-list ham_acl
Router(config-rite)# exit
Router(config)# interface FastEthernet 0/0
Router(config-if)# ip traffic-export apply corp1
```

The following example shows how to configure the profile "corp2," which captures IP traffic and stores it in a local router memory buffer of 10,000,000 bytes. This profile also captures 1 in every 50 packets and allows incoming traffic only from the access control list (ACL) "ham_ACL."

```
Router(config)# ip traffic-export profile corp2 mode capture
Router(config-rite)# bidirectional
Router(config-rite)# outgoing sample one-in-every 50
Router(config-rite)# incoming access-list ham_acl
Router(config-rite)# length 512
Router(config-rite)# exit
Router(config)# interface FastEthernet 0/0
Router(config-if)# ip traffic-export apply corp2 size 10000000
```

Related Commands

Command	Description
bidirectional	Enables incoming and outgoing IP traffic to be exported or captured across a monitored interface.
incoming	Configures filtering for incoming export or capture traffic.
interface (RITE)	Specifies the outgoing interface for exporting traffic
ip traffic-export apply profile	Applies an IP traffic export or IP traffic capture profile to a specific interface.
length	Specifies the length of the packet in capture mode.
mac-address	Specifies the Ethernet address of the destination host in traffic export.
outgoing	Configures filtering for outgoing export or capture traffic.
traffic-export interface	Controls the operation of IP traffic capture mode.

ip trigger-authentication (global)

To enable the automated part of double authentication at a device, use the **ip trigger-authentication** command in global configuration mode. To disable the automated part of double authentication, use the **no** form of this command.

ip trigger-authentication [**timeout** *seconds*] [**port** *number*]

no ip trigger-authentication

Syntax Description

timeout *seconds*	(Optional) Specifies how frequently the local device sends a User Datagram Protocol (UDP) packet to the remote host to request the user's username and password (or PIN). The default is 90 seconds. See "The Timeout Keyword" in the Usage Guidelines section for details.
port *number*	(Optional) Specifies the UDP port to which the local router should send the UPD packet requesting the user's username and password (or PIN). The default is port 7500. See "The Port Keyword" in the Usage Guidelines section for details.

Command Default

The default timeout is 90 seconds, and the default port number is 7500.

Command Modes

Global 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.(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

Configure this command on the local device (router or network access server) that remote users dial in to. Use this command only if the local device has already been configured to provide double authentication; this command enables automation of the second authentication of double authentication.

The timeout Keyword

During the second authentication stage of double authentication--when the remote user is authenticated--the remote user must send a username and password (or PIN) to the local device. With automated double authentication, the local device sends a UDP packet to the remote user's host during the second user-authentication stage. This UDP packet triggers the remote host to launch a dialog box requesting a username and password (or PIN).

If the local device does not receive a valid response to the UDP packet within a timeout period, the local device will send another UDP packet. The device will continue to send UDP packets at the timeout intervals until it receives a response and can authenticate the user.

By default, the UDP packet timeout interval is 90 seconds. Use the **timeout** keyword to specify a different interval.

(This timeout also applies to how long entries will remain in the remote host table; see the **show ip trigger-authentication** command for details.)

The port Keyword

As described in the previous section, the local device sends a UDP packet to the remote user's host to request the user's username and password (or PIN). This UDP packet is sent to UDP port 7500 by default. (The remote host client software listens to UDP port 7500 by default.) If you need to change the port number because port 7500 is used by another application, you should change the port number using the **port** keyword. If you change the port number you need to change it in both places--both on the local device and in the remote host client software.

Examples

The following example globally enables automated double authentication and sets the timeout to 120 seconds:

```
ip trigger-authentication timeout 120
```

Related Commands

Command	Description
ip trigger-authentication (interface)	Specifies automated double authentication at an interface.
show ip trigger-authentication	Displays the list of remote hosts for which automated double authentication has been attempted.

ip trigger-authentication (interface)

To specify automated double authentication at an interface, use the **ip trigger-authentication**command in interface configuration mode. To turn off automated double authentication at an interface, use the **no** form of this command.

ip trigger-authentication

no ip trigger-authentication

Syntax Description

This command has no arguments or keywords.

Command Default

Automated double authentication is not enabled for specific interfaces.

Command Modes

Interface 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.(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

Configure this command on the local router or network access server that remote users dial into. Use this command only if the local device has already been configured to provide double authentication and if automated double authentication has been enabled with the **ip trigger-authentication**(global) command.

This command causes double authentication to occur automatically when users dial into the interface.

Examples

The following example turns on automated double authentication at the ISDN BRI interface BRI0:

```
interface BRI0
 ip trigger-authentication
 encapsulation ppp
 ppp authentication chap
```

Related Commands

Command	Description
ip trigger-authentication (global)	Enables the automated part of double authentication at a device.

ip urlfilter alert

To enable URL filtering system alert messages, use the **ip urlfilter alert** command in global configuration mode. To disable the system alert, use the **no** form of this command.

ip urlfilter alert [**vrf** *vrf-name*]

no ip urlfilter alert

Syntax Description

vrf *vrf-name*	(Optional) Enables URL filtering system alert messages only for the specified Virtual Routing and Forwarding (VRF) interface.

Command Default

URL filtering messages are enabled.

Command Modes

Global configuration

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.

Usage Guidelines

Use the **ip urlfilter alert** command to display system messages, such as a server entering allow mode, a server going down, or a URL that is too long for the lookup request.

Examples

The following example shows how to enable URL filtering alert messages:

```
ip inspect name test http urlfilter
ip urlfilter cache 5
ip urlfilter exclusive-domain permit .weapons.com
ip urlfilter exclusive-domain deny .nbc.com
ip urlfilter exclusive-domain permit www.cisco.com
ip urlfilter audit-trail
ip urlfilter alert
ip urlfilter server vendor websense 192.168.3.1
```

Afterward, system alert messages such as the following are displayed:

```
%URLF-3-SERVER_DOWN:Connection to the URL filter server 10.92.0.9 is down
```

This level three LOG_ERR-type message is displayed when a configured URL filter server (UFS) goes down. When this happens, the firewall will mark the configured server as secondary and try to bring up one of the other secondary servers and mark that server as the primary server. If there is no other server configured, the firewall will enter into allow mode and display the URLF-3-ALLOW_MODE message described.

```
%URLF-3-ALLOW_MODE:Connection to all URL filter servers are down and ALLOW MODE is OFF
```

This LOG_ERR type message is displayed when all UFSs are down and the system enters into allow mode.

Note Whenever the system goes into allow mode (all filter servers are down), a periodic keepalive timer will be triggered that will try to bring up a server by opening a TCP connection.

```
%URLF-5-SERVER_UP:Connection to an URL filter server 10.92.0.9 is made, the system is
returning from ALLOW MODE
```

This LOG_NOTICE-type message is displayed when the UFSs are detected as being up and the system is returning from allow mode.

```
%URLF-4-URL_TOO_LONG:URL too long (more than 3072 bytes), possibly a fake packet?
```

This LOG_WARNING-type message is displayed when the URL in a lookup request is too long; any URL longer than 3K will be dropped.

```
%URLF-4-MAX_REQ:The number of pending request exceeds the maximum limit <1000>
```

This LOG_WARNING-type message is displayed when the number of pending requests in the system exceeds the maximum limit and all further requests are dropped.

ip urlfilter allowmode

To turn on the default mode (allow mode) of the filtering algorithm, use the **ip urlfilter allowmode**command in global configuration mode. To disable the default mode, use the **no** form of this command.

ip urlfilter allowmode [**on**| **off**] [**vrf** *vrf-name*]

no ip urlfilter allowmode [**on**| **off**]

Syntax Description

on	(Optional) Allow mode is on.
off	(Optional) Allow mode is off.
vrf *vrf-name*	(Optional) Turns on the default mode of the filtering algorithm only for the specified Virtual Routing and Forwarding (VRF) interface.

Command Default

Allow mode is off.

Command Modes

Global configuration

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.

Usage Guidelines

The system will go into allow mode when connections to all vendor servers (Websense or N2H2) are down. The system will return to normal mode when a connection to at least one web vendor server is up. Allow mode directs your system to forward or drop all packets on the basis of the configurable allow mode setting: if allow mode is on and the vendor servers are down, the HTTP requests will be allowed to pass; if allow mode is off and the vendor servers are down, the HTTP requests will be forbidden.

Examples

The following example shows how to enable allow mode on your system:

```
ip urlfilter allowmode on
```

Afterward, the following alert message will be displayed when the system goes into allow mode:

```
%URLF-3-ALLOW_MODE: Connection to all URL filter servers are down and ALLOW MODE if OFF
```

The following alert message will be displayed when the system returns from allow mode:

```
%URLF-5-SERVER_UP: Connection to an URL filter server 12.0.0.3 is made, the system is
returning from allow mode
```

ip urlfilter audit-trail

To log messages into the syslog server or router, use the **ip urlfilter audit-trail**command in global configuration mode. To disable this functionality, use the **no** form of this command.

ip urlfilter audit-trail [**vrf** *vrf-name*]

no ip urlfilter audit-trail

Syntax Description

vrf *vrf-name*	(Optional) Logs messages into the syslog server or router only for the specified Virtual Routing and Forwarding (VRF) interface.

Command Default

This command is disabled.

Command Modes

Global configuration

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.

Usage Guidelines

Use the **ip urlfilter audit-trail** command to log messages such as URL request status (allow or deny) into your syslog server.

Examples

The following example shows how to enable syslog message logging:

```
ip inspect name test http urlfilter
ip urlfilter cache 5
ip urlfilter exclusive-domain permit .weapons.com
ip urlfilter exclusive-domain deny .nbc.com
ip urlfilter exclusive-domain permit www.cisco.com
ip urlfilter audit-trail
ip urlfilter alert
ip urlfilter server vendor websense 209.165.202.130
```

Afterward, audit trail messages such as the following are displayed and logged into the log server:

```
%URLF-6-SITE_ALLOWED:Client 209.165.201.15:12543 accessed server 10.76.82.21:8080
```

This message is logged for each request whose destination IP address is found in the cache. It includes the source IP address, source port number, destination IP address, and destination port number. The URL is not logged in this case because the IP address of the request is found in the cache; thus, parsing the request and extracting the URL is a waste of time.

```
%URLF-4-SITE-BLOCKED: Access denied for the site 'www.sports.com'; client 209.165.200.230:34557
 server 209.165.201.2:80
```

This message is logged when a request finds a match against one of the blocked domains in the exclusive-domain list or the corresponding entry in the IP cache.

```
%URLF-6-URL_ALLOWED:Access allowed for URL http://www.N2H2.com/; client 209.165.200.230:54123
  server 192.168.0.1:80
```

This message is logged for each URL request that is allowed by the vendor server (Websense or N2H2). It includes the allowed URL, source IP address, source port number, destination IP address, and destination port number. Longer URLs will be truncated to 300 bytes and then logged.

```
%URLF-6-URL_BLOCKED:Access denied URL http://www.google.com; client 209.165.200.230:54678
server 209.165.201.2:80
```

This message is logged for each URL request that is blocked by the vendor server. It includes the blocked URL, source IP address, source port number, destination IP address, and destination port number. Longer URLs will be truncated to 300 bytes and then logged.

ip urlfilter cache

To configure cache parameters, use the **ip urlfilter cache**command in global configuration mode. To clear the configuration, use the **no** form of this command.

ip urlfilter cache number [**vrf** *vrf-name*]

no ip urlfilter cache number

Syntax Description

number	Maximum number of destination IP addresses that can be cached into the cache table. The default value is 5000.
vrf *vrf-name*	(Optional) Configures cache parameters only for the specified Virtual Routing and Forwarding (VRF) interface.

Command Default

Maximum number of destination IP addresses is 5000.

The cache table is cleared out every 12 hours.

Command Modes

Global configuration

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.

Usage Guidelines

The cache table consists of the most recently requested IP addresses and respective authorization status for each IP address.

The caching algorithm involves three parameters--the maximum number of IP addresses that can be cached, an idle time, and an absolute time. The algorithm also involves two timers--idle timer and absolute timer. The idle timer is a small periodic timer (1 minute) that checks to see whether the number of cached IP addresses in the cache table exceeds 80 percent of the maximum limit. If the cached IP addresses have exceeded 80 percent, it will start removing idle entries; if it has not exceeded 80 percent, it will quit and wait for the next cycle. The absolute timer is a large periodic timer (1 hour) that is used to remove all of the elapsed entries. (The age of an elapsed entry is greater than the absolute time.) An elapsed entry will also be removed during cache lookup.

The idle time value is fixed at 10 minutes. The absolute time value is taken from the vendor server look-up response, which is often greater than 15 hours. The absolute value for cache entries made out of exclusive-domains is 12 hours. The maximum number of cache entries is configurable by enabling the **ip urlfilter cache**command.

Note The vendor server is not able to inform the Cisco IOS firewall of filtering policy changes in the database.

Examples

The following example shows how to configure the cache table to hold a maximum of five destination IP addresses:

```
ip inspect name test http urlfilter
ip urlfilter cache 5
ip urlfilter exclusive-domain permit .weapons.com
ip urlfilter exclusive-domain deny .nbc.com
ip urlfilter exclusive-domain permit www.cisco.com
ip urlfilter audit-trail
ip urlfilter alert
ip urlfilter server vendor websense 192.168.3.1
```

Related Commands

Command	Description
clear ip urlfilter cache	Clears the cache table.
show ip urlfilter cache	Displays the destination IP addresses that are cached into the cache table.

ip urlfilter exclusive-domain

To add or remove a domain name to or from the exclusive domain list so that the firewall does not have to send lookup requests to the vendor server, use the **ip urlfilter exclusive-domain**command in global configuration mode. To remove a domain name from the exclusive domain name list, use the **no** form of this command.

ip urlfilter exclusive-domain {**permit**| **deny**} *domain-name* [**vrf** *vrf-name*]

no ip urlfilter exclusive-domain {**permit**| **deny**} *domain-name*

Syntax Description

permit	Permits all traffic destined for the specified domain name.
deny	Blocks all traffic destined for the specified domain name.
domain-name	Domain name that is added or removed from the exclusive domain name list; for example, www.cisco.com .
vrf *vrf-name*	(Optional) Adds or removes a domain name only for the specified Virtual Routing and Forwarding (VRF) interface.

Command Default

This command is not enabled.

Command Modes

Global configuration

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.

Usage Guidelines

The **ip urlfilter exclusive-domain**command allows you to specify a list of domain names (exclusive domains) so that the firewall will not create a lookup request for the HTTP traffic that is destined for one of the domains in the exclusive list. Thus, you can avoid sending look-up requests to the web server for HTTP traffic that is destined for a host that is completely allowed to all users.

Flexibility when entering domain names is also provided; that is, the user can enter the complete domain name or a partial domain name.

Complete Domain Name

If the user adds a complete domain name, such as “www.cisco.com,” to the exclusive domain list, all HTTP traffic whose URLs are destined for this domain (such as www.cisco.com/news and www.cisco.com/index) will be excluded from the URL filtering policies of the vendor server (Websense or N2H2), and on the basis of the configuration, the URLs will be permitted or blocked (denied).

Partial Domain Name

If the user adds only a partial domain name to the exclusive domain list, such as “.cisco.com,” all URLs whose domain names end with this partial domain name (such as www.cisco.com/products and www.cisco.com/eng) will be excluded from the URL filtering policies of the vendor server (Websense or N2H2), and on the basis of the configuration, the URLs will be permitted or blocked (denied).

Examples

The following example shows how to add the complete domain name “www. cisco.com ” to the exclusive domain name list. This configuration will block all traffic destined to the www.cisco.com domain.

```
ip urlfilter exclusive-domain deny www.cisco.com
```

The following example shows how to add the partial domain name “. cisco.com ” to the exclusive domain name list. This configuration will permit all traffic destined to domains that end with .cisco.com.

```
ip urlfilter exclusive-domain permit .cisco.com
```

ip urlfilter max-request

To set the maximum number of outstanding requests that can exist at any given time, use the **ip urlfilter max-request**command in global configuration mode. To disable this function, use the **no** form of this command.

ip urlfilter max-request *number* [**vrf** *vrf-name*]

no ip urlfilter max-request *number*

Syntax Description

number	Maximum number of outstanding requests. The default value is 1000.
vrf *vrf-name*	(Optional) Sets the maximum number of outstanding requests only for the specified Virtual Routing and Forwarding (VRF) interface.

Command Default

Maximum number of requests is 1000.

Command Modes

Global configuration

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.

Usage Guidelines

If the specified maximum number of outstanding requests is exceeded, new requests will be dropped.

Note Allow mode is not considered because it should be used only when servers are down.

Examples

The following example shows how to configure the maximum number of outstanding requests to 950:

```
ip inspect name url_filter http
ip urlfilter max-request 950
```

Related Commands

Command	Description
ip inspect name	Defines a set of inspection rules.
ip urlfilter server vendor	Configures a vendor server for URL filtering.

ip urlfilter max-resp-pak

To configure the maximum number of HTTP responses that the firewall can keep in its packet buffer, use the **ip urlfilter max-resp-pak**command in global configuration mode. To return to the default, use the **no** form of this command.

ip urlfilter max-resp-pak *number* [**vrf** *vrf-name*]

no ip urlfilter max-resp-pak *number*

Syntax Description

number	Maximum number of HTTP responses that can be stored in the packet buffer of the firewall. After the maximum number has been reached, the firewall will drop further responses. The default, and absolute maximum, value is 200.
vrf *vrf-name*	(Optional) Sets the maximum number of HTTP responses only for the specified Virtual Routing and Forwarding (VRF) interface.

Command Default

200 HTTP responses

Command Modes

Global configuration

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.

Usage Guidelines

When an HTTP request arrives at a Cisco IOS firewall, the firewall forwards the request to the web server while simultaneously sending a URL look-up request to the vendor server (Websense or N2H2). If the vendor server reply arrives before the HTTP response, the firewall will know whether to permit or block the HTTP response; if the HTTP response arrives before the vendor server reply, the firewall will not know whether to allow or block the response, so the firewall will drop the response until it hears from the vendor server. The **ip urlfilter max-resp-pak** command allows you to configure your firewall to store the HTTP responses in a buffer, which allows your firewall to store a maximum of 200 HTTP responses. Each response will remain in the buffer until an allow or deny message is received from the vendor server. If the vendor server reply allows the URL, the firewall will release the HTTP response from the buffer to the end user; if the vendor server reply denies the URL, the firewall will discard the HTTP response from the buffer and close the connection to both ends.

Examples

The following example shows how to configure your firewall to hold 150 HTTP responses:

```
ip urlfilter max-resp-pak 150
```

ip urlfilter server vendor

To configure a vendor server for URL filtering, use the **ip urlfilter server vendor**command in global configuration mode. To remove a server from your configuration, use the **no** form of this command.

ip urlfilter server vendor {**websense**| **n2h2**} *ip-address* [**port** *port-number*] [**timeout** *seconds*] [**retransmit** *number*] **[outside]** [**vrf** *vrf-name*]

no ip urlfilter server vendor {**websense**| **n2h2**} *ip-address* [**port** *port-number*] [**timeout** *seconds*] [**retransmit** *number*] **[outside]**

Syntax Description

websense	Websense server will be used.
n2h2	N2H2 server will be used.
ip-address	IP address of the vendor server.
port *port-number*	(Optional) Port number that the vendor server listens on. The default port number is 15868.
timeout *seconds*	(Optional) Length of time, in seconds, that the Cisco IOS firewall will wait for a response from the vendor server. The default timeout is 5 seconds.
retransmit *number*	(Optional) Number of times the Cisco IOS firewall will retransmit the request when a response does not arrive for the request. The default value is two times.
outside	(Optional) Vendor server will be deployed on the outside network.
vrf *vrf-name*	(Optional) Configures a vendor server for URL filtering only for the specified Virtual Routing and Forwarding (VRF) interface.

Command Default

A vendor server is not configured.

Command Modes

Global configuration

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.

Release	Modification
12.3(2)T	The **outside** keyword was added.
12.3(14)T	The **vrf** *vrf-name*keyword/argument pair was added.

Usage Guidelines

Use the **ip urlfilter 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 will check the **retransmit** *number* keyword and argument configured for the vendor server. If the firewall has not exceeded the maximum retransmit tries allowed, it will resend the HTTP lookup request. If the firewall has exceeded the maximum retransmit tries allowed, it will delete the outstanding request from the queue and check the status of the allow mode value. The firewall will forward the request if the allow mode is on; otherwise, it will drop the request.

By default, URL lookup requests that are made to the vendor server contain non-natted 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, thereby, allowing Cisco IOS software to send the natted IP address of the client in the URL lookup request.

Primary and Secondary Servers

When users configure multiple vendor servers, the firewall will use 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 will go to the beginning of the configured servers list and try to activate the first server on the list. If the first server on the list is unavailable, it will try the second server on the list; the system will keep 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 will set a flag indicating that all of the servers are down, and it will enter allow mode.

Examples

The following example shows how to configure the Websense server for URL filtering:

```
ip inspect name test http urlfilter
ip urlfilter cache 5
ip urlfilter exclusive-domain permit .weapons.com
ip urlfilter exclusive-domain deny .nbc.com
ip urlfilter exclusive-domain permit www.cisco.com
ip urlfilter audit-trail
ip urlfilter alert
ip urlfilter server vendor websense 192.168.3.1
```

Related Commands

Command	Description
ip urlfilter allowmode	Turns on the default mode (allow mode) of the filtering algorithm.

Command	Description
ip urlfilter max-request	Sets the maximum number of outstanding requests that can exist at any given time.

ip urlfilter source-interface

To allow the URL filter to specify the interface whose IP address is used as the source IP address while a TCP connection is made to the URL filter server (Websense or N2H2), use the **ip urlfilter source-interface** command in global configuration mode. To disable the option, use the **no** form of this command.

ip urlfilter source-interface *interface-type* [**vrf** *vrf-name*]

no ip urlfilter source-interface [**vrf** *vrf-name*]

Syntax Description

interface-type	The interface type that is used as the source IP address.
vrf *vrf-name*	(Optional) Specifies the Virtual Routing and Forwarding (VRF) interface.

Command Default

The URL filter to specify a source interface for TCP is not defined.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

The **ip urlfilter source-interface** command is used to define the source interface from which the URL filter request is sent. This command is recommended to be configured if the URL filter server can only be routed through certain interfaces on the router.

Examples

The following example shows that the URL filtering server is routed to the Ethernet interface type:

```
Router(config)# ip urlfilter source-interface ethernet
```

Related Commands

Command	Description
debug ip urlfilter	Enables debug information of URL filter subsystems.

ip urlfilter truncate

To allow the URL filter to truncate long URLs to the server, use the **ip urlfilter truncate**command in global configuration mode. To disable the truncating option, use the **no** form of this command.

ip urlfilter truncate {**script-parameters| hostname**} [**vrf** *vrf-name*]

no ip urlfilter truncate {**script-parameters| hostname**} [**vrf** *vrf-name*]

Syntax Description

script-parameters	Specifies that only the URL up to the script options is sent. • For example, if the entire URL is http://www.cisco.com/dev/xxx.cgi?when=now, only the URL through http://www.cisco.com/dev/xxx.cgi is sent (if the maximum supported URL length is not exceeded).
hostname	Specifies that only the hostname is sent. • For example, if the entire URL is http://www.cisco.com/dev/xxx.cgi?when=now, only http://www.cisco.com is sent.
vrf *vrf-name*	(Optional) Specifies the Virtual Routing and Forwarding (VRF) interface.

Command Default

URLs that are longer than the maximum supported length are not truncated, and the HTTP request is rejected.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

If both the **script-parameters** and **hostname** keywords are configured, the **script-parameters** keyword takes precedence over the **hostname** keyword. If both the keywords are configured and the script parameters URL is truncated and the maximum supported URL length is exceeded, the URL is truncated up to the hostname.

Note If both **script-parameters** and **hostname** keywords are configured, they must be on separate lines as shown in the “Examples” section. They cannot be combined in one line.

Examples

The following example shows that the URL is to be truncated up to the script options:

```
ip urlfilter truncate script-parameters
```

The following example shows that the URL is to be truncated up to the hostname:

```
ip urlfilter truncate hostname
```

Related Commands

Command	Description
debug ip urlfilter	Enables debug information of URL filter subsystems.

ip urlfilter urlf-server-log

To enable the logging of system messages on the URL filtering server, use the **ip urlfilter urlf-server-log** command in global configuration mode. To disable the logging of system messages, use the **no** form of this command.

ip urlfilter urlf-server-log [**vrf** *vrf-name*]

no ip urlfilter urlf-server-log

Syntax Description

vrf *vrf-name*	(Optional) Enables the logging of system messages on the URL filtering server only for the specified Virtual Routing and Forwarding (VRF) interface.

Command Default

This command is disabled.

Command Modes

Global configuration

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.

Usage Guidelines

Use the **ip urlfilter urlf-server-log** command to enable Cisco IOS to send a log request immediately after the URL lookup request. The firewall will not make a URL lookup request if the destination IP address is in the cache, but it will still make a log request to the server. (The log request contains the URL, hostname, source IP address, and the destination IP address.) The server records the log request into its own log server so your can view this information as necessary.

Examples

The following example shows how to enable system message logging on the URL filter server:

```
ip urlfilter urlf-server-log
```

ip verify drop-rate compute interval

To configure the interval of time between Unicast Reverse Path Forwarding (RPF) drop rate computations, use the **ip verify drop-rate compute interval**command in global configuration mode. To reset the interval to the default value, use the **no** form of this command.

ip verify drop-rate compute interval *seconds*

no ip verify drop-rate compute interval

Syntax Description

seconds	Interval, in seconds, between Unicast RPF drop rate computations. The range is from 30 to 300. The default is 30.

Command Default

The drop rate is not computed.

Command Modes

Global configuration (config)

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

The configured value applies for the computation of all Unicast RPF drop rates (global and per interface).

The value for the compute interval must be less than or equal to the value configured using the **ip verify drop-rate compute window**command. If you configure the **no** form of the **ip verify drop-rate compute interval**command while the cipUrpfDropRateWindow value is configured to be less than the default compute interval value, the following message appears on the console:

```
“urpf drop rate window < interval”
```

This error message means the command was not executed. The compute interval remains at the configured value rather than changing to the default value.

Examples

The following example shows how to configure a compute interval of 45 seconds:

```
Router> enable
```

```
Router# configure terminal
Router(config)# ip verify drop-rate compute interval 45
```

Related Commands

Command	Description
ip verify drop-rate compute window	Configures the interval of time during which the Unicast RPF drop count is collected for the drop rate computation.
ip verify drop-rate notify hold-down	Configures the minimum time between Unicast RPF drop rate notifications.
ip verify unicast notification threshold	Configures the threshold value used to determine whether to send a Unicast RPF drop rate notification.

ip verify drop-rate compute window

To configure the interval of time during which the Unicast Reverse Path Forwarding (RPF) drop count is collected for the drop rate computation, use the **ip verify drop-rate compute window**command in global configuration mode. To reset the window to the default value, use the **no** form of this command.

ip verify drop-rate compute window *seconds*

no ip verify drop-rate compute window

Syntax Description

seconds	Interval, in seconds, during which the Unicast RPF drop count is accumulated for the drop rate computation. The range is from 30 to 300. The default is 300.

Command Default

The drop rate is not calculated.

Command Modes

Global configuration (config)

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 configures the sliding window that begins the configured number of seconds prior to the computation and ends with the Unicast RPF drop rate computation. The configured value applies for the computation of all Unicast RPF drop rates (global and per interface).

The value configured for the "compute window" must be greater than or equal to the value configured using the **ip verify drop-rate compute interval**command. If you configure the **no** form of the **ip verify drop-rate compute window**command while the cipUrpfDropRateInterval value is configured to be greater than the default compute window value, the following message appears on the console:

```
"urpf drop rate window < interval"
```

This error message means that the command was not executed. The compute window remains at the configured value rather than changing to the default value.

Examples

The following example shows how to configure a compute window of 60 seconds:

```
Router> enable
Router# configure terminal
Router(config)# ip verify drop-rate compute window 60
```

Related Commands

Command	Description
ip verify drop-rate compute interval	Configures the interval between Unicast RPF drop rate computations.
ip verify drop-rate notify hold-down	Configures the minimum time between Unicast RPF drop rate notifications.
ip verify unicast notification threshold	Configures the threshold value used to determine whether to send a Unicast RPF drop rate notification.

ip verify drop-rate notify hold-down

To configure the minimum time between Unicast Reverse Path Forwarding (RPF) drop rate notifications, use the **ip verify drop-rate notify hold-down**command in global configuration mode. To reset the hold-down time to the default value, use the **no** form of this command.

ip verify drop-rate notify hold-down *seconds*

no ip verify drop-rate notify hold-down

Syntax Description

seconds	Minimum time, in seconds, between Unicast RPF drop rate notifications. The range is from 30 to 300. The default is 300.

Command Default

No notifications are sent.

Command Modes

Global configuration (config)

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

The configured value applies for the computation of all Unicast RPF drop rates (global and per interface).

Examples

The following example shows how to configure a notify hold-down time of 40 seconds:

```
Router> enable
Router# configure terminal
Router(config)# ip verify drop-rate notify hold-down 40
```

Related Commands

Command	Description
ip verify drop-rate compute interval	Configures the interval of time between Unicast RPF drop rate computations.

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 threshold value used to determine whether to send a Unicast RPF drop rate notification.

ip verify unicast notification threshold

To configure the threshold value used to determine whether to send a Unicast Reverse Path Forwarding (RPF) drop rate notification, use the **ip verify unicast notification threshold**command in interface configuration mode. To set the notification threshold back to the default value, use the **no** form of this command.

ip verify unicast notification threshold *packets-per-second*

no ip verify unicast notification threshold

Syntax Description

packets-per-second	Threshold value, in packets per second, used to determine whether to send a Unicast RPF drop rate notification. The range is from 0 to 4294967295. The default is 1000.

Command Default

No 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 configures the threshold Unicast RPF drop rate which, when exceeded, triggers a notification. Configuring a value of 0 means that any Unicast RPF packet drop triggers a notification.

Examples

The following example shows how to configure a notification threshold value of 900 on Ethernet interface 3/0:

```
Router> enable
Router# configure terminal
Router(config# interface ethernet 3/0
Router(config-if)# ip verify unicast notification threshold 900
```

Related Commands

Command	Description
ip verify drop-rate compute interval	Configures the interval of time between Unicast RPF drop rate computations.
ip verify drop-rate compute window	Configures the interval of time during which the Unicast RPF drop count is collected for the drop rate computation.
i p verify drop-rate notify hold-down	Configures the minimum time between Unicast RPF drop rate notifications.

ip verify unicast reverse-path

Note This command was replaced by the **ip verify unicast source reachable-via**command effective with Cisco IOS Release 12.0(15)S. The **ip verify unicast source reachable-via** command allows for more flexibility and functionality, such as supporting asymmetric routing, and should be used for any Reverse Path Forward implementation. The **ip verify unicast reverse-path** command is still supported.

To enable Unicast Reverse Path Forwarding (Unicast RPF), use the **ip verify unicast reverse-path**command in interface configuration mode. To disable Unicast RPF, use the **no** form of this command.

ip verify unicast reverse-path [*list*]

no ip verify unicast reverse-path [*list*]

Syntax Description

list	(Optional) Specifies a numbered access control list (ACL) in the following ranges: • 1 to 99 (IP standard access list) • 100 to 199 (IP extended access list) • 1300 to 1999 (IP standard access list, expanded range) • 2000 to 2699 (IP extended access list, expanded range)

Command Default

Unicast RPF is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification		
11.1(CC) 12.0	This command was introduced. This command was not included in Cisco IOS Release 11.2 or 11.3	12.1(2)T	Added ACL support using the *list* argument. Added per-interface statistics on dropped or suppressed packets.

Release	Modification
12.0(15)S	The **ip verify unicast source reachable-via** command replaced this command, and the following keywords were added to the **ip verify unicast source reachable-via** command: **allow-default, allow-self-ping**, **rx**, and **any**.
12.1(8a)E	The **ip verify unicast reverse-path**command was integrated into Cisco IOS Release 12.1(8a)E.
12.2(14)S	The **ip verify unicast reverse-path**command was integrated into Cisco IOS Release 12.2(14)S.
12.2(14)SX	The **ip verify unicast reverse-path** command was integrated into Cisco IOS Release 12.2(14)SX.
12.2(33)SRA	The **ip verify unicast reverse-path**command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use the **ip verify unicast reverse-path interface** command to mitigate problems caused by malformed or forged (spoofed) IP source addresses that are received by a router. Malformed or forged source addresses can indicate denial of service (DoS) attacks on the basis of source IP address spoofing.

When Unicast RPF is enabled on an interface, the router examines all packets that are received on that interface. The router checks to ensure that the source address appears in the Forwarding Information Base (FIB) and that it matches the interface on which the packet was received. This "look backwards" ability is available only when Cisco Express Forwarding is enabled on the router because the lookup relies on the presence of the FIB. Cisco Express Forwarding generates the FIB as part of its operation.

To use Unicast RPF, enable Cisco Express Forwarding switching or distributed Cisco Express Forwarding switching in the router. There is no need to configure the input interface for Cisco Express Forwarding switching. As long as Cisco Express Forwarding is running on the router, individual interfaces can be configured with other switching modes.

Note It is very important for Cisco Express Forwarding to be configured globally in the router. Unicast RPF will not work without Cisco Express Forwarding.

Note Unicast RPF is an input function and is applied on the interface of a router only in the ingress direction.

The Unicast Reverse Path Forwarding feature checks to determine whether any packet that is received at a router interface arrives on one of the best return paths to the source of the packet. The feature does this by doing a reverse lookup in the Cisco Express Forwarding table. If Unicast RPF does not find a reverse path for the packet, Unicast RPF can drop or forward the packet, depending on whether an ACL is specified in the Unicast Reverse Path Forwarding command. If an ACL is specified in the command, then when (and only when) a packet fails the Unicast RPF check, the ACL is checked to determine whether the packet should be dropped (using a deny statement in the ACL) or forwarded (using a permit statement in the ACL). Whether a packet is dropped or forwarded, the packet is counted in the global IP traffic statistics for Unicast RPF drops and in the interface statistics for Unicast RPF.

If no ACL is specified in the Unicast Reverse Path Forwarding command, the router drops the forged or malformed packet immediately and no ACL logging occurs. The router and interface Unicast RPF counters are updated.

Unicast RPF events can be logged by specifying the logging option for the ACL entries used by the Unicast Reverse Path Forwarding command. Log information can be used to gather information about the attack, such as source address, time, and so on.

Where to Use RPF in Your Network

Unicast RPF may be used on interfaces in which only one path allows packets from valid source networks (networks contained in the FIB). Unicast RPF may also be used in cases for which a router has multiple paths to a given network, as long as the valid networks are switched via the incoming interfaces. Packets for invalid networks will be dropped. For example, routers at the edge of the network of an Internet service provider (ISP) are likely to have symmetrical reverse paths. Unicast RPF may still be applicable in certain multi-homed situations, provided that optional Border Gateway Protocol (BGP) attributes such as weight and local preference are used to achieve symmetric routing.

With Unicast RPF, all equal-cost "best" return paths are considered valid. This means that Unicast RPF works in cases where multiple return paths exist, provided that each path is equal to the others in terms of the routing cost (number of hops, weights, and so on) and as long as the route is in the FIB. Unicast RPF also functions where Enhanced Internet Gateway Routing Protocol (EIGRP) variants are being used and unequal candidate paths back to the source IP address exist.

For example, routers at the edge of the network of an ISP are more likely to have symmetrical reverse paths than routers that are in the core of the ISP network. Routers that are in the core of the ISP network have no guarantee that the best forwarding path out of the router will be the path selected for packets returning to the router. In this scenario, you should use the new form of the command, **ip verify unicast source reachable-via**, if there is a chance of asymmetrical routing.

Examples

The following example shows that the Unicast Reverse Path Forwarding feature has been enabled on a serial interface:

```
ip cef
! or "ip cef distributed" for RSP+VIP based routers
!
interface serial 5/0/0
 ip verify unicast reverse-path
```

The following example uses a very simple single-homed ISP to demonstrate the concepts of ingress and egress filters used in conjunction with Unicast RPF. The example illustrates an ISP-allocated classless interdomain routing (CIDR) block 192.168.202.128/28 that has both inbound and outbound filters on the upstream interface. Be aware that ISPs are usually not single-homed. Hence, provisions for asymmetrical flows (when outbound traffic goes out one link and returns via a different link) need to be designed into the filters on the border routers of the ISP.

```
ip cef distributed
!
interface Serial 5/0/0
 description Connection to Upstream ISP
 ip address 192.168.200.225 255.255.255.255
 no ip redirects
 no ip directed-broadcast
 no ip proxy-arp
 ip verify unicast reverse-path
 ip access-group 111 in
 ip access-group 110 out
!
access-list 110 permit ip 192.168.202.128 10.0.0.31 any
access-list 110 deny ip any any log
access-list 111 deny ip host 10.0.0.0 any log
access-list 111 deny ip 172.16.0.0 255.255.255.255 any log
access-list 111 deny ip 10.0.0.0 255.255.255.255 any log
access-list 111 deny ip 172.16.0.0 255.255.255.255 any log
access-list 111 deny ip 192.168.0.0 255.255.255.255 any log
access-list 111 deny ip 209.165.202.129 10.0.0.31 any log
access-list 111 permit ip any any
```

The following example demonstrates the use of ACLs and logging with Unicast RPF. In this example, extended ACL 197 provides entries that deny or permit network traffic for specific address ranges. Unicast RPF is configured on Ethernet interface 0 to check packets arriving at that interface.

For example, packets with a source address of 192.168.201.10 arriving at Ethernet interface 0 are dropped because of the deny statement in ACL 197. In this case, the ACL information is logged (the logging option is turned on for the ACL entry) and dropped packets are counted per-interface and globally. Packets with a source address of 192.168.201.100 arriving at Ethernet interface 0 are forwarded because of the permit statement in ACL 197. ACL information about dropped or suppressed packets is logged (the logging option is turned on for the ACL entry) to the log server.

```
ip cef distributed
!
int eth0/1/1
 ip address 192.168.200.1 255.255.255.255
 ip verify unicast reverse-path 197
!
int eth0/1/2
 ip address 192.168.201.1 255.255.255.255
!
access-list 197 deny   ip 192.168.201.0 10.0.0.63 any log-input
access-list 197 permit ip 192.168.201.64 10.0.0.63 any log-input
access-list 197 deny   ip 192.168.201.128 10.0.0.63 any log-input
access-list 197 permit ip 192.168.201.192 10.0.0.63 any log-input
access-list 197 deny ip host 10.0.0.0 any log-input
access-list 197 deny ip 172.16.0.0 255.255.255.255 any log-input
access-list 197 deny ip 10.0.0.0 255.255.255.255 any log-input
access-list 197 deny ip 172.16.0.0 255.255.255.255 any log-input
access-list 197 deny ip 192.168.0.0 255.255.255.255 any log-input
```

Related Commands

Command	Description
ip cef	Enables Cisco Express Forwarding on the route processor card.

ip verify unicast source reachable-via

To enable Unicast Reverse Path Forwarding (Unicast RPF), use the **ip verify unicast source reachable-via** command in interface configuration mode. To disable Unicast RPF, use the **no** form of this command.

ip verify unicast source reachable-via {**any**| **rx [l2-src]**} **[allow-default] [allow-self-ping]** [*access-list*]

no ip verify unicast source reachable-via

Syntax Description

any	Examines incoming packets to determine whether the source address is in the Forwarding Information Base (FIB) and permits the packet if the source is reachable through any interface (sometimes referred to as loose mode).
rx	Examines incoming packets to determine whether the source address is in the FIB and permits the packet only if the source is reachable through the interface on which the packet was received (sometimes referred to as strict mode).
l2-src	(Optional) Enables source IPv4 and source MAC address binding.
allow-default	(Optional) Allows the use of the default route for RPF verification.
allow-self-ping	(Optional) Allows a router to ping its own interface or interfaces. **Caution** Use caution when enabling the **allow-self-ping** keyword. This keyword opens a denial-of-service (DoS) hole.
access-list	(Optional) Specifies a numbered access control list (ACL) in the following ranges: • 1 to 99 (IP standard access list) • 100 to 199 (IP extended access list) • 1300 to 1999 (IP standard access list, expanded range) • 2000 to 2699 (IP extended access list, expanded range)

Command Default

Unicast RPF is disabled.

Source IPv4 and source MAC address binding is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
11.1(CC), 12.0	This command was introduced. This command was not included in Cisco IOS Release 11.2 or 11.3.
12.1(2)T	Added access control list (ACL) support using the *access-list* argument. Added per-interface statistics on dropped or suppressed packets.
12.0(15)S	This command replaced the **ip verify unicast reverse-path** command, and the following keywords were added: **allow-default**, **allow-self-ping**, **rx**, and **any**.
12.1(8a)E	This command was integrated into Cisco IOS Release 12.1(8a)E.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command was introduced on the Supervisor Engine 2.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRC	This command was modified. The **l2-src** keyword was added to support the source IPv4 and source MAC address binding feature on platforms that support the Cisco Express Forwarding software switching path.
15.0(1)M	This command was integrated into Cisco IOS Release 15.0(1)M.

Usage Guidelines

Use the **ip verify unicast source reachable-via** interface command to mitigate problems caused by malformed or forged (spoofed) IP source addresses that pass through a router. Malformed or forged source addresses can indicate DoS attacks based on source IP address spoofing.

To use Unicast RPF, enable Cisco Express Forwarding or distributed Cisco Express Forwarding in the router. There is no need to configure the input interface for Cisco Express Forwarding. As long as Cisco Express Forwarding is running on the router, individual interfaces can be configured with other switching modes.

Note It is important for Cisco Express Forwarding to be configured globally on the router. Unicast RPF does not work without Cisco Express Forwarding.

Note Unicast RPF is an input function and is applied on the interface of a router only in the ingress direction.

When Unicast RPF is enabled on an interface, the router examines all packets that are received on that interface. The router checks to make sure that the source address appears in the FIB. If the **rx** keyword is selected, the source address must match the interface on which the packet was received. If the **any** keyword is selected, the source address must be present only in the FIB. This ability to "look backwards" is available only when Cisco Express Forwarding is enabled on the router because the lookup relies on the presence of the FIB. Cisco Express Forwarding generates the FIB as part of its operation.

Note If the source address of an incoming packet is resolved to a null adjacency, the packet will be dropped. The null interface is treated as an invalid interface by the new form of the Unicast RPF command. The older form of the command syntax did not exhibit this behavior.

Unicast RPF checks to determine whether any packet that is received at a router interface arrives on one of the best return paths to the source of the packet. If a reverse path for the packet is not found, Unicast RPF can drop or forward the packet, depending on whether an ACL is specified in the Unicast RPF command. If an ACL is specified in the command, when (and only when) a packet fails the Unicast RPF check, the ACL is checked to determine whether the packet should be dropped (using a deny statement in the ACL) or forwarded (using a permit statement in the ACL). Whether a packet is dropped or forwarded, the packet is counted in the global IP traffic statistics for Unicast RPF drops and in the interface statistics for Unicast RPF.

If no ACL is specified in the **ip verify unicast source reachable-via** command, the router drops the forged or malformed packet immediately, and no ACL logging occurs. The router and interface Unicast RPF counters are updated.

Unicast RPF events can be logged by specifying the logging option for the ACL entries that are used by the **ip verify unicast source reachable-via** command. Log information can be used to gather information about the attack, such as source address, time, and so on.

Strict Mode RPF

If the source address is in the FIB and reachable only through the interface on which the packet was received, the packet is passed. The syntax for this method is **ip verify unicast source reachable-via rx**.

Exists-Only (or Loose Mode) RPF

If the source address is in the FIB and reachable through any interface on the router, the packet is passed. The syntax for this method is **ip verify unicast source reachable-via any**.

Because this Unicast RPF option passes packets regardless of which interface the packet enters, it is often used on Internet service provider (ISP) routers that are "peered" with other ISP routers (where asymmetrical routing typically occurs). Packets using source addresses that have not been allocated on the Internet, which are often used for spoofed source addresses, are dropped by this Unicast RPF option. All other packets that have an entry in the FIB are passed.

allow-default

Normally, sources found in the FIB but only by way of the default route will be dropped. Specifying the **allow-default** keyword option will override this behavior. You must specify the **allow-default** keyword in the command to permit Unicast RPF to successfully match on prefixes that are known through the default route to pass these packets.

allow-self-ping

This keyword allows the router to ping its own interface or interfaces. By default, when Unicast RPF is enabled, packets that are generated by the router and destined to the router are dropped, thereby, making certain troubleshooting and management tasks difficult to accomplish. Issue the **allow-self-ping** keyword to enable self-pinging.

Caution Caution should be used when enabling the **allow-self-ping** keyword because this option opens a potential DoS hole.

Using RPF in Your Network

Use Unicast RPF strict mode on interfaces where only one path allows packets from valid source networks (networks contained in the FIB). Also, use Unicast RPF strict mode when a router has multiple paths to a given network, as long as the valid networks are switched through the incoming interfaces. Packets for invalid networks will be dropped. For example, routers at the edge of the network of an ISP are likely to have symmetrical reverse paths. Unicast RPF strict mode is applicable in certain multihomed situations, provided that optional Border Gateway Protocol (BGP) attributes, such as weight and local preference, are used to achieve symmetric routing.

Note With Unicast RPF, all equal-cost “best” return paths are considered valid. This means that Unicast RPF works in cases where multiple return paths exist, provided that each path is equal to the others in terms of the routing cost (number of hops, weights, and so on) and as long as the route is in the FIB. Unicast RPF also functions where Enhanced Internet Gateway Routing Protocol (EIGRP) variants are being used and unequal candidate paths back to the source IP address exist.

Use Unicast RPF loose mode on interfaces where asymmetric paths allow packets from valid source networks (networks contained in the FIB). Routers that are in the core of the ISP network have no guarantee that the best forwarding path out of the router will be the path selected for packets returning to the router.

IP and MAC Address Spoof Prevention

In Release 15.0(1)M and later, you can use the **l2-src**keyword to enable source IPv4 and source MAC address binding. To disable source IPv4 and source MAC address binding, use the **no** form of the **ip verify unicast source reachable-via**command.

If an inbound packet fails this security check, it will be dropped and the Unicast RPF dropped-packet counter will be incremented. The only exception occurs if a numbered access control list has been specified as part of the Unicast RPF command in strict mode, and the ACL permits the packet. In this case the packet will be forwarded and the Unicast RPF suppressed-drops counter will be incremented.

Note The **l2-src** keyword cannot be used with the loose uRPF command, **ip verify unicast source reachable-via any**command.

Not all platforms support the **l2-src** keyword. Therefore, not all the possible keyword combinations for strict Unicast RPF in the following list will apply to your platform:

Possible keyword combinations for strict Unicast RPF include the following:

```
allow-default
allow-self-ping
l2-src
<ACL-number>
allow-default allow-self-ping
allow-default l2-src
allow-default <ACL-number>
allow-self-ping l2-src
allow-self-ping <ACL-number>
l2-src <ACL-number>
```

allow-default allow-self-ping l2-src
allow-default allow-self-ping <*ACL-number*>
allow-default l2-src <*ACL-number*>
allow-self-ping l2-src <*ACL-number*>
allow-default allow-self-ping l2-src <*ACL-number*>

Examples

Examples

The following example uses a very simple single-homed ISP connection to demonstrate the concept of Unicast RPF. In this example, an ISP peering router is connected through a single serial interface to one upstream ISP. Hence, traffic flows into and out of the ISP will be symmetric. Because traffic flows will be symmetric, a Unicast RPF strict-mode deployment can be configured.

```
ip cef
! or “ip cef distributed” for Route Switch Processor+Versatile Interface Processor-
(RSP+VIP-) based routers.
!
interface Serial5/0/0
 description - link to upstream ISP (single-homed)
 ip address 192.168.200.225 255.255.255.252
 no ip redirects
 no ip directed-broadcasts
 no ip proxy-arp
 ip verify unicast source reachable-via
```

Examples

The following example demonstrates the use of ACLs and logging with Unicast RPF. In this example, extended ACL 197 provides entries that deny or permit network traffic for specific address ranges. Unicast RPF is configured on interface Ethernet 0/1/1 to check packets arriving at that interface.

For example, packets with a source address of 192.168.201.10 arriving at interface Ethernet 0/1/1 are dropped because of the deny statement in ACL 197. In this case, the ACL information is logged (the logging option is turned on for the ACL entry) and dropped packets are counted per-interface and globally. Packets with a source address of 192.168.201.100 arriving at interface Ethernet 0/1/2 are forwarded because of the permit statement in ACL 197. ACL information about dropped or suppressed packets is logged (the logging option is turned on for the ACL entry) to the log server.

```
ip cef distributed
!
int eth0/1/1
 ip address 192.168.200.1 255.255.255.0
 ip verify unicast source reachable-via rx 197
!
int eth0/1/2
 ip address 192.168.201.1 255.255.255.0
!
access-list 197 deny   ip 192.168.201.0 0.0.0.63 any log-input
access-list 197 permit ip 192.168.201.64 0.0.0.63 any log-input
access-list 197 deny   ip 192.168.201.128 0.0.0.63 any log-input
access-list 197 permit ip 192.168.201.192 0.0.0.63 any log-input
access-list 197 deny ip host 0.0.0.0 any log-input
access-list 197 deny ip 172.16.0.0 0.255.255.255 any log-input
access-list 197 deny ip 10.0.0.0 0.255.255.255 any log-input
access-list 197 deny ip 172.16.0.0 0.15.255.255 any log-input
access-list 197 deny ip 192.168.0.0 0.0.255.255 any log-input
```

Examples

The following example shows how to enable source IPv4 and source MAC address binding on Ethernet 0/0:

```
Router# configure terminal
```

```
Router(config)# interface Ethernet0/0
Router(config-if)# ip address 10.0.0.1 255.255.255.0
Router(config-if)# ip verify unicast source reachable-via rx l2-src
```

Related Commands

Command	Description
ip cef	Enables Cisco Express Forwarding on the route processor card.
ip cef distributed	Enables Cisco Express Forwarding on the line card.

ip virtual-reassembly

To enable virtual fragment reassembly (VFR) on an interface, use the **ip virtual-reassembly** command in interface configuration mode. To disable VFR on an interface, use the **no** form of this command.

ip virtual-reassembly [**max-reassemblies** *number*] [**max-fragments** *number*] [**timeout** *seconds*] **[drop-fragments]**

no ip virtual-reassembly [**max-reassemblies** *number*] [**max-fragments** *number*] [**timeout** *seconds*] **[drop-fragments]**

Syntax Description

max-reassemblies *number*	(Optional) Maximum number of IP datagrams that can be reassembled at any given time. Default value: 16. If the maximum value is reached, all fragments within the following fragment set is dropped and an alert message is logged to the syslog server.
max-fragments *number*	(Optional) Maximum number of fragments that are allowed per IP datagram (fragment set). Default value: 32. If an IP datagram that is being reassembled receives more than the maximum allowed fragments, the IP datagram is dropped and an alert message is logged to the syslog server.
timeout *seconds*	(Optional) Timeout value, from 0 to 60 seconds, for an IP datagram that is being reassembled. Default value: 3 seconds. If an IP datagram does not receive all of the fragments within the specified time, the IP datagram (and all of its fragments) are dropped.
drop-fragments	(Optional) Enables the VFR to drop all fragments that arrive on the configured interface. By default, this function is disabled.

Command Default

VFR is not enabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(8)T	This command was introduced.
IOS XE 3.2S	This command was introduced in Cisco IOS XE Release 3.2S.

Usage Guidelines

A buffer overflow attack can occur when an attacker continuously sends a large number of incomplete IP fragments, causing the firewall to lose time and memory while trying to reassemble the fake packets.

The **max-reassemblies** *number*option and the **max-fragments** *number*option allow you to configure maximum threshold values to avoid a buffer overflow attack and to control memory usage.

In addition to configuring the maximum threshold values, each IP datagram is associated with a managed timer. If the IP datagram does not receive all of the fragments within the specified time (which can be configured through the **timeout** *seconds* option), the timer expires and the IP datagram (and all of its fragments) is dropped.

Note If you are upgrading to Cisco IOS XE Release 3.4 or later and the configured timeout was set to more than 60 seconds, then your configured timeout value is cleared and reset to the default value of 3 seconds.

Automatically Enabling or Disabling VFR

VFR is designed to work with any feature that requires fragment reassembly (such as Cisco IOS Firewall and NAT). Currently, NAT enables and disables VFR internally; that is, when NAT is enabled on an interface, VFR is automatically enabled on that interface.

If more than one feature attempts to automatically enable VFR on an interface, then the VFR maintains a reference count to keep track of the number of features that have enabled VFR. When the reference count is reduced to zero, VFR is automatically disabled

Examples

The following example shows how to configure VFR on interfaces ethernet2/1, ethernet2/2, and serial3/0 to facilitate the firewall that is enabled in the outbound direction on interface serial3/0. In this example, the firewall rules that specify the list of LAN1 and LAN2 originating protocols (FTP, HTTP and SMTP) are to be inspected.

```
ip inspect name INTERNET-FW ftp
ip inspect name INTERNET-FW http
ip inspect name INTERNET-FW smtp!
!
interface Loopback0
 ip address 10.0.1.1 255.255.255.255
!
interface Ethernet2/0
 ip address 10.4.21.9 255.255.0.0
 no ip proxy-arp
 no ip mroute-cache
 duplex half
 no cdp enable
!
interface Ethernet2/1
 description LAN1
 ip address 10.4.0.2 255.255.255.0
 ip virtual-reassembly
 duplex half
!
interface Ethernet2/2
 description LAN2
 ip address 10.15.0.2 255.255.255.0
 ip virtual-reassembly
 duplex half
!
interface Ethernet2/3
 no ip address
 no ip mroute-cache
 shutdown
 duplex half
!
interface Serial3/0
 description Internet
 ip unnumbered Loopback0
 encapsulation ppp
 ip access-group 102 in
 ip inspect INTERNET-FW out
 ip virtual-reassembly
 serial restart-delay 0
```

Related Commands

Command	Description
show ip virtual-reassembly	Displays the configuration and statistical information of the VFR on a given interface.

ip virtual-reassembly-out

To enable virtual fragment reassembly (VFR) on outbound interface traffic after it was disabled by the **no ip virtual-reassembly** command, use the **ip virtual-reassembly-out** command in interface configuration mode. To disable VFR on outbound interface traffic, use the **no** form of this command.

ip virtual-reassembly-out [**max-reassemblies** *number*] [**max-fragments** *number*] [**timeout** *seconds*] **[drop-fragments]**

no ip virtual-reassembly-out [**max-reassemblies** *number*] [**max-fragments** *number*] [**timeout** *seconds*] **[drop-fragments]**

Syntax Description

max-reassemblies *number*	(Optional) Specifies the maximum number of IP datagrams that can be reassembled at any given time. Default value: 16. If the maximum value is reached, all fragments within the following fragment set will be dropped and an alert message will be logged to the syslog server.
max-fragments *number*	(Optional) Specifies the maximum number of fragments that are allowed per IP datagram (fragment set). Default value: 32. If an IP datagram that is being reassembled receives more than the maximum number of allowed fragments, the IP datagram will be dropped and an alert message will be logged to the syslog server.
timeout *seconds*	(Optional) Specifies the timeout value, in seconds, for an IP datagram that is being reassembled. Default value: 3. If an IP datagram does not receive all of the fragments within the specified time, the IP datagram (and all of its fragments) will be dropped.
drop-fragments	(Optional) Enables the VFR to drop all fragments that arrive on the configured interface. By default, this function is disabled.

Command Default

VFR on outbound interface traffic is not enabled.

Command Modes

Interface configuration (config-if)

Command History

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

Usage Guidelines

You can use this command to reenable VFR on outbound interface traffic after it was disabled by the **no ip virtual-reassembly** command. If VFR is enabled on both inbound and outbound interface traffic, you can use the **no ip virtual-reassembly-out** command to disable it on only the outbound interface traffic.

Examples

The following example shows how to manually enable VFR on outbound traffic on interfaces GigabitEthernet0/0/1, GigabitEthernet0/0/0.773, and Serial 3/0:

```
interface Loopback 0
ip address 10.0.1.1 255.255.255.255
!
interface GigabitEthernet0/0/1
description LAN1
ip address 10.4.0.2 255.255.255.0
ip virtual-reassembly-out
!
interface GigabitEthernet0/0/0.773
encapsulation dot1Q 773
description LAN2
ip address 10.15.0.2 255.255.255.0
ip virtual-reassembly-out
!
interface Serial 3/0
description Internet
ip unnumbered Loopback0
encapsulation ppp
ip virtual-reassembly-out
serial restart-delay 0
```

Related Commands

Command	Description
ip virtual-reassembly	Enables VFR on an interface.
show ip virtual-reassembly	Displays the configuration and statistical information of the VFR on a given interface.

ip vrf

To define a VPN routing and forwarding (VRF) instance and to enter VRF configuration mode, use the **ip vrf** command in global configuration mode. To remove a VRF instance, use the **no** form of this command.

ip vrf *vrf-name*

no ip vrf *vrf-name*

Syntax Description

vrf-name	Name assigned to a VRF.

Command Default

No VRFs are defined. No import or export lists are associated with a VRF. No route maps are associated with a VRF.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(5)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 12.2(14)S.
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(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.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.
Cisco IOS XE 3.3SE	This command was implemented in Cisco IOS XE Release 3.3SE.

Usage Guidelines

The **ip vrf** *vrf-name* command creates a VRF instance named *vrf-name*. To make the VRF functional, a route distinguisher (RD) must be created using the **rd** *route-distinguisher* command in VRF configuration mode. The **rd** *route-distinguisher* command creates the routing and forwarding tables and associates the RD with the VRF instance named *vrf-name*.

The **ip vrf default** command can be used to configure a VRF instance that is a NULL value until a default VRF name can be configured. This is typically before any VRF related AAA commands are configured.

Examples

The following example shows how to import a route map to a VRF instance named VPN1:

```
Router(config)# ip vrf vpn1
Router(config-vrf)# rd 100:2
Router(config-vrf)# route-target both 100:2
Router(config-vrf)# route-target import 100:1
```

Related Commands

Command	Description
ip vrf forwarding (interface configuration)	Associates a VRF with an interface or subinterface.
rd	Creates routing and forwarding tables for a VRF and specifies the default route distinguisher for a VPN.

ip vrf forwarding

To associate a Virtual Private Network (VPN) routing and forwarding (VRF) instance with a Diameter peer, use the **ip vrf forwarding** command in Diameter peer configuration mode. To enable Diameter peers to use the global (default) routing table, use the no form of this command.

ip vrf forwarding *name*

no ip vrf forwarding *name*

Syntax Description

name	Name assigned to a VRF.

Command Default

Diameter peers use the global routing table.

Command Modes

Diameter peer configuration (config-dia-peer)

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.2(54)SG	This command was integrated into Cisco IOS Release 12.2(54)SG.

Usage Guidelines

Use the **ip vrf forwarding** command to specify a VRF for a Diameter peer. If a VRF name is not configured for a Diameter server, the global routing table will be used.

If the VRF associated with the specified name has not been configured, the command will have no effect and this error message will appear: **No VRF found with the name***name* .

Examples

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

```
Router (config-dia-peer)# ip vrf forwarding
 diam_peer_1
```

Related Commands

Command	Description
diameter peer	Configures a Diameter peer and enters Diameter peer configuration submode.
ip vrf forwarding (server-group)	Configures the VRF reference of an AAA RADIUS or TACACS+ server group.

ip vrf forwarding (server-group)

To configure the Virtual Private Network (VPN) routing and forwarding (VRF) reference of an authentication, authorization, and accounting (AAA) RADIUS or TACACS+ server group, use the **ip vrf forwarding** command in server-group configuration mode. To enable server groups to use the global (default) routing table, use the no form of this command.

ip vrf forwarding *vrf-name*

no ip vrf forwarding *vrf-name*

Syntax Description

vrf-name	Name assigned to a VRF.

Command Default

Server groups use the global routing table.

Command Modes

Server-group configuration (server-group)

Command History

Release	Modification
12.2(2)DD	This command was introduced on the Cisco 7200 series and Cisco 7401ASR.
12.2(4)B	This command was integrated into Cisco IOS Release 12.2(4)B.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.3(7)T	Functionality was added for TACACS+ servers.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA1	This command was integrated into Cisco IOS Release 12.2(33)SRA1.
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.

Usage Guidelines

Use the **ip vrf forwarding** command to specify a VRF for a AAA RADIUS or TACACS+ server group. This command enables dial users to utilize AAA servers in different routing domains.

Examples

The following example shows how to configure the VRF user to reference the RADIUS server in a different VRF server group:

```
aaa group server radius sg_global
 server-private 172.16.0.0 timeout 5 retransmit 3
!
aaa group server radius sg_water
 server-private 10.10.0.0 timeout 5 retransmit 3 key water
 ip vrf forwarding water
```

The following example shows how to configure the VRF user to reference the TACACS+ server in the server group tacacs1:

```
aaa group server tacacs+tacacs1
    server-private 10.1.1.1 port 19 key cisco
    ip vrf forwarding cisco
    ip tacacs source-interface Loopback0
  ip vrf cisco
   rd 100:1
  interface Loopback0
   ip address 10.0.0.2 255.0.0.0
   ip vrf forwarding cisco
```

Related Commands

Command	Description
aaa group server radius	Groups different RADIUS server hosts into distinct lists and distinct methods.
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.
server-private	Configures the IP address of the private RADIUS server for the group server.

ip wccp web-cache accelerated

To enable the hardware acceleration for WCCP version 1, use the **ip wccp web-cache accelerated** command in global configuration mode. To disable hardware acceleration, use the **no** form of this command.

ip wccp web-cache accelerated[**group-address** *group-address*]| [**redirect-list** *access-list*]| [**group-list** *access-list*]| [[**password** *password*]]

no ip wccp web-cache accelerated

Syntax Description

group-address *group-address*	(Optional) Directs the router to use a specified multicast IP address for communication with the WCCP service group. See the "Usage Guidelines" section for additional information.
redirect-list *access-list*	(Optional) Directs the router to use an access list to control traffic that is redirected to this service group. See the "Usage Guidelines" section for additional information.
group-list *access-list*	(Optional) Directs the router to use an access list to determine which cache engines are allowed to participate in the service group. See the "Usage Guidelines" section for additional information.
password *password*	(Optional) Specifies a string that directs the router to apply MD5 authentication to messages received from the service group specified by the service name given. See the "Usage Guidelines" section for additional information.

Command Default

When this command is not configured, hardware acceleration for WCCPv1 is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
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(18)SXD1	This command was changed to support the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **group-address** *group-address* option requires a multicast address that is used by the router to determine which cache engine should receive redirected messages. This option instructs the router to use the specified multicast IP address to coalesce the “I See You” responses for the “Here I Am” messages that it has received on this group address. In addition, the response is sent to the group address. The default is for no **group-address** to be configured, so that all “Here I Am” messages are responded to with a unicast reply.

The **redirect-list** *access-list* option instructs the router to use an access list to control the traffic that is redirected to the cache engines of the service group that is specified by the service-name given. The *access-list* argument specifies either a number from 1 to 99 to represent a standard or extended access list number, or a name to represent a named standard or extended access list. The access list itself specifies the traffic that is permitted to be redirected. The default is for no **redirect-list** to be configured (all traffic is redirected).

The **group-list** *access-list* option instructs the router to use an access list to control the cache engines that are allowed to participate in the specified service group. The *access-list* argument specifies either a number from 1 to 99 to represent a standard access list number, or a name to represent a named standard access list. The access list specifies which cache engines are permitted to participate in the service group. The default is for no **group-list** to be configured, so that all cache engines may participate in the service group.

The password can be up to seven characters. When you designate a password, the messages that are not accepted by the authentication are discarded. The password name is combined with the HMAC MD5 value to create security for the connection between the router and the cache engine.

Examples

The following example shows how to enable the hardware acceleration for WCCP version 1:

```
Router(config)# ip wccp web-cache accelerated
```

Related Commands

Command	Description
ip wccp version	Specifies which version of WCCP to configure on your router.

ips signature update cisco

To initiate a one-time download of Cisco IOS Intrusion Prevention System (IPS) signatures from Cisco.com, use the **ips signature update cisco** command in Privileged EXEC mode.

ips signature update cisco {**next**| **latest**| **signature**} [**username** *name* **password** *password*]

Syntax Description

next	Specifies the next signature file version from the current signature file on the router.
latest	Specifies the IOS IPS to search for the latest signature file.
signature	This argument specifies a specific signature file on Cisco.com.
username *name*	Defines the username for the automatic signature update function.
password *password*	Defines the password for the automatic signature update function.

Command Default

Privileged EXEC mode (#)

Command History

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

Usage Guidelines

The **ips signature update cisco**command is used to initiate a one-time download of IPS signatures from Cisco.com. If you want IPS signatures to be periodically downloaded from Cisco.com, use the **ip ips auto-update** command in global configuration mode and subsequently the **cisco** command in IPS-auto-update configuration mode to enable automatic signature updates from Cisco.com.

If the *username* and *password* is not specified, then the username and password that is specified in the IPS auto update configuration is used. A user name and password must be configured for updating signatures directly from Cisco.com.

Examples

The following example shows how to get the latest automatic signature update from Cisco.com:

```
Router# ips signature update cisco latest
```

Related Commands

Command	Description
ip ips auto-update	Enables automatic signature updates for Cisco IOS IPS.
cisco	Enables automatic signature updates from Cisco.com.

ipv4 (ldap)

To create an IPv4 address within a Lightweight Directory Access Protocol (LDAP) server address pool, use the **ipv4** command in LDAP server configuration mode. To delete an IPv4 address within an LDAP server address pool, use the **no** form of this command.

ipv4 *ipv4-address*

no ipv4 *ipv4-address*

Syntax Description

ipv4-address	IPv4 address of the LDAP server.

Command Default

No IPv4 addresses are created in the LDAP server address pool.

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 create an IPv4 address in an LDAP server address pool:

```
Router(config)# ldap server server1
Router(config-ldap-server)# ipv4 10.0.0.1
```

Related Commands

Command	Description
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.

ipv6 crypto map

To enable an IPv6 crypto map on an interface, use the **ipv6 crypto map** command in interface configuration mode. To disable, use the **no** form of this command.

ipv6 crypto map *map-name*

no ipv6 crypto map

Syntax Description

map-name	Identifies the crypto map set.

Command Default

No IPv6 crypto maps are enabled on the interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
15.1(4)M	This command was introduced.

Usage Guidelines

This command differentiates IPv6 and IPv4 crypto maps.

Examples

The following example shows how to enable an IPv6 crypto map on an interface:

```
Router# configure terminal
Router(config
)# interface ethernet 0/0
Router(config-if
)# ipv6 crypto map CM_V4
```

Related Commands

Command	Description
crypto map (global IPsec)	Creates or modifies a crypto map entry.

ipv6 cga modifier rsakeypair

To generate an IPv6 cryptographically generated address (CGA) modifier for a specified Rivest, Shamir, and Adelman (RSA) key pair, use the **ipv6 cga modifier rsakeypair**command in global configuration mode. To disable this function, use the **no** form of this command.

ipv6 cga modifier rsakeypair *key-label* **sec-level** *sec-level-value* [**max-iterations value**| *cga-modifier*]

no ipv6 cga modifier rsakeypair

Syntax Description

key-label	The name to be used for RSA key pair
sec-level *sec-level-value*	Specifies the security level, which can be a number from 0 through 3. The most secure level is 1.
max-iterations*value*	(Optional) Maximum iteration for modifier generation. The *value* can be a number from 0 through 40000000.
cga-modifier	(Optional) An IPv6 address used as a CGA modifier.

Command Default

No CGA exists for an RSA key.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(24)T	This command was introduced.
15.1(3)T	The **max-iterations** keyword and *cga-modifier* argument were added.

Usage Guidelines

Use this command to generate the CGA modifier for a specified RSA key pair, which enables the key to be used by Secure Neighbor Discovery (SeND).

Once the RSA key is generated, the modifier must be generated as well, using the **ipv6 cga modifier rsakeypair** command.

A CGA has a security parameter that determines its strength against brute-force attacks. The security level can be either 0 or 1.

Examples

The following example enables the specified key to be used by SeND (that is, generates the modifier):

```
Router(config)# ipv6 cga modifier rsakeypair SEND sec-level 1
```

Related Commands

Command	Description
crypto key generate rsa	Generates RSA key pairs.
ipv6 cga modifier rsakeypair	Generates the CGA modifier for a specified RSA key.
ipv6 cga modifier rsakeypair (interface)	Binds a SeND key to a specified interface.
ipv6 cga rsakeypair	Specifies which RSA key should be used on an interface.

ipv6 cga rsakeypair

To bind a Secure Neighbor Discovery (SeND) key to a specified interface, use the **ipv6 cga rsakeypair**command in interface configuration mode. To disable this function, use the **no** form of this command.

ipv6 cga rsakeypair *key-label*

no ipv6 cga rsakeypair

Syntax Description

key-label	The name to be used for the Rivest, Shamir, and Adelman (RSA) key pair.

Command Default

A SeND key is not bound to an interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(24)T	This command was introduced.

Usage Guidelines

The SeND key is used to generate an IPv6 modifier for a specified Rivest, Shamir and Adelman (RSA) key pair. A SeND key must be bound to the interface prior to its being used in the **ipv6 address** command. Use the **ipv6 cga rsakeypair** command to bind a SeND key to a specified interface.

You can then use the **ipv6 address** command to add the Cryptographic Addresses (CGA).

Examples

The following example binds a SeND key to Ethernet interface 0/0:

```
Router(config)# interface Ethernet0/0
Router(config-if)# ip address 10.0.1.1 255.255.255.0
Router(config-if)# ipv6 cga rsakeypair SEND
```

Related Commands

Command	Description
ipv6 address	Configures an IPv6 address based on an IPv6 general prefix and enables IPv6 processing on an interface.
crypto key generate rsa	Generates RSA key pairs.
ipv6 cga modifier rsakeypair (global configuration)	Generates the CGA modifier for a specified RSA key.

Command	Description
ipv6 cga modifier rsakeypair (interface configuration)	Binds a SeND key to a specified interface.
ipv6 cga rsakeypair	Specifies which RSA key should be used on an interface.

ipv6 inspect

To apply a set of inspection rules to an interface, use the **ipv6 inspect** command in interface configuration mode. To remove the set of rules from the interface, use the **no** form of this command.

ipv6 inspect *inspection-name* {**in**| **out**}

no ipv6 inspect *inspection-name* {**in**| **out**}

Syntax Description

inspection-name	Identifies which set of inspection rules to apply.
in	Applies the inspection rules to inbound traffic.
out	Applies the inspection rules to outbound traffic.

Command Default

If no set of inspection rules is applied to an interface, no traffic will be inspected by Context-Based Access Control (CBAC).

Command Modes

Interface configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

Use this command to apply a set of inspection rules to an interface.

Typically, if the interface connects to the external network, you apply the inspection rules to outbound traffic; alternately, if the interface connects to the internal network, you apply the inspection rules to inbound traffic.

If you apply the rules to outbound traffic, then return inbound packets will be permitted if they belong to a valid connection with existing state information. This connection must be initiated with an outbound packet.

If you apply the rules to inbound traffic, then return outbound packets will be permitted if they belong to a valid connection with existing state information. This connection must be initiated with an inbound packet.

Examples

The following example applies a set of inspection rules named "outboundrules" to an external interface's outbound traffic. This causes inbound IP traffic to be permitted only if the traffic is part of an existing session, and to be denied if the traffic is not part of an existing session.

```
interface serial0
 ipv6 inspect outboundrules out
```

Related Commands

Command	Description
ipv6 inspect name	Defines a set of inspection rules.

ipv6 inspect alert-off

To disable Context-based Access Control (CBAC) alert messages, which are displayed on the console, use the ipv6 inspect alert off command in global configuration mode. To enable Cisco IOS firewall alert messages, use the no form of this command.

ipv6 inspect alert-off

no ipv6 inspect alert-off

Syntax Description

This command has no arguments or keywords.

Command Default

Alert messages are displayed.

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Examples

The following example turns off CBAC alert messages:

```
ipv6 inspect alert-off
```

Related Commands

Command	Description
ipv6 inspect audit trail	Turns on CBAC audit trail messages, which will be displayed on the console after each CBAC session close.
ipv6 inspect name	Applies a set of inspection rules to an interface.

ipv6 inspect audit trail

To turn on Context-based Access Control (CBAC) audit trail messages, which will be displayed on the console after each Cisco IOS firewall session closes, use the ipv6 inspect audit trail command in global configuration mode. To turn off Cisco IOS firewall audit trail message, use the no form of this command.

ipv6 inspect audit trail

no ipv6 inspect audit trail

Syntax Description

This command has no arguments or keywords.

Command Default

Audit trail messages are not displayed.

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

Use this command to turn on CBAC audit trail messages.

Examples

The following example turns on CBAC audit trail messages:

```
ipv6 inspect audit trail
```

Afterward, audit trail messages such as the following are displayed:

```
%FW-6-SESS_AUDIT_TRAIL: tcp session initiator (192.168.1.13:33192) sent 22 bytes -- responder
 (192.168.129.11:25) sent 208 bytes
%FW-6-SESS_AUDIT_TRAIL: ftp session initiator 192.168.1.13:33194) sent 336 bytes -- responder
 (192.168.129.11:21) sent 325 bytes
```

These messages are examples of audit trail messages. To determine which protocol was inspected, refer to the responder's port number. The port number follows the responder's IP address.

Related Commands

Command	Description
ipv6 inspect alert-off	Disables CBAC alert messages.
ipv6 inspect name	Applies a set of inspection rules to an interface.

ipv6 inspect max-incomplete high

To define the number of existing half-open sessions that will cause the software to start deleting half-open sessions, use the ipv6 inspect max-incomplete high command in global configuration mode. To reset the threshold to the default of 500 half-open sessions, use the no form of this command.

ipv6 inspect max-incomplete high *number*

no ipv6 inspect max-incomplete high

Syntax Description

number	Specifies the rate of new unestablished TCP sessions that will cause the software to start deleting half-open sessions. The default is 500 half-open sessions. The value range is 1 through 4294967295.

Command Default

The default is 500 half-open sessions.

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

An unusually high number of half-open sessions (either absolute or measured as the arrival rate) could indicate that a denial-of-service attack is occurring. For TCP, "half-open" means that the session has not reached the established state. For User Datagram Protocol, "half-open" means that the firewall has detected traffic from one direction only.

Context-based Access Control (CBAC) measures both the total number of existing half-open sessions and the rate of session establishment attempts. Both TCP and UDP half-open sessions are counted in the total number and rate measurements. Measurements are made once a minute.

When the number of existing half-open sessions rises above a threshold (the **max-incomplete high** number), the software will delete half-open sessions as required to accommodate new connection requests. The software will continue to delete half-open requests as necessary, until the number of existing half-open sessions drops below another threshold (the **max-incomplete low** number).

The global value specified for this threshold applies to all TCP and UDP connections inspected by CBAC.

Examples

The following example causes the software to start deleting half-open sessions when the number of existing half-open sessions rises above 900, and to stop deleting half-open sessions when the number drops below 800:

```
ipv6 inspect max-incomplete high 900
ipv6 inspect max-incomplete low 800
```

Related Commands

Command	Description
ipv6 inspect max-incomplete low	Defines the number of existing half-open sessions that will cause the software to stop deleting half-open sessions.
ipv6 inspect one-minute high	Defines the rate of new unestablished sessions that will cause the software to start deleting half-open sessions.
ipv6 inspect one-minute low	Defines the rate of new unestablished TCP sessions that will cause the software to stop deleting half-open sessions.
ipv6 inspect tcp max-incomplete host	Specifies the threshold and blocking time values for TCP host-specific denial-of-service detection and prevention.

ipv6 inspect max-incomplete low

To define the number of existing half-open sessions that will cause the software to stop deleting half-open sessions, use the **ipv6 inspect max-incomplete low**command in global configuration mode. To reset the threshold to the default of 400 half-open sessions, use the **no** form of this command.

ipv6 inspect max-incomplete low *number*

no ipv6 inspect max-incomplete low

Syntax Description

number	Specifies the number of existing half-open sessions that will cause the software to stop deleting half-open sessions . The default is 400 half-open sessions. Value range is 1 through 4294967295.

Command Default

The default is 400 half-open sessions.

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

An unusually high number of half-open sessions (either absolute or measured as the arrival rate) could indicate that a denial-of-service attack is occurring. For TCP, "half-open" means that the session has not reached the established state. For User Datagram Protocol, "half-open" means that the firewall has detected traffic from one direction only.

Context-based Access Control (CBAC) measures both the total number of existing half-open sessions and the rate of session establishment attempts. Both TCP and UDP half-open sessions are counted in the total number and rate measurements. Measurements are made once a minute.

When the number of existing half-open sessions rises above a threshold (the **max-incomplete high** number), the software will delete half-open sessions as required to accommodate new connection requests. The software will continue to delete half-open requests as necessary, until the number of existing half-open sessions drops below another threshold (the **max-incomplete low** number).

The global value specified for this threshold applies to all TCP and UDP connections inspected by CBAC.

Examples

The following example causes the software to start deleting half-open sessions when the number of existing half-open sessions rises above 900, and to stop deleting half-open sessions when the number drops below 800:

```
ipv6 inspect max-incomplete high 900
ipv6 inspect max-incomplete low 800
```

Related Commands

Command	Description
ipv6 inspect max-incomplete high	Defines the number of existing half-open sessions that will cause the software to start deleting half-open sessions.
ipv6 inspect one-minute high	Defines the rate of new unestablished sessions that will cause the software to start deleting half-open sessions.
ipv6 inspect one-minute low	Defines the rate of new unestablished TCP sessions that will cause the software to stop deleting half-open sessions.
ipv6 inspect tcp max-incomplete host	Specifies the threshold and blocking time values for TCP host-specific denial-of-service detection and prevention.

ipv6 inspect name

To define a set of ipv6 inspection rules, use the **ipv6 inspect name** command in global configuration mode. To remove the inspection rule for a protocol or to remove the entire set of inspection rules, use the **no** form of this command.

ipv6 inspect name *inspection-name protocol* [**alert** {**on**| **off**}] [**audit-trail** {**on**| **off**}] [**timeout** *seconds*]

no ipv6 inspect name inspection-name [protocol]

Syntax Description

inspection-name	Names the set of inspection rules. If you want to add a protocol to an existing set of rules, use the same inspection name as the existing set of rules.
protocol	A specified protocol. Possible protocol values are **icmp**, **udp**, **tcp**, and **ftp**. This value is optional in the **no** version of this command.
alert {**on** | **off**}	(Optional) For each inspected protocol, the generation of alert messages can be set be on or off. If no option is selected, alerts are generated based on the setting of the ipv6 inspect alert-off command.
audit-trail {**on** | **off**}	(Optional) For each inspected protocol, the audit trail can be set on or off. If no option is selected, audit trail messages are generated based on the setting of the **ipv6 inspect audit-trail** command.
timeout *seconds*	(Optional) Specifies the number of seconds for a different idle timeout to override the global TCP or User Datagram Protocol (UDP) idle timeouts for the specified protocol. This timeout overrides the global TCP and UPD timeouts but will not override the global Domain Name System (DNS) timeout.

timeout seconds (fragmentation)	Configures the number of seconds that a packet state structure remains active. When the **timeout** value expires, the router drops the unassembled packet, freeing that structure for use by another packet. The default **timeout** value is 1 second. If this number is set to a value greater than 1 second, it will be automatically adjusted by the Cisco IOS software when the number of free state structures goes below certain thresholds: when the number of free states is less than 32, the timeout will be divided by 2. When the number of free states is less than 16, the timeout will be set to 1 second.

Command Default

No set of inspection rules is defined.

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.3(11)T	FTP protocol support was added.

Usage Guidelines

To define a set of inspection rules, enter this command for each protocol that you want the Cisco IOS firewall to inspect, using the same *inspection-name*. Give each set of inspection rules a unique *inspection-name*, which should not exceed the 16-character limit. Define either one or two sets of rules per interface--you can define one set to examine both inbound and outbound traffic, or you can define two sets: one for outbound traffic and one for inbound traffic.

To define a single set of inspection rules, configure inspection for all the desired application-layer protocols, and for TCP, UDP, or Internet Control Message Protocol (ICMP) as desired. This combination of TCP, UDP, and application-layer protocols join together to form a single set of inspection rules with a unique name. (There are no application-layer protocols associated with ICMP.)

To remove the inspection rule for a protocol, use the **no** form of this command with the specified inspection name and protocol. To remove the entire set of named inspection rules, use the **no** form of this command with the specified inspection name.

In general, when inspection is configured for a protocol, return traffic entering the internal network will be permitted only if the packets are part of a valid, existing session for which state information is being maintained.

TCP and UDP Inspection

You can configure TCP and UDP inspection to permit TCP and UDP packets to enter the internal network through the firewall, even if the application-layer protocol is not configured to be inspected. However, TCP and UDP inspection do not recognize application-specific commands, and therefore might not permit all return packets for an application, particularly if the return packets have a different port number from the previous exiting packet.

Any application-layer protocol that is inspected will take precedence over the TCP or UDP packet inspection. For example, if inspection is configured for FTP, all control channel information will be recorded in the state table, and all FTP traffic will be permitted back through the firewall if the control channel information is valid for the state of the FTP session. The fact that TCP inspection is configured is irrelevant.

With TCP and UDP inspection, packets entering the network must exactly match an existing session: the entering packets must have the same source or destination addresses and source or destination port numbers as the exiting packet (but reversed). Otherwise, the entering packets will be blocked at the interface.

ICMP Inspection

An ICMP inspection session is on the basis of the source address of the inside host that originates the ICMP packet. Dynamic access control lists (ACLs) are created for return ICMP packets of the allowed types (destination unreachable, echo-reply, time-exceeded, and packet too big) for each session. There are no port numbers associated with an ICMP session, and the permitted IP address of the return packet is wild-carded in the ACL. The wild-card address is because the IP address of the return packet cannot be known in advance for time-exceeded and destination-unreachable replies. These replies can come from intermediate devices rather than the intended destination.

FTP Inspection

Cisco IOS Firewall uses layer 7 support for application modules such as FTP.

Cisco IOS IPv6 Firewall uses RFC 2428 to garner IPv6 addresses and corresponding ports. If an address other than an IPv6 address is present, the FTP data channel is not opened.

IPv6-specific port-to-application mapping (PAM) provides FTP inspection. PAM translates TCP or UDP port numbers into specific network services or applications. By mapping port numbers to network services or applications, an administrator can force firewall inspection on custom configurations not defined by well-known ports. PAM delivers with the standard well-known ports defined as defaults.

The table below describes the transport-layer and network-layer protocols.

Table 15: Protocol Keywords--Transport-Layer and Network-Layer Protocols

Protocol	Keyword
ICMP	**icmp**
TCP	**tcp**
UDP	**udp**
FTP	**ftp**

Use of the timeout Keyword

If you specify a timeout for any of the transport-layer or application-layer protocols, the timeout will override the global idle timeout for the interface to which the set of inspection rules is applied.

If the protocol is TCP or a TCP application-layer protocol, the timeout will override the global TCP idle timeout. If the protocol is UDP or a UDP application-layer protocol, the timeout will override the global UDP idle timeout.

If you do not specify a timeout for a protocol, the timeout value applied to a new session of that protocol will be taken from the corresponding TCP or UDP global timeout value valid at the time of session creation.

The default ICMP timeout is deliberately short (10 seconds) due to the security hole that is opened by allowing ICMP packets with a wild-carded source address back into the inside network. The timeout will occur 10 seconds after the last outgoing packet from the originating host. For example, if you send a set of 10 ping packets spaced one second apart, the timeout will expire in 20 seconds or 10 seconds after the last outgoing packet. However, the timeout is not extended for return packets. If a return packet is not seen within the timeout window, the hole will be closed and the return packet will not be allowed in. Although the default timeout can be made longer if desired, it is recommended that this value be kept relatively short.

Examples

The following example causes the software to inspect TCP sessions and UDP sessions:

```
ipv6 inspect name myrules tcp
ipv6 inspect name myrules udp audit-trail on
```

Related Commands

Command	Description
ipv6 inspect alert-off	Disables CBAC alert messages.
ipv6 inspect audit trail	Turns on CBAC audit trail messages, which will be displayed on the console after each CBAC session close.

ipv6 inspect one-minute high

To define the rate of new unestablished sessions that will cause the software to start deleting half-open sessions, use the **ipv6 inspect one-minute high**command in global configuration mode. To reset the threshold to the default of 500 half-open sessions, use the **no** form of this command.

ipv6 inspect one-minute high *number*

no ipv6 inspect one-minute high

Syntax Description

number	Specifies the rate of new unestablished TCP sessions that will cause the software to start deleting half-open sessions . The default is 500 half-open sessions. Value range is 1 through 4294967295

Command Default

The default is 500 half-open sessions.

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

An unusually high number of half-open sessions (either absolute or measured as the arrival rate) could indicate that a denial-of-service attack is occurring. For TCP, "half-open" means that the session has not reached the established state. For User Datagram Protocol, "half-open" means that the firewall has detected traffic from one direction only.

Context-based Access Control (CBAC) measures both the total number of existing half-open sessions and the rate of session establishment attempts. Both TCP and UDP half-open sessions are included in the total number and rate measurements. Measurements are made once a minute.

When the rate of new connection attempts rises above a threshold (the **one-minute high** number), the software will delete half-open sessions as required to accommodate new connection attempts. The software will continue to delete half-open sessions as necessary, until the rate of new connection attempts drops below another threshold (the **one-minute low** number). The rate thresholds are measured as the number of new session connection attempts detected in the last one-minute sample period. (The rate is calculated as an exponentially-decayed rate.)

The global value specified for this threshold applies to all TCP and UDP connections inspected by CBAC.

Examples

The following example causes the software to start deleting half-open sessions when more than 1000 session establishment attempts have been detected in the last minute, and to stop deleting half-open sessions when fewer than 950 session establishment attempts have been detected in the last minute:

```
ipv6 inspect one-minute high 1000
ipv6 inspect one-minute low 950
```

Related Commands

Command	Description
ipv6 inspect one-minute low	Defines the rate of new unestablished TCP sessions that will cause the software to stop deleting half-open sessions.
ipv6 inspect max-incomplete high	Defines the number of existing half-open sessions that will cause the software to start deleting half-open sessions.
ipv6 inspect max-incomplete low	Defines the number of existing half-open sessions that will cause the software to stop deleting half-open sessions.
ipv6 inspect tcp max-incomplete host	Specifies the threshold and blocking time values for TCP host-specific denial-of-service detection and prevention.

ipv6 inspect one-minute low

To define the rate of new unestablished TCP sessions that will cause the software to stop deleting half-open sessions, use the **ipv6 inspect one-minute low**command in global configuration mode. To reset the threshold to the default of 400 half-open sessions, use the **no** form of this command.

ipv6 inspect one-minute low *number*

no ipv6 inspect one-minute low

Syntax Description

number	Specifies the rate of new unestablished TCP sessions that will cause the software to stop deleting half-open sessions . The default is 400 half-open sessions. Value range is 1 through 4294967295.

Command Default

The default is 400 half-open sessions.

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

An unusually high number of half-open sessions (either absolute or measured as the arrival rate) could indicate that a denial-of-service attack is occurring. For TCP, "half-open" means that the session has not reached the established state. For User Datagram Protocol, "half-open" means that the firewall has detected traffic from one direction only.

Context-based Access Control (CBAC) measures both the total number of existing half-open sessions and the rate of session establishment attempts. Both TCP and UDP half-open sessions are included in the total number and rate measurements. Measurements are made once a minute.

When the rate of new connection attempts rises above a threshold (the **one-minute high** number), the software will delete half-open sessions as required to accommodate new connection attempts. The software will continue to delete half-open sessions as necessary, until the rate of new connection attempts drops below another threshold (the **one-minute low** number). The rate thresholds are measured as the number of new session connection attempts detected in the last one-minute sample period. (The rate is calculated as an exponentially decayed rate.)

The global value specified for this threshold applies to all TCP and UDP connections inspected by CBAC.

Examples

The following example causes the software to start deleting half-open sessions when more than 1000 session establishment attempts have been detected in the last minute, and to stop deleting half-open sessions when fewer than 950 session establishment attempts have been detected in the last minute:

```
ipv6 inspect one-minute high 1000
ipv6 inspect one-minute low 950
```

Related Commands

Command	Description
ipv6 inspect max-incomplete high	Defines the number of existing half-open sessions that will cause the software to start deleting half-open sessions.
ipv6 inspect max-incomplete low	Defines the number of existing half-open sessions that will cause the software to stop deleting half-open sessions.
ipv6 inspect one-minute high	Defines the rate of new unestablished sessions that will cause the software to start deleting half-open sessions.
ipv6 inspect tcp max-incomplete host	Specifies the threshold and blocking time values for TCP host-specific denial-of-service detection and prevention.

ipv6 inspect routing-header

To specify whether Context-based Access Control (CBAC) should inspect packets containing an IPv6 routing header, use the **ipv6 inspect routing-header** command. To drop packets containing an IPv6 routing header, use the no form of this command.

ipv6 inspect routing-header

no ipv6 inspect routing-header

Syntax Description

This command has no arguments or keywords.

Command Default

Packets containing IPv6 routing header are dropped.

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

An IPv6 source uses the routing header to list one or more intermediate nodes to be visited between the source and destination of the packet. The Cisco IOS firewall uses this header to retrieve the destination host address. Cisco IOS firewall will establish the appropriate inspection session based on the retrieved address from the routing header.

The originating node lists all intermediate nodes that the packet must traverse. The source and destination address pair in the IPv6 header identifies the hop between the originating node and the first intermediate node. Once the first intermediate node receives the packet, it looks for a routing header. If the routing header is present, the next intermediate node address is swapped with the destination address in the IPv6 header and the packet is forwarded to the next intermediate node. This sequence continues for each intermediate node listed in the routing until no more entries exist in the routing header. The last entry in the routing header is the final destination address.

Examples

The following example causes the software to inspect TCP sessions and UDP sessions:

```
ip inspect routing-header
```

Related Commands

Command	Description
ipv6 inspect alert-off	Disables CBAC alert messages.

Command	Description
ipv6 inspect audit trail	Turns on CBAC audit trail messages, which will be displayed on the console after each CBAC session close.
ipv6 inspect name	Applies a set of inspection rules to an interface.

ipv6 inspect tcp idle-time

To specify the TCP idle timeout (the length of time a TCP session will still be managed while there is no activity), use the **ipv6 inspect tcp idle-time** command in global configuration mode. To reset the timeout to the default of 3600 seconds (1 hour), use the **no** form of this command.

ipv6 inspect tcp idle-time *seconds*

no ipv6 inspect tcp idle-time

Syntax Description

seconds	Specifies the length of time, in seconds, for which a TCP session will still be managed while there is no activity. The default is 3600 seconds (1 hour).

Command Default

The default is 3600 seconds (1 hour)

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

When the software detects a valid TCP packet that is the first in a session, and if Context-based Access Control (CBAC) inspection is configured for the packet's protocol, 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 continue to manage state information for the session.

The global value specified for this timeout applies to all TCP sessions inspected by CBAC. This global value can be overridden for specific interfaces when you define a set of inspection rules with the **ipv6 inspect name** (global configuration) command.

Note This command does not affect any of the currently defined inspection rules that have explicitly defined timeouts. Sessions created based on these rules still inherit the explicitly defined timeout value. If you change the TCP idle timeout with this command, the new timeout will apply to any new inspection rules you define or to any existing inspection rules that do not have an explicitly defined timeout. That is, new sessions based on these rules (having no explicitly defined timeout) will inherit the global timeout value.

Examples

The following example sets the global TCP idle timeout to 1800 seconds (30 minutes):

```
ipv6 inspect tcp idle-time 1800
```

The following example sets the global TCP idle timeout back to the default of 3600 seconds (one hour):

```
no ipv6 inspect tcp idle-time
```

Related Commands

Command	Description
ipv6 inspect name	Defines a set of IPv6 inspection rules.

ipv6 inspect tcp max-incomplete host

To specify threshold and blocking time values for TCP host-specific denial-of-service detection and prevention, use the **ipv6 inspect tcp max-incomplete host**command in global configuration mode. To reset the threshold and blocking time to the default values, use the **no** form of this command.

ipv6 inspect tcp max-incomplete host *number* **block-time** *minutes*

no ipv6 inspect tcp max-incomplete host

Syntax Description

number	Specifies how many half-open TCP sessions with the same host destination address can exist at a time, before the software starts deleting half-open sessions to the host. Use a number from 1 to 250. The default is 50 half-open sessions. Value range is 1 through 4294967295
block-time	Specifies blocking of connection initiation to a host. Value range is 0 through 35791.
minutes	Specifies how long the software will continue to delete new connection requests to the host. The default is 0 minutes.

Command Default

The default is 50 half-open sessions and 0 minutes.

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

An unusually high number of half-open sessions with the same destination host address could indicate that a denial-of-service attack is being launched against the host. For TCP, "half-open" means that the session has not reached the established state.

Whenever the number of half-open sessions with the same destination host address rises above a threshold (the **max-incomplete host** number), the software will delete half-open sessions according to one of the following methods:

- If the **block-time** *minutes* timeout is 0 (the default):

The software will delete 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 will never exceed the threshold.

- If the **block-time** *minutes* timeout is greater than 0:

The software will delete all existing half-open sessions for the host, and then block all new connection requests to the host. The software will continue to block all new connection requests until the **block-time** expires.

The software also sends syslog messages whenever the **max-incomplete host** number 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 inspected by Context-based Access Control (CBAC).

Examples

The following example changes the **max-incomplete host** number to 40 half-open sessions, and changes the **block-time** timeout to 2 minutes (120 seconds):

```
ipv6 inspect tcp max-incomplete host 40 block-time 120
```

The following example resets the defaults (50 half-open sessions and 0 seconds):

```
no ipv6 inspect tcp max-incomplete host
```

Related Commands

Command	Description
ipv6 inspect max-incomplete high	Defines the number of existing half-open sessions that will cause the software to start deleting half-open sessions.
ipv6 inspect max-incomplete low	Defines the number of existing half-open sessions that will cause the software to stop deleting half-open sessions.
ipv6 inspect one-minute high	Defines the rate of new unestablished sessions that will cause the software to start deleting half-open sessions.
ipv6 inspect one-minute low	Defines the rate of new unestablished TCP sessions that will cause the software to stop deleting half-open sessions.

ipv6 inspect tcp synwait-time

To define how long the software will wait for a TCP session to reach the established state before dropping the session, use the **ipv6 inspect tcp synwait-time**command in global configuration mode. To reset the timeout to the default of 30 seconds, use the **no** form of this command.

ipv6 inspect tcp synwait-time *seconds*

no ipv6 inspect tcp synwait-time

Syntax Description

seconds	Specifies how long, in seconds, the software will wait for a TCP session to reach the established state before dropping the session . The default is 30 seconds. Value range is 1 through 2147483

Command Default

The default is 30 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

Use this command to define how long Cisco IOS software will wait for a TCP session to reach the established state before dropping the session. The session is considered to have reached the established state after the session's first SYN bit is detected.

The global value specified for this timeout applies to all TCP sessions inspected by Context-based Access Control (CBAC).

Examples

The following example changes the "synwait" timeout to 20 seconds:

```
ipv6 inspect tcp synwait-time 20
```

The following example changes the "synwait" timeout back to the default (30 seconds):

```
no ipv6 inspect tcp synwait-time
```

Related Commands

Command	Description
ipv6 inspect udp idle-time	Specifies the User Datagram Protocol idle timeout (the length of time for which a UDP "session" will still be managed while there is no activity).

ipv6 inspect udp idle-time

To specify the User Datagram Protocol idle timeout (the length of time for which a UDP "session" will still be managed while there is no activity), use the **ipv6 inspect udp idle-time** command in global configuration mode. To reset the timeout to the default of 30 seconds, use the **no** form of this command.

ipv6 inspect udp idle-time *seconds*

no ipv6 inspect udp idle-time

Syntax Description

seconds	Specifies the length of time a UDP "session" will still be managed while there is no activity . The default is 30 seconds. Value range is 1 through 2147483

Command Default

The default is 30 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

When the software detects a valid UDP packet, if Context-based Access Control (CBAC) inspection is configured for the packet’s protocol, the software establishes state information for a new UDP "session." Because UDP is a connectionless service, there are no actual sessions, so the software approximates sessions by examining the information in the packet and determining 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 a period of time defined by the UDP idle timeout, the software will not continue to manage state information for the session.

The global value specified for this timeout applies to all UDP sessions inspected by CBAC. This global value can be overridden for specific interfaces when you define a set of inspection rules with the **ipv6 inspect name**command.

Note This command does not affect any of the currently defined inspection rules that have explicitly defined timeouts. Sessions created based on these rules still inherit the explicitly defined timeout value. If you change the UDP idle timeout with this command, the new timeout will apply to any new inspection rules you define or to any existing inspection rules that do not have an explicitly defined timeout. That is, new sessions based on these rules (having no explicitly defined timeout) will inherit the global timeout value.

Examples

The following example sets the global UDP idle timeout to 120 seconds (2 minutes):

```
ipv6 inspect udp idle-time 120
```

The following example sets the global UDP idle timeout back to the default of 30 seconds:

```
no ipv6 inspect udp idle-time
```

ipv6 nd inspection

To apply the Neighbor Discovery Protocol (NDP) Inspection feature, use the **ipv6 nd inspection** command in interface configuration mode. To remove the NDP Inspection feature, use the **no** form of this command.

ipv6 nd inspection [**attach-policy** [*policy-name*] | **vlan** {**add** | **except** | **none** | **remove** | **all**} **vlan** *vlan-id*]]

no ipv6 nd inspection

Syntax Description

attach-policy	(Optional) Attaches an NDP Inspection policy.
policy-name	(Optional) The NDP Inspection policy name.
vlan	(Optional) Applies the ND Inspection feature to a VLAN on the interface.
add	(Optional) Adds a VLAN to be inspected.
except	(Optional) Inspects all VLANs except the one specified.
none	(Optional) Specifies that no VLANs are inspected.
remove	(Optional) Removes the specified VLAN from NDP inspection.
all	(Optional) Inspects NDP traffic from all VLANs on the port.
vlan-id	(Optional) A specific VLAN on the interface. More than one VLAN can be specified. The VLAN number that can be used is from 1 to 4094.

Command Default

All NDP messages are inspected. Secure Neighbor Discovery (SeND) options are ignored. Neighbors are probed based on the criteria defined in the Neighbor Tracking feature. Per-port IPv6 address limit enforcement is disabled. Layer 2 header source MAC address validations are disabled. Per-port rate limiting of the NDP messages in software is disabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.2(50)SY	This command was introduced.

Release	Modification
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SY.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The **ipv6 nd inspection** command applies the NDP Inspection feature on a specified interface. If you enable the optional **attach-policy** or **vlan** keywords, NDP traffic is inspected by policy or by VLAN. If no VLANs are specified, NDP traffic from all VLANs on the port is inspected (which is equivalent to using the **vlan all** keywords).

If no policy is specified in this command, the default criteria are as follows:

- All NDP messages are inspected.
- SeND options are ignored.
- Neighbors are probed based on the criteria defined in neighbor tracking feature.
- Per-port IPv6 address limit enforcement is disabled.
- Layer 2 header source MAC address validations are disabled.
- Per-port rate limiting of the NDP messages in software is disabled.

If a VLAN is specified, its parameter is either a single VLAN number from 1 to 4094 or a range of VLANs described by two VLAN numbers, the lesser one first, separated by a dash (for example, **vlan 1-100,200,300-400**). Do not enter any spaces between comma-separated VLAN parameters or in dash-specified ranges.

Examples

The following example enables NDP inspection on a specified interface:

```
Router(config-if)# ipv6 nd inspection
```

ipv6 nd inspection policy

To define the neighbor discovery (ND) inspection policy name and enter ND inspection policy configuration mode, use the **ipv6 nd inspection** command in ND inspection configuration mode. To remove the ND inspection policy, use the **no** form of this command.

ipv6 nd inspection policy *policy-name*

no ipv6 nd inspection policy *policy-name*

Syntax Description

policy-name	The ND inspection policy name.

Command Default

No ND inspection policies are configured.

Command Modes

ND inspection 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.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The **ipv6 nd inspection policy** command defines the ND inspection policy name and enters ND inspection policy configuration mode. Once you are in ND inspection policy configuration mode, you can use any of the following commands:

- **device-role**
- **drop-unsecure**
- **limit address-count**
- **sec-level minimum**
- **tracking**
- **trusted-port**
- **validate source-mac**

Examples

The following example defines an ND policy name as policy1:

```
Router(config)# ipv6 nd inspection policy policy1
Router(config-nd-inspection)#
```

Related Commands

Command	Description
device-role	Specifies the role of the device attached to the port.
drop-unsecure	Drops messages with no or invalid options or an invalid signature.
limit address-count	Limits the number of IPv6 addresses allowed to be used on the port.
sec-level minimum	Specifies the minimum security level parameter value when CGA options are used.
tracking	Overrides the default tracking policy on a port.
trusted-port	Configures a port to become a trusted port.
validate source-mac	Checks the source MAC address against the link-layer address.

ipv6 nd prefix framed-ipv6-prefix

To add the prefix in a received RADIUS framed IPv6 prefix attribute to the interface's neighbor discovery prefix queue, use the **ipv6 nd prefix framed-ipv6-prefix**command in interface configuration mode. To disable this feature, use the **no** form of this command.

ipv6 nd prefix framed-ipv6-prefix

no ipv6 nd prefix framed-ipv6-prefix

Syntax Description

This command has no arguments or keywords.

Command Default

Prefix is sent in the router advertisements (RAs).

Command Modes

Interface configuration

Command History

Release	Modification
12.3(14)T	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 12.2(33)SRA.

Usage Guidelines

Use the **ipv6 nd prefix framed-ipv6-prefix**command to add the prefix in a received RADIUS framed IPv6 prefix attribute to the interface's neighbor discovery prefix queue and include it in RAs sent on the interface's link. By default, the prefix is sent in RAs. If the prefix in the attribute should be used by other applications such as the Dynamic Host Configuration Protocol (DHCP) for IPv6 server, administrators can disable the default behavior with the **no** form of the command.

Examples

The following example adds the prefix in a received RADIUS framed IPv6 prefix attribute to the interface's neighbor discovery prefix queue:

```
ipv6 nd prefix framed-ipv6-prefix
```

ipv6 nd raguard attach-policy

To apply the IPv6 router advertisement (RA) guard feature on a specified interface, use the **ipv6 nd raguard attach-policy** command in interface configuration mode.

ipv6 nd raguard attach-policy [*policy-name* [**vlan** {**add**| **except**| **none**| **remove**| **all**} *vlan* [*vlan1, vlan2, vlan3...*]]]

Syntax Description

policy-name	(Optional) IPv6 RA guard policy name.
vlan	(Optional) Applies the IPv6 RA guard feature to a VLAN on the interface.
add	Adds a VLAN to be inspected.
except	All VLANs are inspected except the one specified.
none	No VLANs are inspected.
remove	Removes the specified VLAN from RA guard inspection.
all	ND traffic from all VLANs on the port is inspected.
vlan	(Optional) A specific VLAN on the interface. More than one VLAN can be specified (*vlan1*, *vlan2*, *vlan3*...). The range of available VLAN numbers is from 1 through 4094.

Command Default

An IPv6 RA guard policy is not configured.

Command Modes

Interface configuration (config-if)

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

If no policy is specified using the *policy-name* argument, the port device role is set to host and all inbound router traffic (for example, RA and redirect messages) is blocked.

If no VLAN is specified (which is equal to entering the **vlan all** keywords after the *policy-name* argument), RA guard traffic from all VLANs on the port is analyzed.

If specified, the VLAN parameter is either a single VLAN number from 1 through 4094 or a range of VLANs described by two VLAN numbers, the lesser one first, separated by a dash. Do not enter any spaces between comma-separated vlan parameters or in dash-specified ranges; for example, vlan 1-100,200,300-400.

Examples

In the following example, the IPv6 RA guard feature is applied on GigabitEthernet interface 0/0:

```
Device(config)# interface GigabitEthernet 0/0
Device(config-if)# ipv6 nd raguard attach-policy
```

ipv6 nd raguard policy

To define the router advertisement (RA) guard policy name and enter RA guard policy configuration mode, use the **ipv6 nd raguard policy** command in global configuration mode.

ipv6 nd raguardpolicy *policy-name*

Syntax Description

policy-name	IPv6 RA guard policy name.

Command Default

An RA guard policy is not configured.

Command Modes

Global configuration (config)#

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

Use the **ipv6 nd raguard policy** command to configure RA guard globally on a router. Once the device is in ND inspection policy configuration mode, you can use any of the following commands:

- **device-role**
- **drop-unsecure**
- **limit address-count**
- **sec-level minimum**
- **trusted-port**
- **validate source-mac**

After IPv6 RA guard is configured globally, you can use the **ipv6 nd raguard attach-policy** command to enable IPv6 RA guard on a specific interface.

Examples

The following example shows how to define the RA guard policy name as policy1 and place the device in policy configuration mode:

```
Device(config)# ipv6 nd raguard policy policy1
Device(config-ra-guard)#
```

Related Commands

Command	Description
device-role	Specifies the role of the device attached to the port.
drop-unsecure	Drops messages with no or invalid options or an invalid signature.
ipv6 nd raguard attach-policy	Applies the IPv6 RA guard feature on a specified interface.
limit address-count	Limits the number of IPv6 addresses allowed to be used on the port.
sec-level minimum	Specifies the minimum security level parameter value when CGA options are used.
trusted-port	Configures a port to become a trusted port.
validate source-mac	Checks the source MAC address against the link layer address.

ipv6 nd secured certificate-db

To configure the maximum number of entries in an IPv6 Secure Neighbor Discovery (SeND) certificate database, use the **ipv6 nd secured certificate-db**command in global configuration mode. To disable any maximum number of entries set for a SeND certificate database, use the **no** form of this command.

ipv6 nd secured certificate-db max-entries *max-entries-value*

no ipv6 nd secured certificate-db max-entries

Syntax Description

max-entries *max-entries-value*	Specifies the maximum number of entries in the certificate database. The range is from 1 to 1000.

Command Default

No SeND certificate database is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(24)T	This command was introduced.

Usage Guidelines

This command allows you to set up a maximum size for the certificate database (DB), to protect against denial of service (DoS) certificate flooding. When the limit is reached, new certificates are dropped.

The certificate DB is relevant on a router in host mode only, because it stores certificates received from routers.

Examples

The following example configures a SeND certificate database with a maximum number of 500 entries:

```
Router(config)# ipv6 nd secured certificate-db max-entries 500
```

Related Commands

Command	Description
ipv6 nd secured full-secure (global configuration)	Enables SeND security mode on a router.
ipv6 nd secured full-secure (interface configuration)	Enables SeND security mode on a specified interface.
ipv6 nd secured key-length	Configures SeND key-length options.
ipv6 nd secured timestamp	Configures the SeND time stamp.

Command	Description
ipv6 nd secured timestamp-db	Configures the maximum number of entries that did not reach the destination in a SeND time-stamp database.

ipv6 nd secured full-secure

To enable the secure mode for IPv6 Secure Neighbor Discovery (SeND) on a router, use the **ipv6 nd secured full-secure**command in global configuration mode. To disable SeND security mode, use the **no** form of this command.

ipv6 nd secured full-secure

no ipv6 nd secured full-secure

Syntax Description

This command has no arguments or keywords.

Command Default

Non-SeND neighbor discovery messages are accepted by the router.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(24)T	This command was introduced.

Usage Guidelines

The **ipv6 nd secured full-secure** command in global configuration mode allows you to configure the router to accept or reject non-SeND neighbor discovery messages. If this command is enabled, non-SeND messages are rejected by the specified router.

Examples

The following example enables SeND security mode on a router:

```
Router(config)# ipv6 nd secured full-secure
```

Related Commands

Command	Description
ipv6 nd secured full-secure (interface configuration)	Enables SeND security mode on a specified interface.

ipv6 nd secured full-secure (interface)

To enable the secure mode for IPv6 Secure Neighbor Discovery (SeND) on a specified interface, use the **ipv6 nd secured full-secure**command in interface configuration mode. To provide the co-existence mode for secure and nonsecure neighbor discovery messages on an interface, use the **no** form of this command.

ipv6 nd secured full-secure

no ipv6 nd secured full-secure

Syntax Description

This command has no arguments or keywords.

Command Default

Non-SeND messages are accepted by the interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(24)T	This command was introduced.

Usage Guidelines

The **ipv6 nd secured full-secure** command in interface configuration mode allows you to configure a specified interface to accept or reject non-SeND neighbor discovery messages. If this command is enabled, non-SeND messages are rejected by the interface. If this command is not enabled, secure and nonsecure neighbor discovery messages can coexist on the same interface.

Examples

The following example enables SeND security mode on an interface:

```
Router(config)# interface Ethernet0/0
Router(config-if)# ipv6 nd secured full-secure
```

Related Commands

Command	Description
ipv6 nd secured full-secure (global configuration)	Enables SeND security mode on a specified router.

ipv6 nd secured key-length

To configure IPv6 Secure Neighbor Discovery (SeND) key-length options, use the **ipv6 nd secured key-length**command in global configuration mode. To disable the key length, use the **no** form of this command.

ipv6 nd secured key-length [[**minimum**| **maximum**] *value*]

no ipv6 nd secured key-length

Syntax Description

minimum *value*	(Optional) Sets the minimum key-length value, which should be at least 384 bits. The range is from 384 to 2048 bits, and the default key-length value is 1024 bits.
maximum *value*	(Optional) Sets the maximum key-length value. The range is from 384 to 2048 bits, and the default key-length value is 1024 bits.

Command Default

The key length is 1024 bits.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(24)T	This command was introduced.

Usage Guidelines

When used by SeND, the key length is checked against the key-length value, as set in the **ipv6 nd secured key-length** command. When packets are received from a neighbor with a key length that is out of the configured boundaries, the packets are treated as unsecure.

Examples

The following example sets the minimum key-length value to 512 bits and the maximum value to 1024 bits:

```
Router(config)# ipv6 nd secured key-length minimum 512
Router(config)# ipv6 nd secured key-length maximum 1024
```

Related Commands

Command	Description
ipv6 nd secured certificate-db	Configures the maximum number of entries in a SeND certificate database.

Command	Description
ipv6 nd secured full-secure (global configuration)	Enables SeND security mode on a specified router.
ipv6 nd secured full-secure (interface configuration)	Enables SeND security mode on a specified interface.
ipv6 nd secured timestamp	Configures the SeND time stamp.
ipv6 nd secured timestamp-db	Configures the maximum number of entries in a SeND time-stamp database.

ipv6 nd secured sec-level

To configure the minimum security value that IPv6 Secure Neighbor Discovery (SeND) will accept from its peer, use the **ipv6 nd secured sec-level**command in global configuration mode. To disable the security level, use the **no** form of this command.

ipv6 nd secured sec-level [**minimum** *value*]

no ipv6 nd secured sec-level

Syntax Description

minimum *value*	(Optional) Sets the minimum security level, which is a value from 0 through 7. The default security level is 1.

Command Default

The default security level is 1.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(24)T	This command was introduced.

Usage Guidelines

The **ipv6 nd secured sec-level** command allows the user to configure the minimum security value the router will accept from its peer.

Examples

The following example sets the minimum security level to 2:

```
Router(config)# ipv6 nd secured sec-level 2
```

Related Commands

Command	Description
ipv6 nd secured certificate-db	Configures the maximum number of entries in a SeND certificate database.
ipv6 nd secured full-secure (global configuration)	Enables SeND security mode on a specified router.
ipv6 nd secured full-secure (interface configuration)	Enables SeND security mode on a specified interface.

Command	Description
ipv6 nd secured key-length	Configures SeND key-length options.
ipv6 nd secured timestamp	Configures the SeND time stamp.
ipv6 nd secured timestamp-db	Configures the maximum number of unreached entries in a SeND time-stamp database.

ipv6 nd secured timestamp

To configure the IPv6 Secure Neighbor Discovery (SeND) time stamp, use the **ipv6 nd secured timestamp**command in interface configuration mode. To return to the default settings, use the **no** form of this command.

ipv6 nd secured timestamp {**delta** *value*| **fuzz** *value*}

no ipv6 nd secured timestamp

Syntax Description

delta *value*	Specifies the maximum time difference accepted between the sender and the receiver. Default value is 300 seconds.
fuzz *value*	Specifies the maximum age of the message, when the delta is taken into consideration; that is, the amount of time, in seconds, that a packet can arrive after the delta value before being rejected. Default value is 1 second.

Command Default

Default time-stamp values are used.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(24)T	This command was introduced.

Usage Guidelines

The **ipv6 nd secured timestamp** command configures the amount of time the router waits before it accepts or rejects packets it has received.

Examples

The following example configures the SeND time stamp to be 600 seconds:

```
Router(config)# interface Ethernet0/0
Router(config-if)# ipv6 nd secured timestamp delta 600
```

Related Commands

Command	Description
ipv6 nd secured certificate-db	Configures the maximum number of entries in a SeND certificate database.

Command	Description
ipv6 nd secured full-secure (global configuration)	Enables SeND security mode on a specified router.
ipv6 nd secured full-secure (interface configuration)	Enables SeND security mode on a specified interface.
ipv6 nd secured key-length	Configures SeND key-length options.
ipv6 nd secured timestamp-db	Configures the maximum number of unreached entries in a SeND time-stamp database.

ipv6 nd secured timestamp-db

To configure the maximum number of unreached entries in an IPv6 Secure Neighbor Discovery (SeND) time-stamp database, use the **ipv6 nd secured timestamp-db**command in global configuration mode. To return to the default settings, use the **no** form of this command.

ipv6 nd secured timestamp-db max-entries *max-entries-value*

no ipv6 nd secured timestamp-db max-entries

Syntax Description

max-entries *max-entries-value*	Specifies the maximum number of entries in the certificate database. The range is from 1 to 1000.

Command Default

No time-stamp database is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(24)T	This command was introduced.

Examples

The following example configures the time-stamp database on a router:

```
Router(config)# ipv6 nd secured timestamp-db max-entries 345
```

Related Commands

Command	Description
ipv6 nd secured certificate-db	Configures the maximum number of entries in a SeND certificate database.
ipv6 nd secured full-secure (global configuration)	Enables SeND security mode on a specified router.
ipv6 nd secured full-secure (interface configuration)	Enables SeND security mode on a specified interface.
ipv6 nd secured key-length	Configures SeND key-length options.
ipv6 nd secured timestamp	Configures the SeND time stamp.

ipv6 nd secured trustanchor

To specify an IPv6 Secure Neighbor Discovery (SeND) trusted anchor on an interface, use the **ipv6 nd secured trustanchor**command in interface configuration mode. To remove a trusted anchor, use the **no** form of this command.

ipv6 nd secured trustanchor *trustanchor-name*

no ipv6 nd secured trustanchor *trustanchor-name*

Syntax Description

trustanchor-name	The name to be found in the certificate of the trustpoint.

Command Default

No trusted anchor is defined.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(24)T	This command was introduced.

Usage Guidelines

The **ipv6 nd secured trustanchor**command is used to select the certificate authority (CA) you want to authenticate. The trusted anchors configured by this command act as as references to the trustpoints configured.

A crypto Public Key Infrastructure (PKI) trustpoint can be a self-signed root CA or a subordinate CA. The *trustpoint-name*argument refers to the name to be found in the certificate of the trustpoint.

The **ipv6 nd secured trustanchor**and **ipv6 nd secured trustpoint**commands both generate an entry in the SeND configuration database that points to the trustpoint provided. More than one trustpoint can be provided for each command, and the same trustpoint can be used in both commands.

Examples

The following example specifies trusted anchor anchor1 on Ethernet interface 0/0:

```
Router(config)# interface Ethernet0/0
Router(config-if)# ipv6 nd secured trustanchor anchor1
```

Related Commands

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

Command	Description
ipv6 nd secured trustpoint	Specifies which trustpoint should be used for selecting the certificate to advertise.

ipv6 nd secured trustpoint

To specify which trustpoint should be used in the ipv6 Secure Neighbor Discovery (SeND) protocol for selecting the certificate to advertise, use the **ipv6 nd secured trustpoint**command in interface configuration mode. To disable the trustpoint, use the **no** form of this command.

ipv6 nd secured trustpoint *trustpoint-name*

no ipv6 nd secured trustpoint *trustpoint-name*

Syntax Description

trustpoint-name	The name to be found in the certificate of the trustpoint.

Command Default

SeND is not enabled on a specified interface.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.4(24)T	This command was introduced.

Usage Guidelines

The **ipv6 nd secured trustpoint** command enables SeND on an interface and specifies which trustpoint should be used. The trustpoint points to the Rivest, Shamir, and Adelman (RSA) key pair and the trusted anchor (which is the certificate authority [CA] signing your certificate).

The **ipv6 nd secured trustpoint** and **ipv6 nd secured trustanchor**commands both generate an entry in the SeND configuration database that points to the trustpoint provided. More than one trustpoint can be provided for each command, and the same trustpoint can be used in both commands. However, the trustpoint provided in the **ipv6 nd secured trustpoint** command must include a router certificate and the signing CA certificate. It may also include the certificate chain up to the root certificate provided by a CA that hosts (connected to the router) will trust.

The trustpoint provided in the **ipv6 nd secured trustanchor** command must only include a CA certificate.

Examples

The following example specifies trusted anchor anchor1 on Ethernet interface 0/0:

```
Router(config)# interface Ethernet0/0
Router(config-if)# ipv6 nd secured trustpoint trustpoint1
```

Related Commands

Command	Description
crypto pki trustpoint	Declares the trustpoint that your router should use.
ipv6 nd secured trustanchor	Specifies a trusted anchor on an interface.

ipv6 nd suppress-ra

Note Effective with Cisco IOS Release 12.4(2)T, the **ipv6 nd suppress-ra** command is replaced by the **ipv6 nd ra suppress** command. See the **ipv6 nd ra suppress** command for more information.

To suppress IPv6 router advertisement transmissions on a LAN interface, use the **ipv6 nd suppress-ra**command in interface configuration mode. To reenable the sending of IPv6 router advertisement transmissions on a LAN interface, use the **no** form of this command.

ipv6 nd suppress-ra

no ipv6 nd suppress-ra

Syntax Description

This command has no arguments or keywords.

Command Default

IPv6 router advertisements are automatically sent on Ethernet and FDDI interfaces if IPv6 unicast routing is enabled on the interfaces. IPv6 router advertisements are not sent on other types of interfaces.

Command Modes

Interface configuration

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.
12.4(2)T	This command was replaced by the **ipv6 nd ra suppress**command.

Usage Guidelines

Use the no **ipv6 nd suppress-ra**command to enable the sending of IPv6 router advertisement transmissions on non-LAN interface types (for example, serial or tunnel interfaces).

Examples

The following example suppresses IPv6 router advertisements on Ethernet interface 0/0:

```
Router(config)# interface ethernet 0/0
Router(config-if)# ipv6 nd suppress-ra
```

The following example enables the sending of IPv6 router advertisements on serial interface 0/1:

```
Router(config)# interface serial 0/1
Router(config-if)# no ipv6 nd suppress-ra
```

Related Commands

Command	Description
show ipv6 interface	Displays the usability status of interfaces configured for IPv6.

ipv6 neighbor binding

To change the defaults of neighbor binding entries in a binding table, use the **ipv6 neighbor binding** command in global configuration mode. To return the networking device to its default, use the **no** form of this command.

ipv6 neighbor binding [**reachable-lifetime** *value*| **stale-lifetime** *value*]

no ipv6 neighbor binding

Syntax Description

reachable-lifetime *value*	(Optional) The maximum time, in seconds, an entry is considered reachable without getting a proof of reachability (direct reachability through tracking, or indirect reachability through Neighbor Discovery protocol [NDP] inspection). After that, the entry is moved to stale. The range is from 1 through 3600 seconds, and the default is 300 seconds (or 5 minutes).
stale-lifetime *value*	(Optional) The maximum time, in seconds, a stale entry is kept in the binding table before the entry is deleted or proof is received that the entry is reachable. • The default is 24 hours (86,400 seconds).
down-lifetime *value*	(Optional) The maximum time, in seconds, an entry learned from a down interface is kept in the binding table before the entry is deleted or proof is received that the entry is reachable. • The default is 24 hours (86,400 seconds).

Command Default

Reachable lifetime: 300 seconds Stale lifetime: 24 hours Down lifetime: 24 hours

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(50)SY	This command was introduced.

Usage Guidelines

Use the **ipv6 neighbor binding** command to configure information about individual entries in a binding table. If no keywords or arguments are configured, the IPv6 neighbor binding entry defaults are used.

If the **tracking reachable-lifetime** command is configured, it overrides **ipv6 neighbor binding reachable-lifetime** configuration. If the **tracking stale-lifetime** command is configured, it overrides **ipv6 neighbor binding stale-lifetime** configuration.

Examples

The following example shows how to change the reachable lifetime for binding entries to 100 seconds:

```
Router(config)# ipv6 neighbor binding reachable-entries 100
```

Related Commands

Command	Description
ipv6 neighbor tracking	Tracks entries in the binding table.
tracking	Overrides the default tracking policy on a port.

ipv6 neighbor binding down-lifetime

To change the default of a neighbor binding entry's down lifetime, use the **ipv6 neighbor binding down-lifetime**command in global configuration mode. To return the networking device to its default, use the **no** form of this command.

ipv6 neighbor binding down-lifetime {*value*| **infinite**}

no ipv6 neighbor binding down-lifetime

Syntax Description

value	The maximum time, in minutes, an entry learned from a down interface is kept in the table before deletion. The range is from 1 to 3600 minutes. • The default is 24 hours (86,400 seconds).
infinite	Keeps an entry in the binding table for an infinite amount of time.

Command Default

A neighbor binding entry is down for 24 hours before it is deleted from the binding table.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(50)SY	This command was introduced.

Usage Guidelines

Use the **ipv6 neighbor binding down-lifetime**command to change the amount of time a neighbor binding is down before that binding is removed from the binding table.

Examples

The following example shows how to change a binding entry's down lifetime to 2 minutes before it is deleted from the binding table:

```
Router(config)# ipv6 neighbor binding down-lifetime 2
```

Related Commands

Command	Description
ipv6 neighbor tracking	Tracks entries in the binding table.

ipv6 neighbor binding logging

To enable the logging of binding table main events, use the **ipv6 neighbor binding logging** command in global configuration mode. To disable this function, use the **no** form of this command.

ipv6 neighbor binding logging

no ipv6 neighbor binding logging

Syntax Description

This command has no arguments or keywords.

Command Default

Binding table events are not logged.

Command Modes

Global configuration (config)

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 **ipv6 neighbor binding logging** command enables the logging of the following binding table events:

- An entry is inserted into the binding table.
- A binding table entry was updated.
- A binding table entry was deleted from the binding table.
- A binding table entry was not inserted into the binding table, possibly because of a collision with an existing entry, or because the maximum number of entries has been reached.

Examples

The following example shows how to enable binding table event logging:

```
Router(config)# ipv6 neighbor binding logging
```

Related Commands

Command	Description

Command	Description
ipv6 neighbor binding vlan	Adds a static entry to the binding table database.
ipv6 neighbor tracking	Tracks entries in the binding table.
ipv6 snooping logging packet drop	Configures IPv6 snooping security logging.

ipv6 neighbor binding max-entries

To specify the maximum number of entries that are allowed to be inserted in the binding table cache, use the **ipv6 neighbor binding max-entries** command in global configuration mode. To return to the default, use the **no** form of this command.

ipv6 neighbor binding max-entries *entries* [**vlan-limit** *number*| **interface-limit** *number*| **mac-limit** *number*]

no ipv6 neighbor binding max-entries *entries* [**vlan-limit**| **mac-limit**]

Syntax Description

entries	Number of entries that can be inserted into the cache.
vlan-limit *number*	(Optional) Specifies a neighbor binding limit per number of VLANs.
interface-limit *number*	(Optional) Specifies a neighbor binding limit per interface.
mac-limit *number*	(Optional) Specifies a neighbor binding limit per number of Media Access Control (MAC) addresses.

Command Default

This command is disabled.

Command Modes

Global configuration (config)

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 **ipv6 neighbor binding max-entries** command is used to control the content of the binding table. This command specifies the maximum number of entries that are allowed to be inserted in the binding table cache. Once this limit is reached, new entries are refused, and the Neighbor Discovery Protocol (NDP) traffic source with the new entry is dropped.

If the maximum number of entries specified is lower than the current number of entries in the database, no entries are cleared, and the new threshold is reached after normal cache attrition.

The maximum number of entries can be set globally per VLAN, interface, or MAC addresses.

Examples

The following example shows how to specify globally the maximum number of entries inserted into the cache:

```
Router(config)# ipv6 neighbor binding max-entries 100
```

Related Commands

Command	Description
ipv6 neighbor binding vlan	Adds a static entry to the binding table database.
ipv6 neighbor tracking	Tracks entries in the binding table.

ipv6 neighbor binding stale-lifetime

To set the length of time a stale entry is kept in the binding table, use the **ipv6 neighbor binding stale-lifetime**command in global configuration mode. To return to the default setting, use the **no** form of this command.

ipv6 neighbor binding stale-lifetime {*value*| **infinite**}

no ipv6 neighbor binding

Syntax Description

value	The maximum time, in minutes, a stale entry is kept in the table before it is deleted or some proof of reachability is seen. The range is from 1 to 3600 minutes, and the default is 24 hours (or 1440 minutes).
infinite	Keeps an entry in the binding table for an infinite amount of time.

Command Default

Stale lifetime: 1440 minutes (24 hours)

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(50)SY	This command was introduced.

Usage Guidelines

Use the **ipv6 neighbor binding stale-lifetime**command to configure the length of time a stale entry is kept in the binding table before it is removed.

Examples

The following example shows how to change the stale lifetime for a binding entry to 720 minutes (or 12 hours):

```
Router(config)# ipv6 neighbor binding stale lifetime 720
```

Related Commands

Command	Description
ipv6 neighbor binding	Changes the defaults of neighbor binding entries in a binding table.

ipv6 neighbor binding vlan

To add a static entry to the binding table database, use the **ipv6 neighbor binding vlan** command in global configuration mode. To remove the static entry, use the **no** form of this command.

ipv6 neighbor binding vlan *vlan-id* {**interface** *type number*| *ipv6-address*| *mac-address*} [**tracking** [**disable**| **enable**| **retry-interval** *value*]| **reachable-lifetime** *value*]

no ipv6 neighbor binding vlan *vlan-id*

Syntax Description

vlan-id	ID of the specified VLAN.
interface *type number*	Adds static entries by the specified interface type and number.
ipv6-address	IPv6 address of the static entry.
mac-address	Media Access Control (MAC) address of the static entry.
tracking	(Optional) Verifies a static entry's reachability directly.
disable	(Optional) Disables tracking for a particular static entry.
enable	(Optional) Enables tracking for a particular static entry.
retry-interval *value*	(Optional) Verifies a static entry's reachability, in seconds, at the configured interval. The range is from 1 to 3600, and the default is 300.
reachable-lifetime *value*	(Optional) Specifies the maximum time, in seconds, an entry is considered reachable without getting a proof of reachability (direct reachability through tracking, or indirect reachability through Neighbor Discovery Protocol [NDP] inspection). After that, the entry is moved to stale. The range is from 1 to 3600 seconds, and the default is 300 seconds.

Command Default

Retry interval: 300 seconds

Reachable lifetime: 300 seconds

Command Modes

Global configuration (config)

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 **ipv6 neighbor binding vlan** command is used to control the content of the binding table. Use this command to add a static entry in the binding table database. The binding table manager is responsible for aging out entries and verifying their reachability directly by probing them (if the **tracking** keyword is enabled). Use of the **tracking** keyword overrides any general behavior provided globally by the **ipv6 neighbor tracking** command for this static entry. The **disable** keyword disables tracking for this static entry. The **stale-lifetime** keyword defines the maximum time the entry will be kept once it is determined to be not reachable (or stale).

Examples

The following example shows how to change the reachable lifetime for binding entries to 100 seconds:

```
Router(config)# ipv6 neighbor binding vlan reachable-lifetime 100
```

Related Commands

Command	Description
ipv6 neighbor binding max-entries	Specifies the maximum number of entries that are allowed to be inserted in the cache.
ipv6 neighbor tracking	Tracks entries in the binding table.

ipv6 neighbor tracking

To track entries in the binding table, use the **ipv6 neighbor tracking** command in global configuration mode. To disable entry tracking, use the **no** form of this command.

ipv6 neighbor tracking [**retry-interval** *value*]

no ipv6 neighbor tracking [**retry-interval** *value*]

Syntax Description

retry-interval *value*	(Optional) Verifies a static entry's reachability at the configured interval time, in seconds, between two probings. The range is from 1 to 3600, and the default is 300.

Command Default

Entries in the binding table are not tracked.

Command Modes

Global configuration (config)

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 **ipv6 neighbor tracking** command enables the tracking of entries in the binding table. Entry reachability is tested at every interval configured by the optional **retry-interval** keyword (or every 300 seconds, which is the default retry interval) using the neighbor unreachability detection (NUD) mechanism used for directly tracking neighbor reachability.

Reachability can also be established indirectly by using Neighbor Discovery Protocol (NDP) inspection up to the VERIFY_MAX_RETRIES value (the default is 10 seconds). When there is no response, entries are considered stale and are deleted after the stale lifetime value is reached (the default is 1440 minutes).

When the **ipv6 neighbor tracking** command is disabled, entries are considered stale after the reachable lifetime value is met (the default is 300 seconds) and deleted after the stale lifetime value is met.

To change the default values of neighbor binding entries in a binding table, use the **ipv6 neighbor binding** command.

Examples

The following example shows how to track entries in a binding table:

```
Router(config)# ipv6 neighbor tracking
```

Related Commands

Command	Description
ipv6 neighbor binding	Changes the defaults of neighbor binding entries in a binding table.

ipv6 port-map

To establish port-to-application mapping (PAM) for the system, use the **ipv6 port-map** command in global configuration mode. To delete user-defined PAM entries, use the **no** form of this command.

ipv6 port-map *application* **port** *port-num* [**list** *acl-name*]

no ipv6 port-map *application* **port** *port-num* [**list** *acl-name*]

Syntax Description

application	Specifies the predefined application that requires port mapping.
port *port-num*	Specifies a port number. The range is from 1 to 65535.
list *acl-name*	(Optional) Specifies the name of the IPv6 access list (ACL) associated with the port mapping.

Command Default

None

Command Modes

Global configuration

Command History

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

Usage Guidelines

The **ipv6 port-map** command associates TCP or User Datagram Protocol (UDP) port numbers with applications or services, establishing a table of default port mapping information at the firewall. This information is used to support network environments that run services using ports that are different from the registered or well-known ports associated with a service or application.

The port mapping information in the PAM table is of one of three types:

- System-defined
- User-defined
- Host-specific

System-Defined Port Mapping

Initially, PAM creates a set of system-defined entries in the mapping table using well-known or registered port mapping information set up during the system start-up. The Cisco IOS Firewall Context-Based Access Control feature requires the system-defined mapping information to function properly. System-defined mapping information cannot be deleted or changed; that is, you cannot map HTTP services to port 21 (FTP) or FTP services to port 80 (HTTP).

The table below lists the default system-defined services and applications in the PAM table.

Table 16: System-Defined Port Mapping

Application Name	Well-Known or Registered Port Number	Protocol Description
cuseeme	7648	CU-SeeMe Protocol
exec	512	Remote Process Execution
ftp	21	File Transfer Protocol (control port)
h323	1720	H.323 Protocol (for example, MS NetMeeting, Intel Video Phone)
http	80	Hypertext Transfer Protocol
login	513	Remote login
msrpc	135	Microsoft Remote Procedure Call
netshow	1755	Microsoft NetShow
real-audio-video	7070	RealAudio and RealVideo
sccp	2000	Skinny Client Control Protocol (SCCP)
smtp	25	Simple Mail Transfer Protocol (SMTP)
sql-net	1521	SQL-NET
streamworks	1558	StreamWorks Protocol
sunrpc	111	SUN Remote Procedure Call
tftp	69	Trivial File Transfer Protocol
vdolive	7000	VDOLive Protocol

Note You can override the system-defined entries for a specific host or subnet using the **list** keyword in the **ipv6 port-map** command.

User-Defined Port Mapping

Network applications that use non-standard ports require user-defined entries in the mapping table. Use the **ipv6 port-map** command to create default user-defined entries in the PAM table.

To map a range of port numbers with a service or application, you must create a separate entry for each port number.

Note If you try to map an application to a system-defined port, a message appears warning you of a mapping conflict.

Use the **no** form of the **ipv6 port-map** command to delete user-defined entries from the PAM table.

To overwrite an existing user-defined port mapping, use the **ipv6 port-map** command to associate another service or application with the specific port.

Host-Specific Port Mapping

User-defined entries in the mapping table can include host-specific mapping information, which establishes port mapping information for specific hosts or subnets. In some environments, it might be necessary to override the default port mapping information for a specific host or subnet, including a system-defined default port mapping information. Use the **list** keyword for the **ipv6 port-map** command to specify an ACL for a host or subnet that uses PAM.

Note If the host-specific port mapping information is the same as existing system-defined or user-defined default entries, host-specific port changes have no effect.

Examples

The following user-defined port-mapping configuration map port 8080 to the HTTP application:

```
ipv6 port-map http port 8080
```

Host-specific port-mapping configuration maps port 2121 to the FTP application from a particular set of host. First, the user needs to create a permit IPv6 access list for the allowed host(s). In the following example, packets from the hosts in the 2001:0DB8:1:7 subset destined for port 2121 will be mapped to the FTP application:

```
Router(config)# ipv6 access-list ftp-host
Router(config-ipv6-acl)# permit 2001:0DB8:1:7::/64 any
```

The port-map configuration is then configured as follows:

```
Router(config)# ipv6 port-map ftp port 2121 list ftp-host
```

Related Commands

Command	Description
show ipv6 port-map	Displays IPv6 port-mapping information.

ipv6 routing-enforcement-header loose

To provide backward compatibility with legacy IPv6 inspection, use the ipv6 routing-enforcement-header loose command in parameter map type inspect configuration mode. To disable this feature, use the **no** form of this command.

ipv6 routing-enforcement-header loose

no ipv6 routing-enforcement-header loose

Syntax Description

This command has no arguments or keywords.

Command Default

Backward compatibility is not provided.

Command Modes

parameter map type inspect configuration mode (config-profile)

Command History

Release	Modification
15.1(2)T	This command was introduced.

Usage Guidelines

The **ipv6 routing-enforcement-header loose** command provides backward compatibility with legacy IPv6 inspection. Enabling this command ensures that the firewall will not drop IPv6 traffic with routing headers. The default firewall behavior is to drop all IPv6 traffic without a routing header.

Examples

The following example enables backward compatibility with legacy IPv6 inspection on an inspect type parameter map named v6-param-map:

```
Router(config)# parameter-map type inspect v6-param-map
Router (config-profile)# ipv6 routing-header-enforcement loose
```

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.

ipv6 snooping logging packet drop

To enable the logging of dropped packets by the IPv6 first-hop security feature, use the **ipv6 snooping logging packet drop**command in global configuration mode. To disable the logging of dropped packets by the IPv6 first-hop security feature, use the **no** form of this command.

ipv6 snooping logging packet drop

no ipv6 snooping logging packet drop

Syntax Description

This command has no arguments or keywords.

Command Default

Snooping security logging is not enabled.

Command Modes

Global configuration (config)#

Command History

Release	Modification
12.2(50)SY	This command was introduced.

Usage Guidelines

Use the **ipv6 snooping logging packet drop**command to log packets that are dropped when they are received on an unauthorized port. For example, this command will log RA packets that are dropped because of the RA guard feature.

Related Commands

Command	Description
ipv6 neighbor binding logging	Enables the logging of binding table main events.

ipv6 tacacs source-interface

To specify an interface to use for the source address in TACACS packets, use the **ipv6 tacacs source-interface**command in global configuration mode. To remove the specified interface from the configuration, use the **no** form of this command.

ipv6 tacacs source-interface *interface*

no ipv6 tacacs source-interface *interface*

Syntax Description

interface	Interface to be used for the source address in TACACS packets.

Command Default

No interface is specified.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

The **ipv6 tacacs source-interface**command specifies an interface to use for the source address in TACACS packets.

Examples

The following example shows how to configure the Gigabit Ethernet interface to be used as the source address in TACACS packets:

```
Router(config)# ipv6 tacacs source-interface GigabitEthernet 0/0/0
```

Related Commands

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

ipv6 virtual-reassembly

To enable Virtual Fragment Reassembly (VFR) on an interface, use the **ipv6 virtual-reassembly** command in global configuration mode. To remove VFR configuration, use the **no** form of this command.

ipv6 virtual-reassembly [**in**| **out**] [**max-reassemblies** *maxreassemblies*] [**max-fragments** *max-fragments*] [**timeout** *seconds*] **[drop-fragments]**

no ipv6 virtual-reassembly [**in**| **out**] [**max-reassemblies** *maxreassemblies*] [**max-fragments** *max-fragments*] [**timeout** *seconds*] **[drop-fragments]**

Syntax Description

in	(Optional) Enables VFR on the ingress direction of the interface.
out	(Optional) Enables VFR on the egress direction of the interface.
max-reassemblies *maxreassemblies*	(Optional) Sets the maximum number of concurrent reassemblies (fragment sets) that the Cisco IOS software can handle at a time. The default value is 64.
max-fragments *max-fragments*	(Optional) Sets the maximum number of fragments allowed per datagram (fragment set). The default is 16.
timeout *seconds*	(Optional) Sets the timeout value of the fragment state. The default timeout value is 2 seconds. If a datagram does not receive all its fragments within 2 seconds, all of the fragments received previously will be dropped and the fragment state will be deleted.
drop-fragments	(Optional) Turns the drop fragments feature on or off.

Command Default

Max-reassemblies = 64 Fragments = 16 If neither the **in** or **out** keyword is specified, VFR is enabled on the ingress direction of the interface only.**drop-fragments** keyword is not enabled.

Command Modes

Interface configuration (config-if)

Command History

Release	Modification
12.3(7)T	This command was introduced.

Release	Modification
15.1(1)T	The **in** and **out** keywords were added. • The **out** keyword must be used to configure or disable the egress direction of the interface.
Cisco IOS XE Release 3.4S	The **drop-fragments** keyword was added.

Usage Guidelines

When the **ipv6 virtual-reassembly** command is configured on an interface without using one of the command keywords, VFR is enabled on the ingress direction of the interface only. In Cisco IOS XE Release 3.4S, all VFR-related alert messages are suppressed by default.

Maximum Number of Reassemblies

Whenever the maximum number of 256 reassemblies (fragment sets) is crossed, all the fragments in the forthcoming fragment set will be dropped and an alert message VFR-4-FRAG_TABLE_OVERFLOW will be logged to the syslog server.

Maximum Number of Fragments per Fragment Set

If a datagram being reassembled receives more than eight fragments then, tall fragments will be dropped and an alert message VFR-4-TOO_MANY_FRAGMENTS will be logged to the syslog server.

Explicit Removal of Egress Configuration

As of the Cisco IOS 15.1(1)T release, the **no ipv6 virtual-reassembly** command, when used without keywords, removes ingress configuration only. To remove egress interface configuration, you must enter the **out** keyword.

Examples

The following example configures the ingress direction on the interface. It sets the maximum number of reassemblies to 32, maximum fragments to 4, and the timeout to 7 seconds:

```
Router(config)# interface Ethernet 0/0
Router(config-if)# ipv6 virtual-reassembly max-reassemblies 32 max-fragments 4 timeout 7
```

The following example enables the VFR on the ingress direction of the interface. Note that even if the **in** keyword is not used, the configuration default is to configure the ingress direction on the interface:

```
Router(config)# interface Ethernet 0/0
Router(config-if)# ipv6 virtual-reassembly
Router(config-if)# end
Router# show run interface Ethernet 0/0
interface Ethernet0/0
no ip address
ipv6 virtual-reassembly in
```

The following example enables egress configuration on the interface. Note that the **out** keyword must be used to enable and disable egress configuration on the interface:

```
Router(config)# interface Ethernet 0/0
Router(config-if)# ipv6 virtual-reassembly out
Router(config-if)# end
Router# show run interface Ethernet 0/0
interface Ethernet0/0
no ip address
ipv6 virtual-reassembly out
end
```

The following example disables egress configuration on the interface:

```
Router(config)# interface Ethernet 0/0
Router(config-if)# no
 ipv6 virtual-reassembly out
Router(config-if)# end
```

ipv6 virtual-reassembly drop-fragments

To drop all fragments on an interface, use the **ipv6 virtual-reassembly drop-fragments** command in global configuration mode. Use the **no** form of this command to remove the packet-dropping behavior.

ipv6 virtual-reassembly drop-fragments

no ipv6 virtual-reassembly drop-fragments

Syntax Description

This command has no arguments or keywords.

Command Default

Fragments on an interface are not dropped.

Command Modes

Global configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Examples

The following example causes all fragments on an interface to be dropped:

```
ipv6 virtual-reassembly drop-fragments
```

isakmp authorization list

To configure an Internet Key Exchange (IKE) shared secret using the authentication, authorization, and accounting (AAA) server in an Internet Security Association and Key Management Protocol (ISAKMP) profile, use the **isakmp authorization list**command in ISAKMP profile configuration mode. To disable the shared secret, use the **no** form of this command.

isakmp authorization list *list-name*

no isakmp authorization list *list-name*

Syntax Description

list-name	AAA authorization list used for configuration mode attributes or preshared keys for aggresive mode.

Command Default

No default behaviors or values

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

This command allows you to retrieve a shared secret from an AAA server.

Examples

The following example shows that an IKE shared secret is configured using an AAA server on a router:

```
crypto isakmp profile vpnprofile
 isakmp authorization list ikessaaalist
```

Related Commands

Command	Description
aaa authorization	Sets parameters that restrict user access to a network.

issuer-name

To specify the distinguished name (DN) as the certification authority (CA) issuer name for the certificate server, use the **issuer-name** command in certificate server configuration mode. To clear the issuer name and return to the default, use the **no** form of this command.

issuer-name *DN-string*

no issuer-name *DN-string*

Syntax Description

DN-string	Name of the DN string.

Command Default

If the issuer name is not configured, the DN string is the certificate server name.

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.

The DN-string value cannot be changed after the certificate server generates its signed certificate.

Examples

The following example shows how to define an issuer name for the certificate server “mycertserver”:

```
Router(config)# ip http server
Router(config)# crypto pki server mycertserver
Router(cs-server)# database level minimal
Router(cs-server)# database url nvram:
Router(cs-server)# issuer-name CN = ipsec_cs,L = My Town,C = US
```

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.

Command	Description
hash (cs-server)	Specifies the cryptographic hash function the Cisco IOS certificate server uses to sign certificates issued by the CA.
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.
shutdown (cs-server)	Allows a CS to be disabled without removing the configuration.

ivrf

To specify a user-defined VPN routing and forwarding (VRF) or use the global VRF, use the **ivrf** command in IKEv2 profile configuration mode. To delete the VRF specification, use the **no** form of this command.

ivrf *name*

no ivrf

Syntax Description

name	VRF name.

Command Default

VRF 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.

Usage Guidelines

Use this command to specify a user-defined VRF or a global VRF, which should be attached to static and dynamic crypto maps. The inside VRF (IVRF) for a tunnel interface should be configured on the tunnel interface. IVRF specifies the VRF for cleartext packets. The default value for IVRF is Forward VRF (FVRF).

Examples

The following example shows how to specify IVRF:

```
Router(config)# crypto ikev2 profile profile1
Router(config-ikev2-profile)# ivrf vrf1
```

Related Commands

Command	Description
crypto ikev2 profile	Defines an IKEv2 profile.
show crypto ikev2 profile	Displays the IKEv2 profile.

K through L

keepalive (isakmp profile)

To allow the gateway to send dead peer detection (DPD) messages to the peer, use the **keepalive** command in Internet Security Association Key Management Protocol (ISAKMP) profile configuration mode. To return to the default, use the **no** form of this command.

keepalive *seconds* **retry** *retry-seconds*

no keepalive *seconds* **retry** *retry-seconds*

Syntax Description

seconds	Number of seconds between DPD messages. The range is from 10 to 3600 seconds.
retry *retry-seconds*	Number of seconds between retries if DPD message fails. The range is from 2 to 60 seconds.

Command Default

If this command is not configured, a DPD message is not sent to the client.

Command Modes

ISAKMP profile configuration (config-isa-prof)

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.

Usage Guidelines

Use this command to enable the gateway (instead of the client) to send DPD messages to the client. Internet Key Exchange (IKE) DPD is a new keepalive scheme that sends messages to let the router know that the client is still connected.

Examples

The following example shows that DPD messages have been configured to be sent every 60 seconds and every 5 seconds between retries if the peer does not respond:

```
crypto isakmp profile vpnprofile
 keepalive 60 retry 5
```

kerberos clients mandatory

To cause the **rsh**, **rcp**, **rlogin**, and **telnet** commands to fail if they cannot negotiate the Kerberos protocol with the remote server, use the **kerberos clients mandatory** command in global configuration mode. To make Kerberos optional, use the **no** form of this command.

kerberos clients mandatory

no kerberos clients mandatory

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration

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.

Usage Guidelines

If this command is not configured and the user has Kerberos credentials stored locally, the **rsh**, **rcp**, **rlogin**, and **telnet** commands attempt to negotiate the Kerberos protocol with the remote server and will use the non-Kerberized protocols if unsuccessful.

If this command is not configured and the user has no Kerberos credentials, the standard protocols for **rcp** and **rsh** are used to negotiate.

Examples

The following example causes the **rsh**, **rcp**, **rlogin**, and **telnet** commands to fail if they cannot negotiate the Kerberos protocol with the remote server:

```
kerberos clients mandatory
```

Related Commands

Command	Description
connect	Logs in to a host that supports Telnet, rlogin, or LAT.

Command	Description
kerberos credentials forward	Forces all network application clients on the router to forward the Kerberos credentials of users upon successful Kerberos authentication.
rlogin	Logs in to a UNIX host using rlogin.
rsh	Executes a command remotely on a remote rsh host.
telnet	Logs in to a host that supports Telnet.

kerberos credentials forward

To force all network application clients on the router to forward users' Kerberos credentials upon successful Kerberos authentication, use the **kerberos credentials forward** command inglobal configuration mode. To turn off forwarding of Kerberos credentials, use the **no** form of this command.

kerberos credentials forward

no kerberos credentials forward

Syntax Description

This command has no arguments or keywords.

Command Default

Disabled

Command Modes

Global configuration

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.

Usage Guidelines

Enable credentials forwarding to have users' ticket granting tickets (TGTs) forwarded to the host on which they authenticate. In this way, users can connect to multiple hosts in the Kerberos realm without running the KINIT program each time they need to get a TGT.

Examples

The following example forces all network application clients on the router to forward users' Kerberos credentials upon successful Kerberos authentication:

```
kerberos credentials forward
```

Related Commands

Command	Description
connect	Logs in to a host that supports Telnet, rlogin, or LAT.
rlogin	Logs in to a UNIX host using rlogin.
rsh	Executes a command remotely on a remote rsh host.

Command	Description
telnet	Logs in to a host that supports Telnet.

kerberos instance map

To map Kerberos instances to Cisco IOS privilege levels, use the **kerberos instance map** command in global configuration mode. To remove a Kerberos instance map, use the **no** form of this command.

kerberos instance map *instance privilege-level*

no kerberos instance map *instance*

Syntax Description

instance	Name of a Kerberos instance.
privilege-level	The privilege level at which a user is set if the user's Kerberos principal contains the matching Kerberos instance. You can specify up to 16 privilege levels, using numbers 0 through 15. Level 1 is normal EXEC-mode user privileges.

Command Default

Privilege level 1

Command Modes

Global configuration

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.

Usage Guidelines

Use this command to create user instances with access to administrative commands.

Examples

The following example sets the privilege level to 15 for authenticated Kerberos users with the *admin* instance in Kerberos realm:

```
kerberos instance map admin 15
```

Related Commands

Command	Description
aaa authorization	Sets parameters that restrict user access to a network.

kerberos local-realm

To specify the Kerberos realm in which the router is located, use the **kerberos local-realm** command in global configuration mode. To remove the specified Kerberos realm from this router, use the **no** form of this command.

kerberos local-realm *kerberos-realm*

no kerberos local-realm

Syntax Description

kerberos-realm	The name of the default Kerberos realm. A Kerberos realm consists of users, hosts, and network services that are registered to a Kerberos server. The Kerberos realm must be in uppercase characters .

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

The router can be located in more than one realm at a time. However, there can only be one instance of Kerberos local-realm. The realm specified with this command is the default realm.

Examples

The following example specify the Kerberos realm in which the router is located as EXAMPLE.COM:

```
kerberos local-realm EXAMPLE.COM
```

Related Commands

Command	Description
kerberos preauth	Specifies a preauthentication method to use to communicate with the KDC.

Command	Description
kerberos realm	Maps a host name or DNS domain to a Kerberos realm.
kerberos server	Specifies the location of the Kerberos server for a given Kerberos realm.
kerberos srvtab entry	Specifies a krb5 SRVTAB entry.
kerberos srvtab remote	Retrieves a SRVTAB file from a remote host and automatically generate a Kerberos SRVTAB entry configuration.

kerberos password

To set the password shared with the key distribution center, use the **kerberos password**command in global configuration mode. To disable the configured password, use the **no** form of this command.

kerberos password [*text-string*]

no kerberos password [*text-string*]

Syntax Description

text-string	(Optional) The password string.

Command Default

The password is not set.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
12.2(33)SRC	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRB.
12.2(33)SXI	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

Kerberos is a network authentication protocol that allows a secured way of node communication in a nonsecure network.

Examples

The following example shows how to set the password:

```
Router# configure terminal
Router(config)# kerberos password treas123
```

Related Commands

Command	Description
kerberos clients mandatory	Specifies the default direction of filters from RADIUS.

Command	Description
kerberos credentials forward	Forces all network application clients on the router to forward the Kerberos credentials of users upon successful Kerberos authentication.

kerberos preauth

To specify a preauthentication method to use to communicate with the key distribution center (KDC), use the **kerberos preauth**command in global configuration mode. To disable Kerberos preauthentication, use the **no** form of this command.

kerberos preauth [**encrypted-unix-timestamp**| **encrypted-kerberos-timestamp**| **none**]

no kerberos preauth

Syntax Description

encrypted-unix-timestamp	(Optional) Use an encrypted UNIX timestamp as a quick authentication method when communicating with the KDC.
encrypted-kerberos-timestamp	(Optional) Use the RFC1510 kerberos timestamp as a quick authentication method when communicating with the KDC.
none	(Optional) Do not use Kerberos preauthentication.

Command Default

Disabled

Command Modes

Global configuration

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.

Usage Guidelines

It is more secure to use a preauthentication for communications with the KDC. However, communication with the KDC will fail if the KDC does not support this particular version of **kerberos preauth.** If that happens, turn off the preauthentication with the **none** option.

The **no** form of this command is equivalent to using the **none** keyword.

Examples

The following example enables Kerberos preauthentication:

```
kerberos preauth encrypted-unix-timestamp
```

The following example disables Kerberos preauthentication:

```
kerberos preauth none
```

Related Commands

Command	Description
kerberos local-realm	Specifies the Kerberos realm in which the router is located.
kerberos server	Specifies the location of the Kerberos server for a given Kerberos realm.
kerberos srvtab entry	Specifies a krb5 SRVTAB entry.
kerberos srvtab remote	Retrieves a SRVTAB file from a remote host and automatically generate a Kerberos SRVTAB entry configuration.

kerberos processes

To set the number of kerberos processes to service requests, use the **kerberos processes** command in global configuration mode. To disable the configuration, use the **no** form of this command.

kerberos processes *number*

no kerberos processes

Syntax Description

number	Number of processes. The range is from 1 to 10. The default is 1.

Command Default

The default process is 1.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
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 and implemented on the Cisco ASR 1000 Series Aggregation Services Routers.

Examples

The following example shows how to set the number of kerberos processes to 10:

```
Router# configure terminal
Router(config)# kerberos processes
 10
```

Related Commands

Command	Description
debug kerberos	Displays information associated with the Kerberos Authentication Subsystem.

kerberos realm

To map a host name or Domain Name System (DNS) domain to a Kerberos realm, use the **k erberos realm**command in global configuration mode. To remove a Kerberos realm map, use the **no** form of this command.

kerberos realm {*dns-domain*| *host*} *kerberos-realm*

no kerberos realm {*dns-domain*| *host*} *kerberos-realm*

Syntax Description

dns-domain	Name of a DNS domain or host.
host	Name of a DNS host.
kerberos-realm	Name of the Kerberos realm to which the specified domain or host belongs.

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

DNS domains are specified with a leading dot (.) character; host names cannot begin with a dot (.) character. There can be multiple entries of this line.

A Kerberos realm consists of users, hosts, and network services that are registered to a Kerberos server. The Kerberos realm must be in uppercase characters. The router can be located in more than one realm at a time. Kerberos realm names must be in all uppercase characters.

Examples

The following example maps the domain name “example.com” to the Kerberos realm, EXAMPLE.COM:

```
kerberos realm .example.com EXAMPLE.COM
```

Related Commands

Command	Description
kerberos local-realm	Specifies the Kerberos realm in which the router is located.
kerberos server	Specifies the location of the Kerberos server for a given Kerberos realm.
kerberos srvtab entry	Specifies a krb5 SRVTAB entry.
kerberos srvtab remote	Retrieves a SRVTAB file from a remote host and automatically generates a Kerberos SRVTAB entry configuration.

kerberos retry

To configure the number of retry attempts for the key distribution center (KDC) sessions, use the **kerberos retry** command in global configuration mode. To return to the default setting (4 retries), use the **no** form of this command.

kerberos retry *number*

no kerberos retry

Syntax Description

number	Number of retry attempts. The range is from 1 to 5. The default value is 4.

Command Default

The default value is four retry attempts.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
12.2(33)SRC	This command was integrated into a release earlier than Cisco Cisco IOS Release 12.2(33)SRC.
12.2(33)SXI	This command was integrated into a release earlier than Cisco Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

When multiple KDCs are configured, there is no way to control the timeout so that failover occurs. This causes common client applications to fail before the next KDC is contacted. Therefore, the kerberos retry command enables you to establish stable communication with the KDCs.

Examples

The following example shows how to configure the retry value for the KDC session:

```
Router> enable
Router# configure terminal
Router(config)# kerberos retry 3
```

Related Commands

Command	Description
kerberos clients mandatory	Causes the **rsh**, **rcp**, **rlogin**, and **telnet**commands to fail if they cannot negotiate the Kerberos protocol with the remote server.
kerberos credentials forward	Forces all network application clients on the router to forward users' Kerberos credentials upon successful Kerberos authentication.

kerberos server

To specify the location of the Kerberos server for a given Kerberos realm, use the **kerberos server**command in global configuration mode. To remove a Kerberos server for a specified Kerberos realm, use the **no** form of this command.

kerberos server *kerberos-realm* {*host-name*| *ip-address*} [*port-number*]

no kerberos server *kerberos-realm* {*host-name*| *ip-address*}

Syntax Description

kerberos-realm	Name of the Kerberos realm. A Kerberos realm consists of users, hosts, and network services that are registered to a Kerberos server. The Kerberos realm must be in uppercase letters.
host-name	Name of the host functioning as a Kerberos server for the specified Kerberos realm (translated into an IP address at the time of entry).
ip-address	IP address of the host functioning as the Kerberos server for the specified Kerberos realm.
port-number	(Optional) Port that the key distribution center (KDC) monitors (defaults to 88).

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

Use the **kerberos server** command to specify the location of the Kerberos server for a given realm.

Examples

The following example specifies 192.168.47.66 as the Kerberos server for the Kerberos realm EXAMPLE.COM:

```
kerberos server EXAMPLE.COM 192.168.47.66
```

Related Commands

Command	Description
kerberos local-realm	Specifies the Kerberos realm in which the router is located.
kerberos realm	Maps a host name or DNS domain to a Kerberos realm.
kerberos srvtab entry	Specifies a krb5 SRVTAB entry.
kerberos srvtab remote	Retrieves a SRVTAB file from a remote host and automatically generates a Kerberos SRVTAB entry configuration.

kerberos srvtab entry

To retrieve a SRVTAB file from a remote host and automatically generate a Kerberos SRVTAB entry configuration, use the kerberos srvtab entry command in global configuration mode. To remove a SRVTAB entry from the router's configuration, use the **no** form of this command.

kerberos srvtab entry *kerberos-principal principal-type timestamp key-version number key-type key-length encrypted-keytab*

no kerberos srvtab entry *kerberos-principal principal-type*

Syntax Description

kerberos-principal	A service on the router.
principal-type	Version of the Kerberos SRVTAB.
timestamp	Number representing the date and time the SRVTAB entry was created.
key-version number	Version of the encryption key format.
key-type	Type of encryption used.
key-length	Length, in bytes, of the encryption key.
encrypted-keytab	Secret key the router shares with the key distribution center (KDC). It is encrypted with the private Data Encryption Standard (DES) key (if available) when you write out your configuration.

Command Default

No default behavior or values.

Command Modes

Global configuration

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.

Usage Guidelines

When you use the **kerberos srvtab remote** command to copy the SRVTAB file from a remote host (generally the KDC), it parses the information in this file and stores it in the router's running configuration in the **kerberos srvtab entry**format. The key for each SRVTAB entry is encrypted with a private DES key if one is defined on the router. To ensure that the SRVTAB is available (that is, that it does not need to be acquired from the KDC) when you reboot the router, use the **write memory** router configuration command to write the router's running configuration to NVRAM.

If you reload a configuration, with a SRVTAB encrypted with a private DES key, on to a router that does not have a private DES key defined, the router displays a message informing you that the SRVTAB entry has been corrupted, and discards the entry.

If you change the private DES key and reload an old version of the router's configuration that contains SRVTAB entries encrypted with the old private DES keys, the router will restore your Kerberos SRVTAB entries, but the SRVTAB keys will be corrupted. In this case, you must delete your old Kerberos SRVTAB entries and reload your Kerberos SRVTABs on to the router using the **kerberos srvtab remote** command.

Although you can configure **kerberos srvtab entry** on the router manually, generally you would not do this because the keytab is encrypted automatically by the router when you copy the SRVTAB using the **kerberos srvtab remote** command.

Examples

In the following example, host/new-router.example.com@EXAMPLE.COM is the host, 0 is the type, 817680774 is the timestamp, 1 is the version of the key, 1 indicates the DES is the encryption type, 8 is the number of bytes, and .cCN.YoU.okK is the encrypted key:

```
kerberos srvtab entry host/new-router.example.com@EXAMPLE.COM 0 817680774 1 1 8 .cCN.YoU.okK
```

Related Commands

Command	Description
kerberos srvtab remote	Retrieves a krb5 SRVTAB file from the specified host.
key config-key	Defines a private DES key for the router.

kerberos srvtab remote

To retrieve a SRVTAB file from a remote host and automatically generate a Kerberos SRVTAB entry configuration, use the kerberos srvtab remote command in global configuration mode.

kerberos srvtab remote *boot_device:URL*

Syntax Description

URL	Machine that has the Kerberos SRVTAB file.
ip-address	IP address of the machine that has the Kerberos SRVTAB file .
filename	Name of the SRVTAB file.

Command Default

No default behavior or values.

Command Modes

Global configuration

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.

Usage Guidelines

When you use the **kerberos srvtab remote** command to copy the SRVTAB file from the remote host (generally the key distribution center [KDC]), it parses the information in this file and stores it in the router's running configuration in the **kerberos srvtab entry** format. The key for each SRVTAB entry is encrypted with the private Data Encryption Standard (DES) key if one is defined on the router. To ensure that the SRVTAB is available (that is, that it does not need to be acquired from the KDC) when you reboot the router, use the **write memory** configuration command to write the router's running configuration to NVRAM.

Examples

The following example copies the SRVTAB file residing on b1.example.com to a router named s1.example.com:

```
kerberos srvtab remote tftp://b1.example.com/s1.example.com-new-srvtab
```

Related Commands

Command	Description
kerberos srvtab entry	Retrieves a SRVTAB file from a remote host and automatically generate a Kerberos SRVTAB entry configuration.
key config-key	Defines a private DES key for the router.

kerberos timeout

To configure the timeout for key distribution center (KDC) requests, use the **kerberos timeout** command in global configuration mode. To return to the default setting (5 seconds), use the **no** form of this command.

kerberos timeout *seconds*

no kerberos timeout

Syntax Description

seconds	Timeout, in seconds, for KDC requests. The value range is from 1 to 10. The default value is 5 seconds.

Command Default

The timeout for KDC requests is 5 seconds.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
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.

Usage Guidelines

When multiple KDCs are configured, there is no way to control the timeout so that failover occurs. This causes common client applications to fail before the next KDC is contacted. Therefore, the kerberos retry command enables you to establish stable communication with the KDCs.

Examples

The following example shows how to configure the timeout value for KDC requests:

```
Router> enable
Router# configure terminal
Router(config)# kerberos timeout 3
```

Related Commands

Command	Description
kerberos clients mandatory	Causes the **rsh**, **rcp**, **rlogin**, and **telnet**commands to fail if they cannot negotiate the Kerberos protocol with the remote server.
kerberos credentials forward	Forces all network application clients on the router to forward users' Kerberos credentials upon successful Kerberos authentication.

key (config-radius-server)

To specify the authentication and encryption key for all RADIUS communications between the device and the RADIUS server, use the **key** command in RADIUS server configuration mode. To remove the configured key, use the **no** form of this command.

key {**0** *string* | **6** *string* | **7** *string*} *string*

no key

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 (cleartext) shared key.

Command Default

The authentication and encryption key is disabled.

Command Modes

RADIUS server configuration (config-radius-server)

Command History

Release	Modification
15.2(2)T	This command was introduced.
15.4(1)T	This command was modified. The **6** keyword was added.

Usage Guidelines

After enabling authentication, authorization, and accounting (AAA) authentication with the **aaa new-model** command, you must set the authentication and encryption key using the **radius server key** command.

Note Specify a RADIUS key after you issue the **aaa new-model** command.

The key entered must match the key used on the RADIUS server. All leading spaces are ignored, but spaces within and at the end of the key are used. 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.

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

Examples

The following example shows how to specify the host with IP address 192.0.2.2 as the RADIUS server and set rad123 as the encryption key:

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# radius server myserver
Device(config-radius-server)# address ipv4 192.0.2.2
Device(config-radius-server)# key rad123
```

The following example shows how to set the authentication and encryption key to anykey. The keyword 7 specifies that a hidden key follows.

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# radius server myserver
Device(config-radius-server)# address ipv4 192.0.2.2
Device(config-radius-server)# key 7 anykey
```

After you save your configuration and use the **show running-config** command, an encrypted key is displayed as follows:

```
Device> enable
Device# show running-config

radius server myserver
  address ipv4 192.0.2.2
  key 7 19283103834782sda
! The leading 7 indicates that the following text is encrypted.
```

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.
password encryption aes	Enables a type 6 encrypted preshared key.
radius server	Specifies the name for the RADIUS server configuration and enters RADIUS server configuration mode.

Command	Description
show running-config	Displays the current configuration of your routing device.

key (isakmp-group)

To specify the Internet Key Exchange (IKE) preshared key for group policy attribute definition, use the **key** command in Internet Security Association Key Management Protocol (ISAKMP) group configuration mode. To remove a preshared key, use the **no** form of this command.

key *name*

no key *name*

Syntax Description

name	IKE preshared key that matches the password entered on the client. **Note** This value must match the "password" field that is defined in the Cisco VPN Client 3.x configuration GUI.

Command Default

No default behavior or values.

Command Modes

ISAKMP group configuration (config-isakmp-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.

Usage Guidelines

Use the key command to specify the IKE preshared key when defining group policy information for Mode Configuration push. (It follows the crypto isakmp client configuration group command.) You must configure this command if the client identifies itself to the router with a preshared key. (You do not have to enable this command if the client uses a certificate for identification.)

Examples

The following example shows how to specify the preshared key "cisco":

```
crypto isakmp client configuration group default
  key cisco
  dns 10.2.2.2 10.3.2.3
  pool dog
  acl 199
```

Related Commands

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

key (TACACS+)

To configure the per-server encryption key on the TACACS+ server, use the **key** command in TACACS+ server configuration mode. To remove the per-server encryption key, use the **no** form of this command.

key [**0** | **6** | **7**] *key-string*

no key [**0** | **6** | **7**] *key-string*

Syntax Description

0	(Optional) Specifies that an unencrypted key follows.
6	(Optional) Specifies that an advanced encryption scheme (AES) encrypted key follows.
7	(Optional) Specifies that a hidden key follows.
key-string	The unencrypted shared key.

Command Default

No TACACS+ encryption key is configured.

Command Modes

TACACS+ server configuration (config-server-tacacs)

Command History

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.
15.4(1)T	This command was integrated into Cisco IOS Release 15.4(1)T. The **6** keyword was added.

Usage Guidelines

The **key** command allows you to configure a per-server encryption key.

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

Examples

The following example shows how to specify an unencrypted shared key named “key1”:

```
Device> enable
Device# configure terminal
Device(config)# tacacs server server1
Device(config-server-tacacs)# key 0 key1
```

Related Commands

Command	Description
password encryption aes	Enables a type 6 encrypted preshared key.
tacacs server	Configures the TACACS+ server for IPv6 or IPv4 and enters TACACS+ server configuration mode.

key config-key

To define a private DES key for the router, use the **key config-key**command in global configuration mode. To delete a private Data Encryption Standard (DES) key from the router, use the **no** form of this command.

key config-key 1 *string*

no key config-key 1 *string*

Syntax Description

1	Key number. This number is always 1.
string	Private DES key (can be up to eight alphanumeric characters).

Command Default

No DES-key defined.

Command Modes

Global configuration

Command History

Release	Modification
11.2	This command was released.
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 defines a private DES key for the router that will not show up in the router configuration. This private DES key can be used to DES-encrypt certain parts of the router's configuration.

Caution The private DES key is unrecoverable. If you encrypt part of your configuration with the private DES key and lose or forget the key, you will not be able to recover the encrypted data.

Examples

The following example sets *keyxx* as the private DES key on the router:

```
key config-key 1 keyxx
```

Related Commands

Command	Description
kerberos srvtab entry	Specifies a krb5 SRVTAB entry.
kerberos srvtab remote	Retrieves a SRVTAB file from a remote host and automatically generates a Kerberos SRVTAB entry configuration.

key config-key password-encryption

To store a type 6 encryption key in private NVRAM, use the **key config-key password-encryption**command in global configuration mode. To disable the encryption, use the **no** form of this command.

key config-key password-encryption [*text*]

no key config-key password-encryption [*text*]

Syntax Description

text	(Optional) **Password or master key**. **Note** It is recommended that you do not use the *text* argument but instead use interactive mode (using the enter key after you enter the **key config-key password-encryption**command) so that the preshared key will not be printed anywhere and, therefore, cannot be seen.

Command Default

No type 6 password encryption

Command Modes

Global configuration

Command History

Release	Modification
12.3(2)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

You can securely store plain text passwords in type 6 format in NVRAM using a command-line interface (CLI). Type 6 passwords are encrypted. Although the encrypted passwords can be seen or retrieved, it is difficult to decrypt them to find out the actual password. Use the **key config-key password-encryption**command with the **password encryption aes**command to configure and enable the password (symmetric cipher Advanced Encryption Standard [AES] is used to encrypt the keys). The password (key) configured using the **key config-key password-encryption** command is the master encryption key that is used to encrypt all other keys in the router.

If you configure the **password encryption aes**command without configuring the **key config-key password-encryption**command, the following message is printed at startup or during any nonvolatile generation

(NVGEN) process, such as when the **show running-config** or **copy running-config startup-config** commands have been configured:

```
“Can not encrypt password. Please configure a configuration-key with ‘key config-key’”
```

Changing a Password

If the password (master key) is changed, or reencrypted, using the **key config-key password-encryption**command), the list registry passes the old key and the new key to the application modules that are using type 6 encryption.

Deleting a Password

If the master key that was configured using the **key config-key password-encryption**command is deleted from the system, a warning is printed (and a confirm prompt is issued) that states that all type 6 passwords will become useless. As a security measure, after the passwords have been encrypted, they will never be decrypted in the Cisco IOS software. However, passwords can be reencrypted as explained in the previous paragraph.

Caution If the password configured using the **key config-key password-encryption**command is lost, it cannot be recovered. The password should be stored in a safe location.

Unconfiguring Password Encryption

If you later unconfigure password encryption using the **no password encryption aes** command, all existing type 6 passwords are left unchanged, and as long as the password (master key) that was configured using the **key config-key password-encryption**command exists, the type 6 passwords will be decrypted as and when required by the application.

Storing Passwords

Because no one can “read” the password (configured using the **key config-key password-encryption**command), there is no way that the password can be retrieved from the router. Existing management stations cannot “know” what it is unless the stations are enhanced to include this key somewhere, in which case the password needs to be stored securely within the management system. If configurations are stored using TFTP, the configurations are not standalone, meaning that they cannot be loaded onto a router. Before or after the configurations are loaded onto a router, the password must be manually added (using the **key config-key password-encryption**command). The password can be manually added to the stored configuration but is not recommended because adding the password manually allows anyone to decrypt all passwords in that configuration.

Configuring New or Unknown Passwords

If you enter or cut and paste cipher text that does not match the master key, or if there is no master key, the cipher text is accepted or saved, but an alert message is printed. The alert message is as follows:

```
“ciphertext>[for username bar>] is incompatible with the configured master key.”
```

If a new master key is configured, all the plain keys are encrypted and made type 6 keys. The existing type 6 keys are not encrypted. The existing type 6 keys are left as is.

If the old master key is lost or unknown, you have the option of deleting the master key using the **no key config-key password-encryption**command. Deleting the master key using the **no key config-key password-encryption**command causes the existing encrypted passwords to remain encrypted in the router configuration. The passwords will not be decrypted.

Examples

The following example shows that a type 6 encryption key is to be stored in NVRAM:

```
Router (config)# key config-key password-encryption
```

Related Commands

Command	Description
password encryption aes	Enables a type 6 encrypted preshared key.
password logging	Provides a log of debugging output for a type 6 password operation.

key-hash

To specify the Secure Shell (SSH) Rivest, Shamir, and Adleman (RSA) key type and name, use the **key-hash**command in SSH public key configuration mode. To remove the SSH RSA Rivest, Shamir, and Adleman (RSA) public key, use the **no** form of this command.

key-hash *key-type key-name*

no key-hash [*key-type key-name*]

Syntax Description

key-type key-name	The SSH RSA public key type and name.

Command Default

SSH key type and name are not specified.

Command Modes

SSH public key configuration (conf-ssh-pubkey-user)

Command History

Release	Modification
12.2(33)SRA	This command was introduced in release earlier than Cisco IOS Release 12.(33)SRA.

Usage Guidelines

The key type must be **ssh-rsa** for configuration of private-public key pairs. You can use a hashing software to compute the hash of the public key string or you can copy the hash value from another Cisco IOS router. Using the **key-string** command is the preferred method for entering the public key data for the first time.

Examples

The following example shows how to specify the SSH key type and name:

```
Router(config)# ip ssh pubkey-chain
Router(conf-ssh-pubkey)# username test
Router(conf-ssh-pubkey-user)# key-hash ssh-rsa key1
Router(conf-ssh-pubkey-user))# exit
Router(config-pubkey)# exit
Router(config)# exit
```

Related Commands

Command	Description
key-string	Specifies the SSH RSA public key of the remote peer.

keyring

To configure a keyring with an Internet Security Association and Key Management Protocol (ISAKMP) profile, use the **keyring**command in ISAKMP profile configuration mode. To remove the keyring from the ISAKMP profile, use the **no** form of this command.

keyring *keyring-name*

no keyring *keyring-name*

Syntax Description

keyring-name	The keyring name, which must match the keyring name that was defined in the global configuration.

Command Default

If this command is not used, the ISAKMP profile uses the keys defined in the global configuration.

Command Modes

ISAKMP profile configuration (config-isa-prof)

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.

Usage Guidelines

The ISAKMP profile successfully completes authentication of peers if the peer keys are defined in the keyring that is attached to this profile. If no keyring is defined in the profile, the global keys that were defined in the global configuration are used.

Examples

The following example shows that “vpnkeyring” is configured as the keyring name:

```
crypto isakmp profile vpnprofile
 keyring vpnkeyring
```

keyring (IKEv2 profile)

To specify a locally defined or accounting, authentication and authorization (AAA)-based keyring, use the **keyring** command in IKEv2 profile configuration mode. To delete the keyring, use the **no** form of this command.

keyring{**local** *keyring-name*| **aaa** *list-name*[**name-mangler** *mangler-name*| **password** *password*]}

no keyring

Syntax Description

local	Specifies the local keyring.
keyring-name	The keyring name for a locally defined keyring.
aaa	Specifies the AAA-based preshared keys list name.
list-name	The AAA method list name.
name-mangler	Derives the username from the peer identity in the preshared key lookup on the AAA list.
mangler-name	(Optional) Globally defined name mangler.
password *password*	Specifies a password for the password. This argument defines the following values: • **0—**Specifies that the password is unencrypted. • **6—**Specifies that the password is encrypted. • *password***—**Specifies an unencrypted user password.

Command Default

A keyring is not specified.

Command Modes

IKEv2 profile configuration (crypto-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(2)T	This command was modified. The keyword **local** and the keyword argument pair **name-mangler** *mangler-name* was added.

Release	Modification
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
15.3(3)M	This command was modified. The **password** *password* was added.

Usage Guidelines

Use this command to specify a keyring for use with the local and remote preshared key authentication methods. Only one keyring can be configured either local or AAA based with or without the name mangler. If you configure an AAA based keyring with the name mangler, the name mangler cannot be deleted.

Note Local AAA is not supported for AAA-based preshared keys.

If the **name-mangler** keyword is not specified, the entire peer identity is used for key lookup.

Examples

The following example shows how to configure an AAA-based keyring and assign the keyring to a profile:

```
Router(config)# aaa new-model
Router(config)# aaa authentication login aaa-psk-list default group radius
Router(config)# crypto ikev2 profile profile1
Router(config-ikev2-profile)# keyring aaa aaa-psk-list name-mangler mangler1
```

The following example shows how to configure a locally defined keyring:

```
Router(config)# crypto ikev2 profile profile1
Router(config-ikev2-profile)# keyring keyring1
```

Related Commands

Command	Description
crypto ikev2 keyring	Defines an IKEv2 keyring.

key-set

To associate a key set with a TIDP group, use the **key-set** command in TIDP group configuration mode. To remove the key set from the TIDP group configuration, use the **no** form of this command.

Note Effective with Cisco IOS Release 12.4(20)T, the **key-set** command is not available in Cisco IOS software.

key-set *name*

no key-set

Syntax Description

name	Name of the key set.

Command Default

None.

Command Modes

TIDP group configuration (config-tidp-grp)

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 **key-set** command is entered in TIDP group configuration mode to associate a global key set with a TIDP group. A key set must be configured before a TIDP group can be activated. The key set is first configured with the **tidp key-set** command in global configuration mode. This key set defines the authentication key for TIDP peer communication. This key set can be optionally configured with an encryption key to protect the contents of TIDP messages.

Examples

The following example configures TIDP group 10 to use the key set name KEY_1:

```
Router(config)# tidp key-set KEY_1
Router(config-tidp-ks)# authentication-key send key-string 0 Aa1Bb2Cc3
Router(config-tidp-ks)# authentication-key receive key-string 0 Dd4Ee5Ff6
Router(config-tidp-ks)# exit
Router(config)# tidp group 10
Router(config-tidp-grp)# key-set KEY_1

Router(config-tidp-grp)# registration retry-interval min 30 max 600
Router(config-tidp-grp)# peer 10.1.1.1

Router(config-tidp-grp)# peer 10.1.1.2

Router(config-tidp-grp)# peer 10.1.1.3

Router(config-tidp-grp)# active
```

Related Commands

Command	Description
active	Activates a TIDP group.
peer	Configures a consumer as a member of a TIDP group.
registration retry-interval (TIDP)	Configures the length of time and number of attempts for TIDP group registration.
tidp group	Configures a TIDP group.
tidp key-set	Configures a key-set for TIDP peer authentication and/or message encryption.

key-string (IKE)

To specify the Rivest, Shamir, and Adelman (RSA) public key of the remote peer, use the **key-string**command in public key configuration mode. To remove the RSA public key, use the **no** form of this command.

key-string *key-string*

no key-string *key-string*

Syntax Description

key-string	Enter the key in hexadecimal format. While entering the key data, you can press Return to continue entering data.

Command Default

No default behavior or values

Command Modes

Public key 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.(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 2.6	This command was integrated into Cisco IOS XE Release 2.6.

Usage Guidelines

Before using this command, you must enter the **rsa-pubkey** command in the crypto keyring mode.

If possible, to avoid mistakes, you should cut and paste the key data (instead of attempting to type in the data).

To complete the command, you must return to the global configuration mode by typing **quit** at the config-pubkey prompt.

Examples

The following example manually specifies the RSA public keys of an IP Security (IPSec) peer:

```
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-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
crypto keyring	Defines a crypto keyring.
rsa-pubkey	Defines the RSA public key to be used for encryption or signatures during IKE authentication.
show crypto keyring	Displays keyrings on your router.

key-string (SSH)

To specify the Secure Shell (SSH) Rivest, Shamir, and Adleman (RSA) public key of the remote peer, use the **key-string**command in SSH public key configuration mode. To remove the SSH RSA public key, use the **no** form of this command.

key-string

no key-string

Syntax Description

This command has no arguments or keywords.

Command Default

SSH RSA public key of the remote peer is not specified.

Command Modes

SSH public key configuration (conf-ssh-pubkey-user)

Command History

Release	Modification
12.2(33)SRA	This command was introduced in release earlier than Cisco IOS Release 12.(33)SRA.

Usage Guidelines

The **key-string**command specifies the SSH RSA public key of the remote peer and enters public-key data configuration mode. You can obtain the public key value from an open SSH client (.ssh/id_rsa.pub file).

You can return to global configuration mode by entering the **quit** command in public-key data configuration mode and then by entering the **exit** command in public key configuration mode.

Examples

The following example shows how to specify the SSH RSA public keys of the remote peer:

```
Router(config)# ip ssh pubkey-chain
Router(conf-ssh-pubkey)# username test
Router(conf-ssh-pubkey-user)# key-string
Router(conf-ssh-pubkey-data))# quit
Router(config-pubkey)# exit
Router(conf)# exit
```

Related Commands

Command	Description
key-hash	Specifies the SSH key type and name.

language

To specify the language to be used in a webvpn context, use the **language** command in webvpn context configuration mode. To remove the language, use the **no** form of this command.

language {**Japanese**| **customize** *language-name device* **:** *file*}

no language {**Japanese**| **customize** *language-name device* **:** *file*}

Syntax Description

Japanese	Specifies that the language to be used is Japanese.
customize *language-name* *device* **:** *file*	Specifies that a language other than English or Japanese is to be used. - *language-name* --This language will be displayed in the selection box on the login and portal pages. - *device* **:** *file* --Storage device on the system and the file name. The file name should include the directory location.

Command Default

English is the language.

Command Modes

Webvpn context configuration (config-webvpn-context)

Command History

Release	Modification
12.4(22)T	This command was introduced.

Examples

The following example shows that the language to be used is Japanese:

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

The following example shows that the language (mylang) is to be customized from the file "lang.js," which is in flash:

```
Router (config)# webvpn context
 Router (config-webvpn-context)# language customize mylang flash:lang.js
```

Related Commands

Command	Description
webvpn create template	Creates templates for multilanguage support for messages in an SSL VPN.

ldap attribute-map

To configure a dynamic Lightweight Directory Access Protocol (LDAP) attribute map, use the **ldap attribute-map**command in global configuration mode. To remove the attribute maps, use the **no** form of this command.

ldap attribute-map *map-name*

no ldap attribute-map *map-name*

Syntax Description

map-name	Name of the attribute map.

Command Default

Default mapping is applied.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

You can create LDAP attribute maps to map your existing user-defined LDAP attribute names and values to Cisco attribute names and values that are compatible. You can then bind these attribute maps to LDAP server configuration or remove them as required. The default map is displayed using the **show ldap attributes** command.

Examples

The following command shows how to create an unpopulated LDAP attribute map table named att_map_1:

```
Router(config)# ldap attribute-map att_map_1
```

Related Commands

Command	Description
attribute-map	Attaches an attribute map to a particular LDAP server.
map-type	Defines the mapping of a attribute in the LDAP server.
show ldap attribute	Displays information about default LDAP attribute mapping.

ldap search

To search a Lightweight Directory Access Protocol (LDAP) server, use the **ldap search** command in privileged EXEC mode.

ldap search *server-address port-number search-base scope-number search-filter* **ssl**

Syntax Description

server-address	The IP address of the server.
port-number	The remote TCP port. The range is from 0 to 65535.
search-base	The search base.
scope-number	The scope of the search. The range is from 0 to 2, which denotes to search from BASE, ONELEVEL, and SUBTREE.
search-filter	The filter for the search.
ssl	Specifies LDAP over Secure Socket Layer (SSL).

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)M	This command was introduced in a release earlier than Cisco IOS Release 15.0(1)M.
12.2(33)SRB	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRB.
12.2(33)SXI	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.

Examples

The following example shows how to search an LDAP server:

```
Router# ldap search 10.0.0.1 265 c 2 sea ssl
```

Related Commands

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

ldap server

To define a Lightweight Directory Access Protocol (LDAP) server and enter LDAP server configuration mode, use the **ldap server** command in global configuration mode. To remove an LDAP server configuration, use the **no** form of this command.

ldap server *name*

no ldap server *name*

Syntax Description

name	Name of the LDAP server configuration.

Command Default

No LDAP server is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(1)T	This command was introduced.
15.3(2)T	This command was modified. IPv6 transport support for LDAP server was added.

Usage Guidelines

You can define the following parameters in LDAP server configuration mode:

- IP address of the LDAP server
- Transport protocol to connect to the server
- Security protocol for peer-to-peer communication
- LDAP timers

Examples

The following example shows how to define an LDAP server named server1:

```
Device(config)# ldap server server1
```

Related Commands

Command	Description
ipv4 (ldap)	Creates an IPv4 address within an LDAP server address pool.

Command	Description
transport port (ldap)	Configures the transport protocol for establishing a connection with the LDAP server.

length (RITE)

To specify the length the captured portion of the packets being captured in IP traffic export capture mode, use the **length** command in RITE configuration mode. To return to the default condition of capturing entire packets, use the **no** form of this command.

length *bytes*

no length

Syntax Description

bytes	The length in bytes of the packet captured in IP traffic export capture mode. Acceptable values are 128, 256, and 512.

Command Default

When you do not use this command, the entire packet is captured.

Command Modes

RITE configuration

Command History

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

Usage Guidelines

Use this command to limit the length of the portion of the packets being captured in IP traffic export capture mode. The captured portion of the packets are limited to 128, 256, or 512 bytes. If you do not use the **length** command, entire packets are captured.

Examples

The following example shows the use of the **length** command in the configuration of IP traffic export capture mode profile “corp2”:

```
Router(config)# ip traffic-export profile corp2 mode_capture
Router(config-rite)# bidirectional
Router(config-rite)# outgoing sample one-in-every 50
Router(config-rite)# incoming access-list ham_acl
Router(config-rite)# length 512
Router(config-rite)# exit
Router(config)# interface FastEthernet 0/0
Router(config-if)# ip traffic-export apply corp2 size 10000000
```

Related Commands

Command	Description
bidirectional	Enables incoming and outgoing IP traffic to be exported or captured across a monitored interface.
incoming	Configures filtering for incoming IP traffic export or IP traffic capture traffic.
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.
outgoing	Configures filtering for outgoing IP traffic export or IP traffic capture traffic.
traffic-export interface	Controls the operation of IP traffic capture mode.

license (parameter-map)

To configure a license that is sent to ScanSafe for authentication, use the **license** command in parameter-map type inspect configuration mode. To remove the license, use the **no** form of this command.

license {**0** *key*| **7** *key*}

no license {**0** *key*| **7** *key*}

Syntax Description

0 *key*	Specifies an unencrypted 32-character hexadecimal license key.
7 *key*	Specifies an encrypted 66-character hexadecimal license key.

Command Default

The license 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

You must configure the **parameter-map type content-scan global** command before you configure the **license** command.

When the server license or the private key is not configured, content scan drops the traffic. When the server license or private key is wrong, content scan forwards the traffic to ScanSafe and ScanSafe sends a blocked warning page to the end user.

Examples

The following example shows how to configure an unencrypted license key:

```
Device(config)# parameter-map type content-scan global
Device(config-profile)# license 0 D7BF98AFEB0B4AFA5954CB0F81FFB620
```

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.

lifetime (cs-server)

To specify the lifetime of the certification authority (CA) or a certificate, use the **lifetime** command in certificate server configuration mode. To return to the default lifetime values, use the **no** form of this command.

lifetime {**ca-certificate**| **certificate**} *days* [*hours* [*minutes*]]

no lifetime {**ca-certificate**| **certificate**}

Syntax Description

ca-certificate	Specifies that the lifetime applies to the CA certificate of the certificate server.
certificate	Specifies that the lifetime applies to the certificate of the certificate server. The maximum certificate lifetime is 1 month less than the expiration date of the CA certificate’s lifetime.
days	An integer specifying the certificate lifetime in days. Valid values range from 0 to 7305.
hours	(Optional) An integer specifying the certificate lifetime in hours. Valid values range from 0 to 24.
minutes	(Optional) An integer specifying the certificate lifetime in minutes. Valid values range from 0 to 59. It is recommended that if you set the certificate lifetime in minutes, that the value be set to 3 minutes or greater. Setting the certificate lifetime to a value of less than 3 minutes will not allow certificate rollover to function.

Command Default

The default CA certificate lifetime is 1095 days, or 3 years.

The default certificate lifetime is 365 days, or 1 year.

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 the **lifetime** command if you want to specify lifetime values other than the default values for the CA certificate and the certificate of the certificate server.

After the certificate generates its signed certificate, the lifetime cannot be changed. All certificates are valid when they are issued.

Examples

The following example shows how to set the lifetime value for the CA to 30 days:

```
Router(config)# ip http server
Router(config)# crypto pki server mycertserver
Router(cs-server)# lifetime ca certificate 30
```

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.
database username	Specifies the requirement of a username or password to be issued when accessing the primary database location.

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

lifetime (IKE policy)

To specify the lifetime of an Internet Key Exchange (IKE) security association (SA), use the **lifetime**command in Internet Security Association Key Management Protocol (ISAKMP) policy configuration mode . To reset the SA lifetime to the default value, use the **no** form of this command.

lifetime *seconds*

no lifetime

Syntax Description

seconds	Number of many seconds for each each SA should exist before expiring. Use an integer from 60 to 86,400 seconds, which is the default value.

Command Default

The default is 86,400 seconds (one day).

Command Modes

ISAKMP policy 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.(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.

Usage Guidelines

Use this command to specify how long an IKE SA exists before expiring.

When IKE begins negotiations, the first thing it does is agree upon the security parameters for its own session. The agreed-upon parameters are then referenced by an SA at each peer. The SA is retained by each peer until the SA's lifetime expires. Before an SA expires, it can be reused by subsequent IKE negotiations, which can save time when setting up new IPSec SAs. Before an SA expires, it can be reused by subsequent IKE negotiations, which can save time when setting up new IPSec SAs. New IPSec SAs are negotiated before current IPSec SAs expire.

So, to save setup time for IPSec, configure a longer IKE SA lifetime. However, shorter lifetimes limit the exposure to attackers of this SA. The longer an SA is used, the more encrypted traffic can be gathered by an attacker and possibly used in an attack.

Note that when your local peer initiates an IKE negotiation between itself and a remote peer, an IKE policy can be selected only if the lifetime of the remote peer's policy is shorter than or equal to the lifetime of the local peer's policy. Then, if the lifetimes are not equal, the shorter lifetime will be selected. To restate this behavior: If the two peer's policies' lifetimes are not the same, the initiating peer's lifetime must be longer and the responding peer's lifetime must be shorter, and the shorter lifetime will be used.

Examples

The following example configures an IKE policy with a security association lifetime of 600 seconds (10 minutes), and all other parameters are set to the defaults:

```
crypto isakmp policy 15
 lifetime 600
 exit
```

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 Diffie-Hellman group identifier within an IKE policy.
hash (IKE policy)	Specifies the hash algorithm within an IKE policy.
show crypto isakmp policy	Displays the parameters for each IKE policy.

lifetime (IKEv2 profile)

To specify the lifetime for an Internet Key Exchange Version 2 (IKEv2) security association (SA), use the **lifetime**command in IKEv2 profile configuration mode . To reset the SA lifetime to the default value, use the **no** form of this command.

lifetime *seconds*

no lifetime

Syntax Description

seconds	The time that each IKE SA should exist before expiring. Use an integer from 60 to 86,400 seconds.

Command Default

The default is 86,400 seconds (one day).

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.

Usage Guidelines

Use this command to specify the lifetime of an IKE SA. When IKE begins negotiations, IKE agrees on the security parameters for its session that are referenced by an SA at each peer. The SA is retained by each peer until the SA expires, and before an SA expires, it can be reused by subsequent IKE negotiations, which saves time when setting up new IKE SA. Although, SA with a shorter lifetime limits the exposure to attacks, to save time configure an IKE SA that has a longer lifetime. The longer an SA is used, the more encrypted traffic can be gathered by an attacker and possibly used in an attack.

Examples

The following example configures an IKEv2 profile with a security association lifetime of 600 seconds (10 minutes), and all other parameters are set to the defaults:

```
Router(config)# crypto ikev2 profile profile2
Router(config-ikev2-profile)# lifetime 600
```

Related Commands

Command	Description
crypto ikev2 profile	Defines an IKEv2 profile.
show crypto ikev2 profile	Displays the IKEv2 profile.

lifetime crl

To define the lifetime of the certificate revocation list (CRL) that is used by the certificate server, use the **lifetime crl** command in certificate server configuration mode. To return to the default value of 1 week, use the **no** form of this command.

lifetime crl *time*

no lifetime crl *time*

Syntax Description

time	Lifetime value, in hours, of the CRL. Maximum lifetime value is 336 hours (2 weeks). The default value is 168 hours (1 week).

Command Default

168 hours (1 week)

Command Modes

Certificate server configuration

Command History

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

Usage Guidelines

After you create a certificate server via the **crypto pki server**command, use the **lifetime crl** command if you want to specify a value other than the default value for the CRL. The lifetime value is added to the CRL when the CRL is created.

The CRL is written to the specified database location as *ca-label*.crl.

Examples

The following example shows how to set the lifetime value for the CRL to 24 hours:

```
Router(config)# ip http server
Router(config)# crypto pki server mycertserver
Router(cs-server)# lifetime crl 24
```

Related Commands

Command	Description
cdp-url	Specifies that CDP should be used in the certificates that are issued by the certificate server.
crypto pki server	Enables a Cisco IOS certificate server and enters PKI configuration mode.

lifetime enrollment-request

To specify how long an enrollment request should stay in the enrollment database, use the **lifetime enrollment-request**command in certificate server configuration mode. To return to the default value of 1 week, use the **no** form of this command.

lifetime enrollment-request *time*

no lifetime enrollment-request

Syntax Description

time	Lifetime value, in hours, of an enrollment request. The maximum lifetime value is 1000 hours. The default value is 168 hours (1 week).

Command Default

Lifetime value default is 168 hours.

Command Modes

Certificate server configuration

Command History

Release	Modification
12.3(7)T	This command was introduced.

Usage Guidelines

After the certificate server receives an enrollment request, it can leave the request in pending, reject it, or grant it. The request is left in the Enrollment Request Database for the lifetime of the enrollment request until the client polls the certificate server for the result of the request.

Examples

The following example shows how to set the lifetime value for the enrollment request to 24 hours:

```
Router (config)# crypto pki server mycs
Router (cs-server)# lifetime enrollment-request 24
```

Related Commands

Command	Description
crypto pki server	Enables a Cisco IOS certificate server.
crypto pki server grant	Grants all or certain SCEP requests.
crypto pki server remove	Removes enrollment requests that are in the certificate server Enrollment Request Database.

limit address-count

To limit the number of IPv6 addresses allowed to be used on the port, use the **limit address-count**command in Neighbor Discovery Protocol (NDP) inspection policy configuration mode .

limit address-count *maximum*

Syntax Description

maximum	Sets the role of the device to host.

Command Default

The device role is host.

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

The **limit address-count** command limits the number of IPv6 addresses allowed to be used on the port on which the policy is applied. Limiting the number of IPv6 addresses on a port helps limit the binding table size.

Use the **limit address-count**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 limits the number of IPv6 addresses allowed on the port to 25:

```
Router(config)# ipv6 nd inspection policy policy1
Router(config-nd-inspection)# limit address-count 25
```

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.

list (LSP Attributes)

To display the contents of a label switched path (LSP) attribute list, use the **list** command in LSP Attributes configuration mode.

list

Syntax Description

This command has no arguments or keywords.

Command Default

Contents of an LSP attribute list is not displayed.

Command Modes

LSP Attributes configuration (config-lsp-attr)

Command History

Release	Modification
12.0(26)S	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.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

This command displays the contents of the LSP attribute list. You can display each of the following configurable LSP attributes using the **list** command: affinity, auto-bw, bandwidth, lockdown, priority, protection, and record-route.

Examples

The following example shows how to display the contents of an LSP attribute list identified with the string priority:

```
!
Router(config)# mpls traffic-eng lsp attributes priority
Router(config-lsp-attr)# priority 0 0
Router(config-lsp-attr)# list
 priority 0 0
Router(config-lsp-attr)#
```

Related Commands

Command	Description
mpls traffic-eng lsp attributes	Creates or modifies an LSP attribute list.
show mpls traffic-eng lsp attributes	Displays global LSP attribute lists.

list (WebVPN)

To list the currently configured access control list (ACL) entries sequentially, use the **list** command in webvpn acl configuration mode. This command has no **no** form.

list

Syntax Description

This command has no arguments or keywords.

Command Default

Currently configured ACL entries are not listed.

Command Modes

Webvpn acl configuration

Command History

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

Usage Guidelines

Before using this command, you must have configured the web context and the **acl** command.

Examples

The following example shows that currently configured ACL entries are to be listed:

```
webvpn context context1
 acl acl1
  list
```

Related Commands

Command	Description
webvpn context	Configures the WebVPN context and enters SSL VPN configuration mode.
acl	Defines an ACL using a SSL VPN gateway at the Application Layer level.

li-view

To initialize a lawful intercept view, use the **li-view**command in global configuration mode.

li-view *li-password* **user** *username* **password** *password*

Syntax Description

li-password	Password for the lawful intercept view. This password is used by the system administrator or a level 15 privilege user who initialized the lawful intercept view to access and configure it. The password can contain any number of alphanumeric characters. **Note** The password is case sensitive.
user *username*	Specifies the user who can access the lawful intercept view.
password *password*	Provides the password for the specified **user**. The user must provide this password to access the lawful intercept view.

Command Default

A lawful intercept view cannot be accessed.

Command Modes

Global configuration (config)

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

Like a command-line interface (CLI) view, a lawful intercept view restricts access to specified commands and configuration information. Specifically, 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 Network Management Protocol (SNMP) commands that stores information about calls and users.

Commands available in lawful intercept view belong to one of the following categories:

- Lawful intercept commands that should not be made available to any other view or privilege level.
- CLI commands that are useful for lawful intercept users but do not need to be excluded from other views or privilege levels.

Note Only a system administrator or a level 15 privilege user can initialize a lawful intercept view.

Examples

The following example shows how to configure a lawful intercept view, add users to the view, and verify the users that were added to the view:

```
!Initialize the LI-View.
Router(config)# li-view lipass user li_admin password li_adminpass
00:19:25:%PARSER-6-LI_VIEW_INIT:LI-View initialized.
Router(config)# end
! Enter the LI-View; that is, check to see what commands are available within the view.
Router# enable view li-view
Password:
Router#
00:22:57:%PARSER-6-VIEW_SWITCH:successfully set to view 'li-view'.
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# parser view li-view

Router(config-view)# ?
View commands:
  commands  Configure commands for a view
  default   Set a command to its defaults
  exit      Exit from view configuration mode
  name      New LI-View name      ===This option only resides in LI View.
  no        Negate a command or set its defaults
  password  Set a password associated with CLI views
Router(config-view)#
! NOTE:LI View configurations are never shown as part of ‘running-configuration’.
! Configure LI Users.
Router(config)# username lawful-intercept li-user1 password li-user1pass

Router(config)# username lawful-intercept li-user2 password li-user2pass
! Displaying LI User information.
Router# show users lawful-intercept
li_admin
li-user1
li-user2
Router#
```

Related Commands

Command	Description
show users	Displays information about the active lines on the router.
username	Establishes a username-based authentication system.

load-balance (server-group)

To enable RADIUS server load balancing for a named RADIUS server group, use the load-balance command in server group configuration mode. To disable named RADIUS server load balancing, use the **no** form of this command.

load-balance method least-outstanding [**batch-size** *number*] **[ignore-preferred-server]**

no load-balance

Syntax Description

method least-outstanding	Enables least outstanding mode for load balancing.
batch-size	(Optional) The number of transactions to be assigned per batch.
number	(Optional) The number of transactions in a batch. • The default is 25. • The range is 1-2147483647. **Note** Batch size may impact throughput and CPU load. It is recommended that the default batch size, 25, be used because it is optimal for high throughput, without adversely impacting CPU load.
ignore-preferred-server	(Optional) Indicates if a transaction associated with a single authentication, authorization, and accounting (AAA) session should attempt to use the same server or not. • If set, preferred server setting will not be used. • Default is to use the preferred server.

Command Default

If this command is not configured, named RADIUS server load balancing will not occur.

Command Modes

Server group configuration

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.

Release	Modification
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.

Examples

The following example shows load balancing enabled for a named RADIUS server group. It is shown in three parts: the current configuration of RADIUS command output, debug output, and AAA server status information.

Examples

The following shows the relevant RADIUS configuration:

```
Router# show running-config
.
.
.
aaa group server radius server-group1
 server 192.0.2.238 auth-port 2095 acct-port 2096
 server 192.0.2.238 auth-port 2015 acct-port 2016
 load-balance method least-outstanding batch-size 5
!
aaa authentication ppp default group server-group1
aaa accounting network default start-stop group server-group1
.
.
.
```

The lines in the current configuration of RADIUS command output above are defined as follows:

- The **aaa group server radius** command shows the configuration of a server group with two member servers.
- The **load-balance** command enables load balancing for the global RADIUS server groups with the batch size specified.
- The **aaa authentication ppp**command authenticates all PPP users using RADIUS.
- The **aaa accounting** command enables the sending of all accounting requests to the AAA server after the client is authenticated and after the disconnect using the start-stop keyword.

Examples

The debug output below shows the selection of a preferred server and the processing of requests for the configuration above.

```
Router#
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002C):No preferred server available.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:No more transactions in batch. Obtaining a new
server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Obtaining a new least loaded server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Server[0] load:0
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Server[1] load:0
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Selected Server[0] with load 0
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:[5] transactions remaining in batch.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002C):Server (192.0.2.238:2095,2096) now being
 used as preferred server
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002D):No preferred server available.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:[4] transactions remaining in batch. Reusing
server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002D):Server (192.0.2.238:2095,2096) now being
 used as preferred server
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002E):No preferred server available.
```

```
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:[3] transactions remaining in batch. Reusing
server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002E):Server (192.0.2.238:2095,2096) now being
 used as preferred server
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002F):No preferred server available.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:[2] transactions remaining in batch. Reusing
server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(0000002F):Server (192.0.2.238:2095,2096) now being
 used as preferred server
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(00000030):No preferred server available.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT:[1] transactions remaining in batch. Reusing
server.
*Feb 28 13:51:16.019:AAA/SG/SERVER_SELECT(00000030):Server (192.0.2.238:2095,2096) now being
 used as preferred server
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT(00000031):No preferred server available.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:No more transactions in batch. Obtaining a new
server.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:Obtaining a new least loaded server.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:Server[1] load:0
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:Server[0] load:5
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:Selected Server[1] with load 0
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:[5] transactions remaining in batch.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT(00000031):Server (192.0.2.238:2015,2016) now being
 used as preferred server
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT(00000032):No preferred server available.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:Obtaining least loaded server.
*Feb 28 13:51:16.023:AAA/SG/SERVER_SELECT:[4] transactions remaining in batch. Reusing
server.
.
.
.
```

Server Status Information for Named RADIUS Server Group Example

The output below shows the AAA server status for the named RADIUS server group configuration example.

```
Router# show aaa servers
RADIUS:id 8, priority 1, host 192.0.2.238, auth-port 2095, acct-port 2096
     State:current UP, duration 3781s, previous duration 0s
     Dead:total time 0s, count 0
     Quarantined:No
     Authen:request 0, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction:success 0, failure 0
     Author:request 0, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction:success 0, failure 0
     Account:request 0, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction:success 0, failure 0
     Elapsed time since counters last cleared:0m
RADIUS:id 9, priority 2, host 192.0.2.238, auth-port 2015, acct-port 2016
     State:current UP, duration 3781s, previous duration 0s
     Dead:total time 0s, count 0
     Quarantined:No
     Authen:request 0, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction:success 0, failure 0
     Author:request 0, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction:success 0, failure 0
     Account:request 0, timeouts 0
             Response:unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction:success 0, failure 0
     Elapsed time since counters last cleared:0m
Router#
```

The output shows the status of two RADIUS servers. Both servers are alive, and no requests have been processed since the counters were cleared 0 minutes ago.

Related Commands

Command	Description
debug aaa sg-server selection	Shows why the RADIUS and TACACS+ server group system in a router is selecting a particular server.
debug aaa test	Shows when the idle timer or dead timer has expired for RADIUS load balancing.
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 aaa group	Tests RADIUS load balancing server response manually.

load classification

Note Effective with Cisco IOS Release 15.2(4)M, the **load classification** command is not available in Cisco IOS software.

To load a traffic classification definition file (TCDF) for a Flexible Packet Matching (FPM) configuration, use the **load classification** command in global configuration mode. To unload all TCDFs from a specified location or a single TCDF, use the **no** form of this command.

load classification *location* **:** *filename*

no load classification *location* **:** *filename*

Syntax Description

location **:** *filename*	Location of the TCDF that is to be loaded onto the router. When used with the **no** form of this command, all TCDFs loaded from the specified filename will be unloaded. **Note** The location must be local to the routing device.

Command Default

No TCDF is loaded onto the router.

Command Modes

Global configuration

Command History

Release	Modification
12.4(6)T	This command was introduced.
15.2(4)M	This command was removed from the Cisco IOS software.

Usage Guidelines

A TCDF is an Extensible Markup Language (XML) file that you create in a text file or using an XML editor. FPM uses a TCDF to define classes of traffic and to specify actions to apply to the traffic classes for the purpose of blocking attacks on the network. Traffic classification behavior defined in a TCDF is identical to that configured using the command-line interface (CLI).

Use the **load classification** command to load the TCDF onto the routing device. The location to which you load the file must be local to the device. After the TCDF is loaded, you can use service policy CLI commands to attach the TCDF policies to a specific interface or interfaces. TCDP classes and policies, which are loaded, display as normal policies and classes when you issue a **show** command.

The TCDF requires that a relevant protocol header description file (PHDF) is already loaded onto the system through the use of the **load protocol** command. Standard PHDFs are provided with the FPM feature.

Examples

The following example shows how to create a TCDF for slammer packets (UDP 1434) for an FPM XML configuration. The match criteria defined within the **class** element is for slammer packets with an IP length not to exceed 404 (0x194) bytes, UDP port 1434 (0x59A), and pattern 0x4011010 at 224 bytes from start of the IP header. The policy “fpm-udp-policy” is defined with the action to drop slammer packets.

```
<?xml version=”1.0” encoding=”UTF-8”?
>
<tcdf
>
    <class

name
=”ip-udp”
type
=”stack”>
       <match
>
          <eq

field
=”ip.protocol”
value
=”0x11”
next
=”udp”></eq
>
       </match
>
    </c
lass
>
    <class
 name=“slammer
” type
=”access-control” match
=”all”>
       <match
>
          <eq
 field
=”udp.dest-port” value
=”0x59A”></eq
>
          <eq
 field
=”ip.length” value
=”0x194”></eq
>
          <eq
 start
=“l3-start“ offset
=”224” size
=”4” value
=”0x00401010”></eq
>
       </match
>
    </class
>
    <policy
 type=”access-control”
name
```

```
="fpm-udp-policy">
       <class

name
="slammer"></class
>
       <action
>drop</action
>
    </policy
>
</tcdf
>
```

The following example shows how to load relevant PHDFs, load the TCDF file sql-slammer.tcdf, and attach the TCDF-defined policy to the interface Ethernet 0/1:

```
enable
configure terminal
load protocol localdisk1:ip.phdf
load protocol localdisk1:tcp.phdf
load protocol localdisk1:udp.phdf
load classification localdisk1:sql-slammer.tcdf
policy-map type access-control my-policy-1
class ip-udp
service-policy fpm-udp-policy
interface Ethernet 0/1
 service-policy type access control input my-policy-1
 end
```

The following CLI output is associated with the TCDF described in the example:

```
Router# show class-map type stack
.
.
.
class-map type stack match-all ip-udp
   match field IP protocol eq 0x11 next UDP
.
.
.
Router# show class-map type access-control
.
.
.
class-map type access-control match-all slammer
   match field UDP dest-port eq 0x59A
   match field IP length eq 0x194
   match start l3-start offset 224 size 4 eq 0x4011010
.
.
.
Router show policy-map my-policy-1
.
.
.
policy-map type access-control my-policy-1
  class slammer
    drop
.
.
.
```

Related Commands

Command	Description
load protocol	Loads a protocol header description file (PHDF) onto a router.

local-address

To limit the scope of an Internet Security Association and Key Management Protocol (ISAKMP) profile or an ISAKMP keyring configuration to a local termination address or interface, use the **local-address**command in ISAKMP profile configuration and keyring configuration modes. To remove the local address or interface, use the **no** form of this command.

local-address {*interface-name*| *ip-address* [*vrf-tag*]}

no local-address {*interface-name*| *ip-address* [*vrf-tag*]}

Syntax Description

interface-name	Name of the local interface.
ip-address	Local termination address.
vrf-tag	(Optional) Scope of the IP address will be limited to the VRF instance.

Command Default

If this command is not configured, the ISAKMP profile or ISAKMP keyring is available to all local addresses.

Command Modes

ISAKMP profile configuration Keyring configuration

Command History

Release	Modification
12.3(14)T	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.

Examples

The following example shows that the scope of the ISAKMP profile is limited to interface serial2/0:

```
crypto isakmp profile profile1
  keyring keyring1
  match identity address 10.0.0.0 255.0.0.0
  local-address serial2/0
```

The following example shows that the scope of the ISAKMP keyring is limited only to interface serial2/0:

```
crypto keyring
  local-address serial2/0
  pre-shared-key address 10.0.0.1
```

The following example shows that the scope of the ISAKMP keyring is limited only to IP address 10.0.0.2:

```
crypto keyring keyring1
```

```
  local-address 10.0.0.2
  pre-shared-key address 10.0.0.2 key
```

The following example shows that the scope of an ISAKMP keyring is limited to IP address 10.34.35.36 and that the scope is limited to VRF examplevrf1:

```
ip vrf examplevrf1
  rd 12:3456
crypto keyring ring1
  local-address 10.34.35.36 examplevrf1
interface ethernet2/0
  ip vrf forwarding examplevrf1
  ip address 10.34.35.36 255.255.0.0
```

Related Commands

Command	Description
crypto isakmp profile	Defines an ISAKMP profile and audits IPSec user sessions.
crypto keyring	Defines a keyring and enters keyring configuration mode.

local-port (WebVPN)

To remap (forward) an application port number in a port forwarding list, use the **local-port** command in webvpn port-forward list configuration mode. To remove the application port mapping from the forwarding list, use the **no** form of this command.

local-port *number* **remote-server** *name* **remote-port** *number* **description** *text-string*

no local-port *number*

Syntax Description

number	Configures the port number to which the local application is mapped. Valid values are 1 to 65535.
remote-server *name*	Identifies the remote server. An IPv4 address or fully qualified domain name is entered.
remote-port *number*	Specifies the well-known port number of the application, for which port-forwarding is to be configured. Valid values are 1 to 65535.
description *text-string*	Configures a description for this entry in the port-forwarding list. The text string is displayed on the end-user applet window. A text string up to 64 characters in length is entered.

Command Default

An application port number is not remapped.

Command Modes

Webvpn port-forward list configuration (config-webvpn-port-fwd)

Command History

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

Usage Guidelines

The **local-port** command is configured to add an entry to the port-forwarding list. The forward list is created with the **port-forward** command in webvpn context configuration mode. The remote port number is the well-known port to which the application listens. The local port number is the entry configured in the port forwarding list. A local port number can be configured only once in a given port-forwarding list.

Examples

The following example configures port forwarding for well-known e-mail application port numbers:

```
Router(config)# webvpn context context1
Router(config-webvpn-context)# port-forward EMAIL

Router(config-webvpn-port-fwd)# local-port 30016 remote-server mail.company.com remote-port
 110 description POP3

Router(config-webvpn-port-fwd)# local-port 30017 remote-server mail.company.com remote-port
 25 description SMTP

Router(config-webvpn-port-fwd)# local-port 30018 remote-server mail.company.com remote-port
 143 description IMAP
```

Related Commands

Command	Description
port-forward	Enters webvpn port-forward list configuration mode to configure a port-forwarding list.
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

local priority

To set the local key server priority, use the **local priority**command in GDOI redundancy configuration mode. To remove the local key server priority that was set, use the **no** form of this command.

local priority *number*

no local priority *number*

Syntax Description

number	Priority number of the local server. Value = 1 through 255.

Command Default

If the local priority is not set by this command, the local priority defaults to 1.

Command Modes

GDOI redundancy configuration (gdoi-coop-ks-config)

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 Aggregation Services Series Routers.

Usage Guidelines

Configure the priority to determine the order of preference of the key servers (the higher priority device becomes the primary key server). If the priority of two devices is the same, the IP address is used to set the priority. The higher the IP address, the higher the priority.

Note If the **no local priority** option is configured, the default value of 1 is set for that key server.

Examples

The following example shows that the key server 10.1.1.1 has the highest priority and, therefore, becomes the primary key server:

```
address ipv4 10.1.1.1
redundancy
 local priority 10
 peer address ipv4 10.41.2.5
```

peer address ipv4 10.33.5.6

```
address ipv4 10.41.2.5
```

```
redundancy
 peer address ipv4 10.1.1.1
```

peer address ipv4 10.33.5.6

```
address ipv4 10.33.5.6
redundancy
 local priority 5
 peer address ipv4 10.41.2.5
```

peer address ipv4 10.1.1.1

Related Commands

Command	Description
address ipv4	Sets the source address, which is used as the source for packets originated by the local key server.
peer address ipv4	Configures a GDOI redundant peer key server.
redundancy	Enters GDOI redundancy configuration mode and allows for peer key server redundancy.
server local	Designates a device as a GDOI key server and enters GDOI local server configuration mode.

lockdown (LSP Attributes)

To disable reoptimization of the label switched path (LSP), use the **lockdown** command in LSP Attributes configuration mode. To reenable reoptimization, use the **no** form of this command.

lockdown

no lockdown

Syntax Description

This command has no arguments or keywords.

Command Default

Reoptimization of the LSP is enabled.

Command Modes

LSP Attributes configuration (config-lsp-attr)

Command History

Release	Modification
12.0(26)S	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.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.

Usage Guidelines

Use this command to set up in an LSP attribute list the disabling of reoptimization of an LSP triggered by a timer, or the issuance of the **mpls traffic-eng reoptimize** command, or a configuration change that requires the resignalling of an LSP.

To associate the LSP lockdown attribute and the LSP attribute list with a path option for an LSP, you must configure the **tunnel mpls traffic-eng path option** command with the **attributes** *string* keyword and argument, where *string* is the identifier for the specific LSP attribute list.

Examples

The following example shows how to configure disabling of reoptimization in an LSP attribute list:

```
Configure terminal
!
mpls traffic-eng lsp attributes 4
 bandwidth 1000
 priority 1 1
 lockdown
 end
```

Related Commands

Command	Description
mpls traffic-eng lsp attributes	Creates or modifies an LSP attribute list.
show mpls traffic-eng lsp attributes	Displays global LSP attribute lists.

log (policy-map)

To generate a log of messages, use the **log** command in policy-map configuration mode. To disable the log, use the **no** form of this command.

log

no log

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Policy-map configuration

Command History

Release	Modification
12.4(6)T	This command was introduced in Cisco IOS Release 12.4(6)T.
12.4(20)T	This command was modified in Cisco IOS Release 12.4(20)T. This command can now be used after entering the **policy-map type inspect smtp**.

Usage Guidelines

You can use this command only after entering the following commands:

- **policy-map type inspect http**
- **policy-map type inspect imap**
- **policy-map type inspect smtp**

Examples

The following example generates a log of messages:

```
policy-map type inspect http mypolicy
 log
```

Related Commands

Command	Description
policy-map type inspect http	Creates a Layer 7 HTTP policy map.
policy-map type inspect imap	Creates a Layer 7 IMAP policy map.
policy-map type inspect smtp	Create a Layer 7 SMTP policy map

log (parameter-map type)

To log the firewall activity for an inspect parameter map, use the **log** command in parameter-map type inspect configuration mode.

log {**dropped-packets** {**disable**| **enable**}| **summary** [**flows** *number*] [**time-interval** *seconds*]}

Syntax Description

dropped-packets	Logs the packets dropped by the firewall.
disable | enable	Disables or enables logging the dropped packets.
summary	Turns on the summary of the packets dropped during the firewall activity for interzone and intrazone traffic.
flows *number*	(Optional) Specifies the number of flows for which the summary logs must be printed. The default flow is 16.
time-interval *seconds*	(Optional) Specifies the time interval, in seconds. which the summary logs must be printed. The default is 60.

Command Default

The firewall activity is not captured.

Command Modes

Parameter-map type inspect configuration (config-profile)

Command History

Release	Modification
15.1(1)T	This command was introduced.
Cisco IOS-XE 2.4	This command was integrated into Cisco IOS-XE Release 2.4.

Usage Guidelines

Use this command to log the firewall activity as follows:

- Time interval for the summary logs
- Display the protocol information in the summary logs
- Enable summary logs for the specified flows

If the flow is specified as zero as **log summary flow 0**, the log activity is turned off and summary logs are not printed until the flow count is greater than zero.

To display the summary logs, use the **show policy-firewall summary-log** and **clear policy-firewall summary-log** to clear the summary logs.

Examples

The following examples show how to configure the summary logs in two scenarios.

In the following example, the summary logs are printed for 40 flows every 2 minutes:

```
Router(config)# parameter-map type inspect global
Router(config-profile)# log summary flows 40 time-interval 120
In the following example, the summary logs are printed for 30 flows at the default time
interval of 1 minute:
Router(config)# parameter-map type inspect global
Router(config-profile)# log summary flows 30
In the above example, the flow is not configured. Hence, the summary logs are printed by
default for 16 flows every 30 seconds:
Router(config)# parameter-map type inspect global
Router(config-profile)# log summary time-interval 30
```

Related Commands

Command	Description
clear policy-firewall	Clears the information collected by the firewall.
parameter-map type inspect	Defines an inspect type parameter map.
pass	Allows packets to be sent to the router without being inspected.
show policy-firewall summary-log	Displays the summary log of the firewall.

log (type access-control)

Note Effective with Cisco IOS Release 15.2(4)M, the **log** command is not available in Cisco IOS software.

To generate log messages for a predefined traffic class, use the **log** command in policy-map class configuration mode. To disable the log, use the **no** form of this command.

log [all]

no log [all]

Syntax Description

all	(Optional) Logs the entire stream of discarded packets belonging to the traffic class.

Command Default

Log messages are disabled.

Command Modes

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

Command History

Release	Modification
15.1(3)T	This command was introduced.
15.2(4)M	This command was removed from the Cisco IOS software.

Usage Guidelines

If the **log** command is specified with the **all** keyword, then this command can only be used with a predefined session-based Flexible Packet Matching (FPM) traffic class that was created with the **class-map type access-control** command.

The **log all** command is used when configuring a policy map that can be attached to one or more interfaces to specify a service policy that is created with the **policy-map type access-control** command.

Examples

The following example shows how to configure a class map and policy map to specify the protocol stack class, the match criteria and action to take, and a combination of classes using session-based (flow-based) and nonsession-based actions. The **log** command **all** keyword is associated with the action taken on the policy.

```
Router(config)# class-map type access-control match-all my-HTTP
Router(config-cm)# match field tcp destport eq 8080
Router(config-cm)# match start tcp payload-start offset 20 size 10 regex “GET”
Router(config)# class-map type access-control match-all my-FTP
Router(config-cmap)# match field tcp destport eq 21
Router(config)# class-map type access-control match all class1
Router(config-cmap)# match class my-HTTP session
Router(config-cmap)# match start tcp payload-start offset 40 size 20 regex "abc.*def"
Router(config)# policy-map type access-control my_http_policy
Router(config-pmap)# class class1
Router(config-pmap-c)# log all
Router(config)# interface gigabitEthernet 0/1
Router(config-if)# service-policy type access-control input my_http_policy
```

Related Commands

Command	Description
class	Specifies the name of a predefined traffic class, which was configured with the **class-map** command. This command also classifies traffic to the traffic policy and enters policy-map class configuration mode.
class-map type access-control	Creates a class map to be used for matching packets to a specified class and enters class map configuration mode for determining the exact pattern to look for in the protocol stack of interest.
drop	Configures a traffic class to discard packets belonging to a specific class.
match class session	Configures match criteria for a class map used to identify a session (flow) containing packets of interest, which is then applied to all packets transmitted during the session.
policy-map type access-control	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy, and enters policy-map configuration mode.
show class-map	Displays all class maps and their matching criteria.
show policy-map	Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps.
show policy-map interface	Displays the packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific PVC on the interface.

logging (parameter-map)

To enable the logging of content scan events, use the **logging** command in privileged EXEC mode. To disable logging, use the **no** form of this command.

logging

no logging

Syntax Description

This command has no arguments or keywords.

Command Default

Logging of events is disabled.

Command Modes

Parameter-map type inspect configuration (config-profile)

Command History

Release	Modification
15.2(1)T1	This command was introduced.

Usage Guidelines

You must configure the **parameter-map type content-scan global** before you configure the **logging** command.

All content scan-related syslog displays the username, group name, IP address, and port number of the source and destination.

Examples

The following example shows how to enable logging of content scan events:

```
Router(config)# parameter-map type content-scan global
Router(config-profile)# logging
Router(config-profile)# end
```

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.

logging dmvpn

To display Dynamic Multipoint VPN (DMVPN)-specific system logging information, use the **logging dmvpn**command in global configuration mode. To turn off logging, use the **no** form of this command.

logging dmvpn [**rate-limit** *rate*]

no logging dmvpn [**rate-limit** *rate*]

Syntax Description

rate-limit *rate*	(Optional) Specifies the number of DMVPN syslog messages generated per minute. The range is from 1 to 10000. • The default rate is to generate 600 messages per minute.

Command Default

DMVPN system logging messages are not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(9)T	This command was introduced.
Cisco IOS XE Release 2.5	This command was integrated into Cisco IOS XE Release 2.5.
15.0(1)M	This command was modified. The *rate*argument was modified to specify the number of DMVPN syslog messages per minute.

Usage Guidelines

Use the **logging dmvpn rate-limit** *rate*command to specify the rate at which the DMVPN-specific syslog messages are displayed. In Cisco IOS Release 12.4(24)T and earlier releases, the *rate* argument specifies the minimum interval, in seconds, between two DMVPN syslog messages, with a range of 0 to 3600, and a default value of 60.

In Cisco IOS Release 15.0(1)M and later releases, the *rate* argument specifies the number of DMVPN syslog messages per minute. If you have upgraded to Release Cisco IOS 15.0(1)M or later releases, you must reconfigure the DMVPN rate limit settings.

Examples

The following example shows how to configure the router to display five DMVPN-specific syslog messages per minute:

```
Router> enable
Router# configure terminal
Router(config)# logging dmvpn rate-limit 5
```

The following example shows a sample system log with DMVPN messages:

```
%DMVPN-7-CRYPTO_SS: Tunnel101-192.0.2.1 socket is UP
%DMVPN-5-NHRP_NHS: Tunnel101 192.0.2.251 is UP
%DMVPN-5-NHRP_CACHE: Client 192.0.2.2 on Tunnel1 Registered.
%DMVPN-5-NHRP_CACHE: Client 192.0.2.2 on Tunnel101 came UP.
%DMVPN-3-NHRP_ERROR: Registration Request failed for 192.0.2.251 on Tunnel101
```

Related Commands

Command	Description
debug dmvpn	Debugs DMVPN sessions.

logging enabled

To enable syslog messages, use the **logging enabled**command in parameter-map-type consent configuration mode.

logging enabled

Syntax Description

This command has no arguments or keywords.

Command Default

Logging messages are not enabled.

Command Modes

Parameter-map-type consent (config-profile)

Command History

Release	Modification
12.4(15)T	This command was introduced.

Usage Guidelines

After the **logging enabled** command is entered, a log entry (a syslog), including the client's IP address and the time, is created everytime a response is received for the consent web page.

Examples

The following example shows how to define the consent-specific parameter map "consent_parameter_map" and a default consent parameter map. In both parameter maps, logging is enabled.

```
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
```

logging ip access-list cache (global configuration)

To configure the Optimized ACL Logging (OAL) parameters, use the **logging ip access-list cache** command in global configuration mode. To return to the default settings, use the **no** form of this command.

logging ip access-list cache {**entries** *entries*| **interval** *seconds*| **rate-limit** *pps*| **threshold** *packets*}

no logging ip access-list cache [**entries**| **interval**| **rate-limit**| **threshold**]

Syntax Description

entries *entries*	Specifies the maximum number of log entries that are cached in the software; valid values are from 0 to 1048576 entries.
interval *seconds*	Specifies the maximum time interval before an entry is sent to syslog; valid values are from 5 to 86400 seconds.
rate-limit *pps*	Specifies the number of packets that are logged per second in the software; valid values are from 10 to 1000000 pps.
threshold *packets*	Specifies the number of packet matches before an entry is sent to syslog; valid values are from 1 to 1000000 packets.

Command Default

The defaults are as follows:

- *entries* --**8000** entries.
- *seconds* --**300** seconds (5 minutes).
- **rate-limit** *pps* --**0** (rate limiting is off) and all packets are logged.
- **threshold** *packets* --**0** (rate limiting is off) and the system log is not triggered by the number of packet matches.

Command Modes

Global configuration

Command History

Release	Modification
12.2(17d)SXB	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 Supervisor Engine 720 only.

OAL is supported on IPv4 unicast traffic only.

You cannot configure OAL and VACL capture on the same chassis. OAL and VACL capture are incompatible. With OAL configured, use SPAN to capture traffic.

If the entry is inactive for the duration that is specified in the **update-interval** *seconds* command, th e entry is removed from the cache.

If you enter the **no logging ip access-list cache** command without keywords, all the parameters are returned to the default values.

You must set ICMP unreachable rate limiting to 0 if the OAL is configured to log denied packets.

When enabling the IP "too short" check using the mls verify ip length minimum command, valid IP packets with with an IP protocol field of ICMP(1), IGMP(2), IP(4), TCP(6), UDP(17), IPv6(41), GRE(47), or SIPP-ESP(50) will be hardware switched. All other IP protocol fields are software switched.

Caution Using optimized access-list logging (OAL) and the mls verify ip length minimum command together can cause routing protocol neighbor flapping as they are incompatible

Examples

This example shows how to specify the maximum number of log entries that are cached in the software:

```
Router(config)#
logging ip access-list cache entries 200
```

This example shows how to specify the maximum time interval before an entry is sent to the system log:

```
Router(config)#
logging ip access-list cache interval 350
```

This example shows how to specify the number of packets that are logged per second in the software:

```
Router(config)#
logging ip access-list cache rate-limit 100
```

This example shows how to specify the number of packet matches before an entry is sent to the system log:

```
Router(config)#
logging ip access-list cache threshold 125
```

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 (interface configuration)	Enables an OAL-logging cache on an interface that is based on direction.
show logging ip access-list	Displays information about the logging IP access list.

Command	Description
update-interval *seconds*	Removes entries from the cache that are inactive for the duration that is specified in the command.

logging ip access-list cache (interface configuration)

To enable an Optimized ACL Logging (OAL)-logging cache on an interface that is based on direction, use the **logging ip access-list cache** command in interface configuration mode. To disable OAL, use the **no** form of this command.

logging ip access-list cache [**in**| **out**]

no logging ip access-list cache

Syntax Description

in	(Optional) Enables OAL on ingress packets.
out	(Optional) Enables OAL on egress packets.

Command Default

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
12.2(17d)SXB	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 Supervisor Engine 720 only.

This command is supported on traffic that matches the **log** keyword in the applied ACL. You must set ICMP unreachable rate limiting to 0 if the OAL is configured to log denied packets.

On systems that are configured with a PFC3A, support for the egress direction on tunnel interfaces is not supported.

OAL is supported on IPv4 unicast traffic only.

You cannot configure OAL and VACL capture on the same chassis. OAL and VACL capture are incompatible. With OAL configured, use SPAN to capture traffic.

If the entry is inactive for the duration that is specified in the **update-interval** *seconds* command, th e entry is removed from the cache.

If you enter the **no logging ip access-list cache** command without keywords, all the parameters are returned to the default values.

When enabling the IP "too short" check using the mls verify ip length minimum command, valid IP packets with with an IP protocol field of ICMP(1), IGMP(2), IP(4), TCP(6), UDP(17), IPv6(41), GRE(47), or SIPP-ESP(50) will be hardware switched. All other IP protocol fields are software switched.

Caution Using optimized access-list logging (OAL) and the mls verify ip length minimum command together can cause routing protocol neighbor flapping as they are incompatible

Examples

This example shows how to enable OAL on ingress packets:

```
Router(config-if)#
logging ip access-list cache in
```

This example shows how to enable OAL on egress packets:

```
Router(config-if)#
logging ip access-list cache out
```

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.
show logging ip access-list	Displays information about the logging IP access list.
update-interval *seconds*	Removes entries from the cache that are inactive for the duration that is specified in the command.

login authentication

To enable authentication, authorization, and accounting (AAA) authentication for logins, use the **login authentication**command inline configuration mode. To return to the default specified by the aaa authentication login command, use the **no** form of this command.

login authentication {**default**| *list-name*}

no login authentication {**default**| *list-name*}

Syntax Description

default	Uses the default list created with the **aaa authentication login** command.
list-name	Uses the indicated list created with the **aaa authentication login**command.

Command Default

Uses the default set with **aaa authentication login**.

Command Modes

Line configuration

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.

Usage Guidelines

This command is a per-line command used with AAA that specifies the name of a list of AAA authentication methods to try at login. If no list is specified, the default list is used (whether or not it is specified in the command line).

Caution If you use a *list-name* value that was not configured with the **aaa authentication login**command, you will disable login on this line.

Entering the **no** version of **login authentication** has the same effect as entering the command with the **default** keyword.

Before issuing this command, create a list of authentication processes by using the global configuration **aaa authentication login**command.

Examples

The following example specifies that the default AAA authentication is to be used on line 4:

```
line 4
 login authentication default
```

The following example specifies that the AAA authentication list called *list1*is to be used on line 7:

```
line 7
 login authentication list1
```

Related Commands

Command	Description
aaa authentication login	Sets AAA authentication at login.

login block-for

To configure your Cisco IOS device for login parameters that help provide denial-of-service (DoS) detection, use the **login block-for**command in global configuration mode. To disable the specified login parameters and return to the default functionality, use the **no** form of this command.

login block-for *seconds* **attempts** *tries* **within** *seconds*

no login block-for

Syntax Description

seconds	Duration of time in which login attempts are denied (also known as a quiet period) by the Cisco IOS device. Valid values range from 1 to 65535 (18 hours) seconds.
attempts *tries*	Maximum number of failed login attempts that triggers the quiet period. Valid values range from 1 to 65535 tries.
within *seconds*	Duration of time in which the allowed number of failed login attempts must be made before the quiet period is triggered. Valid values range from 1 to 65535 (18 hours) seconds.

Command Default

No login parameters are defined.

A quiet period is not enabled.

Command Modes

Global configuration (config)

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).
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

If the specified number of connection attempts (via the **attempts** *tries* option) fail within a specified time (via the **within** *seconds* option), the Cisco IOS device will not accept any additional login attempts for a specified period of time (via the *seconds* argument).

All login parameters are disabled by default. You must issue the **login block-for** command, which enables default login functionality, before using any other login commands. After the **login block-for** command is enabled, the following defaults are enforced:

- A default login delay of 1 second
- All login attempts made via Telnet and secure shell (SSH) are denied during the quiet period; that is, no access control lists (ACLs) are exempt from the login period until the **login quiet-mode access-class** command is issued. If this command is not configured, then the default ACL **sl_def_acl** is created on the router. This ACL is hidden in the running configuration. Use the **show access-list sl_def_acl** to view the parameters for the default ACL.

For example:

```
Router#show access-lists sl_def_acl
Extended IP access list sl_def_acl
    10 deny tcp any any eq telnet
    20 deny tcp any any eq www
    30 deny tcp any any eq 22
    40 permit ip any any
```

System Logging Messages

The following logging message is generated after the router switches to quiet mode:

```
00:04:07:%SEC_LOGIN-1-QUIET_MODE_ON:Still timeleft for watching failures is 158 seconds,
[user:sfd] [Source:10.4.2.11] [localport:23] [Reason:Invalid login], [ACL:22] at 16:17:23
UTC Wed Feb 26 2003
```

The following logging message is generated after the router switches from quiet mode back to normal mode:

```
00:09:07:%SEC_LOGIN-5-QUIET_MODE_OFF:Quiet Mode is OFF, because block period timed out at
16:22:23 UTC Wed Feb 26 2003
```

Examples

The following example shows how to configure your router to block all login requests for 100 seconds if 15 failed login attempts are exceeded within 100 seconds. Thereafter, the **show login** command is issued to verify the login settings.

```
Router(config)# login block-for 100 attempts 15 within 100
Router(config)# exit
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 example shows how to disable login parameters. Thereafter, the **show login** command is issued to verify that login parameters are no longer configured.

```
Router(config)# no login block-for
Router(config)# exit
```

```
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
```

Related Commands

Command	Description
login delay	Configures a uniform delay between successive 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 login	Displays login parameters.

login delay

To configure a uniform delay between successive login attempts, use the **login delay**command in global configuration mode. To return to the default functionality (which is a 1 second delay), use the **no** form of this command.

login delay *seconds*

no login delay

Syntax Description

seconds	Number of seconds between each login attempt. Valid values range from 1 to 10 seconds.

Command Default

If this command is not enabled, a login delay of 1 second is automatically enforced.

Command Modes

Global configuration (config)

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

A Cisco IOS device can accept connections (such as Telnet, secure shell (SSH), and HTTP) as fast as they can be processed. The **login delay** command introduces a uniform delay between successive login attempts. (The delay occurs for all login attempts--failed or successful attempts.) Thus, user users can better secure their Cisco IOS device from dictionary attacks, which are an attempt to gain username and password access to your device.

Although the **login delay** command allows users to configure a specific a delay, a uniform delay of 1 second is enabled if the **auto secure** command is issued. After the **auto secure** command is enabled, the autosecure dialog prompts users for login parameters; if login parameters have already been configured, the autosecure dialog will retain the specified values.

Examples

The following example shows how to configure your router to issue a delay of 10 seconds between each successive login attempt:

```
Router(config)# login delay 10
```

Related Commands

Command	Description
auto secure	Secures the management and forwarding planes of the router.
login block-for	Configures your Cisco IOS device for login parameters that help provide DoS detection.
show login	Displays login parameters.

login-message

To configure a login message for the text box on the user login page, use the **login-message** command in webvpn context configuration mode. To reconfigure the SSL VPN context configuration to display the default message, use the **no** form of this command.

login-message [*message-string*]

no login-message [*message-string*]

Syntax Description

message-string	*(Optional) Login message string up to 255 characters in length. The string value may contain 7-bit ASCII values, HTML tags, and escape sequences.*

Command Default

The following message is displayed if this command is not configured or if the **no** form is entered:

“Please enter your username and password”

Command Modes

Webvpn context configuration

Command History

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

Usage Guidelines

The optional form of this command is used to change or enter a login message. A text string up to 255 characters in length can be entered. The **no** *form of this command is entered to configure the default message to be displayed. When the* **login-message** *command is entered without the optional text string, no login message is displayed.*

Examples

The following example changes the default login message to “Please enter your login credentials”:

```
Router(config)#
webvpn context context1

Router(config-webvpn-context)# login-message “Please enter your login credentials”
```

Related Commands

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

login quiet-mode access-class

To specify an access control list (ACL) that is to be applied to the router when the router switches to quiet mode, use the **login quiet-mode access-class**command in global configuration mode. To remove this ACL and allow the router to deny all login attempts, use the **no** form of this command.

login quiet-mode access-class {*acl-name*| *acl-number*}

no login quiet-mode access-class {*acl-name*| *acl-number*}

Syntax Description

acl-name	Named ACL that is to be enforced during quiet mode.
acl-number	Numbered (standard or extended) ACL that is to be enforced during quiet mode.

Command Default

All login attempts via Telnet, secure shell (SSH), and HTTP are denied.

Command Modes

Global configuration (config)

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

Before using this command, you must issue the **login block-for** command, which allows you to specify the necessary parameters to enable a quiet period.

- Use the **login quiet-mode access-class** command to selectively allow hosts on the basis of a specified ACL. You may use this command to grant an active client or list of clients an infinite number of failed attempts that are not counted by the router; that is, the active clients are placed on a “safe list” that allows them access to the router despite a quiet period. If this command is not configured, then the default ACL **sl_def_acl** is created on the router. This ACL is hidden in the running configuration. Use the **show access-list sl_def_acl** to view the parameters for the default ACL.

For example:

```
Router#show access-lists sl_def_acl
Extended IP access list sl_def_acl
10 deny tcp any any eq telnet
20 deny tcp any any eq www
30 deny tcp any any eq 22
40 permit ip any any
```

System Logging Messages

The following logging message is generated after the router switches to quiet mode:

```
00:04:07:%SEC_LOGIN-1-QUIET_MODE_ON:Still timeleft for watching failures is 158 seconds,
[user:sfd] [Source:10.4.2.11] [localport:23] [Reason:Invalid login], [ACL:22] at 16:17:23
UTC Wed Feb 26 2003
```

The following logging message is generated after the router switches from quiet mode back to normal mode:

```
00:09:07:%SEC_LOGIN-5-QUIET_MODE_OFF:Quiet Mode is OFF, because block period timed out at
16:22:23 UTC Wed Feb 26 2003
```

Examples

The following example shows how to configure your router to accept hosts only from the ACL “myacl” during the next quiet period:

```
Router(config)# login quiet-mode access-class myacl
```

Related Commands

Command	Description
login block-for	Configures your Cisco IOS device for login parameters that help provide DoS detection.
show login	Displays login parameters.

login-photo

To set the photo parameters on a Secure Socket Layer Virtual Private Network (SSL VPN) login page, use the **login-photo** command in web vpn context configuration mode. To display the login page with no photo but with a message that spans the message and the photo columns, use the **no** form of this command.

login-photo [**file** *file-name*| **none**]

no login-photo

Syntax Description

file *file-name*	Points to a file to be displayed on the login page. The *file-name* argument can be **jpeg**, **bitmap**, or **gif**. However, gif files are recommended.
none	No photo appears on the login page.

Command Default

No photo appears, and the message spans the two columns (message and photo columns).

Command Modes

Webvpn context configuration (config-webvpn-context)

Command History

Release	Modification
12.4(15)T	This command was introduced.

Usage Guidelines

To display no photo, use the **login-photo none** option. To display no photo and have the message span both columns (message column and photo column), use the **no login-photo** option.

The best resolution for login photos is 179 x 152 pixels.

Examples

The following example shows that no photo is displayed:

```
Router (config)# webvpn context
Router (config-webvpn-context)# login-photo none
```

Related Commands

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

logo

To configure a custom logo to be displayed on the login and portal pages of an SSL VPN, use the **logo** command in SSLVPN configuration mode. To configure the Cisco logo to be displayed, use the **no** form of this command.

logo [**file** *filename*| **none**]

no logo [**file** *filename*| **none**]

Syntax Description

file *filename*	(Optional) Specifies the location of an image file. A gif, jpg, or png file can be specified. The file can be up to 100 KB in size. The name of the file can be up 255 characters in length.
none	(Optional) No logo is displayed.

Command Default

The Cisco logo is displayed if the **no** form of this command is not configured or if the **no** form is entered.

Command Modes

SSLVPN configuration

Command History

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

Usage Guidelines

The source image file for the logo is a gif, jpg, or png file that is up to 255 characters in length (filename) and up to 100 kilobytes (KB) in size. The file is referenced from a local file system, such as flash memory. An error message will be displayed if the file is not referenced from a local file system. No logo will be displayed if the image file is removed from the local file system.

Examples

The following example references mylogo.gif (from flash memory) to use as the SSL VPN logo:

```
Router(config)#
webvpn context SSLVPN

Router(config-webvpn-context)#
logo file flash:/mylogo.gif

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

In the following example, no logo is to be displayed on the login or portal pages:

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

```
Router(config-webvpn-context)#
logo none
Router(config-webvpn-context)#
```

The following example configures the SSL VPN to display the default logo (Cisco) on the login and portal pages:

```
Router(config)#
webvpn context SSLVPN

Router(config-webvpn-context)#
logo none
Router(config-webvpn-context)#
```

Related Commands

Command	Description
webvpn context	Enters SSLVPN configuration mode to configure the WebVPN context.