Cisco IOS Security Command Reference: Commands D to L - ip source-track through ivrf [Support]

Published: 2025-11-27 · Archived: 2026-04-05 17:02:01 UTC

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.

Release	Modification
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

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 client algorithm encryption

To define the order of encryption algorithms in a Cisco IOS secure shell (SSH) client, use the ip ssh {server | client} algorithm encryption command in global configuration mode. To disable an algorithm from the configured list, use the no form of this command. To return to the default behavior in which all encryption algorithms are enabled in the predefined order, use the default form of this command.

ip ssh client algorithm encryption {aes128-ctr | aes192-ctr | aes256-ctr | aes128-cbc | 3des-cbc | aes192-cbc | aes256-cbc}

no ip ssh client algorithm encryption {aes128-ctr | aes192-ctr | aes256-ctr | aes128-cbc | 3des-cbc | aes192-cbc | aes256-cbc}

Syntax Description

aes128-ctr	Configures Advanced Encryption Standard Counter Mode (AES-CTR) encryption for 128-bit key length.

aes192-ctr	Configures AES-CTR encryption for 192-bit key length.
aes256-ctr	Configures AES-CTR encryption for 256-bit key length.
aes128-cbc	Configures AES Cipher Block Chaining (AES-CBC) 128-bit key length.
3des-cbc	Configures Triple Data Encryption Standard (3DES) CBC algorithm.
aes192-cbc	Configures AES-CBC encryption for 192-bit key length.
aes256-cbc	Configures AES-CBC encryption for 256-bit key length.

Command Default

SSH encryption algorithms are set to the following default order:

```
Encryption Algorithms: aes128-ctr, aes192-ctr, aes256-ctr, aes128-cbc, 3des-cbc, aes192-cbc, aes256-cbc
```

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS 15.5(2)S	This command was introduced.
Cisco IOS XE 3.15S	This command was integrated into Cisco IOS XE Release 3.15S.

Release	Modification
Cisco IOS 15.5(2)T	This command was integrated into Cisco IOS Release 15.5(2)T.

Usage Guidelines

To start an encrypted session between an SSH client and server, the preferred mode of encryption needs to be decided. For increased security, the preferred crypto algorithm for an SSH session is AES-CTR.

SSH Version 2 (SSHv2) supports AES-CTR encryption for 128-bit, 192-bit, and 256-bit key length. From the supported AES-CTR algorithms, the preferred algorithm is chosen based on the processing capability. The greater the length of the key, the stronger the encryption.

The Cisco IOS SSH servers and clients support three types of crypto algorithms to encrypt data and select an encryption mode in the following order of preferred encryption:

1. AES-CTR
2. AES-CBC
3. 3DES

If the SSH session uses a remote device that does not support AES-CTR encryption mode, the encryption mode for the session falls back to AES-CBC mode.

The default order of the encryption algorithms are:

```
Encryption Algorithms: aes128-ctr, aes192-ctr, aes256-ctr, aes128-cbc, 3des-cbc, aes192-cbc, aes256-cbc
```

To disable more than one algorithm, use the no form of the command multiple times with different algorithm names. If you try to disable the last encryption algorithm in the configuration, the following message is displayed, and the command is rejected:

```
% SSH command rejected: All encryption algorithms cannot be disabled
```

Examples

The following example shows how to configure encryption algorithms on Cisco IOS SSH clients:

```
Device> enable
Device# configure terminal
Device(config)# ip ssh client algorithm encryption aes128-ctr aes192-ctr aes256-ctr aes128-cbc 3des-cbc aes192-c
Device(config)# end
```

The following example shows how to return to the default behavior in which all encryption algorithms are enabled in the predefined order:

```
 Device> enable
Device# configure terminal
Device(config)# default ip ssh client algorithm encryption
Device(config)# end
```

Related Commands

Command	Description
ip ssh client algorithm mac	Defines the order of MAC algorithms in a Cisco IOS SSH client.
ip ssh server algorithm encryption	Defines the order of encryption algorithms in a Cisco IOS SSH server.
show ip ssh	Displays the status of SSH server connections.

ip ssh client algorithm mac

To define the order of Message Authentication Code (MAC) algorithms in a Cisco IOS secure shell (SSH) client, use the ip ssh client algorithm mac command in global configuration mode. To disable an algorithm from the configured list, use the no form of this command. To return to the default behavior in which all MAC algorithms are enabled in the predefined order, use the default form of this command.

ip ssh client algorithm mac { hmac-sha2-256-etm@openssh.com | hmac-sha2-512-etm@openssh.com | hmac-sha2-256 | hmac-sha2-512 }

no ip ssh client algorithm mac { hmac-sha2-256-etm@openssh.com | hmac-sha2-512-etm@openssh.com | hmac-sha2-256 | hmac-sha2-512 }

Syntax Description

hmac-sha2-256	Configures the HMAC algorithm of HMAC-SHA2-256 as a cryptographic algorithm with a digest size of 256 bits and a key length of 256 bits.
hmac-sha2-512	Configures the HMAC algorithm of HMAC-SHA2-512 as a cryptographic algorithm with a digest size of 512 bits and a key length of 512 bits.
hmac-sha2-256-etm@openssh.com	Configures the HMAC algorithm of HMAC-SHA2-256-Encrypt-then-MAC@openssh.com as a cryptographic algorithm with a digest size of 256 bits and a key length of 256 bits.
hmac-sha2-512-etm@openssh.com	Configures the HMAC algorithm of HMAC-SHA2-512-Encrypt-then-MAC@openssh.com as a cryptographic algorithm with a digest size of 512 bits and a key length of 512 bits.

Command Default

SSH MAC algorithms are set to the following default order:

```
MAC Algorithms: hmac-sha2-256-etm@openssh.com, hmac-sha2-512-etm@openssh.com, hmac-sha2-256, hmac-sha2-512
```

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS 15.5(2)S	This command was introduced.

Release	Modification
Cisco IOS XE 3.15S	This command was integrated into Cisco IOS XE Release 3.15S.
Cisco IOS 15.5(2)T	This command was integrated into Cisco IOS Release 15.5(2)T.
Cisco IOS XE 17.3	The hmac-sha2-256-ETM@openssh.com and hmac-sha2-512-ETM@openssh.com were introduced.

Usage Guidelines

The Cisco IOS SSH servers and clients must have at least one configured Hashed Message Authentication Code (HMAC) algorithm. The Cisco IOS SSH servers and clients support the MAC algorithms in the following order:

1. hmac-sha2-256-etm@openssh.com
2. hmac-sha2-512-etm@openssh.com
3. hmac-sha2-256
4. hmac-sha2-512

The default order of the MAC algorithms are:

```
MAC Algorithms:hmac-sha2-256-etm@openssh.com,hmac-sha2-512-etm-etm@openssh.com, hmac-sha2-256, hmac-sha2-512
@openssh.com
```

To disable more than one algorithm, use the no form of the command multiple times with different algorithm names. If you try to disable the last MAC algorithm in the configuration, the following message is displayed, and the command is rejected:

```
% SSH command rejected: All mac algorithms cannot be disabled
```

Examples

The following example shows how to configure MAC algorithms on Cisco IOS SSH clients:

```
Device> enable
Device# configure terminal
Device(config)# ip ssh client algorithm mac hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha
Device(config)# end
```

The following example shows how to return to the default behavior in which all MAC algorithms are enabled in the predefined order:

```
 Device> enable
Device# configure terminal
Device(config)# default ip ssh client algorithm mac
Device(config)# end
```

Related Commands

Command	Description
ip ssh client algorithm encryption	Defines the order of encryption algorithms in a Cisco IOS SSH client.
ip ssh server algorithm mac	Defines the order of MAC algorithms in a Cisco IOS SSH server.
show ip ssh	Displays the status of SSH server connections.

ip ssh dh min size

To configure the modulus size on the IOS Secure Shell (SSH) server and client, use the ip ssh dh min size command in global configuration mode. To configure the default value of 2048 bits, use the no form or the default form of this command.

ip ssh dh min size *number*

no ip ssh dh min size

default ip ssh dh min size

Syntax Description

number	Minimum number of bits in the key size. The available options are 2048, and 4096. The default value is 2048.

Command Default

Minimum size of Diffie-Hellman (DH) key on IOS SSH server and client is 2048 bits.

Command Modes

Global configuration (config)

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.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

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.

IOS SSH supports the following Diffie-Hellman (DH) key exchange methods:

- Fixed Group Method (diffie-hellman-group14-sha1 [2048 bits])
- Group Exchange Method (diffie-hellman-group-exchange-sha1 [2048 bits, 4096 bits])

In both DH key exchange methods, IOS SSH server and client negotiates and establishes connections with only groups (ranges) whose modulus sizes are equal to or higher than the value configured in the CLI.

Examples

The following example shows how to set the minimum modulus size to 2048 bits:

```
Device> enable
Device# configure terminal
Device(config)# 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 logging events

To create a log statement of an ssh attempt, use the ip ssh logging events command in Global Configuration Mode.

ip ssh logging events

Syntax Description

This command has no arguments or keywords.

Command Default

This command is enabled by default.

Command Modes

Global configuration mode

Command History

Release	Modification
12.3 T	This command was introduced.
Cisco IOS XE Dublin 17.12.1a release	This command was modified. The command is enabled by default.

Usage Guidelines

To create a log statement of an ssh attempt, use the ip ssh logging events command in global configuration mode.

Examples

This example shows the logging events:

```
Router(Config)# ip ssh logging events

*Jul 19 23:15:00.822: %SSH-5-SSH2_SESSION: SSH2 Session request from 10.232.24.222 (tty = 4) using crypto cipher
*Jul 19 23:15:04.794: %SSH-5-SSH2_USERAUTH: User 'test' authentication for SSH2 Session from 10.232.24.222 (tty
*Jul 19 23:16:10.898: %SSH-5-SSH2_CLOSE: SSH2 Session from 10.232.24.222 (tty = 4) for user 'test' using crypto
```

ip ssh maxstartups

If the SSH server negotiates the establishment of too many SSH sessions at the same time, it could cause high CPU consumption. To control the maximum number of SSH sessions that can be started simultaneously, 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.

Release	Modification
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.

Release	Modification
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.

Command	Description
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 algorithm authentication

To define the order of user authentication algorithms in a Cisco IOS Secure Shell (SSH) server, use the ip ssh server algorithm authentication command in global configuration mode. To disable an algorithm from the configured list, use the no form of this command. To return to the default behavior in which all user authentication algorithms are enabled in the predefined order, use the default form of this command.

ip ssh server algorithm authentication {publickey | keyboard | password}

no ip ssh server algorithm authentication {publickey | keyboard | password}

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

SSH user authentication algorithms are set to the following default order:

```
Authentication methods: publickey, keyboard-interactive, password
```

```
```

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS 15.5(2)S	This command was introduced.
Cisco IOS XE 3.15S	This command was integrated into Cisco IOS XE Release 3.15S.
Cisco IOS 15.5(2)T	This command was integrated into Cisco IOS Release 15.5(2)T.

Usage Guidelines

To start a session between an SSH client and server, the preferred mode of user authentication needs to be decided. The IOS SSH server must have at least one configured user authentication algorithm.

The default order of the encryption algorithms are:

```
Authentication methods:publickey,keyboard-interactive,password
```

To disable more than one algorithm, use the no form of the command multiple times with different algorithm names. If you try to disable the last user authentication algorithm in the configuration, the following message is displayed, and the command is rejected:

```
% SSH command rejected: All authentication algorithms can not be disabled.
```

Examples

The following example shows how to configure user authentication algorithms on Cisco IOS SSH servers:

```
Device> enable
Device# configure terminal
Device(config)# ip ssh server algorithm authentication publickey keyboard password
Device(config)# end
```

The following example shows how to return to the default behavior in which all user authentication algorithms are enabled in the predefined order:

```
 Device> enable
Device# configure terminal
Device(config)# default ip ssh server algorithm authentication
Device(config)# end
```

Related Commands

Command	Description
ip ssh client algorithm encryption	Defines the order of encryption algorithms in a Cisco IOS SSH client.
ip ssh server algorithm hostkey	Defines the order of host key algorithms in a Cisco IOS SSH server.
ip ssh server algorithm mac	Defines the order of MAC algorithms in a Cisco IOS SSH server.
ip ssh server algorithm publickey	Defines the order of public key algorithms in a Cisco IOS SSH server.
show ip ssh	Displays the status of SSH server connections.

ip ssh server algorithm encryption

To define the order of encryption algorithms in a Cisco IOS secure shell (SSH) server, use the ip ssh server algorithm encryption command in global configuration mode. To disable an algorithm from the configured list, use the no form of this command. To return to the default behavior in which all encryption algorithms are enabled in the predefined order, use the default form of this command.

ip ssh server algorithm encryption {aes128-ctr | aes192-ctr | aes256-ctr | aes128-cbc | 3des-cbc | aes192-cbc | aes256-cbc}

no ip ssh server algorithm encryption {aes128-ctr | aes192-ctr | aes256-ctr | aes128-cbc | 3des-cbc | aes192-cbc | aes256-cbc}

Syntax Description

aes128-ctr	Configures Advanced Encryption Standard Counter Mode (AES-CTR) encryption for 128-bit key length.
aes192-ctr	Configures AES-CTR encryption for 192-bit key length.
aes256-ctr	Configures AES-CTR encryption for 256-bit key length.
aes128-cbc	Configures AES Cipher Block Chaining (AES-CBC) 128-bit key length.
3des-cbc	Configures Triple Data Encryption Standard (3DES) CBC algorithm.
aes192-cbc	Configures AES-CBC encryption for 192-bit key length.
aes256-cbc	Configures AES-CBC encryption for 256-bit key length.

Command Default

SSH encryption algorithms are set to the following default order:

```
Encryption Algorithms: aes128-ctr, aes192-ctr, aes256-ctr, aes128-cbc, 3des-cbc, aes192-cbc, aes256-cbc
```

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS 15.5(2)S	This command was introduced.
Cisco IOS XE 3.15S	This command was integrated into Cisco IOS XE Release 3.15S.
Cisco IOS 15.5(2)T	This command was integrated into Cisco IOS Release 15.5(2)T.

Usage Guidelines

To start an encrypted session between an SSH client and server, the preferred mode of encryption needs to be decided. For increased security, the preferred crypto algorithm for an SSH session is AES-CTR.

SSH Version 2 (SSHv2) supports AES-CTR encryption for 128-bit, 192-bit, and 256-bit key length. From the supported AES-CTR algorithms, the preferred algorithm is chosen based on the processing capability. The greater the length of the key, the stronger the encryption.

The Cisco IOS SSH servers and clients support three types of crypto algorithms to encrypt data and select an encryption mode in the following order of preferred encryption:

1. AES-CTR
2. AES-CBC
3. 3DES

If the SSH session uses a remote device that does not support AES-CTR encryption mode, the encryption mode for the session falls back to AES-CBC mode.

The default order of the encryption algorithms are:

```
Encryption Algorithms: aes128-ctr, aes192-ctr, aes256-ctr, aes128-cbc, 3des-cbc, aes192-cbc, aes256-cbc
```

To disable more than one algorithm, use the no form of the command multiple times with different algorithm names. If you try to disable the last encryption algorithm in the configuration, the following message is displayed, and the command is rejected:

```
% SSH command rejected: All encryption algorithms cannot be disabled
```

Examples

The following example shows how to configure encryption algorithms on Cisco IOS SSH servers:

```
Device> enable
Device# configure terminal
Device(config)# ip ssh server algorithm encryption aes128-ctr aes192-ctr aes256-ctr aes128-cbc 3des-cbc aes192-c
Device(config)# end
```

The following example shows how to return to the default behavior in which all encryption algorithms are enabled in the predefined order:

```
 Device> enable
Device# configure terminal
Device(config)# default ip ssh server algorithm encryption
Device(config)# end
```

Related Commands

Command	Description
ip ssh client algorithm encryption	Defines the order of encryption algorithms in a Cisco IOS SSH client.
ip ssh server algorithm hostkey	Defines the order of host key algorithms in a Cisco IOS SSH server.
ip ssh server algorithm mac	Defines the order of MAC algorithms in a Cisco IOS SSH server.
show ip ssh	Displays the status of SSH server connections.

ip ssh server algorithm kex

To define the order of kex algorithms in a Cisco IOS secure shell (SSH) server, use the ip ssh server algorithm kex command in global configuration mode. To disable an algorithm from the configured list, use the no form of this

command. To return to the default behavior in which all kex algorithms are enabled in the predefined order, use the default form of this command.

ip ssh server algorithm kex

no ip ssh server algorithm kex

Syntax Description

diffie-hellman-group14-sha1	DH_GRP14_SHA1 diffie-hellman key exchange algorithm
ecdh-sha2-nistp256	ECDH_SHA2_P256 ecdh key exchange algorithm
ecdh-sha2-nistp384	ECDH_SHA2_P384 ecdh key exchange algorithm
ecdh-sha2-nistp521	ECDH_SHA2_P521 ecdh key exchange algorithm

Command Default

SSH kex algorithms are set to the following default order:

```
Kex Algorithms: ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group14-sha1
```

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE 16.3	This command was introduced.

Usage Guidelines

The Cisco IOS SSH server and client must have at least one configured kex algorithm. The Cisco IOS SSH servers support the kex algorithms in the following order:

1. ecdh-sha2-nistp256
2. secdh-sha2-nistp384
3. ecdh-sha2-nistp521
4. diffie-hellman-group14-sha1

The default order of the kex algorithms are:

```
Kex Algorithms: ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group14-sha1
```

To disable more than one algorithm, use the no form of the command multiple times with different algorithm names. If you try to disable the last kex algorithm in the configuration, the following message is displayed, and the command is rejected:

```
% SSH command rejected: All kex algorithms cannot be disabled
```

Examples

The following example shows how to configure kex algorithms on Cisco IOS SSH servers:

```
Device> enable
Device# configure terminal
Device(config)# ip ssh server algorithm kex ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hel
Device(config)# end
```

The following example shows how to return to the default behavior in which all kex algorithms are enabled in the predefined order:

```
 Device> enable
Device# configure terminal
Device(config)# default ip ssh server algorithm kex
```

```
Device(config)# end
```

Related Commands

Command	Description
ip ssh server algorithm hostkey	Defines the order of host key algorithms in a Cisco IOS SSH server.
ip ssh server algorithm mac	Defines the order of MAC algorithms in a Cisco IOS SSH server.
ip ssh server algorithm publickey	Defines the order of public key algorithms in a Cisco IOS SSH server.
show ip ssh	Displays the status of SSH server connections.

ip ssh server algorithm hostkey

To define the order of host key algorithms in a Cisco IOS secure shell (SSH) server, use the ip ssh server algorithm hostkey command in global configuration mode. To disable an algorithm from the configured list, use the no form of this command. To return to the default behavior in which all host key algorithms are enabled in the predefined order, use the default form of this command.

ip ssh server algorithm hostkey {x509v3-ssh-rsa | ssh-rsa}

no ip ssh server algorithm hostkey {x509v3-ssh-rsa | ssh-rsa}

Syntax Description

x509v3-ssh-rsa	Configures certificate-based authentication.
ssh-rsa	Configures public key based authentication.

Command Default

SSH host key algorithms are set to the following default order:

```
Hostkey Algorithms: x509v3-ssh-rsa, ssh-rsa
```

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS 15.5(1)S	This command was introduced.
Cisco IOS XE 3.14S	This command was integrated into Cisco IOS XE Release 3.14S.
Cisco IOS 15.5(2)T	This command was integrated into Cisco IOS Release 15.5(2)T.

Usage Guidelines

The IOS SSH server and client must have at least one configured host key algorithm. The Cisco IOS SSH servers support the host key algorithms in the following order:

1. x509v3-ssh-rsa
2. ssh-rsa

The default order of the host key algorithms are:

```
Hostkey Algorithms: x509v3-ssh-rsa, ssh-rsa
```

To disable more than one algorithm, use the no form of the command multiple times with different algorithm names. If you try to disable the last host key algorithm in the configuration, the following message is displayed, and the command is rejected:

```
% SSH command rejected: All hostkey algorithms cannot be disabled
```

Examples

The following example shows how to configure host key algorithms on Cisco IOS SSH servers:

```
Device> enable
Device# configure terminal
Device(config)# ip ssh server algorithm hostkey x509v3-ssh-rsa ssh-rsa
Device(config)# end
```

The following example shows how to return to the default behavior in which all host key algorithms are enabled in the predefined order:

```
 Device> enable
Device# configure terminal
Device(config)# default ip ssh server algorithm hostkey
Device(config)# end
```

Related Commands

Command	Description
ip ssh server algorithm encryption	Defines the order of encryption algorithms in a Cisco IOS SSH server.
ip ssh server algorithm mac	Defines the order of MAC algorithms in a Cisco IOS SSH server.
ip ssh server algorithm publickey	Defines the order of public key algorithms in a Cisco IOS SSH server.
show ip ssh	Displays the status of SSH server connections.

ip ssh server algorithm mac

To define the order of Message Authentication Code (MAC) algorithms in a Cisco IOS secure shell (SSH) server and client, use the ip ssh server algorithm mac command in global configuration mode. To disable an algorithm

from the configured list, use the no form of this command. To return to the default behavior in which all MAC algorithms are enabled in the predefined order, use the default form of this command.

ip ssh server algorithm mac { hmac-sha2-256-etm@openssh.com | hmac-sha2-512-etm@openssh.com | hmac-sha2-256 | hmac-sha2-512 }

no ip ssh server algorithm mac { hmac-sha2-256-etm@openssh.com | hmac-sha2-512-etm@openssh.com | hmac-sha2-256 | hmac-sha2-512 }

Syntax Description

hmac-sha2-256	Configures the HMAC algorithm of HMAC-SHA2-256 as a cryptographic algorithm with a digest size of 256 bits and a key length of 256 bits.
hmac-sha2-512	Configures the HMAC algorithm of HMAC-SHA2-512 as a cryptographic algorithm with a digest size of 512 bits and a key length of 512 bits.
hmac-sha2-256-etm@openssh.com	Configures the HMAC algorithm of HMAC-SHA2-256-Encrypt-then-MAC@openssh.com as a cryptographic algorithm with a digest size of 256 bits and a key length of 256 bits.
hmac-sha2-512-etm@openssh.com	Configures the HMAC algorithm of HMAC-SHA2-512-Encrypt-then-MAC@openssh.com as a cryptographic algorithm with a digest size of 512 bits and a key length of 512 bits.

Command Default

SSH MAC algorithms are set to the following default order:

```
MAC Algorithms: hmac-sha2-256-etm@openssh.com, hmac-sha2-512-etm@openssh.com, hmac-sha2-256, hmac-sha2-512
```

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS 15.5(2)S	This command was introduced.
Cisco IOS XE 3.15S	This command was integrated into Cisco IOS XE Release 3.15S.
Cisco IOS 15.5(2)T	This command was integrated into Cisco IOS Release 15.5(2)T.
Cisco IOS XE Everest 16.5.1b	The Hmac-SHA2 mac algorithm for SSH was introduced.
Cisco IOS XE Amsterdam 17.3	The Hmac-SHA2-256ETM@openssh.com and Hmac-SHA2-512ETM@openssh.com mac algorithm for SSH were introduced.

Usage Guidelines

The Cisco IOS SSH servers and clients must have at least one configured Hashed Message Authentication Code (HMAC) algorithm and can have more than one HMAC algorithm configured. The Cisco IOS SSH servers and clients support the MAC algorithms in the following order:

1. hmac-sha2-256-etm@openssh.com
2. hmac-sha2-512-etm@openssh.com
3. hmac-sha2-256
4. hmac-sha2-512

The default order of the MAC algorithms are:

```
MAC Algorithms: hmac-sha2-256, hmac-sha2-512, hmac-sha2-256-etm@openssh.com, hmac-sha2-512-etm@openssh.com
```

To disable more than one algorithm, use the no form of the command multiple times with different algorithm names. If you try to disable the last MAC algorithm in the configuration, the following message is displayed, and the command is rejected:

```
% SSH command rejected: All mac algorithms cannot be disabled
```

Examples

The following example shows how to configure MAC algorithms on Cisco IOS SSH servers:

```
Device> enable
Device# configure terminal
Device(config)# ip ssh server algorithm mac hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha
Device(config)# end
```

The following example shows how to return to the default behavior in which all MAC algorithms are enabled in the predefined order:

```
 Device> enable
Device# configure terminal
Device(config)# default ip ssh server algorithm mac
Device(config)# end
```

Related Commands

Command	Description
ip ssh client algorithm mac	Defines the order of MAC algorithms in a Cisco IOS SSH client.
ip ssh server algorithm encryption	Defines the order of encryption algorithms in a Cisco IOS SSH server.
ip ssh server algorithm hostkey	Defines the order of host key algorithms in a Cisco IOS SSH server.
show ip ssh	Displays the status of SSH server connections.

ip ssh server algorithm publickey

To define the order of public key algorithms in a Cisco IOS secure shell (SSH) server for user authentication, use the ip ssh server algorithm publickey command in global configuration mode. To disable an algorithm from the configured list, use the no form of this command. To return to the default behavior in which all public key algorithms are enabled in the predefined order, use the default form of this command.

ip ssh server algorithm publickey {x509v3-ssh-rsa | ssh-rsa}

no ip ssh server algorithm publickey {x509v3-ssh-rsa | ssh-rsa}

Syntax Description

x509v3-ssh-rsa	Configures certificate-based authentication.
ssh-rsa	Configures public key based authentication.

Command Default

SSH public key algorithms are set to the following default order:

```
Authentication Publickey Algorithms: x509v3-ssh-rsa, ssh-rsa
```

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS 15.5(1)S	This command was introduced.
Cisco IOS XE 3.14S	This command was integrated into Cisco IOS XE Release 3.14S.
Cisco IOS 15.5(2)T	This command was integrated into Cisco IOS Release 15.5(2)T.

Usage Guidelines

The IOS SSH server and client must have at least one configured public key algorithm. The Cisco IOS SSH servers support the public key algorithms in the following order:

1. x509v3-ssh-rsa
2. ssh-rsa

The default order of the host key algorithms are:

```
Authentication Publickey Algorithms: x509v3-ssh-rsa, ssh-rsa
```

To disable more than one algorithm, use the no form of the command multiple times with different algorithm names. If you try to disable the last public key algorithm in the configuration, the following message is displayed, and the command is rejected:

```
% SSH command rejected: All publickey algorithms cannot be disabled.
```

Examples

The following example shows how to configure public key algorithms on Cisco IOS SSH servers:

```
Device> enable
Device# configure terminal
Device(config)# ip ssh server algorithm publickey x509v3-ssh-rsa ssh-rsa
Device(config)# end
```

The following example shows how to return to the default behavior in which all public key algorithms are enabled in the predefined order:

```
 Device> enable
Device# configure terminal
Device(config)# default ip ssh server algorithm publickey
Device(config)# end
```

Related Commands

Command	Description
ip ssh client algorithm encryption	Defines the order of encryption algorithms in a Cisco IOS SSH client.
ip ssh client algorithm mac	Defines the order of MAC algorithms in a Cisco IOS SSH client.
ip ssh server algorithm encryption	Defines the order of encryption algorithms in a Cisco IOS SSH server.
ip ssh server algorithm hostkey	Defines the order of host key algorithms in a Cisco IOS SSH server.
ip ssh server algorithm mac	Defines the order of MAC algorithms in a Cisco IOS SSH server.
show ip ssh	Displays the status of SSH server connections.

ip ssh server authenticate user

To enable the user authentication methods available in a Cisco IOS Secure Shell (SSH) server, use the ip ssh server authenticate user command in global configuration mode. To disable the user authentication methods available in a Cisco IOS 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> (tt
```

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* vrf *vrf-name*

no ip tacacs source-interface

Syntax Description

subinterface-name	Name of the interface that TACACS+ uses for all of its outgoing packets.
vrf *vrf-name*	VPN routing/forwarding parameter name.

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.

Release	Modification
12.2(54)SG	This command was integrated into Cisco IOS Release 12.2(54)SG.
Cisco IOS XE Fuji 16.9.1	The vrf *vrf-name* keyword-argument pair was added.

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 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 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

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 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 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 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 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.

Command	Description
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.

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

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.

Command	Description
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.

Release	Modification
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 and 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 and 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 209.165.2
```

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.
```

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 209.165.201.2:8
```

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 and 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 and 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 and 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 and 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

Effective with Cisco IOS Release 15.4(3)M, the ip urlfilter server vendor command is not available in Cisco IOS software.

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.
12.3(2)T	The outside keyword was added.
12.3(14)T	The vrf *vrf-name* keyword and argument pair was added.
15.4(3)M	This command was removed.

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.
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

Effective with Cisco IOS Release 15.4(3)M, the ip urlfilter urlf-server-log command is not available in Cisco IOS software.

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 and argument pair was added.
15.4(3)M	This command was removed.

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.
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.

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.
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.
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 .

Release	Modification
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

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

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.

Release	Modification
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.
15.4(3)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Router.

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.

Release	Modification
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.

ipsec profile

To associate an IPsec profile to an Easy VPN tunnel and to avoid fragmentation of Quick Mode (QM) packets, use the ipsec profile command. To disable, use the no form of this command.

ipsec profile *name*

no crypto ipsec profile

Syntax Description

Command Default

If no IPsec profile is configured, Easy VPN Remote router sends all supported transform-sets during ISAKMP QM negotiations, which makes ISAKMP packets bigger and can cause fragmentation.

Command Modes

Cisco Easy VPN Remote configuration (config-crypto-ezvpn)

Command History

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

Usage Guidelines

Use the ipsec profile command to configure IPsec transform-sets to avoid fragmentation of ISAKMP QM packets.

Examples

```
 crypto ipsec transform-set set1 esp-aes esp-sha-hmac

crypto ipsec profile prof1
 set transform-set set1
 set pfs group2

crypto ipsec client ezvpn EZVPN_CLIENT
 connect auto
 group hw-clients key cisco
 mode network-extension
 peer 10.1.1.2
 ipsec-profile prof1
 virtual-interface 1
 username router1 password cisco
 xauth userid mode local
```

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

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.

Command	Description
crypto key generate rsa	Generates RSA key pairs.
ipv6 cga modifier rsakeypair (global configuration)	Generates the CGA modifier for a specified RSA key.
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.

Command	Description
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
%FW-6-SESS_AUDIT_TRAIL: ftp session initiator 192.168.1.13:33194) sent 336 bytes -- responder (192.168.129.11:21
```

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.

Command	Description
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 1. 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

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.
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.

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 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.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SY. The limited-broadcast keyword was deprecated.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE. The limited-broadcast keyword was deprecated.

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.

Release	Modification
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

Table 2.

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.
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.
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.
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.
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
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.

Release	Modification
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 3. 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

Application Name	Well-Known or Registered Port Number	Protocol Description
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 radius source-interface

To specify an interface to use for the source address in RADIUS packets, use the ipv6 radius source-interface command in global configuration mode. To remove the specified interface from the configuration, use the no form of this command.

ipv6 radius source-interface *interface* vrf *vrf-name*

no ipv6 radius source-interface *interface*

Syntax Description

interface	Interface to be used for the source address in RADIUS packets.
vrf *vrf-name*	VPN routing/forwarding parameter name.

Command Default

No interface is specified.

Command Modes

Global configuration (config)

Command History

Release	Modification

Release	Modification
Cisco IOS XE Release 3.2S	This command was introduced.
Cisco IOS XE Fuji 16.9.1	The vrf *vrf-name* keyword-argument pair was added.

Usage Guidelines

The ipv6 radius source-interface command specifies an interface to use for the source address in RADIUS packets.

Examples

The following example shows how to configure the Gigabit Ethernet interface to be used as the source address in RADIUS packets:

```
Router(config)# ipv6 radius source-interface GigabitEthernet 0/0/0
```

Related Commands

Command	Description
radius server	Configures the RADIUS server for IPv6 or IPv4 and enters RADIUS server configuration mode.

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* vrf *vrf-name*

no ipv6 tacacs source-interface *interface*

Syntax Description

interface	Interface to be used for the source address in TACACS packets.
vrf *vrf-name*	VPN routing/forwarding parameter name.

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.
Cisco IOS XE Fuji 16.9.1	The vrf *vrf-name* keyword-argument pair was added.

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.
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
```

ipv6 vrf forwarding

To configure the Virtual Private Network (VPN) routing and forwarding (VRF) parameters to use with the TACACS+ server group, use the ipv6 vrf forwarding command in TACACS+ server-group configuration mode. To enable server groups to use the global (default) routing table, use the **no** form of this command.

ipv6 vrf forwarding *vrf-name*

no ipv6 vrf forwarding *vrf-name*

Syntax Description

vrf-name	Name assigned to a VRF.

Command Default

Server groups use the global routing table.

Command Modes

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

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.1	This command was introduced.

Usage Guidelines

Use the ipv6 vrf forwarding command to specify a VRF for a TACACS+ server group.

Examples

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
    ipv6 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
   ipv6 vrf forwarding cisco
```

The following example shows a scenario where the ipv6 vrf forwarding command is used to choose one of the global source interfaces configured if the source interface is not configured under the server group:

```
Example:
Global configurations:
ip radius source-interface Loopback0 vrf RED
ip radius source-interface Loopback1 vrf BLUE
ip radius source-interface Loopback2 vrf GREEN

Server Group configuration: Case 1
aaa group server radius radius-group1
ipv6 vrf forwarding RED
ipv6 radius source-interface Loopback0
>>> Here Loopback0 is considered as the source-interface.

Server Group configuration: Case 2
aaa group server radius radius-group1
ipv6 vrf forwarding BLUE
>>>> As the source interface is not mentioned under the server group, the command checks
for the vrf forwarding configured with the group and checks for the global source interface
configurations associated with vrf BLUE, which is Loopback1, so here Loopback1 is used as
the source interface.

Server Group configuration: Case 3
aaa group server radius radius-group1
ipv6 vrf forwarding GREEN
>>> Loopback2 is considered as the source-interface.
```

Related Commands

Command	Description

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.

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.
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.

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.
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

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

Command	Description
crypto ikev2 profile	Defines an IKEv2 profile.
show crypto ikev2 profile	Displays the IKEv2 profile.

Back to Top
