mitigation through outgoing

mitigation

To specify the Transitory Messaging Services (TMS) parameter map associated with this TMS class, use the **mitigation** command in policy-map class configuration mode. To detach the parameter map from the policy map, use the **no** form of this command.

Note Effective with Cisco IOS Release 12.4(20)T, the **mitigation** command is not available in Cisco IOS software.

mitigation *parameter-map-name*

no mitigation *parameter-map-name*

Syntax Description

parameter-map-name	Name of a TMS parameter map.

Command Default

None.

Command Modes

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

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.4(15)XZ	This command was integrated into Cisco IOS Release 12.4(15)XZ.

Usage Guidelines

The **mitigation** command is entered in policy-map class configuration mode to attach a TMS type parameter map to a TMS type class map under a policy map. The same parameter map can be attached to one or more class maps. If there are multiple class maps attached to a policy map, each can be associated with the same parameter map or a different parameter map.

Examples

The following example configures the **mitigation** command to attach the TMS type parameter map to the policy map:

```
Router(config)# class-map type control tms TMS_CLASS_1
Router(config-cmap)# match tidp-group 10-20
Router(config-cmap)# exit
Router(config)# parameter-map type tms TMS_PAR_1
router(config-profile)# controller ipv4 10.1.1.1
Router(config-profile)# exit
Router(config)# policy-map type control tms TMS_POL_1
```

```
Router(config-pmap)# class TMS_CLASS_1
Router(config-pmap-c)# mitigation TMS_PAR_1
Router(config-pmap-c)# end
```

Related Commands

Command	Description
policy-map type tms	Configures a TMS type policy map.

mls acl tcam consistency enable

To enable consistency checking of a device's Ternary Content Addressable Memory (TCAM) table by the Multi-Link Switching (MLS) access check list (ACL) lookup engine, use the **mls acl tcam consistency enable** command in global configuration mode. To return to the default value, use the **no** form of this command.

mls acl tcam consistency enable

Syntax Description

This command has no arguments or keywords.

Command Default

The MLS ACL TCAM consistency checker is disabled after a device reloads.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.3(1)S	This command was introduced.

Usage Guidelines

Use this command to explicitly enable the MLS ACL TCAM consistency checker.

To display the results from the consistency checker, use the **show mls acl consistency** command.

Examples

```
Device (config)# mls acl tcam consistency enable
Device(config)# exit
Device# show running-config
.
.
.
mls acl tcam consistency enable
mls cef error action freeze
multilink bundle-name authenticated
!
```

Related Commands

Command	Description
show mls acl consistency	Displays results from the MLS TCAM ACL consistency checker.

mls acl tcam default-result

To set the default action during the ACL TCAM update, use the **mls acl tcam default-result** command in global configuration mode. To return to the default settings, use the **no** form of this command.

mls acl tcam default-result {**permit**| **deny**| **bridge**}

no mls acl tcam default-result

Syntax Description

permit	Permits all traffic.
deny	Denies all traffic.
bridge	Bridges all Layer 3 traffic up to MSFC, RP, or to software.

Command Default

deny

Command Modes

Global configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

In the transition time between when an existing ACL is removed and a new ACL is applied, a default **deny** is programmed in the hardware. Once the new ACL has been applied completely in the hardware, the default **deny** is removed.

Use the **mls acl tcam default-result permit** command to permit all traffic in the hardware or bridge all traffic to the software during the transition time.

Examples

This example shows how to permit all traffic to pass during the ACL TCAM update:

```
Router(config)# mls acl tcam default-result permit
```

This example shows how to deny all traffic during the ACL TCAM update:

```
Router(config)# mls acl tcam default-result deny
```

This example shows how to bridge all Layer 3 traffic during the ACL TCAM update:

```
Router(config)# mls acl tcam default-result bridge
```

mls acl tcam override dynamic dhcp-snooping

To allow web-based authentication (webauth) and IP Source Guard (IPSG) to function together on the same interface, use the **mls acl tcam override dynamic dhcp-snooping** command in global configuration mode. To disable this compatibility function, use the **no** form of this command.

mls acl tcam override dynamic dhcp-snooping

no mls acl tcam override dynamic dhcp-snooping

Syntax Description

This command has no arguments or keywords.

Command Default

This function is disabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SXI2	This command was introduced.

Usage Guidelines

On the Catalyst 6500 series switch, when both webauth and IPSG are configured on the same access port and DHCP snooping is enabled on the access VLAN, the webauth downloadable ACLs (DACLs) can interfere with the DHCP snooping functionality. To prevent this interference, enter the **mls acl tcam override dynamic dhcp-snooping** command in global configuration mode. This command causes DHCP snooping entries to be replicated in the DACLs.

Examples

This example shows how to configure compatibility between webauth and IPSG:

```
Router(config)# mls acl tcam override dynamic dhcp-snooping
```

Related Commands

Command	Description
ip admission	Configures web-based authentication on the interface.
ip dhcp snooping	Enables DHCP snooping.
ip verify source	Enables IP Source Guard on the port.

mls acl tcam share-global

To enable sharing of the global default ACLs, use the **mls acl tcam share-global** command in global configuration mode. To turn off sharing of the global defaults, use the **no** form of this command.

mls acl tcam share-global

no mls acl tcam share-global

Syntax Description

This command has no arguments or keywords.

Command Default

Enabled

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

If you power cycle one of the DFCs, we recommend that you reset all the DFCs across the ACLs of the different DFCs.

Examples

This example shows how to enable sharing of the global default ACLs:

```
Router(config)# mls acl tcam share-global
```

mls acl vacl apply-self

To enable VACL lookups on software-switched and router-generated packets on the Catalyst 6500 Supervisor Engine 2, use the **mls acl vacl apply-self**command in global configuration mode. To disable VACL lookups for software packets, use the **no** form of this command.

mls acl vacl apply-self

no mls acl vacl apply-self

Syntax Description

This command has no keywords or arguments.

Command Default

VACL lookup on the egress VLAN for software packets are not enabled on switches with Supervisor Engine 2.

Command Modes

Global configuration

Command History

Release	Modification
12.2SXF15	Support for this command was introduced on the Supervisor Engine 2.

Usage Guidelines

On the Supervisor Engine 2 based switches running Cisco IOS Release 12.2(18)SXF15 or a later release, you can enable VACL lookups on software-switched and router generated packets for the VLAN filter configured on the egress VLAN by entering the **mls acl vacl apply-self** command.

On both the Supervisor Engine 720 and Supervisor Engine 32, software-switched packets and router-generated packets are always subjected to VACL lookups on the egress VLAN.

Examples

This example shows how to enable VACL lookups on software-switched and router-generated packets:

```
Router(config)# mls acl vacl apply-self
Router(config)#
```

mls aclmerge algorithm

To select the type of ACL merge method to use, use the **mls aclmerge algorithm**command in global configuration mode.

mls aclmerge algorithm {**bdd**| **odm**}

Syntax Description

bdd	Specifies the binary decision diagram (BDD)-based algorithm.
odm	Specifies the order dependent merge (ODM)-based algorithm.

Command Default

bdd

Command Modes

Global configuration

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(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 720.

The BDD-based ACL merge uses Boolean functions to condense entries into a single merged list of Ternary Content Addressable Memory (TCAM) entries that can be programmed into the TCAM.

You cannot disable the ODM-based ACL merge on Cisco 7600 series routers that are configured with a Supervisor Engine 720.

The ODM-based ACL merge uses an order-dependent merge algorithm to process entries that can be programmed into the TCAM.

Note The ODM-based ACL merge supports both security ACLs and ACLs that are used for QoS filtering.

If you change the algorithm method, the change is not retroactive. For example, ACLs that have had the merge applied are not affected. The merge change applies to future merges only.

Use the **show fm summary** command to see the status of the current merge method.

Examples

This example shows how to select the BDD-based ACL to process ACLs:

```
Router(config)# mls aclmerge algorithm bdd
The algorithm chosen will take effect for new ACLs which are being applied, not
for already applied ACLs.
Router(config)
```

This example shows how to select the ODM-based ACL merge to process ACLs:

```
Router(config)# mls aclmerge algorithm odm
The algorithm chosen will take effect for new ACLs which are being applied, not
for already applied ACLs.
```

Related Commands

Command	Description
show fm summary	Displays a summary of feature manager information.

mls ip acl port expand

To enable ACL-specific features for Layer 4, use the **mls ip acl port expand** comman d in global configuration mode. To disable the ACL-specific Layer 4 features, use the **no** form of this command.

mls ip acl port expand

no mls ip acl port expand

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default settings.

Command Modes

Global configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 720 was extended to Cisco IOS Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

Examples

This example shows how to enable the expansion of ACL logical operations on Layer 4 ports:

```
Router(config)#
mls ip acl port expand
```

mls ip inspect

To permit traffic through any ACLs that would deny the traffic through other interfaces from the global configuration command mode, use the **mls ip inspect** command. Use the **no** form of this command to return to the default settings.

mls ip inspect *acl-name*

no mls ip inspect *acl-name*

Syntax Description

acl-name	ACL name.

Command Default

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.

Usage Guidelines

On a Cisco 7600 series routers, when interfaces are configured to deny traffic, the CBAC permits traffic to flow bidirectionally only through the interface that is configured with the **ip inspect** command.

Examples

This example shows how to permit the traffic through a specific ACL (named den-ftp-c):

```
Router(config)# mls ip inspect deny-ftp-c
Router(config)#
```

Related Commands

Command	Description
ip inspect	Applies a set of inspection rules to an interface.

mls rate-limit all

To enable and set the rate limiters common to unicast and multicast packets in the global configuration command mode, use the **mls rate-limit all**command. Use the **no** form of this command to disable the rate limiters.

mls rate-limit all {**mtu-failure**| **ttl-failure**} *pps* [*packets-in-burst*]

no mls rate-limit all {**mtu-failure**| **ttl-failure**}

Syntax Description

all	Specifies rate limiting for unicast and multicast packets.
mtu-failure	Enables and sets the rate limiters for MTU-failed packets.
ttl-failure	Enables and sets the rate limiters for TTL-failed packets.
pps	Packets per second; valid values are from 10 to 1000000 packets per second.
packets-in-burst	(Optional) Packets in burst; valid values are from 1 to 255.

Command Default

The Layer 2 rate limiters are off by default. If you enable and set the rate limiters, the default *packets-in-burst* is **10**.

Command Modes

Global configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

Rate limiters can rate-limit packets that are punted from the data path in the hardware up to the data path in the software. Rate limiters protect the control path in the software from congestion by dropping the traffic that exceeds the configured rate.

Note For Cisco 7600 series routers configured with a PFC3A, enabling the Layer 2 rate limiters has a negative impact on the multicast traffic. This negative impact does not apply to Cisco 7600 series routers configured with a PFC3BXL.

Examples

This example shows how to set the TTL-failure limiter for unicast and multicast packets:

```
Router(config)# mls rate-limit all ttl-failure 15
Router(config)#
```

Related Commands

Command	Description
show mls rate-limit	Displays information about the MLS rate limiter.

mls rate-limit layer2

To enable and rate limit the control packets in Layer 2, use the **mls rate-limit layer2** command in global configuration mode. To disable the rate limiter in the hardware, use the **no** form of this command.

mls rate-limit layer2 {**ip-admission**| **l2pt**| **pdu**| **port-security**| **unknown**} *pps* [*packets-in-burst*]

no mls rate-limit layer2 [**l2pt**| **pdu**| **port-security**| **unknown**]

Syntax Description

ip-admission *pps*	Specifies the rate limit for IP admission on Layer 2 ports; valid values are from 10 to 1000000 packets per second.
l2pt *pps*	Specifies the rate limit for control packets in Layer 2 with a protocol-tunneling multicast-MAC address in Layer 2; valid values are from 10 to 1000000 packets per second.
pdu *pps*	Specifies the rate limit for Bridge Protocol Data Unit (BPDU), Cisco Discovery Protocol (CDP), Protocol Data Unit (PDU), and VLAN Trunk Protocol (VTP) PDU Layer 2 control packets; valid values are from 10 to 1000000 packets per second.
port-security *pps*	Specifies the rate limit for port security traffic; valid values are from 10 to 1000000 packets per second.
unknown	Specifies the rate limit for unknown unicast flooding on Layer 2 ports; valid values are from 10 to 1000000 packets per second.
packets-in-burst	(Optional) Packets in burst; valid values are from 1 to 255.

Command Default

The Layer 2 rate limiters are off by default. If you enable and set the rate limiters, the default *packets-in-burst* value is 10 and *pps* value has no default setting.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(17a)SX	This command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.(33)SRA.

Release	Modification
12.2(18)SXF5	This **port-security** keyword was added.
12.2(33)SXH	The **ip-admission** keyword was added.

Usage Guidelines

MLS provides high-performance hardware-based Layer 3 switching at Layer 2.

This command is not supported on Catalyst 6500 series switches and Cisco 7600 series routers that are configured with a Supervisor Engine 2.

The **unknown** keyword is only available on PFC3C line cards. When PFC3C and PFC3B linecards are powered on in the same chassis the chassis will downgrade to the PFC3B linecard and the **unknown** keyword will be unavailable.

You cannot configure the Layer 2 rate limiters if the global switching mode is set to truncated mode.

The following restrictions are pertinent to the use of the **port-security** *pps* keywords and argument:

- The PFC2 does not support the port-security rate limiter.
- The truncated switching mode does not support the port-security rate limiter.
- The lower the value, the more the CPU is protected.

Rate limiters control packets as follows:

- The frames are classified as Layer 2 control frames by the destination MAC address. The destination MAC address used are as follows:
  - 0180.C200.0000 for IEEE BPDU
  - 0100.0CCC.CCCC for CDP
  - 0100.0CCC.CCCD for Per VLAN Spanning Tree (PVST)/Shared Spanning Tree Protocol (SSTP) BPDU
- The software allocates an Local Target Logic (LTL) index for the frames.
- The LTL index is submitted to the forwarding engine for aggregate rate limiting of all the associated frames.

The Layer 2 control packets are as follows:

- General Attribute Registration Protocol (GARP) VLAN Registration Protocol (GVRP)
- BPDUs
- CDP/Dynamic Trunking Protocol (DTP)/Port Aggregation Protocol (PAgP)/UniDirectional Link Detection Protocol (UDLD)/Link Aggregation Control Protocol (LACP) /VTP PDUs
- PVST/SSTP PDUs

If the rate of the traffic exceeds the configured rate limit, the excess packets are dropped at the hardware.

The **pdu** and **l2pt** rate limiters use specific hardware rate-limiter numbers only, such as 9 through 12. Enter the **show mls rate-limit usage** command to display the available rate-limiter numbers. The available numbers

are displayed as “Free” in the output field. If all four of those rate limiters are in use by other features, a system message is displayed telling you to turn off a feature to rate limit the control packets in Layer 2.

When a MAC move occurs and a packet is seen on two ports, the packet is redirected to the software. If one of those ports has the violation mode set to restrict or protect, the packet is dropped in software. You can use the port-security rate limiter to throttle the number of such packets redirected to software. This helps in protecting the software from high traffic rates.

Examples

This example shows how to enable and set the rate limiters for the protocol-tunneling packets in Layer 2:

```
Router(config)# mls rate-limit layer2 l2pt 3000
```

This example shows how to configure the **port-security** rate limiter:

```
Router(config)# mls rate-limit layer2 port-security 500
```

This example shows how to configure the **ip-admission** rate limiter:

```
Router(config)# mls rate-limit layer2 ip-admission 560
```

Related Commands

Command	Description
show mls rate-limit	Displays information about the MLS rate limiter.

mls rate-limit unicast l3-features

To enable and set the Layer 3 security rate limiters for the unicast packets in the global configuration command mode, use the **mls rate-limit unicast l3-features**command. Use the **no** form of this command to disable the rate limiters.

mls rate-limit unicast l3-features *pps* [*packets-in-burst*]

no mls rate-limit unicast l3-features *pps* [*packets-in-burst*]

Syntax Description

pps	Packets per second; see the "Usage Guidelines" section for valid values.
packets-in-burst	(Optional) Packets in burst; valid values are from 1 to 255.

Command Default

The defaults are as follows:

- Enabled at **2000** *pps* and *packets-in-burst* is set to **1**.
- If the *packets-in-burst* is not set, **10** is programmed for unicast cases.

Command Modes

Global configuration

Command History

Release	Modification
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.(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 720.

Examples

This example shows how to set the Layer 3 security rate limiters for the unicast packets:

```
Router(config)# mls rate-limit unicast l3-features 5000
Router(config)#
```

Related Commands

Command	Description
show mls rate-limit	Displays information about the MLS rate limiter.

mls rate-limit multicast ipv4

To enable and set the rate limiters for the IPv4 multicast packets in the global configuration command mode, use the **mls rate-limit multicast ipv4**command. Use the **no** form of this command to disable the rate limiters.

mls rate-limit multicast ipv4 {**connected**| **fib-miss**| **igmp**| **ip-option**| **partial**| **pim**| **non-rpf**} *pps* [*packets-in-burst*]

no mls rate-limit multicast ipv4 {**connected**| **fib-miss**| **igmp**| **ip-option**| **partial**| **pim**| **non-rpf**}

Syntax Description

connected	Enables and sets the rate limiters for multicast packets from directly connected sources.
fib-miss	Enables and sets the rate limiters for the FIB-missed multicast packets.
igmp	Enables and sets the rate limiters for the IGMP packets.
ip-option	Enables and sets the rate limiters for the multicast packets with IP options.
partial	Enables and sets the rate limiters for the multicast packets during a partial SC state.
pim	Enables and sets the rate limiters for the PIM IPv4 multicast packets.
non-rpf	Enables and sets the rate limiters for the multicast packets failing the RPF check.
pps	Packets per second; valid values are from 10 to 1000000 packets per second.
packets-in-burst	(Optional) Packets in burst; valid values are from 1 to 255.

Command Default

The defaults are as follows:

- If the *packets-in-burst* is not set, a default of **100** is programmed for multicast cases.
- **fib-miss** --Enabled at **100000** *pps* and *packet-in-burst* is set to **100**.
- **ip-option** --Disabled.
- **partial** --Enabled at **100000** *pps* and *packet-in-burst* is set to **100**.

Command Modes

Global configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17b)SXA	This command was changed to support the **igmp** and **ip-option**keywords.
12.2(18)SXD	This command was changed to include the **ipv4** keyword.
12.2(33)SXH	This command was changed to add the **pim** keyword.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

You cannot configure the IPv4 rate limiters if the global switching mode is set to truncated mode.

The rate limiters can rate limit the packets that are punted from the data path in the hardware up to the data path in the software. The rate limiters protect the control path in the software from congestion and drop the traffic that exceeds the configured rate.

The **ip-option** keyword is supported in PFC3BXL or PFC3B mode only.

Examples

This example shows how to set the rate limiters for the multicast packets failing the RPF check :

```
Router(config)# mls rate-limit multicast ipv4 non-rpf 100
Router(config)#
```

This example shows how to set the rate limiters for the multicast packets during a partial SC state:

```
Router(config)# mls rate-limit multicast ipv4 partial 250
Router(config)#
```

This example shows how to set the rate limiters for the FIB-missed multicast packets:

```
Router(config)# mls rate-limit multicast ipv4 fib-miss 15
Router(config)#
```

Related Commands

Command	Description
show mls rate-limit	Displays information about the MLS rate limiter.

mls rate-limit multicast ipv6

To configure the IPv6 multicast rate limiters, use the **mls rate-limit multicast ipv6**command in global configuration mode. To disable the rate limiters, use the **no** form of this command.

mls rate-limit multicast ipv6 {**connected pps [packets-in-burst]**| **rate-limiter-name share** {**auto**| **target-rate-limiter**}}

no mls rate-limit multicast ipv6 {**connected**| *rate-limiter-name*}

Syntax Description

connected *pps*	Enables and sets the rate limiters for the IPv6 multicast packets from a directly connected source ; valid values are from 10 to 1000000 packets per second.
packets-in-burst	(Optional) Packets in burst; valid values are from 1 to 255.
rate-limiter-name	Rate-limiter name; valid values are default-drop , route-cntl , secondary-drop , sg , starg-bridge , and starg-m-bridge . See the “Usage Guidelines” section for additional information.
share	Specifies the sharing policy for IPv6 rate limiters; see the “Usage Guidelines” section for additional information.
auto	Decides the sharing policy automatically.
target-rate-limiter	Rate-limiter name that was the first rate-limiter name programmed in the hardware for the group; valid values are default-drop , route-cntl , secondary-drop , sg , starg-bridge , and starg-m-bridge . See the “Usage Guidelines” section for additional information.

Command Default

If the *burst* is not set, a default of **100** is programmed for multicast cases.

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXD	This command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

The *rate-limiter-name*argument must be a rate limiter that is not currently programmed.

The *target-rate-limiter*argument must be a rate limiter that is programmed in the hardware and must be the first rate limiterprogrammed for its group.

The table below lists the IPv6 rate limiters and the class of traffic that each rate limiter serves.

Table 1: IPv6 Rate Limiters

Rate-Limiter ID	Traffic Classes to be Rate Limited
Connected	Directly connected source traffic
Default-drop	* (*, G/m)SSM * (*, G/m)SSM non-rpf
Route-control	* (*, FF02::X/128)
Secondary-drop	* (*, G/128) SPT threshold is infinity
SG	* (S, G) RP-RPF post-switchover * (*, FFx2/16)
Starg-bridge	* (*, G/128) SM * SM non-rpf traffic when (*, G) exists
Starg-M-bridge	* (*, G/m) SM * (*, FF/8) * SM non-rpf traffic when (*, G) does not exist

You can configure rate limiters for IPv6 multicast traffic using one of the following methods:

- Direct association of the rate limiters for a traffic class--Select a rate and associate the rate with a rate limiter. This example shows how to pick a rate of 1000 pps and 20 packets per burst and associate the rate with the **default-drop** rate limiter:

```
Router(config)# mls rate-limit multicast ipv6 default-drop 1000 20
```

- Static sharing of a rate limiter with another preconfigured rate limiter--When there are not enough adjacency-based rate limiters available, you can share a rate limiter with an already configured rate limiter (target rate limiter). This example shows how to share the **route-cntl** rate limiter with the **default-drop** target rate limiter:

```
Router(config)# mls rate-limit multicast ipv6 route-cntl share default-drop
```

If the target rate limiter is not configured, a message displays that the target rate limiter must be configured for it to be shared with other rate limiters.

- Dynamic sharing of rate limiters--If you are not sure about which rate limiter to share with, use the **share auto** keywords to enable dynamic sharing. When you enable dynamic sharing, the system picks a preconfigured rate limiter and shares the given rate limiter with the preconfigured rate limiter. This example shows how to choose dynamic sharing for the **route-cntrl** rate limiter:

```
Router(config)# mls rate-limit multicast ipv6 route-cntl share auto
```

Examples

This example shows how to set the rate limiters for the IPv6 multicast packets from a directly connected source:

```
Router(config)# mls rate-limit multicast ipv6 connected 1500 20
Router(config)#
```

This example shows how to configure a direct association of the rate limiters for a traffic class:

```
Router(config)# mls rate-limit multicast ipv6 default-drop 1000 20
Router(config)#
```

This example shows how to configure the static sharing of a rate limiter with another preconfigured rate limiter:

```
Router(config)# mls rate-limit multicast ipv6 route-cntl share default-drop
Router(config)#
```

This example shows how to enable dynamic sharing for the **route-cntrl** rate limiter:

```
Router(config)# mls rate-limit multicast ipv6 route-cntl share auto
Router(config)#
```

Related Commands

Command	Description
show mls rate-limit	Displays information about the MLS rate limiter.

mls rate-limit unicast acl

To enable and set the ACL-bridged rate limiters in global configuration command mode, use the **mls rate-limit unicast acl**command. Use the **no** form of this command to disable the rate limiters.

mls rate-limit unicast acl {**input**| **output**| **vacl-log**} *pps* [*packets-in-burst*]

Syntax Description

input	Specifies the rate limiters for the input ACL-bridged unicast packets.
output	Specifies the rate limiters for the output ACL-bridged unicast packets.
vacl-log	Specifies the rate limiters for the VACL log cases.
pps	Packets per second; see the “Usage Guidelines” section for valid values.
packets-in-burst	(Optional) Packets in burst; valid values are from 1 to 255.

Command Default

The defaults are as follows:

- **input** --Disabled.
- **output** --Disabled.
- **vacl-log** --Enabled at **2000** *pps* and *packets-in-burst* is set to **1**.
- If the *packets-in-burst* is not set, **10** is programmed for unicast cases.

Command Modes

Global configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17a)SX	The **mls rate-limit unicast** command was reformatted.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.

Usage Guidelines

The **input** and **output** keywords are not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

The rate limiters can rate limit the packets that are punted from the data path in the hardware up to the data path in the software. The rate limiters protect the control path in the software from congestion and drop the traffic that exceeds the configured rate.

When setting the *pps*, valid values are as follows:

- ACL input and output cases--10 to 1000000 *pps*
- VACL log cases--10 to 5000 *pps*

You cannot change the **vacl-log** *packets-in-burst*keyword and argument; it is set to **1** by default.

Some cases (or scenarios) share the same hardware register. These cases are divided into the following two groups:

- Group1:
  - Egress ACL-bridged packets
  - Ingress ACL-bridged packets
- Group 2:
  - RPF failure
  - ICMP unreachable for ACL drop
  - ICMP unreachable for no-route
  - IP errors

All the components of each group use or share the same hardware register. For example, ACL-bridged ingress and egress packets use register A. ICMP-unreachable, no-route, and RPF failure use register B.

In most cases, when you change a component of a group, all the components in the group are overwritten to use the same hardware register as the first component changed. A warning message is printed out each time that an overwriting operation occurs, but only if you enable the service internal mode. The overwriting operation does not occur in these situations:

- The *pps* value is set to **0** (zero) for a particular case.
- When the i ngress or egress ACL-bridged packet cases are disabled, overwriting does not occur until the cases are enabled again. If either case is disabled, the other is not affected as long as the remaining case is enabled. For example, if you program the ingress ACL-bridged packets with a 100-pps rate, and then you configure the egress ACL-bridged packets with a 200-pps rate, the ingress ACL-bridged packet value is overwritten to 200 pps and both the ingress and the egress ACL-bridged packets have a 200-pps rate.

Examples

This example shows how to set the input ACL-bridged packet limiter for unicast packets:

```
Router(config)# mls rate-limit unicast acl input 100
Router(config)#
```

Related Commands

Command	Description
show mls rate-limit	Displays information about the MLS rate limiter.

mls rate-limit unicast cef

To enable and set the Cisco Express Forwarding rate limiters in global configuration command mode, use the **mls rate-limit unicast cef**command. Use the **no** form of this command to disable the rate limiters.

mls rate-limit unicast cef {**receive**| **glean**} *pps* [*packets-in-burst*]

Syntax Description

receive	Enables and sets the rate limiters for receive packets.
glean	Enables and sets the rate limiters for ARP-resolution packets.
pps	Packets per second; valid values are from 10 to 1000000 packets per second.
packets-in-burst	(Optional) Packets in burst; valid values are from 1 to 255.

Command Default

The defaults are as follows:

- **receive** --Disabled.
- **glean** --Disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(17a)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB. The default for **glean** was changed to disabled.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.

Usage Guidelines

If you enable the CEF rate limiters, the following behaviors occur (if the behavior that is listed is unacceptable, disable the CEF rate limiters):

- If a packet hits a glean/receive adjacency, the packet may be dropped instead of being sent to the software if there is an output ACL on the input VLAN and the matched entry result is deny.

- If the matched ACL entry result is bridge, the packet is subject to egress ACL bridge rate limiting (if turned ON) instead of glean/receive rate limiting.
- The glean/receive adjacency rate limiting is applied only if the output ACL lookup result is permit or there is no output ACLs on the input VLAN.

Examples

This example shows how to set the CEF-glean limiter for the unicast packets:

```
Router(config)# mls rate-limit unicast cef glean 5000
Router(config)#
```

Related Commands

Command	Description
show mls rate-limit	Displays information about the MLS rate limiter.

mls rate-limit unicast ip

To enable and set the rate limiters for the unicast packets in global configuration command mode, use the **mls rate-limit unicast ip**command. Use the **no** form of this command to disable the rate limiters.

mls rate-limit unicast ip {**errors**| **features**| **options**| **rpf-failure**} *pps* [*packets-in-burst*]

mls rate-limit unicast ip icmp {**redirect**| **unreachable acl-drop** *pps*| **no-route** *pps*} [*packets-in-burst*]

no mls rate-limit unicast ip {**errors**| **features**| **icmp** {**redirect**| **unreachable** {**acl-drop**| **no-route**}}| **options**| **rpf-failure**} *pps* [*packets-in-burst*]

Syntax Description

errors	Specifies rate limiting for unicast packets with IP checksum and length errors.
features	Specifies rate limiting for unicast packets with software-security features in Layer 3 (for example, authorization proxy, IPsec, and inspection).
options	Specifies rate limiting for unicast IPv4 packets with options.
rpf-failure	Specifies rate limiting for unicast packets with RPF failures.
pps	Packets per second; see the “Usage Guidelines” section for valid values.
packets-in-burst	(Optional) Packets in burst; valid values are from 1 to 255.
icmp redirect	Specifies rate limiting for unicast packets requiring ICMP redirect.
icmp unreachable acl-drop *pps*	Enables and sets the rate limiters for the ICMP unreachables for the ACL-dropped packets.
icmp unreachable no-route *pps*	Enables and sets the rate limiters for the ICMP unreachables for the FIB-miss packets.

Command Default

The defaults are as follows:

- If the *packets-in-burst* is not set, a default of **10** is programmed as the burst for unicast cases.
- **errors** -- Enabled at **500** *pps* and *packets-in-burst* set to **10**.
- **rpf-failure** --Enabled at **500** *pps* and *packets-in-burst* set to **10**

- **icmp unreachable acl-drop** -- Enabled at **500** *pps* and *packets-in-burst* set to **10**
- **icmp unreachable no-route** -- Enabled at **500** *pps* and *packets-in-burst* set to **10**
- **icmp redirect** -- Disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17a)SX	The **mls rate-limit unicast** command added the **ip** keyword to the following: • **options** • **icmp** • **rpf-failure** • **errors** • **features** These keywords were changed as follows: • The **features** keyword replaced the **l3-features**keyword. • The **mls rate-limit unicast icmp redirect** command replaced the **mls rate-limit unicast icmp-redirect**command. • The **mls rate-limit unicast icmp unreachable** command replaced the **mls rate-limit unicast icmp-unreachable**command.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

To provide OAL support for denied packets, enter the **mls rate-limit unicast ip icmp unreachable acl-drop 0** command.

OAL and VACL capture are incompatible. Do not configure both features on the switch. With OAL configured, use SPAN to capture traffic.

The rate limiters can rate limit the packets that are punted from the data path in the hardware up to the data path in the software. The rate limiters protect the control path in the software from congestion and drop the traffic that exceeds the configured rate.

Note When you configure an ICMP rate limiter, and an ICMP redirect occurs, exiting data traffic is dropped while the remaining traffic on the same interface is forwarded.

When setting the *pps*, the valid values are **0** and from 10 to 1000000. Setting the *pps* to **0** globally disables the redirection of the packets to the route processor. The **0** value is supported for these rate limiters:

- ICMP unreachable ACL-drop
- ICMP unreachable no-route
- ICMP redirect
- IP rpf failure

Some cases (or scenarios) share the same hardware register. These cases are divided into the following two groups:

- Group1:
  - Egress ACL-bridged packets
  - Ingress ACL-bridged packets
- Group 2:
  - RPF failure
  - ICMP unreachable for ACL drop
  - ICMP unreachable for no-route
  - IP errors

All the components of each group use or share the same hardware register. For example, ACL-bridged ingress and egress packets use register A. ICMP-unreachable, no-route, and RPF failure use register B.

In most cases, when you change a component of a group, all the components in the group are overwritten to use the same hardware register as the first component changed. A warning message is printed out each time that an overwriting operation occurs, but only if you enable the service internal mode. The overwriting operation does not occur in these situations:

- The *pps* value is set to **0** (zero) for a particular case.
- When the i ngress or egress ACL-bridged packet cases are disabled, overwriting does not occur until the cases are enabled again. If either case is disabled, the other is not affected as long as the remaining case is enabled. For example, if you program the ingress ACL-bridged packets with a 100-pps rate, and then you configure the egress ACL-bridged packets with a 200-pps rate, the ingress ACL-bridged packet value is overwritten to 200 pps and both the ingress and the egress ACL-bridged packets have a 200-pps rate.

Examples

This example shows how to set the ICMP-redirect limiter for unicast packets:

```
Router(config)# mls rate-limit unicast ip icmp redirect 250
Router(config)#
```

Related Commands

Command	Description
show mls rate-limit	Displays information about the MLS rate limiter.

mls rate-limit unicast vacl-log

To enable and set the VACL-log case rate limiters in the global configuration command mode, use the **mls rate-limit unicast vacl-log**command. Use the **no** form of this command to disable the rate limiters.

mls rate-limit unicast vacl-log *pps* [*packets-in-burst*]

Syntax Description

pps	Packets per second; see the "Usage Guidelines" section for valid values.
packets-in-burst	(Optional) Packets in burst; valid values are from 1 to 255.

Command Default

The defaults are as follows:

- Enabled at **2000** *pps* and *packets-in-burst* is set to **1**.
- If the *packets-in-burst* is not set, **10** is programmed for unicast cases.

Command Modes

Global configuration

Command History

Release	Modification
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.(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 720.

The rate limiters can rate limit the packets that are punted from the data path in the hardware up to the data path in the software. The rate limiters protect the control path in the software from congestion and drop the traffic that exceeds the configured rate.

When setting the *pps*, valid values are as follows:

- ACL input and output cases--10 to 1000000 *pps*
- VACL log cases--10 to 5000 *pps*

Setting the *pps* to **0** globally disables the redirection of the packets to the route processor.

You cannot change the **vacl-log** *packets-in-burst*keyword and argument; it is set to **1** by default.

Some cases (or scenarios) share the same hardware register. These cases are divided into the following two groups:

- Group1:
  - Egress ACL-bridged packets
  - Ingress ACL-bridged packets
- Group 2:
  - RPF failure
  - ICMP unreachable for ACL drop
  - ICMP unreachable for no-route
  - IP errors

All the components of each group use or share the same hardware register. For example, ACL-bridged ingress and egress packets use register A. ICMP-unreachable, no-route, and RPF failure use register B.

In most cases, when you change a component of a group, all the components in the group are overwritten to use the same hardware register as the first component changed. A warning message is printed out each time that an overwriting operation occurs, but only if you enable the service internal mode. The overwriting operation does not occur in these situations:

- The *pps* value is set to **0** (zero) for a particular case.
- When the i ngress or egress ACL-bridged packet cases are disabled, overwriting does not occur until the cases are enabled again. If either case is disabled, the other is not affected as long as the remaining case is enabled. For example, if you program the ingress ACL-bridged packets with a 100-pps rate, and then you configure the egress ACL-bridged packets with a 200-pps rate, the ingress ACL-bridged packet value is overwritten to 200 pps and both the ingress and the egress ACL-bridged packets have a 200-pps rate.

Examples

This example shows how to set the VACL-log case packet limiter for unicast packets:

```
Router(config)# mls rate-limit unicast vacl-log 100
Router(config)#
```

Related Commands

Command	Description
show mls rate-limit	Displays information about the MLS rate limiter.

mode (IPSec)

To change the mode for a transform set, use the **mode** command in crypto transform configuration mode. To reset the mode to the default value of tunnel mode, use the **no** form of this command.

mode [**tunnel**| **transport**]

no mode

Syntax Description

tunnel >| **transport**	(Optional) Specifies the mode for a transform set: either tunnel or transport mode. If neither **tunnel** nor **transport** is specified, the default (tunnel mode) is assigned.

Command Default

Tunnel mode

Command Modes

Crypto transform 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

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

Use this command to change the mode specified for the transform. This setting is only used when the traffic to be protected has the same IP addresses as the IPSec peers (this traffic can be encapsulated either in tunnel or transport mode). This setting is ignored for all other traffic (all other traffic is encapsulated in tunnel mode).

If the traffic to be protected has the same IP address as the IP Security peers and transport mode is specified, during negotiation the router will request transport mode but will accept either transport or tunnel mode. If tunnel mode is specified, the router will request tunnel mode and will accept only tunnel mode.

After you define a transform set, you are put into the crypto transform configuration mode. While in this mode you can change the mode to either tunnel or transport. This change applies only to the transform set just defined.

If you do not change the mode when you first define the transform set, but later decide you want to change the mode for the transform set, you must re-enter the transform set (specifying the transform name and all its transforms) and then change the mode.

If you use this command to change the mode, the change will only affect the negotiation of subsequent IPSec security associations via crypto map entries which specify this transform set. (If you want the new settings to take effect sooner, you can clear all or part of the security association database. See the **clear crypto sa** command for more details.

Tunnel Mode

With tunnel mode, the entire original IP packet is protected (encrypted, authenticated, or both) and is encapsulated by the IPSec headers and trailers (an Encapsulation Security Protocol header and trailer, an Authentication Header, or both). Then a new IP header is prefixed to the packet, specifying the IPSec endpoints as the source and destination.

Tunnel mode can be used with any IP traffic. Tunnel mode must be used if IPSec is protecting traffic from hosts behind the IPSec peers. For example, tunnel mode is used with Virtual Private Networks (VPNs) where hosts on one protected network send packets to hosts on a different protected network via a pair of IPSec peers. With VPNs, the IPSec peers "tunnel" the protected traffic between the peers while the hosts on their protected networks are the session endpoints.

Transport Mode

With transport mode, only the payload (data) of the original IP packet is protected (encrypted, authenticated, or both). The payload is encapsulated by the IPSec headers and trailers (an ESP header and trailer, an AH header, or both). The original IP headers remain intact and are not protected by IPSec.

Use transport mode only when the IP traffic to be protected has IPSec peers as both the source and destination. For example, you could use transport mode to protect router management traffic. Specifying transport mode allows the router to negotiate with the remote peer whether to use transport or tunnel mode.

Examples

The following example defines a transform set and changes the mode to transport mode. The mode value only applies to IP traffic with the source and destination addresses at the local and remote IPSec peers.

```
crypto ipsec transform-set newer esp-des esp-sha-hmac
 mode transport
 exit
```

Related Commands

Command	Description
crypto ipsec transform-set	Defines a transform set--an acceptable combination of security protocols and algorithms.

mode ra

To place the public key infrastructure (PKI) server into Registration Authority (RA) certificate server mode, use the **mode ra**command in certificate server configuration mode. To remove the PKI server from RA certificate mode, use the **no** form of this command.

mode ra [transparent]

no mode ra [transparent]

Syntax Description

transparent	Allows the CA server in RA mode to interoperate with more than one type of CA server.

Command Default

The PKI server is not placed into RA certificate server mode.

Command Modes

Certificate server configuration (cs-server)

Command History

Release	Modification
12.3(7)T	This command was introduced.
15.1(2)T	This command was modified. In Cisco IOS Release 15.1(2)T, the **transparent** keyword was introduced that allows the IOS CA server in RA mode to interoperate with more than one type of CA server.

Usage Guidelines

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

When this command is configured, ensure that the **crypto pki trustpoint** command has also been configured and that the enrollment URL is pointed to a Cisco IOS issuing certification authority (CA). If the **mode ra** command is not configured and the certificate server is enabled for the first time, a self-signed CA certificate will be generated and the certificate server will operate as a root CA.

The Cisco IOS certificate server can act as an RA for a Cisco IOS CA or another third party CA. The **transparent** keyword is used if a third-party CA is used.

When the **transparent** keyword is used, the original PKCS#10 enrollment message is not re-signed and is forwarded unchanged. This enrollment message makes the IOS RA certificate server work with CA servers like the Microsoft CA server.

Examples

The following configuration example shows that a RA mode certificate server named "myra" has been configured:

```
Router (config)# crypto pki trustpoint myra
Router (ca-trustpoint)# enrollment url http://10.3.0.6
Router (ca-trustpoint)# subject-name cn=myra, ou=ioscs RA, o=cisco, c=us
Router (ca-trustpoint)# exit
Router (config)# crypto pki server myra
Router (cs-server)# mode ra
Router (cs-server)# no shutdown
```

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.

Command	Description
grant auto rollover	Enables automatic granting of certificate reenrollment requests for a Cisco IOS subordinate CA server or RA mode CA.
grant auto trustpoint	Specifies the CA trustpoint of another vendor from which the Cisco IOS certificate server automatically grants certificate enrollment requests.
grant none	Specifies all certificate requests to be rejected.
grant ra-auto	Specifies that all enrollment requests from an RA be granted automatically.
hash (cs-server)	Specifies the cryptographic hash function the Cisco IOS certificate server uses to sign certificates issued by the CA.
issuer-name	Specifies the DN as the CA issuer name for the CS.
lifetime (cs-server)	Specifies the lifetime of the CA or a certificate.
mode 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.

mode secure

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

mode secure [no-negotiation]

no mode secure [no-negotiation]

Syntax Description

no-negotiation	(Optional) Specifies the Transport Layer Security (TLS) specific parameter.

Command Default

The secure mode is disabled.

Command Modes

LDAP server configuration (config-ldap-server)

Command History

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

Usage Guidelines

Use the **mode secure** command to establish a TLS connection with the LDAP server. This command will help to secure all the transactions.

Examples

The following example shows how to configure the secure mode on the LDAP server:

```
Router(config)# ldap server server1
Router(config-ldap-server)# mode secure no-negotiation
```

Related Commands

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

mode sub-cs

To place the public key infrastructure (PKI) server into sub-certificate server mode, use the **mode sub-cs**command in certificate server mode. To remove the PKI server from sub-certificate mode, use the **no** form of this command.

mode sub-cs

no mode sub-cs

Syntax Description

This command has no arguments or keywords.

Command Default

The PKI server is not placed into sub-certificate server mode.

Command Modes

Certificate server configuration (cs-server)

Command History

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

Usage Guidelines

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

When this command is configured, ensure that the **crypto pki trustpoint** command has also been configured and that the enrollment URL is pointed to a Cisco IOS root certification authority (CA). If the **mode sub-cs** command is not configured and the certificate server is enabled for the first time, a self-signed CA certification is generated and the certificate server will operate as a root CA.

Note The **no mode sub-cs** command has no effect if the server has been configured already. For example, if you want to make the subordinate CA a root CA, you must delete the server and re-create it.

Examples

The following configuration example shows that a subordinate certificate server named “sub” has been configured:

```
Router (config)# crypto pki trustpoint sub
Router (ca-trustpoint)# enrollment url http://10.3.0.6
Router (ca-trustpoint)# exit
Router (config)# crypto pki server sub
Router (cs-server)# issuer-name CN=sub CA, O=Cisco, C=us
Router (cs-server)# mode sub-cs
Router (cs-server)# no shutdown
```

Related Commands

Command	Description
auto-rollover	Enables the automated CA certificate rollover functionality.
cdp-url	Specifies a CDP to be used in certificates that are issued by the certificate server.
crl (cs-server)	Specifies the CRL PKI CS.
crypto pki server	Enables a CS and enters certificate server configuration mode, or immediately generates shadow CA credentials
database archive	Specifies the CA certificate and CA key archive format--and the password--to encrypt this CA certificate and CA key archive file.
database level	Controls what type of data is stored in the certificate enrollment database.
database url	Specifies the location where database entries for the CS is stored or published.
database username	Specifies the requirement of a username or password to be issued when accessing the primary database location.
default (cs-server)	Resets the value of the CS configuration command to its default.
grant auto rollover	Enables automatic granting of certificate reenrollment requests for a Cisco IOS subordinate CA server or RA mode CA.
grant auto trustpoint	Specifies the CA trustpoint of another vendor from which the Cisco IOS certificate server automatically grants certificate enrollment requests.

Command	Description
grant none	Specifies all certificate requests to be rejected.
grant ra-auto	Specifies that all enrollment requests from an RA be granted automatically.
hash (cs-server)	Specifies the cryptographic hash function the Cisco IOS certificate server uses to sign certificates issued by the CA.
issuer-name	Specifies the DN as the CA issuer name for the CS.
lifetime (cs-server)	Specifies the lifetime of the CA or a certificate.
mode ra	Enters the PKI server into RA certificate server mode.
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.

monitor event-trace dmvpn

To monitor and control Dynamic Multipoint VPN (DMVPN) traces, use the **monitor event-trace dmvpn** command in privileged EXEC or global configuration mode.

Privileged EXEC

monitor event-trace dmvpn {**dump [merged] pretty**| **nhrp** {**error**| **event**| **exception**}| **clear**| **continuous [cancel]**| **disable**| **enable**| **one-shot**| **tunnel**}

Global Configuration

monitor event-trace dmvpn {**dump-file** *url*| {**nhrp** {**error**| **event**| **exception**}| **tunnel**} {**disable**| **dump-file** *url*| **enable**| **size**| **stacktrace** *value*}}

no monitor event-trace dmvpn {**dump-file** *url*| {**nhrp** {**error**| **event**| **exception**}| **tunnel**} {**disable**| **dump-file** *url*| **enable**| **size**| **stacktrace** *value*}}

Syntax Description

dump	Displays all event traces.
merged	(Optional) Displays entries in all the event traces sorted by time.
pretty	Displays the event traces in ASCII format.
nhrp	Monitors Next Hop Resolution Protocol (NHRP) traces.
error	Monitors NHRP error traces.
event	Monitors NHRP event traces.
exception	Monitors NHRP exception errors.
tunnel	Monitors all tunnel events.
clear	Clears the trace.
continuous	Displays the latest event trace entries continuously.
cancel	(Optional) Cancels continuous display of the latest trace entries.
disable	Disables NHRP or tunnel tracing.
enable	Enables NHRP or tunnel tracing.
one-shot	Clears the trace, sets the running configuration, and then disables the configuration at the wrap point.

tunnel	Monitors all tunnel events.
dump-file *url*	Sets the name of the dump file.
stacktrace *value*	Specifies the trace buffer stack to be cleared first. The stack range is from 1 to 16.

Command Default

DMVPN event tracing is disabled.

Command Modes

Privileged EXEC (#) Global configuration (config)

Command History

Release	Modification
15.1(4)M	This command was introduced.

Usage Guidelines

You can use the **monitor event-trace dmvpn**command to configure the DMVPN Event Tracing feature. The DMVPN Event Tracing feature provides a trace facility for troubleshooting Cisco IOS DMVPN. This feature enables you to monitor DMVPN events, errors, and exceptions. During runtime, the event trace mechanism logs trace information in a buffer space. A display mechanism extracts and decodes the debug data.

Note You can configure the DMVPN Event Tracing feature in privileged EXEC mode or global configuration mode based on the desired parameters.

Examples

The following example shows how to configure a router to monitor and control NHRP event traces in privileged EXEC mode:

```
Router# monitor event-trace dmvpn nhrp event enable
```

The following example shows how to configure a router to monitor and control NHRP exception traces in privileged EXEC mode:

```
Router# monitor event-trace dmvpn nhrp exception enable
```

The following example shows how to configure a router to monitor and control NHRP error traces in privileged EXEC mode:

```
Router# monitor event-trace dmvpn nhrp error enable
```

The following example shows how to configure a router to monitor and control NHRP event traces in global configuration mode:

```
Router# enable
Router(config)# monitor event-trace dmvpn nhrp event enable
```

The following example shows how to configure a router to monitor and control NHRP exception traces in global configuration mode:

```
Router# enable
Router(config)# monitor event-trace dmvpn nhrp exception enable
```

The following example shows how to configure a router to monitor and control NHRP error traces in global configuration mode:

```
Router# enable
Router(config)# monitor event-trace dmvpn nhrp error enable
```

Related Commands

Command	Description
show monitor event-trace dmvpn	Displays DMVPN trace information.

monitor event-trace gdoi

To configure event tracing for the Group Domain of Interpretation (GDOI) software subsystem component, use the **monitor event-trace gdoi** command in global configuration mode.

monitor event-trace gdoi dump-file *url*

monitor event-trace gdoi {**coop**| **exit**| **infra**| **registration**| **rekey**} [**dump-file** *url*| **size** *number-of-entries*| **stacktrace** [*depth*]]

no monitor event-trace gdoi dump-file *url*

no monitor event-trace gdoi {**coop**| **exit**| **infra**| **registration**| **rekey**} [**dump-file** *url*| **size**]

Syntax Description

dump-file	Dump merged traces to a file.
url	Destination to store merged traces.
coop	Monitor cooperative key server (KS) traces.
exit	Monitor GDOI exit traces.
infra	Monitor GDOI infrastructure event traces.
registration	Monitor GDOI registration event traces.
rekey	Monitor GDOI rekey exception errors.
size	Size of the trace.
number-of-entries	Number from 1 to 1000000 that sets the size of the trace.
stacktrace	Trace the call stack at tracepoints (clear the trace buffer first).
depth	Number from 1 to 16 that sets the depth of the stack trace.

Command Default

GDOI event tracing is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(3)T	This command was introduced.
Cisco IOS XE Release 3.8S	This command was integrated into Cisco IOS XE Release 3.8S.

Usage Guidelines

Use the **monitor event-trace gdoi** command to enable or disable event tracing for GDOI and to configure event trace parameters for the Cisco IOS software GDOI subsystem component.

Note Event tracing is intended for use as a software diagnostic tool and should be configured only under the direction of a Technical Assistance Center (TAC) representative.

Additionally, default settings do not appear in the configuration file. If the subsystem software enables event tracing by default, the **monitor event-trace** *component* **enable** command will not appear in the configuration file of the networking device; however, disabling event tracing that has been enabled by default by the subsystem will create a command entry in the configuration file.

Note The amount of data collected from the trace depends on the trace message size configured using the **monitor event-trace gdoi** command for each instance of a trace.

To determine whether event tracing is enabled by default for the subsystem, use the **show monitor event-trace gdoi** command to display trace messages.

To specify the trace call stack at tracepoints, you must first clear the trace buffer.

Examples

The following example shows how to enable event tracing for GDOI subsystem component in Cisco IOS software and configure the size to 4096 messages. The trace messages file is set to gdoi-dump in slot0 (flash memory).

```
Device> enable
Device# configure terminal
Device(config)# monitor event-trace gdoi dump-file slot0:gdoi-dump
Device(config)# monitor event-trace gdoi size 4096
```

Related Commands

Command	Description
show monitor event-trace gdoi	Displays event trace messages for the Cisco IOS software GDOI subsystem component.
monitor event-trace gdoi (privileged EXEC)	Configures event tracing for the GDOI software subsystem component.

monitor event-trace gdoi (privileged EXEC)

To configure event tracing for the Group Domain of Interpretation (GDOI) software subsystem component, use the **monitor event-trace gdoi** command in privileged exec mode.

monitor event-trace gdoi dump [**[merged] pretty**]

monitor event-trace gdoi {**coop**| **exit**| **infra**| **registration**| **rekey**} {**clear**| **continuous [cancel]**| **disable**| **dump** [**[merged] pretty**]| **enable**| **one-shot**}

Syntax Description

dump	Dump all event traces.
merged	Dump entries in all event traces sorted by time.
pretty	Dump in ASCII format.
coop	Monitor cooperative key server (KS) traces.
exit	Monitor GDOI exit traces.
infra	Monitor GDOI infrastructure event traces.
registration	Monitor GDOI registration event traces.
rekey	Monitor GDOI rekey exception errors.
clear	Clear the trace.
continuous	Continuously display latest event trace entries.
cancel	Cancel continuous display of latest trace entries.
disable	Disable tracing.
enable	Enable tracing.
one-shot	Clear the trace, set running, then disable at wrap point. Each buffer is a circular linked list that is overwritten when the buffer is full replacing the oldest entry first; this keyword disables overwriting the buffer by filling it once and stopping collection of the event and exit traces when the buffer is full.

Command Default

GDOI event tracing is disabled.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(3)T	This command was introduced.
Cisco IOS XE Release 3.8S	This command was integrated into Cisco IOS XE Release 3.8S.

Usage Guidelines

Use the **monitor event-trace gdoi** command to enable or disable event tracing for GDOI and to configure event trace parameters for the Cisco IOS software GDOI subsystem component.

Note Event tracing is intended for use as a software diagnostic tool and should be configured only under the direction of a Technical Assistance Center (TAC) representative.

Additionally, default settings do not appear in the configuration file. If the subsystem software enables event tracing by default, the **monitor event-trace** *component* **enable** command will not appear in the configuration file of the networking device; however, disabling event tracing that has been enabled by default by the subsystem will create a command entry in the configuration file.

To determine whether event tracing is enabled by default for the subsystem, use the **show monitor event-trace gdoi** command to display trace messages.

Examples

The following example shows how to disable event tracing for cooperative KSs.

```
Device> enable
Device# monitor event-trace gdoi coop disable
```

Related Commands

Command	Description
show monitor event-trace gdoi	Displays event trace messages for the Cisco IOS software GDOI subsystem component.
monitor event-trace gdoi	Configures event tracing for the GDOI software subsystem component.

monitor event-trace ipv6 spd

To monitor Selective Packet Discard (SPD) state transition events, use the monitor event-trace ipv6 spd command in privileged EXEC mode. To disable this function, use the **no** form of this command.

monitor event-trace ipv6 spd

no monitor event-trace ipv6 spd

Syntax Description

This command has no arguments or keywords.

Command Default

This command is disabled.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(3)T	This command was introduced.

Usage Guidelines

Use the **monitor event-trace ipv6 spd** command to check SPD state transition events.

mtu

To adjust the maximum packet size or maximum transmission unit (MTU) size, use the **mtu** command in interface configuration mode, connect configuration mode, or xconnect subinterface configuration mode. To restore the MTU value to its original default value, use the **no** form of this command.

mtu *bytes*

no mtu

Syntax Description

bytes	MTU size, in bytes.

Command Default

The table below lists default MTU values according to media type.

Table 2: Default Media MTU Values

Media Type	Default MTU (Bytes)
Ethernet	1500
Serial	1500
Token Ring	4464
ATM	4470
FDDI	4470
HSSI (HSA)	4470

Command Modes

Interface configuration (config-if) Connect configuration (xconnect-conn-config) xconnect subinterface configuration (config-if-xconn)

Command History

Release	Modification
10.0	This command was introduced.
12.0(26)S	This command was modified. This command was updated to support the connect configuration mode for Frame Relay Layer 2 interworking.
12.2(14)SX	This command was integrated into Cisco IOS Release 12.2(14)SX. Support for this command was introduced on the Supervisor Engine 720.

Release	Modification
12.2(17d)SXB	This command was modified. 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.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.2(33)SCB	This command was integrated into Cisco IOS Release 12.2(33)SCB.
Cisco IOS XE Release 2.4	This command was integrated into Cisco IOS XE Release 2.4. This command supports xconnect subinterface configuration mode.
Cisco IOS XE Release 3.7S	This command was modified as part of the MPLS-based Layer 2 VPN (L2VPN) command modifications for cross-OS support. This command was made available in template configuration mode.
15.3(1)S	This command was integrated in Cisco IOS Release 15.3(1)S.

Usage Guidelines

Each interface has a default maximum packet size or MTU size. This number generally defaults to the largest size possible for that interface type. On serial interfaces, the MTU size varies but cannot be set to a value less than 64 bytes.

Note The connect configuration mode is used only for Frame Relay Layer 2 interworking.

Changing the MTU Size

Changing the MTU size is not supported on a loopback interface.

Changing the MTU size on a Cisco 7500 series router results in the recarving of buffers and resetting of all interfaces. The following message is displayed: RSP-3-Restart:cbus complex .

You can configure native Gigabit Ethernet ports on the Cisco 7200 series router to a maximum MTU size of 9216 bytes. The MTU values range from 1500 to 9216 bytes. The MTU values can be configured to any range that is supported by the corresponding main interface.

MTU Size for an IPSec Configuration

In an IPSec configuration, such as in a crypto environment, an MTU value that is less than 256 bytes is not accepted. If you configure an MTU value less than 256 bytes, then the MTU value is automatically overwritten and given a value of 256 bytes.

Protocol-Specific Versions of the mtu Command

Changing the MTU value with the **mtu** interface configuration command can affect values for the protocol-specific versions of the command (the **ip mtu** command, for example). If the value specified with the **ip mtu** interface configuration command is the same as the value specified with the **mtu** interface configuration command, and you change the value for the **mtu** interface configuration command, the **ip mtu** value automatically matches the new **mtu** interface configuration command value. However, changing the values for the **ip mtu** configuration commands has no effect on the value for the **mtu** interface configuration command.

ATM and LANE Interfaces

ATM interfaces are not bound by what is configured on the major interface. By default, the MTU on a subinterface is equal to the default MTU (4490 bytes). A client is configured with the range supported by the corresponding main interface. The MTU can be changed on subinterfaces, but it may result in recarving of buffers to accommodate the new maximum MTU on the interface.

VRF-Aware Service Infrastructure Interfaces

The mtu command does not support the VRF-Aware Service Infrastructure (VASI) type interface.

Cisco 7600 Valid MTU Values

On the Cisco 7600 platform, the following valid values are applicable:

- For the SVI ports: from 64 to 9216 bytes
- For the GE-WAN+ ports: from 1500 to 9170 bytes
- For all other ports: from 1500 to 9216 bytes

You can receive jumbo frames on access subinterfaces also. The MTU values can be configured to any range that is supported by the corresponding main interface. If you enable the jumbo frames, the default is 64 bytes for the SVI ports and 9216 bytes for all other ports. The jumbo frames are disabled by default.

Cisco uBR10012 Universal Broadband Router

While configuring the interface MTU size on a Gigabit Ethernet SPA on a Cisco uBR10012 router, consider the following guidelines:

- The default interface MTU size accommodates a 1500-byte packet, plus 22 additional bytes to cover the following overhead:
  - Layer 2 header--14 bytes
  - Dot1Q header--4 bytes
  - CRC--4 bytes
- If you are using MPLS, be sure that the **mpls mtu** command is configured with a value less than or equal to the interface MTU.
- If you are using MPLS labels, you should increase the default interface MTU size to accommodate the number of MPLS labels. Each MPLS label adds 4 bytes of overhead to a packet.

Note For the Gigabit Ethernet SPAs on the Cisco uBR10012 router, the default MTU size is 1500 bytes. When the interface is being used as a Layer 2 port, the maximum configurable MTU is 9000 bytes.

Examples

The following example shows how to specify an MTU of 1000 bytes:

```
Device(config)# interface serial 1
Device(config-if)# mtu 1000
```

Examples

The following example shows how to specify an MTU size on a Gigabit Ethernet SPA on the Cisco uBR10012 router:

```
Device(config)# interface GigabitEthernet3/0/0
Device(config-if)# mtu 1800
```

Examples

The following example shows how to specify an MTU size on a pseudowire interface:

```
Device(config)#  interface pseudowire 100
Device(config-if)# encapsulation mpls
Device(config-if)# mtu 1800
```

Examples

The following example shows how to configure a template and specify an MTU size in template configuration mode: :

```
Device(config)#  template type pseudowire template1
Device(config-if)# encapsulation mpls
Device(config-if)# mtu 1800
```

Related Commands

Command	Description
encapsulation (pseudowire)	Specifies an encapsulation type for tunneling Layer 2 traffic over a pseudowire.
encapsulation smds	Enables SMDS service on the desired interface.
ip mtu	Sets the MTU size of IP packets sent on an interface.

name

To configure the redundancy group with a name, use the **name**command in redundancy application group configuration mode. To remove the name of a redundancy group, use the **no** form of this command.

name *group-name*

no name *group-name*

Syntax Description

group-name	Name of the redundancy group.

Command Default

The redundancy group is not configured with a name.

Command Modes

Redundancy application group configuration (config-red-app-grp)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.

Examples

The following example shows how to configure the redundancy group name as group1:

```
Router# configure terminal
Router(config)# redundancy
Router(config-red)# application redundancy
Router(config-red-app)# group 1
Router(config-red-app-grp)# name group1
```

Related Commands

Command	Description
application redundancy	Enters redundancy application configuration mode.
group(firewall)	Enters redundancy application group configuration mode.
shutdown	Shuts down a group manually.

name (view)

To change the name of a lawful intercept view, use the **name**command in view configuration mode. To return to the default lawful intercept view name, which is "li-view," use the **no** form of this command.

name *new-name*

no name *new-name*

Syntax Description

new-name	Lawful intercept view name.

Command Default

A lawful intercept view is called "li-view."

Command Modes

View configuration (config-view)

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
12.2(33)SXI	This command was integrated into Cisco IOS Release 12.2(33)SXI.

Usage Guidelines

Only a system administrator or a level 15 privilege user can change the name of a lawful intercept view.

Examples

The following example shows how to configure a lawful intercept view and change the view name to "myliview":

```
!Initialize the LI-View.
Router(config-view)# li-view lipass user li_admin password li_adminpass
00:19:25:%PARSER-6-LI_VIEW_INIT:LI-View initialized.
Router(config-view)# name myliview
Router(config-view)# end
```

Related Commands

Command	Description
li-view	Initializes a lawful intercept view.

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

named-key

To specify which peer's RSA public key you will manually configure and enter public key configuration mode, use the **named-key** command in public key chain configuration mode. This command should be used only when the router has a single interface that processes IP Security (IPSec).

named-key *key-name* [**encryption**| **signature**]

Syntax Description

key-name	Specifies the name of the remote peer's RSA keys. This is always the fully qualified domain name of the remote peer; for example, router.example.com.
encryption	(Optional) Indicates that the RSA public key to be specified will be an encryption special-usage key.
signature	(Optional) Indicates that the RSA public key to be specified will be a signature special-usage key.

Command Default

If neither the **encryption** nor the **signature** keyword is used, general-purpose keys will be specified.

Command Modes

Public key chain 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

Use this command or the **addressed-key** command to specify which IPSec peer's RSA public key you will manually configure next.

Follow this command with the **key-string** command to specify the key.

If you use the **named-key** command, you also need to use the **address** public key configuration command to specify the IP address of the peer.

If the IPSec remote peer generated general purpose RSA keys, do not use the **encryption** or **signature** keyword.

If the IPSec remote peer generated special usage keys, you must manually specify both keys: perform this command and the **key-string** command twice and use the **encryption** and **signature** keywords in turn.

Examples

The following example manually specifies the RSA public keys of two IPSec peers. The peer at 10.5.5.1 uses general-purpose keys, and the other peer uses special-purpose keys.

```
crypto key pubkey-chain rsa
  named-key otherpeer.example.com
  address 10.5.5.1
  key-string
 005C300D 06092A86 4886F70D 01010105
 00034B00 30480241 00C5E23B 55D6AB22
 04AEF1BA A54028A6 9ACC01C5 129D99E4
 64CAB820 847EDAD9 DF0B4E4C 73A05DD2
 BD62A8A9 FA603DD2 E2A8A6F8 98F76E28
 D58AD221 B583D7A4 71020301 0001
 quit
 exit
  addressed-key 10.1.1.2 encryption
  key-string
 00302017 4A7D385B 1234EF29 335FC973
 2DD50A37 C4F4B0FD 9DADE748 429618D5
 18242BA3 2EDFBDD3 4296142A DDF7D3D8
 08407685 2F2190A0 0B43F1BD 9A8A26DB
 07953829 791FCDE9 A98420F0 6A82045B
 90288A26 DBC64468 7789F76E EE21
 quit
  exit
  addressed-key 10.1.1.2 signature
  key-string
 0738BC7A 2BC3E9F0 679B00FE 098533AB
 01030201 42DD06AF E228D24C 458AD228
 58BB5DDD F4836401 2A2D7163 219F882E
 64CE69D4 B583748A 241BED0F 6E7F2F16
 0DE0986E DF02031F 4B0B0912 F68200C4
 C625C389 0BFF3321 A2598935 C1B1
 quit
  exit
  exit
```

Related Commands

Command	Description
address	Specifies the IP address of the remote RSA public key of the remote peer you will manually configure.
addressed-key	Specifies the RSA public key of the peer you will manually configure.
crypto key pubkey-chain rsa	Enters public key configuration mode (to allow you to manually specify the RSA public keys of other devices).
key-string (IKE)	Specifies the RSA public key of a remote peer.
show crypto key pubkey-chain rsa	Displays peer RSA public keys stored on your router.

nas

To add an access point or router to the list of devices that use the local authentication server, use the **nas**command in local RADIUS server configuration mode. To remove the identity of the network access server (NAS) that is configured on the local RADIUS server, use the **no** form of this command.

nas *ip-address* **key shared-key**

no nas *ip-address* **key shared-key**

Syntax Description

ip-address	IP address of the access point or router.
key	Specifies a key.
shared-key	Shared key that is used to authenticate communication between the local authentication server and the access points and routers that use this authenticator.

Command Default

No default behavior or values

Command Modes

Local RADIUS server configuration

Command History

Release	Modification
12.2(11)JA	This command was introduced on the Cisco Aironet Access Point 1100 and the Cisco Aironet Access Point 1200.
12.3(11)T	This command was integrated into Cisco IOS Release 12.3(11)T and implemented on the following platforms: Cisco 2600XM, Cisco 2691, Cisco 2811, Cisco 2821, Cisco 2851, Cisco 3700, and Cisco 3800 series routers.

Examples

The following command adds the access point having the IP address 192.168.12.17 to the list of devices that use the local authentication server, using the shared key named shared256.

```
Router(config-radsrv)# nas 192.168.12.17 key shared256
```

Related Commands

Command	Description
block count	Configures the parameters for locking out members of a group to help protect against unauthorized attacks.

Command	Description
clear radius local-server	Clears the statistics display or unblocks a user.
debug radius local-server	Displays the debug information for the local server.
group	Enters user group configuration mode and configures shared setting for a user group.
radius-server host	Specifies the remote RADIUS server host.
radius-server local	Enables the access point or router to be a local authentication server and enters into configuration mode for the authenticator.
reauthentication time	Specifies the time (in seconds) after which access points or wireless-aware routers must reauthenticate the members of a group.
show radius local-server statistics	Displays statistics for a local network access server.
ssid	Specifies up to 20 SSIDs to be used by a user group.
user	Authorizes a user to authenticate using the local authentication server.
vlan	Specifies a VLAN to be used by members of a user group.

nasi authentication

To enable authentication, authorization, and accounting (AAA) authentication for NetWare Asynchronous Services Interface (NASI) clients connecting to a router, use the **nasi authentication** command in line configuration mode. To return to the default, as specified by the **aaa authentication nasi** command, use the **no** form of the command.

nasi authentication {**default**| *list-name*}

no nasi authentication {**default**| *list-name*}

Syntax Description

default	Uses the default list created with the **aaa authentication nasi** command.
list-name	Uses the list created with the **aaa authentication nasi**command.

Command Default

Uses the default set with the **aaa authentication nasi** command.

Command Modes

Line configuration

Command History

Release	Modification
11.1	This command was introduced.
12.2(15)T	This command is no longer supported in Cisco IOS Mainline or Technology-based (T) releases. It may continue to appear in 12.2S-family releases.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

This command is a per-line command used with AAA authentication that specifies the name of a list of authentication methods to try at login. If no list is specified, the default list is used, even if it is not specified in the command line. (You create defaults and lists with the **aaa authentication nasi** command.) Entering the **no** form of this command has the same effect as entering the command with the **default** argument.

Caution If you use a *list-name* value that was not configured with the **aaa authentication nasi**command, you will disable login on this line.

Before issuing this command, create a list of authentication processes by using the **aaa authentication nasi** global configuration command.

Examples

The following example specifies that the default AAA authentication be used on line 4:

```
line 4
 nasi authentication default
```

The following example specifies that the AAA authentication list called *list1*be used on line 7:

```
line 7
 nasi authentication list1
```

Related Commands

Command	Description
aaa authentication nasi	Specifies AAA authentication for NASI clients connecting through the access server.
ipx nasi-server enable	Enables NASI clients to connect to asynchronous devices attached to a router.
show ipx nasi connections	Displays the status of NASI connections.
show ipx spx-protocol	Displays the status of the SPX protocol stack and related counters.

nat (IKEv2 profile)

To configure Network Address Translation (NAT) keepalive for Internet Key Exchange Version 2 (IKEv2), use the **nat**command in IKEv2 profile configuration mode. To delete NAT keepalive configuration, use the **no** form of this command.

nat keepalive *interval*

no nat keepalive

Syntax Description

keepalive *interval*	Specifies the NAT keepalive interval in seconds.

Command Default

NAT keepalive is disabled.

Command Modes

IKEv2 profile configuration (config-ikev2-profile)

Command History

Release	Modification
15.1(1)T	This command was introduced.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.

Usage Guidelines

Use this command to configure NAT keepalive. NAT keepalive configuration specified in an IKEv2 profile overrides the global configuration. NAT keepalive prevents the NAT translation entries from deletion in the absence of any traffic when there is NAT between IKE peers.

Examples

The following example shows how to specify the NAT keepalive interval:

```
Router(config)# crypto ikev2 profile prf1
Router(config-ikev2-profile)# nat keepalive 500
```

Related Commands

Command	Description
crypto ikev2 nat	Defines NAT keepalive globally for all peers.
crypto ikev2 profile	Defines an IKEv2 profile.

nbns-list

To enter the webvpn NBNS list configuration mode to configure a NetBIOS Name Service (NBNS) server list for Common Internet File System (CIFS) name resolution, use the **nbns-list** command in webvpn context configuration mode. To remove the NBNS server list from the SSL VPN context configuration, use the **no** form of this command.

nbns-list *name*

no nbns-list *name*

Syntax Description

name	Name of the NBNS list. The name can be up to 64 characters in length. This argument is case sensitive.

Command Default

Webvpn NBNS list configuration mode is not entered, and a NBNS server list cannot be configured.

Command Modes

Webvpn context configuration

Command History

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

Usage Guidelines

The NBNS server list is used to configure a list of Windows Internet Name Service (WINS) to resolve Microsoft file-directory shares. Entering the **nbns-list**command places the router in webvpn NBNS list configuration mode. You can specify up to three NetBIOS name servers. A single server is configured as the master browser if multiple servers are specified in the server list.

Note NBNS and CIFS resolution is supported only on Microsoft Windows 2000 or Linux Samba servers.

Examples

The following example configures an NBNS server list:

```
Router(config)# webvpn context context1

Router(config-webvpn-context)# nbns-list SERVER_LIST
Router(config-webvpn-nbnslist)# nbns-server 172.16.1.1 master

Router(config-webvpn-nbnslist)# nbns-server 172.16.2.2 timeout 10 retries 5

Router(config-webvpn-nbnslist)# nbns-server 172.16.3.3 timeout 10 retries 5

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

Related Commands

Command	Description
nbns-server	Adds a server to an NBNS server list.
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

nbns-list (policy group)

To attach a NetBIOS name service (NBNS) server list to a policy group configuration, use the **nbns-list**command in webvpn group policy configuration mode. To remove the NBNS server list from the policy group configuration, use the **no** form of this command.

nbns-list *name*

no nbns-list

Syntax Description

name	Name of the NBNS server list that was configured in webvpn context configuration mode.

Command Default

An NBNS server list is not attached to a policy group configuration.

Command Modes

Webvpn group policy configuration

Command History

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

Usage Guidelines

The configuration of this command applies to only clientless mode configuration.

Examples

The following example applies the NBNS server list to the policy group configuration:

```
Router(config)# webvpn context context1

Router(config-webvpn-context)# nbns-list SERVER_LIST
Router(config-webvpn-nbnslist)# nbns-server 172.16.1.1 master

Router(config-webvpn-nbnslist)# nbns-server 172.16.2.2 timeout 10 retries 5

Router(config-webvpn-nbnslist)# nbns-server 172.16.3.3 timeout 10 retries 5

Router(config-webvpn-nbnslist)# exit

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

Router(config-webvpn-group)# nbns-list SERVER_LIST

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

Related Commands

Command	Description
nbns-list	Enters webvpn NBNS list configuration mode to configure a NBNS server list for CIFS name resolution.
nbns-server	Adds a server to an NBNS server list.
policy group	Enters webvpn group policy configuration mode to configure a group policy.
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

nbns-server

To add a server to a NetBIOS name service (NBNS) server list, use the **nbns-server** command in webvpn NBNS list configuration mode. To remove the server entry from the NBNS server list, use the **no** form of this command.

nbns-server *ip-address* **[master]** [**timeout** *seconds*] [**retries** *number*]

no nbns-server *ip-address* **[master]** [**timeout** *seconds*] [**retries** *number*]

Syntax Description

ip-address	The IPv4 address of the NetBIOS server.
master	(Optional) Configures a single NetBIOS server as the master browser.
timeout *seconds*	(Optional) Configures the length of time, in seconds, that the networking device will wait for a query reply before sending a query to another NetBIOS server. A number from 1 through 30 can be configured for this argument.
retries *number*	(Optional) Number of times that the specified NetBIOS server will be queried. A number from 0 through 10 can be configured for this argument. Entering the number 0 configures the networking device not to resend a query.

Command Default

The following default values are used if this command is not configured or if the **no** form is entered:

timeout 2 **retries** 2

Command Modes

Webvpn NBNS list configuration

Command History

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

Usage Guidelines

The server specified with the *ip-address*argument can be a primary domain controller (PDC) in a Microsoft network. A Windows Internet Naming Service (WINS) server cannot and should not be specified. When multiple NBNS servers are specified, a single server is configured as master browser.

Examples

The following example adds three servers to an NBNS server list:

```
Router(config)# webvpn context context1

Router(config-webvpn-context)# nbns-list SERVER_LIST
Router(config-webvpn-nbnslist)# nbns-server 172.16.1.1 master

Router(config-webvpn-nbnslist)# nbns-server 172.16.2.2 timeout 10 retries 5

Router(config-webvpn-nbnslist)# nbns-server 172.16.3.3 timeout 10 retries 5
```

Related Commands

Command	Description
nbns-list	Enters webvpn NBNS list configuration mode to configure a NBNS server list for CIFS name resolution.
webvpn context	Enters webvpn context configuration mode to configure the SSL VPN context.

netmask

To specify the subnet mask to be used by the client for local connectivity, use the **netmask** command in ISAKMP group configuration mode or IKEv2 group configuration mode. To disable the mask, use the **no** form of this command.

netmask *mask*

no netmask *mask*

Syntax Description

mask	Subnet mask address.

Command Default

Default mask is used.

Command Modes

ISAKMP group configuration (config-isakmp-group) IKEv2 client group configuration (config-ikev2-client-config-group)

Command History

Release	Modification
12.2(8)T	This command was introduced on the Easy VPN remote.

Usage Guidelines

Use this command to specify the subnet mask for the IP address assigned to the client.

Examples

The following example shows that the subnet mask 255.255.255.255 is to be downloaded to the client:

```
crypto isakmp client configuration group group1
 netmask 255.255.255.255
```

no crypto engine software ipsec

To disable hardware crypto engine failover to the software crypto engine, use the **no crypto engine software ipsec**command in global configuration mode. To reenable failover, use the **crypto engine software ipsec**form of this command.

no crypto engine software ipsec

crypto engine software ipsec

Syntax Description

This command has no arguments or keywords.

Command Default

Failover is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.1E	This command was introduced.
12.3(14)T	This command was integrated into Cisco IOS Release 12.3(14)T.
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 for those situations in which the amount of IP Security (IPSec) traffic is more than can be handled (because of bandwidth) by the software routines on the CPU.

Examples

The following example shows that hardware crypto engine failover to the software crypto engine has been disabled:

```
no crypto engine software ipsec
```

The following example shows that hardware crypto engine failover has been reenabled:

```
crypto engine software ipsec
```

Related Commands

Command	Description
crypto engine accelerator	Enables the onboard hardware accelerator of the router for IPSec encryption.

no crypto xauth

To ignore extended authentication (Xauth) during an Internet Key Exchange (IKE) Phase 1 negotiation, use the **no crypto xauth** command in global configuration mode. To consider Xauth proposals, use the **crypto xauth** command.

no crypto xauth *interface*

crypto xauth *interface*

Syntax Description

interface	Interface whose IP address is the local endpoint to which the remote peer will send IKE requests.

Command Default

No default behaviors or values

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

The **no** version of this command was introduced to support Unity clients that do not require Xauth when using Internet Security Association and Key Management Protocol (ISAKMP) profiles.

Note This command does not support loopback interfaces.

Examples

The following example shows that Xauth proposals on Ethernet 1/1 are to be ignored:

```
no crypto xauth Ethernet1/1
```

no ip inspect

To turn off Context-based Access Control (CBAC) completely at a firewall, use the **no ip inspect** command in global configuration mode.

no ip inspect

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
11.2 P	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

Turn off CBAC with the **no ip inspect** global configuration command.

Note The **no ip inspect** command removes all CBAC configuration entries and resets all CBAC global timeouts and thresholds to the defaults. All existing sessions are deleted and their associated access lists are removed.

Examples

The following example turns off CBAC at a firewall:

```
no ip inspect
```

no ip ips sdf builtin

To instruct the router not to load the built-in signatures if it cannot find the specified signature definition files (SDFs), use the **no ip ips sdf builtin**command in global configuration mode.

no ip ips sdf builtin

Syntax Description

This command has no arguments or keywords.

Command Default

If the router fails to load the SDF, the router will load the default, built-in signatures.

Command Modes

Global configuration

Command History

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

Usage Guidelin

Caution If the **no ip ips sdf builtin** command is issued and the router running Intrusion Prevention System (IPS) fails to load the SDF, you will receive an error message stating that IPS is completely disabled.

Examples

The following example shows how to instruct the router not to refer to the default, built-in signature if the attack-drop.sdf file fails to load:

```
Router(config) no ip ips sdf builtin
```

Related Commands

Command	Description
copy ips-sdf	Loads or saves the SDF in the router.
ip ips sdf location	Specifies the location in which the router will load the SDF.

non-standard (config-radius-server)

To identify that the security server is using a vendor-proprietary implementation of RADIUS, use the **non-standard** command in RADIUS server configuration mode. To delete the specified vendor-proprietary RADIUS host, use the **no** form of this command.

non-standard

no non-standard

Syntax Description

This command has no arguments or keywords.

Command Default

Nonstandard RADIUS attributes are not supported.

Command Modes

RADIUS server configuration (config-radius-server)

Command History

Release	Modification
15.2(2)T	This command was introduced.

Usage Guidelines

Use the **non-standard** command to identify that the RADIUS server is using a vendor-proprietary implementation of RADIUS. Although an IETF draft standard for RADIUS specifies a method for communicating information between the network access server and the RADIUS server, some vendors have extended the RADIUS attribute set in a unique way. This command enables the Cisco IOS software to support the most common vendor-proprietary RADIUS attributes. Vendor-proprietary attributes will not be supported unless you use the **non-standard** command in RADIUS server configuration mode.

For a list of supported vendor-specific RADIUS attributes, refer to the appendix "RADIUS Attributes" in the *Cisco IOS Security Configuration Guide*.

Examples

The following example shows how to specify a vendor-proprietary RADIUS server host 192.0.2.2:

```
Device(config)# aaa new-model
Device(config)# radius server myserver
Device(config-radius-server)# address ipv4 192.0.2.2
Device(config-radius-server)# non-standard
```

Related Commands

Command	Description
aaa new-model	Enables the AAA access control model.
address ipv4	Configures the IPv4 address for the RADIUS server accounting and authentication parameters.

Command	Description
radius server	Specifies the name for the RADIUS server configuration and enters RADIUS server configuration mode.

object-group (Catalyst 6500 series switches)

To define object groups that you can use to optimize your configuration, use the **object-group** global configuration mode command. To remove object groups from the configuration use the **no** form of this command .

object-group ip {**address** *obj-grp-id*| **port** *obj-grp-id*}

no object-group ip {**address** *obj-grp-id*| **port** *obj-grp-id*}

Syntax Description

ip	Specifies the IP object group.
address *obj-grp-id*	Specifies the IP address of the object group and allows you to define the object group name and enter IP-address object-group configuration mode. See the "Usage Guidelines" section for more information.
port *obj-grp-id*	Specifies the IP port of the object group and allows you to create or modify a PBACL protocol port object group. See the "Usage Guidelines" section for more information.

Command Default

This command has no default settings.

Command Modes

The following table shows the modes in which you can enter the command:

Command Mode	Firewall Mode	Security Context			
Routed	Transparent	Single	Multiple		
			Context	System	
Global configuration	Yes	Yes	Yes	Yes	No

Command History

Release	Modification
12.2(33)SXH	This command was introduced on the Catalyst 6500 series switches.

Usage Guidelines

This command supports IPv4 and IPv6 addresses.

Objects such as hosts, protocols, or services can be grouped, and then you can issue a single command using the group name to apply to every item in the group.

When you define a group with the **object-group** command and then use any security appliance command, the command applies to every item in that group. This feature can significantly reduce your configuration size.

Once you define an object group, you must use the **object-group** keyword before the group name in all applicable security appliance commands as follows:

```
Router# show running-config object-group group-name
```
where group-name is the name of the group.

This example shows the use of an object group once it is defined:

```
Router(config)# access-list access_list_name permit tcp any object-group group-name
```
In addition, you can group access list command arguments:

Individual Argument	Object Group Replacement
protocol	**object-group** *protocol*
host and subnet	**object-group** *network*
service	**object-group** *service*
icmp-type	**object-group** *icmp-type*

You can group commands hierarchically; an object group can be a member of another object group.

To use object groups, you must do the following:

- Use the object-group keyword before the object group name in all commands as follows:

```
Router(config)# access-list acl permit tcp object-group remotes object-group locals
object-group eng-svc
```
where **remotes** and **locals** are sample object group names.

- The object group must be nonempty.
- You cannot remove or empty an object group if it is being used in a command.

Use the **exit**, **quit**, or any valid config-mode commands such as **access-list** to close an object-group mode and exit the object-group main command.

The **show running-config object-group** command displays all defined object groups by their grp-id when the **show running-config object-group** *group-id* command is entered, and by their group type when you enter the **show running-config object-group** *group-type* command. When you enter the **show running-config object-group** command without an argument, all defined object groups are shown.

Use the **clear configure object-group** command to remove a group of previously defined object-group commands. Without an argument, the **clear configure object-group** command lets you to remove all defined object groups that are not being used in a command. Use of the group-type argument removes all defined object groups that are not being used in a command for that group type only.

You can use all other security appliance commands in an object-group mode, including the **show running-config** and **clear configure** commands

Commands within the object-group mode appear indented when displayed or saved by the **show running-config object-group**, **write**, or **config** commands.

Commands within the object-group mode have the same command privilege level as the main command.

When you use more than one object group in an access-list command, the elements of all object groups that are used in the command are linked, starting with the elements of the first group with the elements of the second group, then the elements of the first and second groups together with the elements of the third group, and so on.

The starting position of the description text is the character right immediately following the white space (a blank or a tab) following the description keyword.

When you enter the object-group ip address command, the prompt changes to Router(config-ipaddr-ogroup)# and allows you to create or modify a PBACL protocol port object group.

The following IP address object-group configuration commands are available:

- **A.B.C.D** --Specifies the network address of the object-group members.
- **end** --Exits from configuration mode.
- **exit** --Exits from IP object-group configuration mode.
- **host** *address* or **host** *name*--Specifies the host address or name of the object-group member.
- **no** --Negates or sets the default values of a command.

Use the **no** form of the command to delete the object group with the specified name.

When you enter the object-group ip port command, the prompt changes to Router(config-port-ogroup)# and allows you to define the object group name and enter port object-group configuration mode. The following port object-group configuration commands are available:

- **end** --Exits from configuration mode.
- eq number--Matches only packets on a given port number; valid values are from 0 to 65535.
- **exit** --Exits from the IP object-group configuration mode.
- gt number--Matches only packets on a given port number; valid values are from 0 to 65535.
- lt number--Matches only packets with a lower port number; valid values are from 0 to 65535.
- neq number--Matches only packets with a lower port number; valid values are from 0 to 65535.
- **no** --Negates or sets default values of a command.
- range number number--Matches only packets in the range of port numbers; valid values are from 0 to 65535.

Use the **no** form of the command to delete the object group with the specified name.

Examples

This example shows how to create an object group with three hosts and a network address:

```
Router(config)# object-group ip address myAG
Router(config-ipaddr-pgroup)# host 10.20.20.1
```

```
Router(config-ipaddr-pgroup)# host 10.20.20.5
Router(config-ipaddr-pgroup)# 10.30.0.0 255.255.0.0
```

This example shows how to create a port object group that matches protocol port 100 and any port greater than 200, except 300:

```
Router(config)# object-group ip port myPG
Router(config-port-pgroup)# eq 100
Router(config-port-pgroup)# gt 200
Router(config-port-pgroup)# neq 300
```

Related Commands

Command	Description
clear configure object-group	Removes all the object group commands from the configuration.
group-object	Adds network object groups.
network-object	Adds a network object to a network object group.
port-object	Adds a port object to a service object group.
show running-config object-group	Displays the current object groups.

object-group network

To define network object groups for use in object group-based ACLs (OGACLs) and enter network object-group configuration mode (config-network-group), use the **object-group network** command in global configuration mode. To remove network object groups from the configuration, use the **no** form of this command.

object-group network *object-group-name*

no object-group network *object-group-name*

Syntax Description

object-group-name	Specifies a name for a network type of object group. *object-group-name* is a sequence of 1 to 64 characters consisting of letters, digits, underscores (_), dashes (-), or periods (.). *object-group-name* must start with a letter.

Command Default

No network object groups are created.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(20)T	This command was introduced.
15.0(1)M	This command was modified. The any command was added as a command in network object-group configuration mode.

Usage Guidelines

A network object group is a group of any of the following objects: hostnames, host IP addresses, subnets, ranges of IP addresses, or existing network object groups. A network object group is an ordered list and can be used in an ACL or in other commands. You can use a single command using the group name to apply to every object in the group.

This command supports only IPv4 addresses.

Commands within the network object-group mode appear indented when displayed or saved by the **write memory**or **show running-config** commands.

Commands within the network object-group mode have the same command privilege level as the main command.

When you enter the **object-group network** command, the command mode enters network object-group configuration mode (config-network-group) and allows you to populate or modify a network OGACL. The following commands are available in this mode:

- **any** --Specifies any IP address for an object group. The effect is to to allow any IP address in the range of 0.0.0.0 to 255.255.255.255 to be used in an object group.

This command supports only IPv4 addresses.

- **description** *description-text* --Description of the object or object group (you can use up to 200 characters).
- **group-object** *nested-object-group-name* --Existing network object group (child) to be included in the current object group (parent).

The type of child object group must match that of the parent (for example, if you are creating a network object group, you must specify another network object group as the child).

You can use duplicated objects in an object group if it is because of the inclusion of group objects. For example, if object 1 is in both group A and group B, you can define a group C that includes both A and B. However, you cannot include a group object that causes the group hierarchy to become circular (for example, you cannot include group A in group B and then also include group B in group A).

You can use an unlimited number of nested object groups (however, a maximum of two levels is recommended).

- **host** {*host-address* | *host-name*}--Host object. If you specify a host address, you must use an IPv4 address.
- **network-address {/nn | network-mask}** --Specifies a subnet object for the object group.

When the command is used in the network-address /nn format to create a subnet object, for example 209.165.201.0 /27, the 27 most significant bits are allocated for the network prefix number, and the remaining 5 bits are reserved for host addressing. If the same subnet object is created using the network-address network-mask format of the command, the command appears as 209.165.201.31 255.255.255.224. In this case, the subnet mask is 255.255.255.224. The default subnet mask is 255.255.255.255.

Using a subnet mask of 0.0.0.0 includes any address in the range 0.0.0.0 to 255.255.255.255 in the subnet object--this gives the subnet object the same range as the range specified by the **any** command.

The network-address command supports only IPv4 addresses.

- **range** *host-address1 host-address2* --Species the range of host IP addresses for an object group.

If the range specified is 0.0.0.0 to 255.255.255.255 this specifies that any IP address can be used as a host IP address--this has the same effect as the **any** command, which specifies that any IP address can be used.

If the same IP address is used for host-address1 and host-address2, the effect is the same as using the **host** command--the identical IP address specified becomes the single host IP address for the object group.

This command supports only IPv4 addresses.

Use the **no** form of the command to delete the object group with the specified name. (You cannot delete an object group that is being used within an ACL or a CPL policy.)

Examples

The following example shows how to configure a network object group named my_network_object_group that contains two hosts and a subnet as objects.

```
Router> enable
Router# configure terminal
Router(config)# object-group network my_network_object_group
Router(config-network-group)# host 10.20.20.1
```

```
Router(config-network-group)# host 10.20.20.5
Router(config-network-group)# 10.30.0.0 255.255.0.0
```

The following example shows how to configure a network object group named sjc_ftp_servers that contains two hosts , a subnet, and an existing object group (child) named sjc_eng_ftp_servers as objects.

```
Router> enable
Router# configure terminal
Router(config)#object-group network sjc_ftp_servers
Router(config-network-group)# host sjc.eng.ftp
Router(config-network-group)# host 172.23.56.195
Router(config-network-group)# 209.165.200.225 255.255.255.224
Router(config-network-group)# group-object sjc_eng_ftp_servers
```

The following example creates an object group called printer_users and specifies any IP address for the object group:

```
Router> enable
Router# configure terminal
Router(config)# object-group network printer_users
Router(config-network-group)# description sw_engineers
Router(config-network-group)# any
```

The following example creates an object group called printer_users and specifies a range of host IP addresses from 209.165.202.129 to 255.255.255.255 for the object group:

```
Router> enable
Router# configure terminal
Router(config)# object-group network printer_users
Router(config-network-group)# description sw_engineers
Router(config-network-group)# range 209.165.202.129 255.255.255.255
```

Related Commands

Command	Description
deny	Sets conditions in a named IP access list or OGACL that will deny packets.
ip access-group	Applies an ACL or OGACL to an interface or a service policy map.
ip access-list	Defines an IP access list or OGACL by name or number.
object-group service	Defines service object groups for use in OGACLs.
permit	Sets conditions in a named IP access list or OGACL that will permit packets.
show ip access-list	Displays the contents of IP access lists or OGACLs.
show object-group	Displays information about object groups that are configured.

object-group security

To create an object group to identify traffic coming from a specific user or endpoint, use the **object-group security** command in global configuration mode. To remove the object group, use the **no** form of this command.

object-group security *name*

no object-group security *name*

Syntax Description

name	Object group name.

Command Default

No object group is defined.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

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

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

Examples

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

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

Related Commands

Command	Description
debug object-group event	Enables debug messages for object-group events.
group-object	Specifies a nested reference to a type of user group.
match group-object security	Matches traffic from a user in the security group.
security-group	Specifies the membership of the security group for an object group.
show object-group	Displays the content of all user groups.

object-group service

To define service object groups for use in object group-based ACLs (OGACLs), use the **object-group service**command in global configuration mode. To remove service object groups from the configuration, use the **no** form of this command.

object-group service *object-group-name*

no object-group service *object-group-name*

Syntax Description

object-group-name	Specifies a service type of object group.

Command Default

No service object groups are created.

Command Modes

Global configuration (config)

Command History

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

Usage Guidelines

A service object group is a group of any of the following objects:

- Source and destination protocol ports (such as Telnet or SNMP)
- ICMP types (such as echo, echo-reply, or host-unreachable)
- Top-level protocols (such as TCP, UDP, or ESP)
- Existing service object groups

A service object group is an ordered list and can be used in an ACL or other commands. You can use a single command using the group name to apply to every object in the group.

This command supports only IPv4 addresses.

Commands within the service object-group mode appear indented when displayed or saved by the **write**or **config** commands.

Commands within the service object-group mode have the same command privilege level as the main command.

When you use more than one object group in an access-list command, the elements of all object groups that are used in the command are linked, starting with the elements of the first group with the elements of the second group, then the elements of the first and second groups together with the elements of the third group, and so on.

When you enter the object-group service command, the prompt changes to Router(config-service-group)# and allows you to populate or modify a service OGACL. The following commands are available in this mode:

- **description** *description-text* --Description of the object or object group (you can use up to 200 characters).
- *protocol* --(Required) Specifies an IP protocol number or name. You can use any one of the following values:
  - *number*--IP protocol number. The range is 0 to 255.
  - **ahp**--Authentication Header Protocol.
  - **eigrp**--Cisco EIGRP routing protocol.
  - **esp**--Encapsulation Security Payload.
  - **gre**--Cisco GRE tunneling.
  - **igmp**--Internet Gateway Message Protocol.
  - **ip**--Any Internet Protocol.
  - **ipinip**--IP in IP tunneling.
  - **nos**--KA9Q NOS compatible IP over IP tunneling.
  - **ospf**--OSPF routing protocol.
  - **pcp**--Payload Compression Protocol.
  - **pim**--Protocol Independent Multicast.
- **tcp** | **udp** | **tcp-udp**[source {{[eq] | lt | gt } *port1* | range *port1 port2*}] [{[eq] | lt | gt } *port1* | range *port1 port2*] --Transmission Control Protocol, User Datagram Protocol, or both.
  - **source**--Specifies a source port or ports. Specifying a source port or ports is optional, but when specifying them, the **source**keyword is required. Specifying a destination port or ports is optional. To specify destination ports, you specify an optional or required operator and a port value or values.
  - *operator port1*[*port2*]--Use the following operator keywords to specify a port value or a range of ports:

eq --Single port value *port1*. When no *operator*is specified, the default is **eq**. However, this keyword is always present in the configuration file.

The following keywords are required when specifying a range of ports.

range --Range of ports between *port1* and *port2*, inclusive.

l**t**--All port values that are less than *port1*.

gt --All port values that are greater than *port1*.

- • *port1* [*port2*]--Decimal number or name of a TCP and/or UDP service. The value of the number ranges from 0 to 65535. If a name is specified, the name must be one of the supported TCP or UDP port name (or both). If a number is specified, translation to its corresponding name (if one exists) based on the protocol type will be made when showing the object configuration.

Following are the supported services for TCP:

0 -65535--Port number.

bgp --Border Gateway Protocol (179).

chargen --Character generator (19).

cmd --Remote commands (rcmd, 514).

daytime --Daytime (13).

discard --Discard (9).

domain --Domain Name Service (53).

drip --Dynamic Routing Information Protocol (3949).

echo --Echo (7).

exec --Exec (rsh, 512).

finger --Finger (79).

ftp --File Transfer Protocol (21).

ftp-data --FTP data connections (20).

gopher --Gopher (70).

hostname --NIC hostname server (101).

ident --Ident Protocol (113).

irc --Internet Relay Chat (194).

klogin --Kerberos login (543).

kshell --Kerberos shell (544).

login --Login (rlogin, 513).

lpd --Printer service (515).

nntp --Network News Transport Protocol (119).

pim-auto-rp PIM Auto-RP (496).

pop2 --Post Office Protocol v2 (109).

pop3 --Post Office Protocol v3 (110).

smtp --Simple Mail Transport Protocol (25).

sunrpc --Sun Remote Procedure Call (111).

tacacs --TAC Access Control System (49).

talk --Talk (517).

telnet --Telnet (23).

time --Time (37).

uucp --Unix-to-Unix Copy Program (540).

whois --Nicname (43).

www --World Wide Web (HTTP, 80).

Following are the supported services for UDP:

0 -65535--Port number.

biff --Biff (mail notification, comsat, 512).

bootpc --Bootstrap Protocol (BOOTP) client (68).

bootps --Bootstrap Protocol (BOOTP) server (67).

discard --Discard (9).

dnsix --DNSIX security protocol auditing (195).

domain --Domain Name Service (DNS, 53).

echo --Echo (7).

isakmp --Internet Security Association and Key Management Protocol (500).

mobile-ip --Mobile IP registration (434).

nameserver --IEN116 name service (obsolete, 42).

netbios-dgm --NetBios datagram service (138).

netbios-ns --NetBios name service (137).

netbios-ss --NetBios session service (139).

non500-isakmp Internet Security Association and Key Management Protocol (4500).

ntp --Network Time Protocol (123).

pim-auto-rp --PIM Auto-RP (496).

rip --Routing Information Protocol (router, in.routed, 520).

snmp --Simple Network Management Protocol (161).

snmptrap --SNMP Traps (162).

sunrpc --Sun Remote Procedure Call (111).

syslog --System Logger (514).

tacacs --TAC Access Control System (49).

talk --Talk (517).

tftp --Trivial File Transfer Protocol (69).

time --Time (37).

who --Who service (rwho, 513).

xdmcp --X Display Manager Control Protocol (177).

Following are the supported services for TCP and UDP:

0 -65535--Port number.

discard --Discard (9).

domain --Domain Name Service (53).

echo --Echo (7).

pim-auto-rp --PIM Auto-RP (496).

sunrpc --Sun Remote Procedure Call (111).

syslog --Syslog (514).

tacacs --TAC Access Control System (49).

talk --Talk (517).

- **icmp** *icmp-type* --Decimal number or name of an Internet Control Message Protocol (ICMP) type:

Following are the supported ICMP types:

- - **0 -65535**--Port number.
  - **alternate-address** --Alternate address.
  - **conversion-error** --Datagram conversion.
  - **echo** --Echo (ping).
  - **echo-reply** --Echo reply.
  - **information-reply** --Information replies.
  - **information-request** --Information requests.
  - **mask-reply** --Mask replies.
  - **mask-request** --Mask requests.
  - **mobile-redirect** --Mobile host redirect.
  - **parameter-problem** --All parameter problems.
  - **redirect** --All redirects.
  - **router-advertisement** --Router discovery advertise.
  - **router-solicitation** --Router discovery solicitations.
  - **source-quench** --Source quenches.
  - **time-exceeded** --All time exceededs.
  - **timestamp-reply** --Timestamp replies.
  - **timestamp-request** --Timestamp requests.
  - **traceroute** --Traceroute.
  - **unreachable** --All unreachables.

- **group-object** *nested-object-group-name* --Existing network object group (child) to be included in the current object group (parent).

The type of child object group must match that of the parent (for example, if you are creating a network object group, you must specify another network object group as the child).

You can use duplicated objects in an object group if it is because of the inclusion of group objects. For example, if object 1 is in both group A and group B, you can define a group C that includes both A and B. However, you cannot include a group object that causes the group hierarchy to become circular (for example, you cannot include group A in group B and then also include group B in group A).

You can use an unlimited number of nested object groups (however, a maximum of two levels is recommended).

Use the **no** form of the command to delete the object group with the specified name. (You cannot delete an object group that is being used within an ACL or a CPL policy.)

Examples

This example shows how to create a service object group that matches protocol port 100 and any port greater than 200, except 300:

```
Router> enable
Router# configure terminal
Router(config)# object-group service my_service_object_group
Router(config-service-group)# eq 100
Router(config-service-group)# gt 200
Router(config-service-group)# neq 300
```

Related Commands

Command	Description
deny	Sets conditions in a named IP access list or OGACL that will deny packets.
ip access-group	Applies an ACL or OGACL to an interface or a service policy map.
ip access-list	Defines an IP access list or OGACL by name or number.
object-group network	Defines network object groups for use in OGACLs.
permit	Sets conditions in a named IP access list or OGACL that will permit packets.
show ip access-list	Displays the contents of IP access lists or OGACLs.
show object-group	Displays information about object groups that are configured

occur-at (ips-auto-update)

To define a preset time for which the Cisco IOS Intrusion Prevention System (IPS) automatically obtains updated signature information, use the **occur-at**command in IPS-auto-update configuration mode.

occur-at [**monthly**| **weekly**] *day minutes hours*

Syntax Description

monthly	Monthly update option in days of the month from 1 to 31, minutes from the top of the hour from 0 to 59 and hours of the day from 0 to 23, in which automatic signature updates occur.
weekly	Weekly update option in days of the week from 0 to 6, minutes from the top of the hour from 0 to 59 and hours of the day from 0 to 23, in which automatic signature updates occur.

Command Default

The default value is defined in the signature definition XML.

Command Modes

IPS-auto-update configuration (config-ips-auto-update)

Command History

Release	Modification
12.4(11)T	This command was introduced.
12.4(22)T	The command was modified with the **monthly** and **weekly** keywords in Cisco IOS Release 12.4(22)T.

Usage Guidelines

Automatic signature updates allow users to override the existing IPS configuration and automatically keep signatures up to date on the basis of a preset time, which can be configured to a preferred setting.

Use the **ip ips auto-update** command to enable Cisco IOS IPS to automatically update the signature file on the system. Thereafter, issue the **occur-at** command to define how often the Cisco IOS IPS signature files should be automatically updated.

Examples

The following example shows how to configure automatic signature updates and set the frequency in which updates are made. In this example, the signature package file is pulled from the TFTP server at the third hour of the 5 day of the month, at the 56th minute of this hour.

Note Adjustments are made for months without 31 days and daylight savings time.

```
Router# clock set ?
hh:mm:ss Current Time
Router# clock set 10:38:00 20 apr 2006
Router#
*Apr 20 17:38:00.000: %SYS-6-CLOCKUPDATE: System clock has been updated from 10:37:55 MST
Thu Apr 20 2006 to 10:38:00 MST Thu Apr 20 2006, configured from console by cisco on console.
Router(config)# ip ips auto-update
Router(config-ips-auto-update)# occur-at monthly 5 56 3
Router(config-ips-auto-update)# $s-auto-update/IOS_reqSeq-dw.xml

Router(config-ips-auto-update)#^Z
Router#
*May 4 2006 15:50:28 MST: IPS Auto Update: setting update timer for next update: 0 hrs 10
min
*May 4 2006 15:50:28 MST: %SYS-5-CONFIG_I: Configured from console by cisco on console
Router#
Router# show ip ips auto-update

IPS Auto Update Configuration
URL : tftp://192.168.0.2/jdoe/ips-auto-update/IOS_reqSeq-dw.xml
Username : not configured
Password : not configured
Auto Update Intervals
minutes (0-59) : 56
hours (0-23) : 3
days of month (1-31) : 5
days of week: (0-6) :
```

Related Commands

Command	Description
ip ips auto-update	Enables automatic signature updates for Cisco IOS IPS.
cisco	Enables automatic signature updates from Cisco.com.

ocsp

To specify online certificate status protocol (OCSP) settings for the public key infrastructure (PKI) trustpool, use the **ocsp** command in ca-trustpool configuration mode. To disable the OCSP server or return to the default, use the **no** form of this command.

ocsp {**disable-nonce**| **url** *url*}

no ocsp {**disable-nonce**| **url** *url*}

Syntax Description

disable-nonce	Disables the OCSP Nonce Extension.
url *url*	Specifies the OCSP server URL to override (if one exists) in the Authority Info Access (AIA) extension of the certificate. All certificates associated with a configured PKI trustpool are checked by the OCSP server at the specified HTTP URL. The URL can be a hostname, an IPv4 address, or an IPv6 address.

Command Default

The router uses the OCSP server URL in the AIA extension of the certificate. The revocation check fails if no URL exists.

Command Modes

Ca-trustpool configuration (ca-trustpool)

Command History

Release	Modification
15.2(2)T	This command was introduced.
15.1(1)SY	This command was integrated into Cisco IOS Release 15.1(1)SY.

Usage Guidelines

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

A central OCSP server is configured to collect and update certificate revocation lists (CRLs) from different certification authority (CA) servers so that devices within the network can rely on the OCSP server to check the certificate status without retrieving and caching each CRL for every device.

If the OCSP URL is specified through the HTTP file system, then the URL must be written in the following formats:

- http://*OCSPname*:80, where *OCSP_name* is the Domain Name System (DNS) of the OCSP server.
- http://*ipv4-address*:80. For example: http://10.10.10.1:80.

- http://*[ipv6-address]:80*. For example: http://[2001:DB8:1:1::1]:80. The IPv6 address is in hexadecimal notation and must be enclosed in brackets in the URL.

Examples

The following example shows how to configure your router to use the OCSP server at the http://ocspts.identrust.com URL:

```
Router(config)# crypto pki trustpool policy
Router(ca-trustpool)# ocsp url http://ocspts.identrust.com
Router(ca-trustpool)# revocation-check ocsp none
```

Note If the server is down, the revocation check is ignored.

Related Commands

Command	Description
cabundle url	Configures the URL from which the PKI trustpool CA bundle is downloaded.
chain-validation	Enables chain validation from the peer's certificate to the root CA certificate in the PKI trustpool.
crl	Specifes the CRL query and cache options for the PKI trustpool.
crypto pki trustpool import	Manually imports (downloads) the CA certificate bundle into the PKI trustpool to update or replace the existing CA bundle.
crypto pki trustpool policy	Configures PKI trustpool policy parameters.
default	Resets the value of a ca-trustpool configuration command to its default.
match	Enables the use of certificate maps for the PKI trustpool.
revocation-check	Disables revocation checking when the PKI trustpool policy is being used.
show	Displays the PKI trustpool policy of the router in ca-trustpool configuration mode.

Command	Description
show crypto pki trustpool	Displays the PKI trustpool certificates of the router and optionally shows the PKI trustpool policy.
source interface	Specifies the source interface to be used for CRL retrieval, OCSP status, or the downloading of a CA certificate bundle for the PKI trustpool.
storage	Specifies a file system location where PKI trustpool certificates are stored on the router.
vrf	Specifies the VRF instance to be used for CRL retrieval.

ocsp url

To specify the URL of an online certificate status protocol (OCSP) server to override the OCSP server URL (if one exists) in the Authority Info Access (AIA) extension of the certificate, use the **ocsp url** command in ca-trustpoint configuration mode. To disable the OCSP server, use the **no** form of this command.

ocsp url *url*

no ocsp url *url*

Syntax Description

url	All certificates associated with a configured trustpoint are checked by the OCSP server at the specified HTTP URL. The URL can be a hostname, IPv4 address, or an IPv6 address.

Command Default

The router uses the OCSP server URL in AIA extension of the certificate. If a URL does not exist, then the revocation check fails.

Command Modes

Ca-trustpoint configuration (config-ca-trustpoint)

Command History

Release	Modification
12.3(2)T	This command was introduced.
15.2(1)T	This command was modified. Support for specifying the IPv6 address in a URL for the OCSP server was added.

Usage Guidelines

A central OCSP server is configured to collect and update certificate revocation lists (CRLs) from different certification authority (CA) servers so that devices within the network can rely on the OCSP server to check the certificate status without retrieving and caching each CRL for every device.

The OCSP URL is specified through the HTTP file system, then the URL must be written in the following formats:

- http://*OCSP_name*:80, where *OCSP_name* is the Domain Name System (DNS) of the OCSP server.
- http://*ipv4-address*:80. For example: http://10.10.10.1:80
- *http:///[ipv6-address]:80*. For example: http://[2001:DB8:1:1::1]:80. The IPv6 address is in hexadecimal notation and must be enclosed in brackets in the URL.

Examples

The following example shows how to configure your router to use the OCSP server at the HTTP URL http://myocspserver:81.

```
Router(config)# crypto pki trustpoint mytp
Router(ca-trustpoint)# ocsp url http://myocspserver:81
Router(ca-trustpoint)# revocation-check ocsp none
```

The following example shows how to configure your router to use the OCSP server at the IPv6 HTTP URL http://[2001DB8:1:1::2]:80.

```
Router(config)# crypto pki trustpoint mytp
Router(ca-trustpoint)# ocsp url http://[2001DB8:1:1::2]:80
Router(ca-trustpoint)# revocation-check ocsp none
```

Note If the server is down, the revocation check is ignored.

Related Commands

Command	Description
crl query	Queries the CRL to ensure that the certificate of the peer has not been revoked.
crypto pki authenticate	Authenticates the CA (by getting the certificate of the CA).
crypto pki enroll	Obtains the certificate or certificates of your router from the CA.
crypto pki trustpoint	Declares the CA that your router should use.
enrollment url (ca-trustpoint)	Specifies the enrollment parameters of a CA.
revocation-check	Checks the revocation status of a certificate.

on

To specify the location where Rivest, Shamir, and Adelman (RSA) keys will be generated upon initial auto enrollment, use the **on** command in ca-trustpoint configuration mode.

on *devicename:*

Syntax Description

devicename:	Specifies the RSA key storage device.

Command Default

Keys are generated and stored in NVRAM.

Command Modes

Ca-trustpoint

Command History

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

Usage Guidelines

Locations that may be specified include a USB token, local disk, or NVRAM.

A USB token may be used as a cryptographic device in addition to a storage device. Using a USB token as a cryptographic devices allows RSA operations such as key generation, signing, and authentication to be performed on the token. Private keys are not distributed and remain on the token by default, however you may configure the private key storage location.

Keys that reside on a USB token, or on-token keys, are saved to persistent token storage when they are generated. Key deletion will remove the on-token keys from persistent storage immediately. (Keys that do not reside on a token are saved to or deleted from non-token storage locations only when the **write memory** or similar command is issued.)

Examples

The following example shows the configuration for the “mytp-A” certificate server and its associated trustpoint, where RSA keys generated by the initial auto enrollment for the trustpoint will be stored on a USB token, “usbtoken0”:

```
crypto pki server mytp-A
   database level complete
   issuer-name CN=company, L=city, C=country
   grant auto
! Specifies that certificate requests will be granted automatically.
!
crypto pki trustpoint mytp-A
   revocation-check none
   rsakeypair myTP-A
   storage usbtoken0:
! Specifies that keys will be stored on usbtoken0:.
   on usbtoken0:
```

```
! Specifies that keys generated on initial auto enroll will be generated on and stored on
! usbtoken0:
```

Related Commands

Command	Description
crypto key generate rsa	Generates RSA key pairs.
crypto key import rsa	Imports RSA key pairs.
crypto pki trustpoint	Declares the trustpoint that the router will use.

one-minute

To define the number of new unestablished sessions that will cause the system to start deleting half-open sessions and stop deleting half-open sessions, use the **one-minute**command in parameter-map type inspect configuration mode. To disable the value, use the **no** form of this command.

one-minute {**low** *number-of-connections*| **high** *number-of-connections*}

no one-minute {**low** *number-of-connections*| **high** *number-of-connections*}

Syntax Description

low *number-of-connections*	Number of new unestablished sessions that will cause the system to stop deleting half-open sessions.
high *number-of-connections*	Number of new unestablished sessions that will cause the system to start deleting half-open sessions.

Command Default

None

Command Modes

Parameter-map type inspect configuration

Command History

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

Usage Guidelines

When you are configuring an inspect type parameter map, you can enter the **one-minute**subcommand after you enter the **parameter-map type inspect** command.

Enter the **one-minute** command twice; once to specify a high number at which the system will start deleting half-open sessions, and once to specify a low number at which the system will stop deleting half-open sessions.

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

Examples

The following example causes the system to start deleting half-open sessions when there are 300 unestablished sessions, and to stop deleting half-open sessions when there are 400 unestablished systems:

```
parameter-map type inspect internet-policy
 one minute high 400
 one minute low 300
```

Related Commands

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

other-config-flag

To verify the advertised “other” configuration parameter, use the **other-config-flag** command in RA guard policy configuration mode.

other-config-flag {**on**| **off**}

Syntax Description

on	Verification is enabled.
off	Verification is disabled.

Command Default

Verification is not enabled.

Command Modes

RA guard policy configuration (config-ra-guard)

Command History

Release	Modification
12.2(50)SY	This command was introduced.
15.2(4)S	This command was integrated into Cisco IOS Release 15.2(4)S.
15.0(2)SE	This command was integrated into Cisco IOS Release 15.0(2)SE.
Cisco IOS XE Release 3.2SE	This command was integrated into Cisco IOS XE Release 3.2SE.

Usage Guidelines

The **other-config-flag** command enables verification of the advertised "other" configuration parameter (or "O" flag). This flag could be set by an attacker to force hosts to retrieve other configuration information through a Dynamic Host Configuration Protocol for IPv6 (DHCPv6) server that may not be trustworthy.

Examples

The following example shows how the command defines a router advertisement (RA) guard policy name as raguard1, places the router in RA guard policy configuration mode, and enables O flag verification:

```
Router(config)# ipv6 nd raguard policy raguard1
Router(config-ra-guard)# other-config-flag on
```

Related Commands

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

out-of-band telemetry

To enable out-of-band telemetry and content-scan exception rules, use the **out-of-band telemetry** command in parameter-map type inspect configuration mode. To disable out-of-band telemetry and content-scan exception rules, use the **no** form of this command.

out-of-band telemetry interval *interval*

no out-of-band telemetry interval

Syntax Description

interval *interval*	Specifies the content-scan telemetry interval, in minutes. The range is from 5 to 43200.

Command Default

Out-of-band telemetry and content-scan exception rules are not enabled.

Command Modes

Parameter-map type inspect configuration (config-profile)

Command History

Release	Modification
15.3(3)M	This command was introduced.

Usage Guidelines

Telemetry is an automated communications process in which measurements are made and data that is collected at remote sites is transmitted to receiving equipment for monitoring.

The device on which the Cloud Web Security is configured is monitored, and data is generated periodically. Because most of these devices do not have a large amount of memory or secondary storage, the generated data is exported and stored in the Cloud Web Security tower. The device connects to a URL hosted by the Cloud Web Security tower by using the HTTP POST method to send telemetry data periodically.

Because the Cloud Web Security tower does not have information about all web traffic, a connector (a persistent, out-of-band secure channel between the device and the Cloud Web Security tower) periodically sends all exception rules to the tower. The connector makes a POST request and pushes all exception rules to a URL. This URL is separate from the telemetry URL.

Content scan does a scan of the HTTP and secure HTTP (HTTPS) traffic to protect the Cloud Web Security from malware attacks.

Examples

The following example shows how to enable out-of-band telemetry, which allows the storing of messages generated by the device on which Cloud Web Security is configured:

```
Device# configure terminal
Device(config)# parameter-map type content-scan
Device(config-profile)# out-of-band telemetry interval 60
Device(config-profile)# end
```

Related Commands

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

outgoing

To configure filtering for outgoing export traffic, use the **outgoing** command in router IP traffic export (RITE) configuration mode. To disable filtering for outgoing traffic, use the **no** form of this command.

outgoing {**access-list** {*standard*| *extended*| *named*}| **sample one-in-every** *packet-number*}

no outgoing {**access-list** {*standard*| *extended*| *named*}| **sample one-in-every** *packet-number*}

Syntax Description

access-list *standard* | *extended named*	An existing numbered (standard or extended) or named access control list (ACL). **Note** The filter is applied only to exported traffic.
sample one-in-every *packet-number*	Export only one packet out of every specified number of packets. Valid range for the *packet-number* argument is 2 to 2147483647 packets.

Command Default

If this command is not enabled, outgoing IP traffic is not exported.

Command Modes

RITE configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.

Usage Guidelines

When configuring a network device for IP traffic export, you can issue the **outgoing** command to filter unwanted outgoing traffic via the following methods:

- ACLs, which accept or deny an IP packet for export
- Sampling, which allows you to export one in every few packets in which you are interested. Use this option when it is not necessary to export all incoming traffic. Also, sampling is useful when a monitored ingress interface can send traffic faster than the egress interface can transmit it.

Note If you issue this command, you must also issue the **bidirectional** command, which enables outgoing traffic to be exported. However, only routed traffic (such as passthrough traffic) is exported; that is, traffic that originates from the network device is not exported.

Examples

The following example shows how to configure the profile “corp1,” which will send captured IP traffic to host “00a.8aab.90a0” at the interface “FastEthernet 0/1.” This profile is also configured to export one in every 50 packets and to allow incoming traffic only from the ACL “ham_ACL.”

```
Router(config)# ip traffic-export profile corp1
Router(config-rite)# interface FastEthernet 0/1
Router(config-rite)# bidirectional
Router(config-rite)# mac-address 00a.8aab.90a0
Router(config-rite)# outgoing sample one-in-every 50
Router(config-rite)# incoming access-list ham_acl
Router(config-rite)# exit
Router(config)# interface FastEthernet 0/0
Router(config-if)# ip traffic-export apply corp1
```

Related Commands

Command	Description
bidirectional	Enables incoming and outgoing IP traffic to be exported across a monitored interface.
ip traffic-export profile	Creates or edits an IP traffic export profile and enables the profile on an ingress interface.
incoming	Configures filtering for incoming IP traffic.