

show parameter-map type consent through show users

- show parameter-map type consent, on page 4
- show parameter-map type inspect, on page 5
- show parameter-map type inspect-global, on page 8
- show parameter-map type inspect-vrf, on page 11
- show parameter-map type inspect-zone, on page 13
- show parameter-map type ooo global, on page 14
- show parameter-map type protocol-info, on page 15
- show parameter-map type regex, on page 17
- show parameter-map type trend-global, on page 18
- show parameter-map type urlf-glob, on page 19
- show parameter-map type urlfilter, on page 20
- show parameter-map type urlfpolicy, on page 22
- show parser view, on page 23
- show platform hardware qfp feature alg, on page 25
- show platform hardware qfp act feature ipsec datapath memory, on page 31
- show platform hardware qfp active feature acl dp hsl configuration, on page 32
- show platform hardware qfp active feature ipsec, on page 33
- Show platorm hardware qfp active statistics drop history, on page 40
- show platform hardware qfp active statistics drop thresholds, on page 41
- show platform hardware qfp feature alg statistics sip, on page 42
- show platform hardware qfp feature firewall, on page 45
- show platform hardware qfp feature firewall datapath scb, on page 49
- show platform hardware qfp feature td, on page 51
- show platform software audit, on page 53
- show platform software cerm-information, on page 55
- show platform software firewall, on page 56
- show platform software ipsec policy statistics, on page 62
- show platform software ipsec f0 encryption-processor registers, on page 64
- show platform software ipsec fp active flow, on page 65
- show platform software ipsec fp active spd-map, on page 71
- show platform software ipsec modexp-throttle0-stats, on page 74

- show platform software urpf qfp active configuration, on page 75
- show policy-firewall config, on page 76
- show policy-firewall mib, on page 80
- show policy-firewall session, on page 84
- show policy-firewall stats, on page 87
- show policy-firewall stats vrf, on page 89
- show policy-firewall stats vrf global, on page 91
- show policy-firewall stats zone, on page 92
- show policy-firewall summary-log, on page 94
- show policy-map type inspect, on page 95
- show policy-map type inspect urlfilter, on page 96
- show policy-map type inspect zone-pair, on page 97
- show policy-map type inspect zone-pair urlfilter, on page 103
- show port-security, on page 105
- show ppp queues, on page 107
- show pppoe session, on page 109
- show private-hosts access-lists, on page 113
- show private-hosts configuration, on page 115
- show private-hosts interface configuration, on page 117
- show private-hosts mac-list, on page 118
- show privilege, on page 119
- show radius local-server statistics, on page 120
- show radius server-group, on page 122
- show radius statistics, on page 124
- show radius table attributes, on page 129
- show redundancy application asymmetric-routing, on page 150
- show redundancy application control-interface group, on page 152
- show redundancy application data-interface, on page 153
- show redundancy application faults group, on page 154
- show redundancy application group, on page 155
- show redundancy application if-mgr, on page 159
- show redundancy application protocol, on page 161
- show redundancy application transport, on page 163
- show redundancy linecard-group, on page 164
- show running-config, on page 165
- show running-config vrf, on page 173
- show sasl, on page 176
- show secure bootset, on page 178
- show smm, on page 179
- show snmp mib nhrp status, on page 181
- show ssh, on page 182
- show ssl-proxy module state, on page 184
- show tacacs, on page 185
- show tcp intercept connections, on page 187
- show tcp intercept statistics, on page 189
- show tech-support alg, on page 190

- show tech-support ipsec, on page 193
- show tech-support pki, on page 196
- show tunnel endpoints, on page 206
- show usb controllers, on page 208
- show usb device, on page 210
- show usb driver, on page 213
- show usb port, on page 215
- show usb-devices summary, on page 216
- show usb tree, on page 217
- show usbtoken, on page 218
- show user-group, on page 219
- show users, on page 221

show parameter-map type consent

To display consent parameter map information, use the **show parameter-map type consent**command in privileged EXEC mode.

show parameter-map type consent [*parameter-map-name* | **default**]

Syntax Description

parameter-map-name	(Optional) Name of the parameter map.
default	(Optional) Specifies default consent parameter map information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(15)T	This command was introduced.
12.4(20)T	The command was modified. The *parameter-map-name* argument was added.

Examples

The following is sample output from the **show parameter-map type consent**command. The fields are self-explanatory.

```
Router# show parameter-map type consent
parameter-map type consent map1
    Syslog : Enabled
    File download time(in minutes) : 456
    Number of Accepted Users : 0
    Number of Denied Users : 0
```

show parameter-map type inspect

To display user-configured or default inspect-type parameter maps, use the **show parameter-map type inspect** command in privileged EXEC mode.

show parameter-map type inspect [*parameter-map-name* | **default** | **global**]

Syntax Description

parameter-map-name	(Optional) Name of the parameter map.
default	(Optional) Displays the default inspect-type parameter-map values. **Note** Use this keyword when no parameter map is attached to the inspect action.
global	(Optional) Displays the global inspect type parameter map values.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(6)T	This command was introduced.
15.1(1)T	This command was modified. The **global** keyword was added.
Cisco IOS XE Release 3.4S	This command was modified. Support for General Packet Radio Service (GPRS) Tunneling Protocol (GTP) was added.
Cisco IOS XE Release 3.9S	This command was modified. The *parameter-map-name* argument was added.
Cisco IOS XE Release 3.11S	This command was modified. The command output was modified to display the number of simultaneous packets per flow.
Cisco IOS XE Release 3.13S	This command was modified. The command output was modified to display the Locator/ID Separation Protocol (LISP) inner-packet inspection information.
Cisco IOS XE Release 3.14S	This command was modified. The command output was modified to display the Network-Based Application Recognition (NBAR) information.

Usage Guidelines

When the **nbar-classify** command is configured, the output of **show parameter-map type inspect global** displays this information.

Examples

The following is sample output from the **show parameter-map type inspect** command. The fields in the output are self-explanatory.

```
Device# show parameter-map type inspect

 audit-trail off
 alert on
 max-incomplete low 2147483647
 max-incomplete high 2147483647
 one-minute low 2147483647
```

```
 one-minute high 2147483647
 udp idle-time 30
 icmp idle-time 10
 dns-timeout 5
 tcp idle-time 3600
 tcp finwait-time 5
 tcp synwait-time 30
 tcp max-incomplete host 4294967295 block-time 0
 tcp window scaling enforcement loose off
 sessions maximum 2147483647
 sessions packet default
```

The following is sample output from the **show parameter-map type inspect** *parameter-map-name* command. The fields in the output are self-explanatory.

```
Device# show parameter-map type inspect pmap1

parameter-map type inspect pmap1
  log dropped-packet off
  audit-trail on
  alert on
  max-incomplete low  unlimited
  max-incomplete high unlimited
  one-minute low  unlimited
  one-minute high unlimited
  sessions rate low  unlimited
  sessions rate high unlimited
  sessions packet default
  udp idle-time 30 ageout-time 30
  udp halfopen idle-time 30000 ms ageout-time 30000 ms
  icmp idle-time 50 ageout-time 50
  dns-timeout 5
  tcp window scaling enforcement loose off
  tcp idle-time 3600 ageout-time 3600
  tcp finwait-time 1 ageout-time 1
  tcp synwait-time 30 ageout-time 30
  tcp half-open on, half-close on, idle on
  tcp max-incomplete host unlimited block-time 0
  sessions maximum 3000
  gtp permit error off
  gtp  request-queue 40000
  gtp  tunnel-limit 40000
  gtp  gsn timeout 30
  gtp  pdp-context timeout 300
  gtp  request-queue timeout 60
  gtp  signaling timeout 30
  gtp  tunnel timeout 60
```

The following is sample output from the **show parameter-map type inspect default** command. The fields in the output are self-explanatory.

```
Device# show parameter-map type inspect default

 parameter-map type inspect default values
  log dropped-packet off
  audit-trail off
  alert on
  max-incomplete low  unlimited
  max-incomplete high unlimited
  one-minute low  unlimited
  one-minute high unlimited
  sessions rate low  unlimited
  sessions rate high unlimited
```

```
 sessions packet default
 udp idle-time 30 ageout-time 30
 udp halfopen idle-time 30000 ms ageout-time 30000 ms
 icmp idle-time 10 ageout-time 10
 dns-timeout 5
 tcp idle-time 3600 ageout-time 3600
 tcp finwait-time 1 ageout-time 1
 tcp synwait-time 30 ageout-time 30
 tcp max-incomplete host unlimited block-time 0
 tcp window scaling enforcement loose off
 sessions maximum unlimited
 gtp permit error off
 gtp  request-queue 40000
 gtp  tunnel-limit 40000
 gtp  gsn timeout 30
 gtp  pdp-context timeout 30
 gtp  request-queue timeout 60
 gtp  signaling timeout 30
 gtp  tunnel timeout 60
```

The following is sample output from the **show parameter-map type inspect global** command. The fields in the output are self-explanatory.

```
Device# show parameter-map type inspect global

alert on
 sessions maximum 2147483647
 waas disabled
 l2-transparent dhcp-passthrough disabled
 log dropped-packets disabled
 log summary disabled
 max-incomplete low 2147483647
 max-incomplete high 2147483647
 one-minute low 2147483647
 one-minute high 2147483647
 vrf vrf2 inspect vrf-default
 lisp inner-packet-inspection
 exporter not-configured
 nbar-classify
```

Related Commands

Command	Description
parameter-map type inspect	Configures an inspect-type parameter map for connecting thresholds, timeouts, and other parameters pertaining to the **inspect** action.
lisp inner-packet-inspection	Enables LISP inner-packet inspection.

show parameter-map type inspect-global

To display global inspect-type parameter map information, use the **show parameter-map type inspect-global** command in user EXEC or privileged EXEC mode.

show parameter-map type inspect-global [**gtp**]

Syntax Description

gtp	(Optional) Displays information about the General Packet Radio Service (GPRS) tunneling protocol (GTP).

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.5S	This command was introduced.
Cisco IOS XE Release 3.7S	This command was modified. The **gtp** keyword was added.
Cisco IOS XE Release 3.9S	This command was modified. The output was enhanced to display GTP and GTPv2 configuration.
Cisco IOS XE Release 3.13S	This command was modified. The output was enhanced to display Locator ID Separation Protocol (LISP) inner packet inspection information.

Usage Guidelines

The command output displays all configured parameters and their values and all unconfigured parameters with their box-level default values. (Box refers to the entire firewall session table.)

Examples

The following is sample output from the **show parameter-map type inspect-global** command:

```
Device# show parameter-map type inspect-global

parameter-map type inspect-global
  log dropped-packet off
  alert on
  aggressive aging disabled
  lisp inner-packet-inspection
  syn_flood_limit  unlimited
  tcp window scaling enforcement loose off
  max incomplete unlimited  aggressive aging disabled
  max_incomplete TCP unlimited
  max_incomplete UDP unlimited
  max_incomplete ICMP unlimited
  application-inspect all
  vrf default inspect vrf-default
  vrf vrf2 inspect vrf-default
  vrf vrf3 inspect vrf-defautl
```

The following table describes the fields shown in the display.

Table 1: show parameter-map type inspect-global Field Descriptions

Field	Description
log dropped-packet	Debugging message log of dropped packets is not enabled. If you configure the **log** command in parameter-map type inspect configuration mode, a log of dropped packets is displayed.
alert	Stateful packet inspection of alert messages is on. Valid values are on and off.
aggressive aging	Aggressive aging of half-opened firewall sessions. A half-opened session is a session that has not reached the established state.
lisp inner-packet-inspection	LISP inner-packet packet inspection is enabled.
syn_flood_limit	TCP synchronization (SYN) flood rate limit. When the configured maximum limit is reached, the TCP SYN cookie protection is triggered.
max_incomplete	Maximum half-opened session limit.
max_incomplete TCP	Maximum half-opened TCP connection limit.
max_incomplete UDP	Maximum half-opened UDP connection limit.
max_incomplete ICMP	Maximum half-opened Internet Control Message Protocol (ICMP) connection limit.
vrf default	Default VRF is bound to the inspect-VRF parameter map.

The following is sample output from the **show parameter-map type inspect-global gtp** command:

```
Device# show parameter-map type inspect-global gtp

parameter-map type inspect global-gtp
  gtp request-queue 40000 (default)
  gtp tunnel-limit 40000 (default)
  gtp pdp-context timeout 351
  gtp request-queue timeout 2167
  permit-error Disable (default)
  gtp-in-gtp blocking Disable (default)
  gtpv2 request-queue 40000 (default)
  gtpv2 tunnel-limit 40000 (default)
  gtpv2 echo-rate-limit 10 (default)
```

The following table describes the fields shown in the display.

Table 2: show parameter-map type inspect-global gtp Field Descriptions

Field	Description
gtp request-queue	Displays the number of GTP requests that are queued to wait for a response.
gtp tunnel-limit	Displays the number of GTP tunnels that can be configured.

Field	Description
gtp pdp-context timeout	Displays the timeout, in minutes, for inactive Packet Data Protocol (PDP) contexts.
gtp request-queue timeout	Displays the timeout, in seconds, for inactive request queues.
permit-error	Displays the permissible errors. By default, the permit-error is disabled.
gtpv2 request-queue	Displays the number of GTP requests for GTPv2 protocol that are queued to wait for a response.
gtpv2 tunnel-limit	Displays the number of GTP tunnels that can be configured for gtpv2 protocol.

Related Commands

Command	Description
parameter-map type inspect-global	Configures a global parameter map.
lisp inner-packet-inspection	Enables LISP inner-packet inspection.

show parameter-map type inspect-vrf

To display information about the configured inspect VPN Routing and Forwarding (VRF) type parameter map, use the **show parameter-map type inspect-vrf** command in user EXEC or privileged EXEC mode.

show parameter-map type inspect-vrf [*name* | **default**]

Syntax Description

name	(Optional) Name of the inspect VRF type parameter map.
default	(Optional) Specifies the default inspect VRF type parameter map.

Command Default

This command has no default settings.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.3S	This command was introduced.

Examples

The following is sample output from the **show parameter-map type inspect-vrf** command:

```
Router# show parameter-map type inspect-vrf vpmap01
  VRF: vrf001, Parameter-Map: vpmap01
       total_session_cnt: 3500
       exceed_cnt:        40
       tcp_half_open_cnt: 3520
       syn_exceed_cnt:    40
```

The table below describes the significant fields shown in the display.

Table 3: show parameter-map type inspect-vrf Field Descriptions

Field	Description
total_session_cnt	Total session count.
exceed_cnt	Number of sessions that exceeded the configured session count.
tcp_half_open_cnt	TCP half-open sessions configured for each VRF. When the configured session limit is reached, the TCP synchronization (SYN) cookie verifies the source of the half-open TCP sessions before creating more sessions. A TCP half-open session is a session that has not reached the established state.
syn_exceed_count	Number of SYN packets that exceeded the configured SYN flood rate limit.

Related Commands

Command	Description
parameter-map type inspect-vrf	Configures an inspect VRF type parameter map.

show parameter-map type inspect-zone

To display information about the configured inspect zone-type parameter map, use the **show parameter-map type inspect-zone** command in user EXEC or privileged EXEC mode.

show parameter-map type inspect-zone [*name* | **default**]

Syntax Description

name	(Optional) Name of the inspect zone-type parameter map.
default	(Optional) Specifies the default inspect zone-type parameter map.

Command Default

This command has no default settings.

Command Modes

User EXEC (>)
Privileged EXEC(#)

Command History

Release	Modification
Cisco IOS XE Release 3.3S	This command was introduced.

Examples

The following is sample output from the **show parameter-map type inspect-zone** command:

```
Router# show parameter-map type inspect-zone zone-pmap

parameter-map type inspect-zone zone-pmap
 tcp syn-flood-rate 400
 max-destination 10000
```

The table below describes the fields shown in the display.

Table 4: show parameter-map type inspect-zone Field Descriptions

Field	Description
parameter-map type inspect-zone	Name of the inspect zone-type parameter map.
tcp syn-flood-rate	TCP synchronization (SYN) flood rate limit. When the configured maximum packet rate is reached, the TCP SYN cookie protection is triggered.
max-destination	Maximum number of destinations that a firewall can track.

Related Commands

Command	Description
parameter-map type inspect-zone	Configures an inspect zone-type parameter map.

show parameter-map type ooo global

To display Out-of-Order (OoO) global parameter-map information, use the **show parameter-map type ooo global** command in privileged EXEC mode.

show parameter-map type ooo global

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

The output of the **show parameter-map type ooo global** command displays configurations related to OoO packet processing. If you do not configure the **parameter-map type ooo global** command, the output of the **show parameter-map type ooo global** command displays default values of the OoO packet-processing parameters.

Examples

The following is sample output from the **show parameter-map type ooo global** command:

```
Device# show parameter-map type ooo global

 parameter-map type ooo global
   tcp reassembly timeout 5
   tcp reassembly queue length 16
   tcp reassembly memory limit 1024
   tcp reassembly alarm off
```

The following table describes the fields shown in the display.

Table 5: show parameter-map type ooo global Field Descriptions

Field	Description
tcp reassembly timeout	Timeout, in seconds, for OoO-TCP queues.
tcp reassembly queue length	Length of the OoO queues.
tcp reassembly memory limit	Limit of the OoO buffer size.
tcp reassembly alarm	Indicates if alert messages for TCP sessions are enabled. Valid values are on and off.

Related Commands

parameter-map type ooo global	Configures an OoO global parameter map for all firewall policies.
tcp reassembly	Changes the default parameters for OoO queue processing of TCP sessions.
tcp reassembly memory limit	Specifies the limit of the OoO queue size for TCP sessions.

show parameter-map type protocol-info

To display protocol parameter map information, use the **show parameter-map type protocol-info**command in privileged EXEC mode.

show parameter-map type protocol-info [*parameter-map-name* [**dns-cache**] | **dns-cache** | **msrpc** | **zone-pair** *zone-pair-name* | **stun-ice** [*parameter-map-name*]]

Syntax Description

parameter-map-name	(Optional) Name of the parameter map.
dns-cache	(Optional) Displays the protocol information about the Domain Name System (DNS) cache.
msrpc	(Optional) Displays the protocol information about the Microsoft Remote Procedure Call (MSRPC) parameter map.
zone-pair *zone-pair-name*	(Optional) Specifies the name of the zone pair.
stun-ice	(Optional) Displays the protocol information of Session Traversal Utilities for Network Address Translation (NAT) and Interactive Connectivity Establishment (STUN-ICE). STUN is an Internet standards-track suite of methods, including a network protocol, used in NAT traversal for applications of real-time voice, video, messaging, and other interactive IP communications. ICE is a technique used in computer networking involving NATs in Internet applications of VoIP, peer-to-peer communications, video, instant messaging, and other interactive media. In such applications, NAT traversal is an important component to facilitate communications involving hosts on private network installations, which often are located behind firewalls.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(11)T	This command was introduced.
12.4(22)T	The command was modified. The **stun-ice** keyword was added.
15.1(4)M	This command was modified. The **msrpc** keyword was added.

Examples

The following is sample output from the **show parameter-map type protocol-info** command. The fields are self-explanatory.

```
Router# show parameter-map type protocol-info
parameter-map type protocol-info map2
  server ip 192.168.1.1
```

Related Commands

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

show parameter-map type regex

To display regular expression parameter-map information, use the **show parameter-map type regex** command in privileged EXEC mode.

show parameter-map type regex[*parameter-map-name*]

Syntax Description

parameter-map-name	(Optional) Name of the parameter map.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(11)T	This command was introduced.
Cisco IOS XE Release 3.2S	This command was integrated into Cisco IOS XE Release 3.2S.

Examples

The following is sample output from the **show parameter-map type regex** command. The output fields are self-explanatory.

```
Router# show parameter-map type regex

parameter-map type regex map3
 pattern x*y
```

Related Commands

Command	Description
parameter-map type regex	Configures a parameter-map type to match a specific traffic pattern.

show parameter-map type trend-global

To display the parameter map for the global parameters for a Trend Micro URL filtering policy, use the **show parameter-map type trend-global** command in privileged EXEC mode.

show parameter-map type trend-global [*parameter-map-name*] [**default**]

Syntax Description

parameter-map-name	(Optional) The name of the parameter map for which to display parameters.
default	(Optional) Specifies that the default values for the global Trend Micro filtering parameters be displayed.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

Use the **show parameter-map type trend-global**command to display the global parameters for Trend Micro URL filtering policies.

Examples

The following is sample output from the **show parameter-map type trend-global default**command:

```
Router# show parameter-map type trend-global
 default
parameter-map type trend-global default values
   server trps.trendmicro.com http-port 80 https-port 443 retrans 3 timeout 60
   alert on
   cache-size 256 KB
   cache-lifetime 24
```

The following is sample output from the **show parameter-map type trend-global**command when the server name and maximum cache size have been specified in the parameter map Global-Parameters:

```
Router# show parameter-map type trend-global
 Global-Parameters

parameter-map type trend-global Global-Parameters
   server trps1.example.com http-port 80 https-port 443 retrans 3 timeout 60
   alert on
   cache-size 300 KB
   cache-lifetime 24
```

Related Commands

Command	Description
show parameter-map type urlfpolicy	Displays the parameters for a URL filtering policy.

show parameter-map type urlf-glob

To display the parameter maps for local URL filtering, use the **show parameter-map type urlf-glob** command in privileged EXEC mode.

show parameter-map type urlf-glob [*parameter-map-name*]

Syntax Description

parameter-map-name	(Optional) Name of the URL filtering parameter map to display.

Command Default

The parameter maps for all local URL filtering policies are displayed.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

Use the **show parameter-map type urlf-glob** command to display the parameter maps for local URL filtering policies.

Examples

The following is sample output from the **show parameter-map type urlf-glob**command when two parameter maps for local URL filtering have been configured:

```
Router# show parameter-map type urlf-glob

parameter-map type urlf-glob trusted-domain-param
 pattern www.example.com
 pattern *.example1.com
parameter-map type urlf-glob untrusted-domain-param
 pattern www.example3.com
 pattern *.example4.com
```

Related Commands

Command	Description
show parameter-map type trend-global	Displays the global parameters for a Trend Micro URL filtering policy.
show parameter-map type urlfpolicy	Displays the parameters for a URL filtering policy.

show parameter-map type urlfilter

Note Effective with Cisco IOS Release 12.4(15)XZ, the **show parameter-map type urlfilter** command is not available in Cisco IOS software.

To display user-configured or default URL filter type parameter maps, use the **show parameter-map type urlfilter**command in privileged EXEC mode.

show parameter-map type urlfilter [**default**]

Syntax Description

default	(Optional) Displays the default urlfilter parameter map values. **Note** If this keyword is not issued, user-configured parameter maps will be displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.4(15)XZ	This command was removed.

Examples

The following example shows sample output from the **show parameter-map type urlfilter** command:

```
Router# show parameter-map type urlfilter
 parameter-map type urlfilter default values
  urlf-server-log off
  audit-trail off
  alert on
  max-request 1000
  max-resp-pak 200
  source-interface default
  allow-mode off
  cache 5000
```

The following example shows sample output from the **show parameter-map type urlfilter default**command:

```
Router# show parameter-map type urlfilter default
parameter-map type urlfilter default values
 urlf-server-log off
 audit-trail off
 alert on
 max-request 1000
 max-resp-pak 200
 source-interface default
 allow-mode off
```

cache 5000

show parameter-map type urlfpolicy

To display the parameter maps associated with a URL filtering policy, use the **show parameter-map type urlfilter**command in privileged EXEC mode.

show parameter-map type urlfpolicy {**local** | **trend** | **n2h2** | **websense**} [*param-map-name*] [**default**]

Syntax Description

local	Specifies that the parameters for local URL filtering policies be displayed.
trend	Specifies that the parameters for Trend Micro URL filtering policies be displayed.
n2h2	Specifies that the parameters for SmartFilter URL filtering policies be displayed.
websense	Specifies that the parameters for Websense URL filtering policies be displayed.
param-map-name	(Optional) The name of the parameter map for a URL filtering policy to be displayed.
default	(Optional) Displays the default values for the URL filtering policy. **Note** If this keyword is not issued, user-configured values will be displayed.

Command Default

The paramater maps for all URL filtering policies of the type specified (**local**, **trend**, **n2h2**, or **websense**) are displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(15)XZ	This command was introduced.

Examples

The following example shows the default values for a Websense URL filtering policy:

```
Router# show parameter-map type urlfpolicy websense default
 parameter-map type urlfilter websense default values
  urlf-server-log off
  audit-trail off
  alert on
  max-request 1000
  max-resp-pak 200
  source-interface default
  allow-mode off
  cache 5000
```

show parser view

To display command-line interface (CLI) view information, use the **show parser view** command in privileged EXEC mode.

show parser view [**all**]

Syntax Description

all	(Optional) Displays information about all CLI views that are configured on the router.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

The **show parser view**command will display information only about the view that the user is currently in. This command is available for both root view users and lawful intercept view users--except for the **all** keyword, which is available only to root view users. However, the **all** keyword can be configured by a user in root view to be available for users in lawful intercept view.

The **show parser view** command cannot be excluded from any view.

Examples

The following example shows how to display information from the root view and the CLI view "first":

```
Router# enable view
Router#
01:08:16:%PARSER-6-VIEW_SWITCH:successfully set to view 'root'.
Router#
! Enable the show parser view command from the root view
Router# show parser view

Current view is 'root'
! Enable the show parser view command from the root view to display all views
Router# show parser view all

Views Present in System:
View Name:   first
View Name:   second
! Switch to the CLI view "first."
Router# enable view first

Router#
01:08:09:%PARSER-6-VIEW_SWITCH:successfully set to view 'first'.
! Enable the show parser view command from the CLI view "first."
```

```
Router# show parser view
Current view is 'first'
```

Related Commands

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

show platform hardware qfp feature alg

To display application layer gateway (ALG)-specific information in the Cisco Quantum Flow Processor (QFP), use the **show platform hardware qfp feature alg** command in privileged EXEC mode.

show platform hardware qfp {**active** | **standby**} **feature alg** {**debugging** | **memory** | **statistics** [*protocol* | **clear**]}

Syntax Description

active	Displays the active instance of the processor.
standby	Displays the standby instance of the processor.
debugging	Displays ALG debugging information.
memory	Displays ALG memory usage information of the processor.
statistics	Displays ALG common statistics information of the processor.

protocol	(Optional) Protocol name. Use one of the following values for the *protocol* argument: • **dns**—Displays Domain Name System (DNS) ALG information in the QFP datapath. • **exec**—Displays exec ALG information in the QFP datapath. • **ftp**—Displays FTP ALG information in the QFP datapath. • **gtp**—Displays General Packet Radio Service (GPRS) Tunneling Protocol (GTP) ALG information in the QFP datapath. • **h323**—Displays H.323 ALG information in the QFP datapath. • **http**—Displays HTTP ALG information in the QFP datapath. • **imap**—Displays Internet Message Access Protocol (IMAP) ALG information in the QFP datapath. • **ldap**—Displays Lightweight Directory Access Protocol (LDAP) ALG information in the QFP datapath. • **login**—Displays login ALG information in the QFP datapath. • **msrpc**—Displays Microsoft Remote Procedure Call (MSRPC) ALG information in the QFP datapath. • **netbios**—Displays Network Basic Input Output System (NetBIOS) ALG information in the QFP datapath. • **pop3**—Displays Post Office Protocol 3 (POP3) ALG information in the QFP datapath. • **pptp**—Displays Point-to-Point Tunneling Protocol (PPTP) ALG information in the QFP datapath. • **rtsp**—Displays Rapid Spanning Tree Protocol (RSTP) ALG information in the QFP datapath. • **shell**—Displays shell ALG information in the QFP datapath. • **sip**—Displays Session Initiation Protocol (SIP) ALG information in the QFP datapath. • **skinny**—Displays Skinny Client Control Protocol (SCCP) ALG information in the QFP datapath. • **smtp**—Displays Simple Mail Transfer Protocol (SMTP) ALG information in the QFP datapath. • **sunrpc**—Displays Sun RPC ALG information in the QFP datapath. • **tftp**—Displays TFTP ALG information in the QFP datapath.
clear	(Optional) Clears common ALG counters after display.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 2.2	This command was introduced.
Cisco IOS XE Release 3.1S	This command was modified. Support for the NetBIOS protocol was added.
Cisco IOS XE Release 3.2S	This command was modified. The **sip** keyword was added.
Cisco IOS XE Release 3.9S	This command was modified. The **gtp** and **pptp** keywords were added.

Usage Guidelines

The **show platform hardware qfp feature alg statistics netbios** command displays the NetBIOS ALG memory usage and statistics information of the processor.

Examples

The following sample output from the **show platform hardware qfp feature alg statistics netbios** command displays the NetBIOS ALG statistics information of the processor:

```
Device# show platform hardware qfp active feature alg statistics netbios

NetBIOS ALG Statistics:
  No. of allocated chunk elements in L7 data pool:0
  No. of times L7 data is allocated:0  No. of times L7 data is freed:0
  Datagram Service statistics
    Total packets            :0
    Direct unique packets    :0
    Direct group packets     :0
    Broadcast packets        :0
    DGM Error packets        :0
    Query request packets    :0
    Positive Qry response packets :0
    Negative Qry response packets:0
    Unknown packets          :0
    Total error packets      :0
  Name Service statistics
    Total packets            :0
    Query request packets    :0
    Query response packets   :0
    Registration req packets :0
    Registration resp packets:0
    Release request packets  :0
    Release response packets :0
    WACK packets             :0
    Refresh packets          :0
    Unknown packets          :0
    Total error packets      :0
  Session Service statistics
    Total packets            :0
    Message packets          :0
    Request packets          :0
    Positive response packets:0
    Negative response packets:0
    Retarget response packets:0
    Keepalive packets        :0
    Unknown packets          :0
    Total error packets      :0
```

The table below describes the significant fields shown in the display.

Table 6: show platform hardware qfp feature alg statistics netbios Field Descriptions

Field	Description
No. of allocated chunk elements in L7 data pool	Number of memory chunks allocated for processing NetBIOS packets.
No. of times L7 data is allocated:0 No. of times L7 data is freed	Number of times memory is allocated and freed for processing NetBIOS packets.
Direct unique packets	Number of direct unique NetBIOS packets processed.
Direct group packets	Number of direct group NetBIOS packets processed.
Broadcast packets	Number of broadcast NetBIOS packets processed.
DGM Error packets	Number of Datagram Error NetBIOS packets processed.
Query request packets	Number of query request NetBIOS packets processed.
Positive Qry response packets	Number of positive query response NetBIOS packets processed.
Negative Qry response packets	Number of negative query response NetBIOS packets processed.
Unknown packets	Number of unknown packets.
Total error packets	Counter tracking number of error packets.

The following sample output from the **show platform hardware qfp feature alg statistics sip** command displays SIP statistics information of the processor.

```
Device# show platform hardware qfp active feature alg statistics sip

SIP info pool used chunk entries number: 6

RECEIVE
Register:           0 -> 200-OK:           0
Invite:             6 -> 200-OK:           6    Re-invite           0
Update:             0 -> 200-OK:           0
Bye:                0 -> 200-OK:           0
Subscribe:          0 -> 200-OK:           0
Refer:              0 -> 200-OK:           0
Prack:              0 -> 200-OK:           0
Trying:             0    Ringing:          6    Ack:                5
Info:               0    Cancel:           0    Sess Prog:          0
Message:            0    Notify:           0
Publish:            0    Options:          0
1xx:                0    2xx:              0
OtherReq:           0    OtherOk:          0    3xx-6xx:            0

Events
Null dport:                 0   Media Port Zero:              0
Malform Media:              0   No Content Length:            0
Cr Trunk Chnls:             6   Del Trunk Chnls:              0
start trunk timer:          6   restart trunk timer:          6
```

```
stop trunk timer:             6   trunk timer timeout:            0
Media Addr Zero:              0   Need More Data:                 0
SIP PKT Alloc:               23   SIP PKT Free:                  23
SIP MSG Alloc:                0   SIP MSG Free:                   0

Errors
Create Token Err:             0    Add portlist Err:              0
Invalid Offset:               0    Invalid Pktlen:                0
Free Magic:                   0    Double Free:                   0
Sess Retmem Failed:           0    Sess Malloc Failed             0
Pkt Retmem Failed:            0    Pkt Malloc Failed:             0
Msg Retmem Failed:            0    Msg Malloc Failed:             0
Bad Format:                   0    Invalid Proto:                 0
Add ALG state Fail:           0    No Call-id:                    0
Parse SIP Hdr Fail:           0    Parse SDP Fail:                0
Error New Chnl:               0    Huge Size:                     0
Create Failed:                0    Not SIP Msg:                   0

Writeback Errors
Offset Err:                   0    PA Err:                        0
No Info:                      0
```

The table below describes the significant fields shown in the display.

Table 7: show platform hardware qfp feature alg statistics sip Field Descriptions

Field	Description
Register	Registers the address listed in the To field of the SIP ALG header with a SIP server.
Invite	Indicates that a user or a service is invited to participate in a call session.
Bye	Terminates a call. This message can be sent either by the caller or the called party.
Refer	Indicates that the user (recipient) should contact a third party for transferring a call.
PRACK	Improves the network reliability by adding an acknowledgment system to the provisional responses. PRACK is a Provisional Response Acknowledgment message.

The following sample output from the **show platform hardware qfp feature alg statistics gtp** command displays GTP (GTPv0, GTPv1, and GTPv2) ALG information. The field descriptions are self-explanatory.

```
Device# show platform hardware qfp active feature alg statistics gtp

Global info:
        Total pkts passed inspection:0
        GTP V0: Request: 0, Response: 0, Data: 0, Unknown: 0
        GTP V1: Request: 0, Response: 0, Data: 0, Unknown: 0
        GTP V2: Request: 0, Response: 0, Data: 0, Unknown: 0
        VFRed packets: 0
Drop counters:
        Total dropped: 0
        Fatal error:
           Internal SW error: 0
        Packets subject to policy inspection:
           Policy not-exist: 0
           Policy dirty-bit set: 0
           Policy-mismatch: 0
        GTP global Info:
           GTP message rejected: 0
```

```
            GTP Request wasn't found: 0
            GTP info element is missing: 0
            GTP info element is incorrect: 0
            GTP info element out of order: 0
            GTP Request retransmit: 0
          GTPv0 Info:
              Message rejected: 0
              Request wasn't found: 0
              Info element is missing: 0
              Info element is incorrect: 0
              Info element out of order: 0
              Request retransmit: 0
          GTPv1 Info:
              Message rejected: 0
              Request wasn't found: 0
              Info element is missing: 0
              Info element is incorrect: 0
              Info element out of order: 0
              Request retransmit: 0
          GTPv2 Info:
              Message rejected: 0
              Request wasn't found: 0
              Info element is missing: 0
              Info element is incorrect: 0
              Info element out of order: 0
              Request retransmit: 0
Memory management:
   GTP ctxt      - allocated: 0, freed: 0, failed: 0
   GTP Primary   - allocated: 0, freed: 0, failed: 0
   GTP Secondary - allocated: 0, freed: 0, failed: 0
   GTP Tunnel DB - allocated: 0, freed: 0, failed: 0
   GTP Req/Res   - allocated: 0, freed: 0, failed: 0
   GTP Req/Resp entry   - allocated: 0, freed: 0, failed: 0
   GTPv2 Session - allocated: 0, freed: 0, failed: 0
   GTPv2 Bearer - allocated: 0, freed: 0, failed: 0
```

Related Commands

Command	Description
debug platform hardware qfp feature	Debugs feature-specific information in the Cisco QFP.

show platform hardware qfp act feature ipsec datapath memory

To display debugging information about the consumption of IPsec datapath memory, use the **show platform hardware qfp act feature ipsec datapath memory** command in privileged EXEC or diagnostic mode.

show platform hardware qfp act feature ipsec datapath memory

Command Default

No default behavior or values

Command Modes

Privileged EXEC (#)

Diagnostic (diag)

Command History

Release	Modification
Cisco IOS XE Release 2.4.2	This command was introduced on the Cisco ASR 1000 Series Routers.

Usage Guidelines

This command displays the consumption of dynamic random access memory (DRAM) on the IPSec Cisco QuantumFlow Processor (QFP) datapath.

```
show platform hardware qfp act feature ipsec datapath memory
pstate chunk totalfree: 80000, allocated: 0
```

Related Commands

Command	Description
show platform software ipsec f0 encryption-processor registers	Displays dubugging information about the crypto engine processor registers.

show platform hardware qfp active feature acl dp hsl configuration

To display the current high-speed logging (HSL) configuration for security group access control lists (SGACLs), use the **show platform hardware qfp active feature acl dp hsl configuration**in privileged EXEC mode.

show platform hardware qfp active feature acl dp hsl configuration

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 17.15.1	This command was introduced on the following platforms: • Cisco ASR 1000 Series Aggregation Services Routers • Cisco Catalyst 8500 Series Edge Platforms

Usage Guidelines

The **show platform hardware qfp active feature acl dp hsl configuration** command displays an overview of how SGACL logging is set up, including parameters such as logging destinations, rates, and formats, specifically within the data plane's hardware component.

Example

The following is a sample output from the **show platform hardware qfp active feature acl dp hsl configuration** command.

```
SGACL HSL Config
----------------
HSL Config Initialized/Set: TRUE
HSL Enabled: TRUE
HSL Base Memory Address: 0p0xXXXX
HSL Memory Size (bytes): 131072
HSL Handle: 0x00001A
HSL Version: 9
HSL Maximum Records: 512
HSL Record Threshold: 1024
HSL Export Timeout (ms): 4
SGACL_EXPORT_HSL_MTU_SIZE (bytes): 1450
SGACL_EXPORT_HSL_BFR_THRHLD (bytes): 32000 /* (256 * 128) */
SGACL_EXPORT_HSL_REC_THRHLD : 128   /* (512 / 4) */
SGACL_EXPORT_HSL_TMP_RFSH_TMR: 0
SGACL_EXPORT_HSL_TMP_RFSH_PKTS: 0
SGACL_EXPORT_HSL_SRC_ID: 495
SGACL_EXPORT_HSL_BFR_SIZE (bytes): 131072  /* (256 * 512) */
SGACL_EXPORT_HSL_MAX_REC_SIZE(bytes): 256
```

show platform hardware qfp active feature ipsec

To display IPsec feature-specific information in the IPsec Cisco Quantum Flow Processor (QFP), use the **show platform hardware qfp active feature ipsec** command in the privileged EXEC mode.

show platform hardware qfp active feature ipsec {**event-monitor** | **interface** *interface-name* | **spi** | **sp-obj** *number* | **spd** | **datapath drops** | **clear** | {**all** *qfp-spd-number* | [**ace** *spd-class-group-id* | [*qfp-spd-class-id*]]}}

Syntax Description

event-monitor	Displays IPsec monitored events and event-count thresholds.
interface *interface-name*	Displays QFP information for the specified interface.
spi	Displays QFP IPsec security parameter index (SPI) information.
sp-obj *number*	Displays security policy information. The range is from 0 to 4294967295.
spd	Displays Security Policy Database (SPD) information.
datapath drops	Displays datapath drop counters, indicating the number of dropped packets, and a code number for the error type. Error codes vary, depending on platform.
clear	Clears the datapath drop counters.
state	Displays QFP IPsec state information.
all	Displays information about all SPDs.
qfp-spd-number	Specific handle in IPsec Cisco QFP.
ace	(Optional) Displays information about QFP IPsec SPD Cisco Application Control Engine (ACE).
spd-class-group-id	(Optional) SPD class group ID in Cisco ACE.
qfp-spd-class-id	(Optional) QFP class ID.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.9S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.
Cisco IOS 12.2 XN	The **event-monitor type** keyword was added.
Cisco IOS XE Fuji 16.8.1	Updated the error codes in the output when using **datapath drops**.

Usage Guidelines

This command displays information that can help you to troubleshoot issues about IPsec flows.

Examples

The following is a sample output of the **show platform hardware qfp active feature ipsec event-monitor** command. (The fields in the output are self-explanatory.)

```
Device# show platform hardware qfp active feature ipsec event-monitor

AntiReplay Threshold Setting: 1
Decryption Threshold Setting: 1000
Encryption Threshold Setting: 0
```

The following is a sample output from the **show platform hardware qfp active feature ipsec interface** command:

```
Device# show platform hardware qfp active feature ipsec interface gigabitEthernet 1/1/3

QFP ipsec intf sub-block Information

Ingress subblock for interface : 10
                         spd_id : 1
                  flags: 8000 (INTF ENABLED)
           spi tbl ptr: 0x898e4c00
            num labels: 1
                cce_w0: 0x10004
                cce_w1: 0x1084441
                 def_q: 0x0
                 pri_q: 0x0
  Ingress Statistics:

             pkts decrypted: 1
       pkts sent to crypto: 1
      pkts recv from crypt: 1
    pkts failed decryption: 0
  pkts failed policy check: 0

Egress subblock for interface : 10
                         spd_id : 1
                  flags: 8000 (INTF ENABLED)
           spi tbl ptr: 0x0
            num labels: 1
                cce_w0: 0x10004
                cce_w1: 0x1084441
                 def_q: 0x0
                 pri_q: 0x0
  Egress Statistics:

             pkts encrypted : 1
       pkts sent to crypto : 1
       pkts recv from crypt: 1
    pkts failed encryption: 0
```

The following table describes the significant fields shown in the display.

Table 8: show platform hardware qfp active feature ipsec interface Field Descriptions

Field	Description
Ingress subblock for interface	Incoming block for the interface.
spd_id	SPD identifier.
flags	Flags set for the interface.
spi tbl ptr	SPI table pointer.
num labels	Numerical labels.
def_q	Deferral queue.
pri_q	Priority queue.
Ingress Statistics	Incoming statistics.
pkts decrypted	Number of packets decrypted.
pkts sent to crypto	Number of packets sent to the crypto engine.
pkts recv from crypt	Number of packets received from the crypto engine.
pkts failed decryption	Number of packets that failed decryption.
pkts failed policy check	Number of packets that failed security policy check.
Egress subblock for interface	Outgoing block for the interface.
Egress Statistics	Outgoing statistics.
pkts encrypted	Number of packets encrypted.
pkts failed encryption	Number of packets that failed encryption.

The following is a sample output from the **show platform hardware qfp active feature ipsec spi** command:

```
Device# show platform hardware qfp active feature ipsec spi

QFP IPSEC SPI TABLE:

  IDX      SPI          PPE_ADDR     NXT_PPE      PROTO   VRF      SPD        SA
ADDR

-------------------------------------------------------------------------------------------

  0x992    0x95002492   0x89afb420   0x0          0x32    0        1          7
IPV4
```

The following table describes the significant fields shown in the display.

Table 9: show platform hardware qfp active feature ipsec spi Field Descriptions

Field	Description
IDX	Identifier.
SPI	SPI.
PPE_ADDR	Memory address where the SPI is stored in the QFP.
NXT_PPE	Address of the next SPI.
PROTO	IPSec protocol of the SA which is associated with the SPI.
VRF	Virtual routing and forwarding id of the SA.
SPD	QFP handle of the SPD that the SPI belongs to.
SA	QFP handle of the SA that the SPI belongs to.
Addr	Type of address.

The following is a sample output from the **show platform hardware qfp active feature ipsec sp-obj** command for SP ID 1:

```
Device# show platform hardware qfp active feature ipsec sp-obj 4

QFP ipsec sp Information

           QFP sp id: 4
           pal sp id: 6
          QFP spd id: 1
     number of intfs: 0
    cgid.cid.fid.rid: 1.2.2.1
```

The following table describes the significant fields shown in the display.

Table 10: show platform hardware qfp active feature ipsec sp-obj Field Descriptions

Field	Description
QFP sp id	QFP SP identifier.
QFP spd id	QFP SPD identifier.
number of intfs	Number of interfaces.

The following is a sample output from the **show platform hardware qfp active feature ipsec spd all** command:

```
Device# show platform hardware qfp active feature ipsec spd all

Current number CONTEXTs: 8
Current number SPDs: 1
Current number SPs: 5
Current number SAs: 2
    Active IN  SAs: 1          (pending: 0)
```

```
  Active OUT SAs: 1          (pending: 0)

---spd_id--------cg_id-----------num of intf---

     1             1              1
```

The following table describes the significant fields shown in the display.

Table 11: show platform hardware qfp active feature ipsec spd all Field Descriptions

Field	Description
Current number CONTEXTs	Number of SPD contexts in the system.
Current number SPDs	Number of SPDs in the system.
Current number SPs	Number of SPs in the system.
Current number SAs	Number of SAs in the system.
Active IN SAs	Number of active SAs.
spd_id	SPD identifier.
cg_id	Class group identifier.
num of intf	Number of interfaces.

The following is a sample output from the **show platform hardware qfp active feature ipsec spd** command for SPD ID 1:

```
Device# show platform hardware qfp active feature ipsec spd 1

            QFP id: 1
            pal id: 1
      num of aces: 6
     num of intfs: 1
  first intf name: GigabitEthernet1/1/3
             cgid: 1
       num of cm: 3
          cce_w0: 0x10004
          cce_w1: 0x1084441

---cgid.cid.fid----------num of aces---

     1.1.1                 2
     1.2.2                 2
     1.3.3                 2
```

The following table describes the significant fields shown in the display.

Table 12: show platform hardware qfp active feature ipsec spd Field Descriptions

Field	Description
QFP id	QFP identifier.
num of aces	Number of Cisco Application Control Engines (ACEs).

Field	Description
num of intfs	Number of interfaces.
first intf name	Name of the first interface.

The following is a sample output from the **show platform hardware qfp active feature ipsec state** command:

```
Device# show platform hardware qfp active feature ipsec state

QFP IPSEC state:

Message counter:
  Type                  Request          Reply (OK)       Reply (Error)
  ------------------------------------------------------------------------
  Initialize            1                1                0
  SPD Create            1                1                0
  SPD Intf Bind         1                1                0
  SPD CM Bind           3                3                0
  SP Create             5                5                0
  In SA Add             1                1                0
  Intf Enable           1                1                0
  Bulk SA Stats         128              128              0
  CGM Begin Batch       4                4                0
  CGM End Batch         4                4                0
  Inv SPI Notify        0                2                0
  Out SA Add Bind       1                1                0
```

The following table describes the significant fields shown in the display.

Table 13: show platform hardware qfp active feature ipsec state Field Descriptions

Field	Description
Message counter	Number of messages.
Initialize	Number of messages exchanged to initialize a connection.
SPD Create	Number of messages exchanged to create an SPD.
SPD Intf Bind	Number of messages exchanged to bind the SPD interface.
SPD CM Bind	Number of messages exchanged to bind to the SPD crypto map.
SP Create	Number of messages exchanged to create an SP.
In SA Add	Number of messages exchanged to create an inbound SA.
Intf Enable	Number of messages exchanged to enable an interface.
Bulk SA Stats	SA statistics.
CGM Begin Batch	Number of messages exchanged to start Class Group Manager (CGM).
CGM End Batch	Number of messages exchanged to end CGM.

Field	Description
Inv SPI Notify	Number of messages exchanged to notify an inverse SPI.
Out SA Add Bind	Number of messages exchanged to create an outbound SA.

The following is a sample output from the **show platform hardware qfp active feature ipsec datapath drops** command, showing information about dropped packets. For dropped packets, the **datapath drops** output includes an error code number for the type of packet drop, the name of the error, and the number of dropped packets.

```
Device#show platform hardware qfp active feature ipsec datapath drops
------------------------------------------------------------------------------
Drop Type  Name                                          Packets
------------------------------------------------------------------------------
30  IN_V4_POST_INPUT_POLICY_FAIL                          25

Device#show platform hard qfp acti feat ipsec datapath drops clear
------------------------------------------------------------------------------
Drop Type  Name                                          Packets
------------------------------------------------------------------------------
```

The following is a sample output from the **show platform hardware qfp active feature ipsec datapath drops clear** command, which clears the datapath drops counters.

```
Device#show platform hard qfp acti feat ipsec datapath drops clear
------------------------------------------------------------------------------
Drop Type  Name                                          Packets
------------------------------------------------------------------------------
```

Related Commands

Command	Description
show platform software ipsec fp active flow	Displays information about active instances of IPsec flows in the ESP.
show platform software ipsec fp active spd-map	Displays information about the active instances of IPsec SPD map objects.

Show platorm hardware qfp active statistics drop history

To display the history of QFP drops for all interfaces in Packet Processor Engine (PPE), use the **show platformhardwareqfpactivestatisticsdrophistory**command.

show platform hardware qfp active statistics drop history

Syntax Description

This command has no keywords or arguments.

Command Default

No default behaviour or values.

Command Modes

Privileged EXEC mode

Command History

Release	Modification
Cisco IOS XE Dublin 17.13.1a	Command introduced

Usage Guidelines

The wrapper command **show drops history qfp** is the short hand notation of the **show platform hardware qfp active statistics drop history** command.

Example

The following example displays the history of QFP drops for all interfaces in Packet Processor Engine.

```
Router# show platform hardware qfp active statistics
drop history
Last clearing of QFP drops statistics : Mon Jun 26
07:29:14 2023
(21s ago)
---------------------------------------------------
---------------------------------------------------
-----------------
Global Drop Stats 1-Min
5-Min 30-Min
All
---------------------------------------------------
---------------------------------------------------
-----------------
Ipv4NoAdj 0
0 0 99818
Ipv4NoRoute 0
0 0 99853
```

Related Commands

Command	Description
show platform hardware qfp active feature ipsec datapath drops	Displays QFP IPSEC Datapath Drop Counters.

show platform hardware qfp active statistics drop thresholds

To display the warning thresholds for per drop cause and/or total QFP drop in packets per second, use the **show platform hardware qfp active statistics drop thresholds** command.

show platform hardware qfp active statistics drop thresholds

Syntax Description

This command has no keywords or arguments.

Command Default

No default behaviour or values.

Command Modes

Privileged EXEC mode

Command History

Release	Modification
Cisco IOS XE 17.14.1a	Command introduced

Usage Guidelines

The wrapper command **show drops thresholds** is the short hand notation of the **show platform hardware qfp active statistics drop thresholds** command.

Note The wrapper command **show drops thresholds** is currently not available on Catalyst 8500L Edge Platform.

Example

The following example displays the warning thresholds for per drop cause and/or total QFP drop.

```
Router#show platform hardware qfp active statistics drop thresholds
-----------------------------------------------------
Drop ID         Drop Cause Name             Threshold
-----------------------------------------------------
10             BadIpChecksum                 100
206            PuntPerCausePolicerDrops      10
20             QosPolicing                   200
               Total                          30
```

Related Commands

Command	Description
platform qfp drops threshold	Configures the warning thresholds for per drop cause and/or total QFP drop.

show platform hardware qfp feature alg statistics sip

To display Session Initiation Protocol (SIP) application layer gateway (ALG)-specific statistics information in the Cisco Quantum Flow Processor (QFP), use the **show platform hardware qfp feature alg statistics sip** command in privileged EXEC mode.

show platform hardware qfp feature alg statistics sip [**clear** | **dbl** [**all** | **clear** | **entry** *entry-string* [**clear**]] | **dblcfg** | **l7data** {**callid** *call-id* | **clear**} | **processor** | **timer**]

Syntax Description

clear	(Optional) Clears ALG counters after display.
dbl	(Optional) Displays brief information about all SIP blocked list data.
all	(Optional) Displays all dynamic blocked list entries: blocked list and non blocked list entries.
entry *entry-string*	(Optional) Clears the specified blocked list entry.
dblcfg	(Optional) Displays all SIP blocked list settings.
l7data	(Optional) Displays brief information about all SIP Layer 7 data.
callid *call-id*	(Optional) Displays information about the specified SIP call ID.
processor	(Optional) Displays SIP processor settings.
timer	(Optional) Displays SIP timer settings.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

This command displays the following error details:

- Session write lock exceeded
- Global write lock exceeded
- Blocked list

This command also displays the following event details:

- Blocked list triggered
- Blocked list timeout

A blocked list is a list of entities that are denied a particular privilege, service, or access.

Examples

The following is sample output from the **show platform hardware qfp active feature alg statistics sip** command:

```
Device#  show platform hardware qfp active feature alg statistics sip
```

```
Events
...
Cr dbl entry:                10   Del dbl entry:                 10
Cr dbl cfg entry:             8   Del dbl cfg entry:              4
start dbl trig tmr:          10   restart dbl trig tmr:        1014
stop dbl trig tmr:           10   dbl trig timeout:            1014
start dbl blk tmr:            0   restart dbl blk tmr:            0
stop dbl blk tmr:             0   dbl blk tmr timeout:            0
start dbl idle tmr:          10   restart dbl idle tmr:         361
stop dbl idle tmr:            1   dbl idle tmr timeout:           9

DoS Errors
Dbl Retmem Failed:            0    Dbl Malloc Failed:             0
DblCfg Retm Failed:           0    DblCfg Malloc Failed:          0
Session wlock ovflw:          0    Global wlock ovflw:            0
Blacklisted:                561
```

The table below describes the significant fields shown in the display.

Table 14: show platform hardware qfp active feature alg statistics sip Field Descriptions

Field	Description
CR dbl entry	Number of dynamic blocked list entries.
start dbl blk tmr	Number of events that have started the dynamic blocked list timer.
stop dbl idle tmr	Number of events that have stopped the dynamic blocked list idle timer.
Del dbl entry	Number of dynamic blocked list entries deleted.
restart dbl trig tmr	Number of dynamic blocked list trigger timers restarted.
dbl trig timeout	Number of dynamic blocked list trigger timers timed out.
restart dbl blk tmr	Number of dynamic blocked list timers to be restarted.
dbl idle tmr timeout	Number of dynamic blocked list idle timers timed out.
DoS Errors	Denial of service (DoS) related errors.
Dbl Retmem Failed	Number of dynamic blocked list return memory failures.
DblCfg Retm Failed	Number of dynamic blocked list configuration return memory failures.
Session wlock ovflw	Number of packets that are dropped because the session-level write lock number is exceeded.
Blocked list	Number of packets dropped by dynamic blocked list.
Dbl Malloc Failed	Number of dynamic blocked list memory allocation failures.
DblCfg Malloc Failed	Number of dynamic blocked list configuration memory allocation failures.

Field	Description
Global wlock ovflw	Number of packets dropped because the global-level write-lock number is exceeded.

The following is sample output from the **show platform hardware qfp active feature alg statistics sip dbl entry** command:

```
Device# show platform hardware qfp active feature alg statistics sip dbl entry a4a051e0a4a1ebd

req_src_addr: 10.74.30.189              req_dst_addr: 10.74.5.30
trigger_period:     1000(ms)            block_timeout:       30(sec)
idle_timeout:       60(sec)             dbl_flags: 0x        1
cfg_trig_cnt:        5                  cur_trig_cnt:        0
```

The table below describes the significant fields shown in the display.

Table 15: show platform hardware qfp active feature alg statistics sip Field Descriptions

Field	Description
req_src_addr	Source IP address of a SIP request message.
trigger_period	Dynamic blocked list trigger period.
idle_timeout	Dynamic blocked list idle timeout entry.
cfg_trig_cnt	Configured trigger counter.
req_dst_addr	Destination IP address of a SIP request message.
block_timeout	Dynamic blocked list block timeout.
dbl_flags	Dynamic blocked list entry flags.
cur_trig_cnt	Current trigger counter.

Related Commands

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

show platform hardware qfp feature firewall

To display firewall feature-specific information in the Cisco Quantum Flow Processor (QFP), use the **show platform hardware qfp feature firewall** command in privileged EXEC mode.

show platform hardware qfp {**active** | **standby**} **feature firewall** {**memory** | **runtime** | **client** {**l7 policy** {*zone-pair-id layer4-class-id* | **all**} | **statistics**} | **sess-query-context** | **session** {**create** | **delete** | **more**} *session-context number-of-sessions* [**zonepair** *zonepair-id*] | **zonepair** *zonepair-id*}

Syntax Description

active	Displays the active instance of the processor.
standby	Displays the standby instance of the processor.
memory	Displays information about the Cisco QFP firewall datapath memory.
runtime	Displays information about the Cisco QFP firewall datapath runtime.
client	Displays information about the Cisco QFP firewall client.
l7 policy *zone-pair-id layer4-class-id*	Displays information about the Layer 7 policy that has the specified zone-pair ID and Layer 4 class ID.
all	Displays information about all Cisco QFP firewall client Layer 7 policies.
statistics	Displays information about Cisco QFP firewall client statistics.
sess-query-context	Displays information about Cisco QFP firewall session query context.
session	Displays information about the Cisco QFP firewall sessions.
create	Creates new show session contexts.
delete	Deletes the specified session context.
more	Reads all configured sessions that have the specified context.
session-context	Session context. Valid values are 0 to 4294967295.
number-of-sessions	Number of sessions to read. Valid values are from 0 to 4294967295.
zonepair *zonepair-id*	Displays information about Cisco QFP firewall zone pairs. Valid values are from 0 to 4294967295.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.9S	This command was introduced.
Cisco IOS XE Release 3.11S	This command was modified. The command output was modified to include the number of simultaneous packets per flow.

Usage Guidelines

Use this command to troubleshoot firewall issues related to memory usage, runtime errors, and so on.

Example

The following is sample output from the **show platform hardware qfp active feature firewall memory** command:

```
Device# show platform hardware qfp active feature firewall memory

                     ==FW memory info==
Chunk-Pool   Allocated     Total_Free   Init-Num     Low_Wat
-------------------------------------------------------------
scb          0             16384        16384        4096
hostdb       0             5120         5120         1024
ICMP Error   0             256          256          128
teardown     0             160          160          80
ha retry     0             2048         2048         512
dst pool     0             5120         5120         1024

                          ------------Total History----------
Chunk-Pool   Inuse      |Allocated    Freed       Alloc_Fail|
-------------------------------------------------------------
scb          0           0            0           0
hostdb       0           0            0           0
ICMP Error   0           0            0           0
dst pool     0           0            0           0

Table-Name   Address      Size
-----------------------------------------
-----------------------------------------
scb          0x8bc80000   65536
hostdb       0x89941c00   1024
zonepair     0x89950400   1024
dchannel     0x8994cc00   2048

FW persona timer tbl address 0x8c271020 entries: 131072 num_tbls 9 stagger 17,
FW persona hostdb mtx (lock address): 0x89942c00
FW persona ICMP Error pool address: 0x89956820
FW persona un-created sessions due to max session limit:  0
FW persona agg-age sess teardown halfopen: 0, non-halfopen: 0
```

The following is sample output from the **show platform hardware qfp active feature firewall runtime** command:

```
Device# show platform hardware qfp active feature firewall runtime

FW internal: stop_traffic 0x0
global 0xa2400021
  HA State                  Allow New Sess
  FW Configured             (0x00000020)
  VRF Rsrc Chk              (0x00400000)
  Syslog Deployed           (0x02000000)
  VRF Enabled               (0x20000000)
```

```
  B2B HA Enabled            (0x80000000)
global2 0x192c0012
  Global number of simultaneous packet per session allowed 44  <<<<<<<<<<<<
  Default number of simultaneous packet per session allowed  25
debug 0x00008041
.
.
.
```

The following is sample output from the **show platform hardware qfp active feature firewall client statistics** command:

```
Device# show platform hardware qfp active feature firewall client statistics

Zonepair table entry count: 1
Filler block count: 0
Action block count: 0
L7 params block count: 0
Statistics table count: 0
Statistics block count: 0
Class name table entry count: 0
Number of vrf interfaces with zone: 0
Number of zoned interfaces: 2
Number of zones: 2
Number of zone pairs with policy: 0
Inspect parameter map count: 3
VRF related objects: VRF-ParameterMap count: 1, VRF-ParameterMap Binding count: 0
Zone related objects: Zone-ParameterMap count: 0, Zone-ParameterMap Binding count: 0
SCB pool: number of entries: 16384, entry limit: 1048576, size: 4719008, number of additions:
 0
Synflood Hostdb pool: number of entries: 5120, entry limit: 0, size: 573856, number of
additions: 0
Session Teardown pool: number of entries: 160, entry limit: 0, size: 5536, number of
additions: 0
Syncookie Destination pool: number of entries: 5120, entry limit: 262144, size: 410016,
number of additions: 0
```

The following is sample output from the **show platform hardware qfp active feature firewall zonepair** command:

```
Device# show platform hardware qfp active feature firewall zonepair 1

Zonepair name:zp-ge000-ge003 | id:1
     Source zone name:ge0-0-0 | id:2
Destination zone name:ge0-0-3 | id:1
     Class group name:policy1 | id:14841376
lookup data in sw: 0x00010003, 0x00084441
lookup data in hw: 0x00010003, 0x00084441

Class name:c-ftp-tcp | id:13549553
Number of Protocols: 4
Protocols: 1, 2, 4, 18
Maxever number of packet per flow: 25
Filler block/Action block/Stats table addresses: 0x8967f400, 0x8d70f400, 0x898d7400
Stats blocks addresses: 0x8d716c00, 0x8d716c40, 0x8d716c80, 0x8d716cc0
Result: 0x08000000, 0x8967f400
Filler block in sw: 0x8d70f400898d7400
Filler block in hw: 0x0000000c00000000
Action block in hw:

Class name:class-default | id:1593
Number of Protocols: 0
Maxever number of packet per flow: 0
Filler block/Action block/Stats table addresses: 0x8967f400, 0x8d70f400, 0x898d7400
```

```
Stats blocks addresses: 0x8d716c00, 0x8d716c40, 0x8d716c80, 0x8d716cc0
Result: 0x08000000, 0x8967f400
Filler block in sw: 0x8d70f400898d7400
Filler block in hw: 0x0000000c00000000
Action block in hw:


Class name:class-default | id:1593
Number of Protocols: 0
Maxever number of packet per flow: 0
Filler block/Action block/Stats table addresses: 0x8967f408, 0x8d70f4f0, 0x898d7520
Result: 0x81000000, 0x8967f408
Filler block in sw: 0x8d70f4f0898d7520
Filler block in hw: 000000000000000000
Action block in hw:
```

The table below describes the significant fields shown in the displays.

Table 16: show platform hardware qfp feature firewall Field Descriptions

Field	Description
scb	Memory allocated for the session control block (SCB) pool.
dst pool	Memory allocated for the destination pool.
HA state	High availability status.
HSL Enabled	Number of sessions for which high-speed logging (HSL) is enabled.
teardowns	Number of queues that were torn down.
Num of ACK exceeds limit	Number of acknowledgment (ACK) requests that exceeded the configured limit.
Num of RST exceeds limit	Number of reset (RST) requests that exceeded the configured limit.
VRF Global Action Block	Information about the global virtual routing and forwarding (VRF) instance.
half-open	Information about the half-opened firewall sessions.
aggr-age high watermark low watermark	Information about the aggressive-aging high and low watermarks. Firewall sessions are aggressively aged to make room for new sessions, thereby protecting the firewall session database from filling. Aggressive aging period starts when the session table crosses the high watermark and ends when it falls below the low watermark.

Related Commands

show platform hardware qfp feature firewall datapath	Displays information about the firewall datapath in the Cisco QFP.
show platform hardware qfp feature firewall drop	Displays information about the firewall packet drops in the Cisco QFP.

show platform hardware qfp feature firewall datapath scb

To display information about the session control block of the Cisco Quantum Flow Processor (QFP), use the **show platform hardware qfp feature firewall datapath scb** command in privileged EXEC mode.

show platform hardware qfp {**active** | **standby**} **feature firewall datapath scb** [*ipv4-address* | *ipv4-address*/*mask* | **any** | **ipv6** *source-ipv6-address*] [*source-port* | **any**] [*destination-ipv4-address* *destination-ipv6-address* | *ipv4-address*/*prefix* | **any**] [*destination-port* | **any**] [*layer4-protocol* | **any**] [**all** | **imprecise** | **session**] [*vrf-id* | **any**] [**detail**]

Syntax Description

active	Displays the active instance of the processor.
standby	Displays the standby instance of the processor.
ipv4-address mask	(Optional) IPv4 address and prefix mask.
any	(Optional) Specifies any source port, destination port, Layer 4 protocol number, or virtual routing and forwarding (VRF) ID.
ipv6 *source-ipv6-address*	(Optional) Specifies an IPv6 address.
source-port	(Optional) Source port number. The range is from 0 to 65535.
destination-ipv4-address	(Optional) Destination IPv4 address.
destination-ipv6-address	(Optional) Destination IPv6 address.
destination-port	(Optional) Destination port number. The range is from 0 to 65535.
layer4-protocol	(Optional) Layer 4 protocol number. The range is from 0 to 255.
all	(Optional) Specifies all firewall databases.
imprecise	(Optional) Specifies the imprecise database.
session	(Optional) Specifies the firewall session database.
vrf-id	(Optional) VRF ID. The range is from 0 to 65535.
detail	(Optional) Provides detailed information about the firewall session and imprecise databases.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

This command provides detailed information about firewall sessions and databases. The **show policy-firewall sessions platform all** command also performs the same action as **show platform hardware qfp active feature firewall datapath scb any any any any any all any detail** command.

Examples

The following is sample output from the **show platform hardware qfp active feature firewall datapath scb any any any any any all any detail** command:

```
Device# show platform hardware qfp active feature firewall datapath scb any any any any any
 all any detail

[s=session  i=imprecise channel  c=control channel  d=data channel]

Session ID:0x00000002  100.0.0.2 8 100.0.0.1 92 proto 1 (0:0)   [sc]
 pscb : 0x8ba00400,  bucket : 55587, fw_flags: 0x204 0x204154c1,

192.168.2.2 1024 192.168.1.2 1024 proto 17 (0:0)       [sd]
 pscb : 0x8bd0ddc0,  bucket : 34846, fw_flags: 0x4 0x20413481,
        scb state: active, scb debug: 0
 nxt_timeout: 360000, refcnt: 1,  ha nak cnt: 0,  rg: 0, sess id: 0
 hostdb: 0x0, L7: 0x0, stats: 0x8d8e3740, child: 0x0
 l4blk0: 29 l4blk1: 1ceabd0a l4blk2: 0 l4blk3: 805a46fd
 l4blk4: 0 l4blk5: 0 l4blk6: 0 l4blk7: 0
 l4blk8: 0 l4blk9: 2
 root scb: 0x0 act_blk: 0x8d8dbde0
 ingress/egress intf: TenGigabitEthernet1/3/0 (1011), TenGigabitEthernet0/3/0 (131057)
 current time 43491794128 create tstamp: 25627209695 last access: 43491799244
 nat_out_local_addr:port: 10.1.1.4:9 nat_in_global_addr:port: 192.0.2.5:7
 syncookie fixup: 0x0
 halfopen linkage: 0x0 0x0
 tw timer: 0x0 0x0 0x37ed5 0xaf32111
 Number of simultaneous packet per session: 70
```

The table below describes the significant fields shown in the display.

Table 17: show platform hardware qfp feature firewall datapath scb Field Descriptions

Field	Description
scb state	State for the SCB; either active or standby.
ingress/egress intf:	Incoming and outgoing interface IP addresses.
nat_out_local_addr:port:	Network Address Translation (NAT) outside local IP address and port number.
nat_in_global_addr:port:	NAT inside global IP address and port number.

Related Commands

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

show platform hardware qfp feature td

To display threat-defense-specific information in the Cisco QuantumFlow Processor (QFP), use the **show platform hardware qfp feature td** command in privileged EXEC mode.

show platform hardware qfp {**active** | **standby**} **feature td** {**client** | **datapath**} **memory**

Syntax Description

active	Displays the active instance of the processor.
standby	Displays the standby instance of the processor.
client	Displays information about the threat defense (TD) client.
datapath	Displays TD information in the datapath.
memory	Displays information about the TD memory usage.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.9S	This command was introduced.

Usage Guidelines

Use this command to check the virtual TCP (vTCP) statistics that are triggered by TCP application layer gateway (ALG) sessions.

Examples

The following is sample output from the **show platform hardware qfp active feature td datapath memory** command:

```
Device# show platform hardware qfp active feature td datapath memory

==VTCP ucode info==
info alloc 0, free 0, fail 0
pkt buf alloc 0, free 0, fail 0
buf size alloc 0, free 0
rx drop 0, tx drop 0, tcp drop 0, alg csum 0
sending: rx ack 0, rst 0, hold rst 0 tx payload: seg 0, rexmit 0
vtcp_info_chunk 0x8d54fcb0, totalfree: 2048, allocated: 0
vtcp_pkt_pool 0x8d5d80c0, total: 1048240, free: 1048240
vtcp_timer_wheel 0x8d6d84d0, vtcp_init 1
td_internal debug 0x0
td_global td_init 0x2
alg_debug_vtcp 0x0
```

The table below describes the significant fields shown in the display.

Table 18: show platform hardware qfp feature td datapath memory Field Descriptions

Field	Description
info alloc	vTCP allocated counts.

Field	Description
pkt buf alloc	Allocated packet buffer size.
buf size alloc	Allocated buffer size.
rx drop	Transmit buffer (Rx) drop. Rx is memory spaces allocated by a device to handle traffic bursts.
tx drop	Receive buffer (Tx) drop. Rx is memory spaces allocated by a device to handle traffic bursts.

Related Commands

Command	Description
show platform hardware qfp feature alg	Displays ALG-specific information in the Cisco QFP.
show tech-support alg	Displays ALG-specific information to assist in troubleshooting.

show platform software audit

To display predefined audit rulesets and audit monitoring status, use the **show platform software audit** command in privileged EXEC mode.

show platform software audit { **ruleset** | **monitor status** }

Syntax Description

ruleset	Displays the predefined audit rules grouped by ruleset name.
monitor status	Displays high-level audit monitoring status, including which rulesets are enabled ordisabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 17.18.2	This command was introduced.

Usage Guidelines

- This command displays ruleset definitions and ruleset status and do not display audit event logs.
- To view audit event syslog messages, use **show logging | i SYSCALL**.
- Audit syslog messages use the identifier `%IOSXE-5-AUDIT_INFO` and are generated at notice level, according to the attached specification.

Example

This example displays the predefined audit rulesets:

```
Device# show platform software audit ruleset

user_group_config_files :
                          :    -a exit,always -F arch=b64 -F path=/etc/passwd -F perm=wa -k
 user_group_config_files
                          :    -a exit,always -F arch=b64 -F path=/etc/shadow -F perm=wa -k
 user_group_config_files

dns_client_files :
                          :    -a exit,always -F arch=b64 -F path=/etc/hosts -F perm=wa -k
dns_client_files
                         :    -a exit,always -F arch=b64 -F path=/etc/resolv.conf -F perm=wa
 -k dns_client_files
kernel_module_mgmt :
                          :    -a exit,always -F arch=b64 -F path=/sbin/insmod -F perm=x -k
 kernel_module_mgmt
                          :    -a exit,always -F arch=b64 -F path=/sbin/rmmod -F perm=x -k
kernel_module_mgmt
user_privilege_mgmt :
                          :    -a always,exit -F arch=b64 -S
setuid,setresuid,setreuid,setfsuid,setgid,setresgid,setregid,setfsgid -F
key=user_privilege_mgmt
                          :    -a always,exit -F arch=b32 -S
system_software :
                          :    -a exit,always -F arch=b64 -F dir=/bin -F perm=wa -k
```

```
system_software
                          :    -a exit,always -F arch=b64 -F dir=/sbin -F perm=wa -k
system_software
```

This example displays high-level audit monitoring status:

```
Device# show platform software audit monitor status
AUDIT RULE SET                          : STATUS
-------------------------------------------------------
DNS_CLIENT_FILES                 : enable
KERNEL_MODULE_MGMT                  : enable
SYSTEM_SOFTWARE               : enable
USER_GROUP_CONFIG_FILES          : enable
USER_PRIVILEGE_MGMT                    : enable
```

show platform software cerm-information

To display Crypto Export Restrictions Manager (CERM) information, use the **show platform software cerm-information** command in privileged EXEC mode.

show platform software cerm-information

Syntax Description

This command has no keywords or arguments.

Command Default

CERM information is not displayed.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

This command displays Crypto Export Restrictions Manager (CERM) information of devices running on Cisco IOS XE software.

Examples

The following is a sample output of the **show platform software cerm-information** command:

```
Device# show platform software cerm-information

Crypto Export Restrictions Manager(CERM) Information:
 CERM functionality: ENABLED
 ---------------------------------------------------------------------
 Resource                       Maximum Limit           Available
 ---------------------------------------------------------------------
 Number of tunnels              1000                    1000
 Number of TLS sessions         1000                    1000
 Resource reservation information:
 D - Dynamic
 ---------------------------------------------------------------------------
 Client         Tunnels    TLS Sessions
 ---------------------------------------------------------------------------
 VOICE           0          0
 IPSEC           0          N/A
 SSLVPN          0          N/A
 Statistics information:
 Failed tunnels:            0
 Failed sessions:           0
 Failed encrypt pkts:                          0
 Failed encrypt pkt bytes:                     0
 Failed decrypt pkts:                          0
 Failed decrypt pkt bytes:                     0
```

show platform software firewall

To display the firewall configuration information, use the **show platform software firewall** command in privileged EXEC mode.

show platform software firewall {**F0** | **F1** } {**bindings** | **pairs** | **parameter-maps** | **port-application-mapping** | **statistics** | **vrf-pmap-bindings** | **zones**}

show platform software firewall {**F0** | **F1** } **sessions** **zone-pair** *zone-pair-name* [**class-id** *class-id*] [**destination** *ip-address* | **ipv6** {**destination** *ipv6-address* | **source** *ipv6-address* [**destination** *ipv6-address*]} | **source** *ip-address* [**destination** *ip-address*]]

show platform software firewall {**R0** | **R1** } {**bindings** | **pairs** | **parameter-maps** | **port-application-mapping** | **statistics** | **vrf-pmap-bindings** | **zones**}

show platform software firewall {**FP** | **RP**} {**active** | **standby**} {**bindings** | **pairs** | **parameter-maps** | **port-application-mapping** | **statistics** | **vrf-pmap-bindings** | **zones**}

Syntax Description

F0	Displays information about the Embedded Service Processor (ESP) slot 0.
F1	Displays information about the ESP slot 1.
bindings	Displays information about the configured security zone bindings.
pairs	Displays information about configured security zone pairs.
parameter-maps	Displays information about configured parameter maps.
port-application-mapping	Displays information about the configured Port-to-Application Mapping (PAM).
sessions	Displays information about existing firewall sessions.
statistics	Displays firewall statistics.
vrf-pmap-bindings	Displays information about the configured virtual routing and forwarding (VRF) instance and parameter map bindings.
zones	Displays information about configured security zones.
zone-pair *zone-pair*	Displays existing firewall sessions for a zone pair.
class-id *class-id*	Displays sessions in a class.

destination *ip-address*	Displays sessions with specified destination IP address.
ipv6	Displays sessions with specified IPv6 address.
ipv6 destination *ipv6-address*	Displays destination IPv6 address.
ipv6 source *ipv6-address*	Displays source IPv6 address.
source *ip-address*	Displays sessions with specified source IP address.
R0	Displays information about the Route Processor (RP) slot 0.
R1	Displays information about the RP slot 1.
FP	Displays information about the ESP.
RP	Displays information about the RP.
active	Displays information about the active instance of the processor.
standby	Displays information about the standby instance of the processor.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.9S	This command was introduced.
Cisco IOS XE Release 3.11S	This command was modified. The command output was modified to display the number of simultaneous packets per flow.

Usage Guidelines

Use this command to view information about the configured firewall policies, parameter maps, security zones, and security zone-pairs.

Example

The following is sample output from the **show platform software firewall FP active parameter-maps** command:

```
Device# show platform software firewall FP active parameter-maps

Forwarding Manager Inspect Parameter-Maps

  Inspect Parameter Map: global, Index 1
  Parameter Map Type: Parameter-Map
      Global Parameter-Map
      Alerts: On, Audits: Off, Drop-Log: Off
      HSL Mode: V9, Host: 10.1.1.1:9000, Port: 54174, Template: 300 sec
      Session Rate High: 2147483647, Session Rate Low: 2147483647, Time Duration: 60 sec
      Half-Open:
```

```
      High: 2147483647, Low: 2147483647, Host: 4294967295, Host Block Time: 0
    Inactivity Times [sec]:
      DNS: 5, ICMP: 10, TCP: 3600, UDP: 30
    Inactivity Age-out Times [sec]:
      ICMP: 10, TCP: 3600, UDP: 30
    TCP Timeouts [sec]:
      SYN wait time: 30, FIN wait time: 1
    TCP Ageout Timeouts [sec]:
      SYN wait time: 30, FIN wait time: 1
    TCP RST pkt control:
      half-open: On, half-close: On, idle: On
    UDP Timeout [msec]:
      UDP Half-open time: 30000
    UDP Ageout Timeout [msec]:
      UDP Half-open time: 30000

    Max Sessions: Unlimited

    Number of Simultaneous Packet per Sessions: 0
    Syn Cookie and Resource Management:
      Global Syn Flood Limit: 4294967295
      Global Total Session : 4294967295
    Global Total Session Aggressive Aging Disabled
    Global alert : Off
    Global max incomplete : 4294967295
    Global max incomplete TCP: 4294967295
    Global max incomplete UDP: 4294967295
    Global max incomplete ICMP: 4294967295
    Global max incomplete Aggressive Aging Disabled
    Per Box Configuration
      syn flood limit : 4294967295
      Total Session Aggressive Aging Disabled
      max incomplete : 4294967295
      max incomplete TCP: 4294967295
      max incomplete UDP: 4294967295
      max incomplete ICMP: 4294967295
      max incomplete Aggressive Aging Disabled

Inspect Parameter Map: vrf-default, Index 2
Parameter Map Type: VRF-Parameter-Map
VRF PMAP syn flood limit : 4294967295
VRF PMAP total session : 4294967295
VRF PMAP total session Aggressive Aging Disabled
VRF PMAP alert : Off
VRF PMAP max incomplete : 4294967295
VRF PMAP max incomplete TCP: 4294967295
VRF PMAP max incomplete UDP: 4294967295
VRF PMAP max incomplete ICMP: 4294967295
VRF PMAP max incomplete Aggressive Aging Disabled

Inspect Parameter Map: pmap-hsl, Index 3
Parameter Map Type: Parameter-Map
    Alerts: On, Audits: On, Drop-Log: Off
    Session Rate High: 2147483647, Session Rate Low: 2147483647, Time Duration: 60 sec
    TCP Window Scaling Loose: off
    session packet default
    Half-Open:
      High: 2147483647, Low: 2147483647, Host: 4294967295, Host Block Time: 0
    Inactivity Times [sec]:
      DNS: 5, ICMP: 10, TCP: 3600, UDP: 30
    Inactivity Age-out Times [sec]:
      ICMP: 10, TCP: 3600, UDP: 30
    TCP Timeouts [sec]:
      SYN wait time: 30, FIN wait time: 1
```

```
    TCP Ageout Timeouts [sec]:
      SYN wait time: 30, FIN wait time: 1
    TCP RST pkt control:
      half-open: On, half-close: On, idle: On
    UDP Timeout [msec]:
      UDP Half-open time: 30000
    UDP Ageout Timeout [msec]:
      UDP Half-open time: 30000

    Max Sessions: Unlimited

    Number of Simultaneous Packet per Sessions: 0
    Syn Cookie and Resource Management:
      Global Syn Flood Limit: 4294967295
      Global Total Session : 4294967295

 Inspect Parameter Map: pmap1, Index 4
 Parameter Map Type: Parameter-Map
    Alerts: On, Audits: On, Drop-Log: Off
    Session Rate High: 2147483647, Session Rate Low: 2147483647, Time Duration: 60 sec
    TCP Window Scaling Loose: off
    session packet default
    Half-Open:
      High: 2147483647, Low: 2147483647, Host: 4294967295, Host Block Time: 0
    Inactivity Times [sec]:
      DNS: 5, ICMP: 10, TCP: 3600, UDP: 30
    Inactivity Age-out Times [sec]:
      ICMP: 10, TCP: 3600, UDP: 30
    TCP Timeouts [sec]:
      SYN wait time: 30, FIN wait time: 1
    TCP Ageout Timeouts [sec]:
      SYN wait time: 30, FIN wait time: 1
    TCP RST pkt control:
      half-open: On, half-close: On, idle: On
    UDP Timeout [msec]:
      UDP Half-open time: 30000
    UDP Ageout Timeout [msec]:
      UDP Half-open time: 30000

    Max Sessions: 3000

    Number of Simultaneous Packet per Sessions: 0
    Syn Cookie and Resource Management:
      Global Syn Flood Limit: 4294967295
      Global Total Session : 4294967295

Inspect Parameter Map: pmap1, Index 4
 Parameter Map Type: Parameter-Map
    Alerts: On, Audits: On, Drop-Log: Off
    Session Rate High: 2147483647, Session Rate Low: 2147483647, Time Duration: 60 sec
    TCP Window Scaling Loose: off
    session packet default
    Half-Open:
      High: 2147483647, Low: 2147483647, Host: 4294967295, Host Block Time: 0
    Inactivity Times [sec]:
      DNS: 5, ICMP: 10, TCP: 3600, UDP: 30
    Inactivity Age-out Times [sec]:
      ICMP: 10, TCP: 3600, UDP: 30
    TCP Timeouts [sec]:
      SYN wait time: 30, FIN wait time: 1
    TCP Ageout Timeouts [sec]:
      SYN wait time: 30, FIN wait time: 1
    TCP RST pkt control:
      half-open: On, half-close: On, idle: On
```

```
UDP Timeout [msec]:
  UDP Half-open time: 30000
UDP Ageout Timeout [msec]:
  UDP Half-open time: 30000

Max Sessions: 3000

Number of Simultaneous Packet per Sessions: 0
Syn Cookie and Resource Management:
  Global Syn Flood Limit: 4294967295
  Global Total Session : 4294967295
```

The table below describes the significant fields shown in the display.

Table 19: show platform software firewall Field Descriptions

Field	Description
Alerts on	Console display of stateful packet inspection alert messages. Valid values are On and Off.
Audits off	Audit trail messages. Valid values are On and Off.
HSL mode	High-speed logging (HSL) messages are logged.
Host	IP address of the host to which HSL messages are logged.
SYN wait time	Time period the software waits for a TCP session to reach the established state before dropping the session.
FIN wait time	Time period a TCP session is managed after the firewall detects a finish (FIN) exchange.
Global SYN Flood limit	Configured TCP half-open session limit before triggering the synchronization (SYN) cookie processing for new SYN packets.

The following is sample output from the show command **show platform software firewall F0 sessions zone-pairs**

```
Device# show platform software firewall F0 sessions zone-pair in-self

Established Sessions
Session ID 0x00000001 (100.0.0.2:8)=>(100.0.0.1:91) icmp SIS_OPEN
  Created 00:00:02, Last heard 00:00:02
  Bytes sent (initiator:responder) [360:360]
```

The following is sample output from the **show platform software firewall RP active statistics** command:

```
Device# show platform software firewall RP active statistics

Forwarding Manager Firewall Statistics

Zones:
  3 Adds (0 errors), 0 Mods (0 errors), 0 Deletes (0 errors)
  6 Downloads (0 errors)

Zone-pairs:
```

```
  1 Adds (0 errors), 0 Mods (0 errors), 0 Deletes (0 errors)
  2 Downloads (0 errors)

Zone-bindings:
  4 Adds (0 errors), 0 Mods (0 errors), 0 Deletes (0 errors)
  8 Downloads (0 errors)

Inspect Parameter-Maps:
  0 Adds (0 errors), 0 Mods (0 errors), 0 Deletes (0 errors)
  0 Downloads (0 errors)

PAMs(Port Application Mapping):
  0 Adds (0 errors), 0 Mods (0 errors), 0 Deletes (0 errors)
  0 Downloads (0 errors)

VRF Bindings:
  0 Adds (0 errors), 0 Mods (0 errors), 0 Deletes (0 errors)
  0 Downloads (0 errors)
```

Related Commands

Command	Description
parameter-map type inspect	Configures an inspect-type parameter map for connecting thresholds, timeouts, and other parameters pertaining to the **inspect** action.
zone-pair security	Creates a zone pair.

show platform software ipsec policy statistics

To display debugging information about the IP security policy statistics, use the **show platform software ipsec policy statistics** command in Privileged EXEC mode.

show platform software ipsec policy statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.8S	This command was introduced.

The following is sample output from the **show platform software ipsec policy statistics** command:

```
Router# show platform software ipsec policy statistics

PAL CMD                 REQUEST   REPLY OK  REPLY ERR      ABORT
SADB_INIT_START               1          1          0          0
SADB_INIT_COMPLETED           1          1          0          0
SADB_DELETE                   0          0          0          0
SADB_ATTR_UPDATE              1          1          0          0
SADB_INTF_ATTACH              1          1          0          0
SADB_INTF_UPDATE              0          0          0          0
SADB_INTF_DETACH              0          0          0          0
ACL_INSERT                    1          1          0          0
ACL_MODIFY                    0          0          0          0
ACL_DELETE                    0          0          0          0
PEER_INSERT                   3          3          0          0
PEER_DELETE                   2          2          0          0
SPI_INSERT                  151        151          0          0
SPI_DELETE                  150        150          0          0
CFLOW_INSERT                  3        151          0          0
CFLOW_MODIFY                148        148          0          0
CFLOW_DELETE                  2          2          0          0
OUT_SA_DELETE               150        150          0          0
TBAR_CREATE                   0          0          0          0
TBAR_UPDATE                   0          0          0          0
TBAR_REMOVE                   0          0          0          0

PAL NOTIFY    RECEIVE    COMPLETE    PROC ERR      IGNORE
NOTIFY_RP           0           0           0           0
SA_DEAD             2           2           0           0
SA_SOFT_LIFE       80          80           0           0
IDLE_TIMER          0           0           0           0
DPD_TIMER           0           0           0           0
INVALID_SPI         0           0           0           0
```

The following table describes the significant fields shown in the display:

Table 20: show platform software ipsec policy statistics Field Descriptions

Field	Description
PAL CMD	Name of a request sent from the IPsec control plane to the IPsec data plane.

REQUEST	Number of IPsec control plane requests sent.
REPLY OK	Number of successful replies sent by the IPsec data plane for the requests sent by the IPsec control plane.
REPLY ERR	Number of failed replies sent by the IPsec data plane for the requests sent by the IPsec control plane.
ABORT	Number of requests terminated because of a timeout.
PAL NOTIFY	Name of a notification sent from the IPsec data plane to the IPsec control plane.
RECEIVE	Number of IPsec data plane notifications received.
COMPLETE	Number of successful IPsec data plane notifications sent to the IPsec control plane.
PROC ERR	Number of IPsec data plane notifications that were not sent because of a process error.
IGNORE	Number of IPsec data plane notifications that can be safely ignored.

Table 21: Related Commands

Command	Description
show platform software ipsec f0 inventory	Displays the IPsec object counts of a forwarding processor.

show platform software ipsec f0 encryption-processor registers

To display debugging information about the crypto engine processor registers, use the **show platform software ipsec f0 encryption-processor registers** command in privileged EXEC or diagnostic mode.

show platform software ipsec f0 encryption-processor registers

Command Default

No default behavior or values

Command Modes

Privileged EXEC (#)

Diagnostic (diag)

Command History

Release	Modification
Cisco IOS XE Release 2.4.2	This command was introduced on the Cisco ASR 1000 Series Routers.

Usage Guidelines

This command displays debugging information for crypto engine processor registers.

```
show platform software ipsec f0 encryption-processor registers
Forwarding Manager Encryption-processor Registers
     reg_addr : 00000000,    reg_val  : 0000ca5b
     reg_addr : 00000008,    reg_val  : 00000000
     reg_addr : 00000010,    reg_val  : 00000000
     reg_addr : 00000018,    reg_val  : 22f10038
     reg_addr : 00000020,    reg_val  : 00000800
     reg_addr : 00000028,    reg_val  : 00002040
     reg_addr : 00000030,    reg_val  : 00000000
     reg_addr : 00000038,    reg_val  : 23158838
```

Related Commands

Command	Description
show platform hardware qfp act feature ipsec datapath memory	Displays debugging information about the consumption of IPsec datapath memory.

show platform software ipsec fp active flow

To display information about active instances of IPsec flows in the Embedded Service Processor (ESP), use the **show platform software fp ipsec active flow** command in privileged EXEC mode.

show platform software ipsec fp active flow {**all** | **identifier** *number*}

Syntax Description

all	Displays information about all active IPsec flows in the instance.
identifier *number*	Displays information about the specified IPsec flow in the instance. The range is from 0-4294967295.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 17.15.1a	The range of IPSec flow was increased to 0 to 4294967295. The initial range was from 0 to 32767.
Cisco IOS XE Release 3.9S	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

This command displays information that can help you to troubleshoot issues about IPsec flows.

Examples

The following is sample output from the **show platform software ipsec fp active flow all** command:

```
Device# show platform software ipsec fp active flow all

========== Flow id: 1
               mode: tunnel
          direction: inbound
           protocol: esp
                SPI: 0x95002492
      local IP addr: 100.0.0.1
     remote IP addr: 100.0.0.2
      crypto map id: 3
             SPD id: 1
    ACE line number: 1
      QFP SA handle: 7
   crypto device id: 0
IOS XE interface id: 11
     interface name: GigabitEthernet1/1/3
       object state: active

========== Flow id: 2
               mode: tunnel
          direction: outbound
           protocol: esp
                SPI: 0xfd2fa486
      local IP addr: 100.0.0.1
     remote IP addr: 100.0.0.2
      crypto map id: 3
             SPD id: 1
    ACE line number: 1
      QFP SA handle: 8
   crypto device id: 0
```

```
IOS XE interface id: 11
     interface name: GigabitEthernet1/1/3
       object state: active
```

The following table describes the significant fields shown in the display.

Table 22: show platform software ipsec fp active flow all Field Descriptions

Field	Description
Flow id	Flow identifier.
mode	Operation mode. In this case, it is tunnel mode.
direction	Flow direction—inbound or outbound. In this case, it is outbound.
protocol	Protocol used. In this case, it is Encapsulating Security Payloads (ESP).
SPI	Security Parameters Index (SPI) that is used to identify the security association (SA).
local IP addr	IP address of the local host.
remote IP addr	IP address of the remote host.
crypto map id	Crypto map identifier.
SPD id	SPI identifier.
ACE line number	Cisco Application Control Engine (ACE) number.
QFP SA handle	Quantum Flow Processor (QFP) SA identifier.
crypto device id	Crypto device identifier.
IOS XE interface id	Interface ID in Cisco IOS XE software.
interface name	Interface name.
use path MTU	Maximum transmission unit (MTU) size.
object state	Object state.
object bind state	State of the object bound.

The following is sample output from the **show platform software ipsec fp active flow** command for flow ID 1:

```
Device# show platform software ipsec fp active flow identifier 1

=========== Flow id: 1
               mode: tunnel
          direction: inbound
           protocol: esp
                SPI: 0x95002492
      local IP addr: 100.0.0.1
     remote IP addr: 100.0.0.2
   crypto device id: 0
```

```
      crypto map id: 3
              SPD id: 1
    ACE line number: 1
      QFP SA handle: 7
IOS XE interface id: 11
     interface name: GigabitEthernet1/1/3
   Crypto SA ctx id: 0x000000002dc3bfde
             cipher: 3DES
               auth: SHA1
 initial seq.number: 0
      timeout, mins: 0
              flags: exp time;exp traffic;DPD;
   Peer Flow handle: 0x0000000080000014
Time limits

         soft limit: 3537
         hard limit: 3597
Traffic limits

         soft limit: 3686400
         hard limit: 4608000
--------------- DPD

               mode: periodic
    rearm countdown: 0
        next notify: *EXPIRED*
     last in packet: 0
     inline_tagging: DISABLED
 anti-replay window: 64
SPI Selector:

   remote addr low: 0.0.0.0
  remote addr high: 0.0.0.0
    local addr low: 100.0.0.1
   local addr high: 100.0.0.1
Classifier: range

   src IP addr low: 1.0.0.0
  src IP addr high: 1.0.0.255
   dst IP addr low: 2.0.0.0
  dst IP addr high: 2.0.0.255
      src port low: 0
     src port high: 65535
      dst port low: 0
     dst port high: 65535
      protocol low: 0
     protocol high: 255
------- Statistics

             octets: 100
       total octets: 4718591900
            packets: 1
    dropped packets: 0
       replay drops: 0
       auth packets: 1
         auth fails: 0
  encrypted packets: 1
      encrypt fails: 0
---- End statistics

       object state: active
--------------- AOM

         cpp aom id: 145
```

```
cgm aom id: 0
 n2 aom id: 142
 if aom id: 0
```

The following table describes the significant fields shown in the display.

Table 23: show platform software ipsec fp active flow identifier Field Descriptions

Field	Description
Flow id	Flow identifier.
mode	Operation mode. In this case, it is tunnel mode.
direction	Flow direction—inbound or outbound. In this case, it is outbound.
protocol	Protocol used. In this case, it is Encapsulating Security Payloads (ESP).
SPI	Security Parameters Index (SPI) that is used to identify the security association (SA).
local IP addr	IP address of the local host.
remote IP addr	IP address of the remote host.
crypto map id	Crypto map identifier.
SPD id	SPI identifier.
ACE line number	Cisco Application Control Engine (ACE) number.
QFP SA handle	Quantum Flow Processor (QFP) SA identifier.
crypto device id	Crypto device identifier.
IOS XE interface id	Interface ID in Cisco IOS XE software.
interface name	Interface name.
Crypto SA ctx id	Context identifier of the crypto SA.
cipher	Type of encryption algorithm.
auth	Type of authentication algorithm.
initial seq.number	Initial sequence number.
timeout, mins	Timeout, in minutes.
flags	Flags set for the packet flow.
Peer Flow handle	Peer flow identifier.
Time limits soft limit	Minimum permissible time limit.
Time limits hard limit	Maximum permissible time limit.

Field	Description
Traffic limits soft limit	Minimum permissible traffic limit.
Traffic limits hard limit	Maximum permissible traffic limit.
DPD	Dead peer detection (DPD).
mode	DPD mode. In this case, it is periodic.
rearm countdown	Rearm for DPD.
next notify	Status of next notification.
last in packet	Status of the last packet.
inline_tagging	Status of inline tagging.
anti-replay window	Status of anti-replay window.
SPI Selector	Information about SPI selection.
remote addr low	Starting range address of the remote host.
remote addr high	Highest range address of the remote host.
local addr low	Starting range address of the local host.
local addr high	Highest range address of the local host.
Classifier	Type of classification.
src IP addr low	Starting range of the source IP address.
src IP addr high	Highest range of the source IP address.
dst IP addr low	Starting range of the destination IP address.
dst IP addr high	Highest range of the destination IP address.
src port low	Starting range of the source port.
src port high	Highest range of the source port.
dst port low	Starting range of the destination port.
dst port high	Highest range of the destination port.
protocol low	Starting range of the protocol.
protocol high	Highest range of the protocol.
octets	Number of octets in the packet.
total octets	Total number of octets.
packets	Number of packets.

Field	Description
dropped packets	Number of packets dropped.
replay drops	Number of packets that were dropped again.
auth packets	Number of packets authenticated.
auth fails	Number of packets for which authentication failed.
encrypted packets	Number of encrypted packets.
encrypt fails	Number of packets for which encryption failed.
object state	Object state. In this case, it is active.
cpp aom id	Cisco Packet Processor Asynchronous Object Manager (AOM) identifier.
cgm aom id	Class Group Manager AOM identifier.
n2 aom id	Cavium NITROX II cryptographic coprocessor AOM identifier.
if aom id	Interface AOM identifier.

Related Commands

Command	Description
show platform hardware qfp active feature ipsec	Display IPsec feature-specific information in IPsec Cisco QFP.
show platform software ipsec fp active spd-map	Displays information about the active instances of IPsec SPD map objects.

show platform software ipsec fp active spd-map

To display information about the active instances of IPsec Security Policy Database (SPD) map objects in the Embedded Service Processor (ESP), use the **show platform software ipsec fp active spd-map** command in privileged EXEC mode.

show platform software ipsec fp active spd-map {**all** | **identifier** *number*}

Syntax Description

all	Displays information about all active IPsec flows in the instance.
identifier *number*	Displays information about the specified IPsec flow in the instance. The range is from 0 to 4294967295.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.9S	This command was introduced on Cisco ASR 1000 Series Routers.

Usage Guidelines

SPD is an ordered list of policies applied to traffic. A policy decides if a packet requires IPsec processing, if should be allowed in clear text, or should be dropped. The IPsec SPDs are derived from user configuration of crypto maps. The Internet Key Exchange (IKE) SPD is configured by the user.

Examples

The following is sample output from the **show platform software ipsec fp active spd-map all** command:

```
Device# show platform software ipsec fp active spd-map all

======== SPD map id: 11
             SPD id: 1
       interface id: 11
     interface name: GigabitEthernet1/1/3
     inbound ACL id: 65535
      local address: 0
       object state: active
         bind state: active
       enable state: active
```

The following table describes the significant fields shown in the display.

Table 24: show platform software ipsec fp active spd-map all Field Descriptions

Field	Description
SPD map id	SPD map identifier.
SPD id	SPD identifier.
interface id	Interface identifier.
interface name	Interface name.

Field	Description
inbound ACL id	Inbound access control list (ACL) identifier.
local address	IP address of the local host.
object state	Object status.
bind state	Bind status.
enable state	Enable status.

The following is sample output from the **show platform software ipsec fp active spd-map identifier** command for ID 11:

```
Device# show platform software ipsec fp active spd-map identifier 11

======== SPD map id: 11
             SPD id: 1
       interface id: 11
     interface name: GigabitEthernet1/1/3
     inbound ACL id: 65535
      local address: 0
       object state: active
       tunnel state: new
         bind state: active
       enable state: active
             aom id: 101
```

The following table describes the significant fields shown in the display.

Table 25: show platform software ipsec fp active spd-map identifier Field Descriptions

Field	Description
SPD map id	SPD map identifier.
SPD id	SPD identifier.
interface id	Interface identifier.
interface name	Interface name.
inbound ACL id	Inbound access control list (ACL) identifier.
local address	IP address of the local host.
object state	Object status.
tunnel state	Tunnel status.
bind state	Bind status.
enable state	Enable status.

Field	Description
aom id	Asynchronous Object Manager (AOM) identifier.

Related Commands

Command	Description
show platform hardware qfp active feature ipsec	Display IPsec feature-specific information in IPsec Cisco QFP.
show platform software ipsec fp active flow	Displays information about active instances of IPsec flows in the ESP.

show platform software ipsec modexp-throttle0-stats

To display modexp throttle statistics for IPsec on a device, use the **show platform software ipsec modexp-throttle0-stats**command in privileged EXEC mode.

show platform software ipsec modexp-throttle0-stats

Syntax Description

This command has no keywords or arguments.

Command Default

Modexp throttle statistics for IPsec is not displayed.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

This command displays modexp throttle statistics information on devices running on Cisco IOS XE software.

Examples

The following is a sample output of the **show platform software ipsec modexp-throttle0-stats** command:

```
Device# show platform software ipsec modexp-throttle0-stats

========= MODEXP Message Statistic Information =======
Window size: 16  Queue max size: 1024
Transmit request total: 59 sent: 59 failed: 0
Transmit send total: 59  without delay: 59  with delay: 0
Queue request total: 0, sent: 0 timeout: 0
Transmit request error: 0
Callback count: 59 pending: 0
Queue max depth: 0 current depth: 0
Transmit request rate (packet per second): 0 average rate: 0 max rate: 0
Callback receive rate (packet per second): 0 average rate: 0 max rate: 0
```

show platform software urpf qfp active configuration

To confirm and display the Unicast Reverse Path Forwarding (uRPF) configuration on a forwarding processor of the Cisco ASR 1000 Series Aggregation Services Routers, use the **show platform software urpf qfp active configuration** command in the privileged EXEC mode.

show platform software urpf qfp active configuration *ip-version interface-name*

Syntax Description

ip-version	Version of the IP. Valid values are, IPv4 and IPv6.
interface-name	Name of the interface.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 2.0S	This command was introduced on the Cisco ASR 1000 Series Aggregation Services Routers.

Usage Guidelines

The uRPF configuration on an IPv4 or IPv6 interface is downloaded from the route processor to a forwarding processor and the configuration is reflected on the forwarding processor. Use the **show platform software urpf qfp active configuration** command to display the uRPF configuration on a forwarding processor.

Examples

The following is a sample output of the **show platform software urpf qfp active configuration** command:

```
Router# show platform software urpf qfp active configuration ipv6 gigabitethernet 0/0/0.777
Forwarding Manager uRPF IPv6 Configuration on Interface

Interface                Index        FLAGS
------------------------------------------------------------------------------
GigabitEthernet0/0/0.777  13

ACL: 1
ACL Binding AOM id: 152
```

The following table describes the significant fields shown in the display.

Table 26: show platform software urpf qfp active configuration

Field	Description
Interface	Interface number.
Index	Interface ID of the QFP.
ACL	Access Control List (ACL) name on uRPF.
ACL Binding	Asynchronous Object Manager (AOM) ID created to enable uRPF ACL support.

show policy-firewall config

To display the firewall configuration on the router, use the **show policy-firewall config** command in privileged EXEC mode.

show policy-firewall config {**all** | **class-map** [*class-map-nameprotocol-name*] | **parameter-map** [*parameter-map-name* | **default** | **global** | **protocol-info** | **regex** [*protocol-info-name*]] | **policy-map** [*policy-map-nameprotocol-name*] | **zone** [**self**] | **zone-pair**}

Command Syntax for Cisco IOS XE Release 3.14S and later

show policy-firewall config [**zone-pair** *zone-pair-name* | **platform** [**standby**]]

Syntax Description

all	Displays the entire firewall configuration on the router.
class-map *class-map-name*	Displays the class-maps configured on the router.
protocol-name	Displays the protocols configured for the class-map.
parameter-map	Displays the parameter-maps configured in the router.
parameter-map-name	Displays configuration information about a specific parameter map.
default	Displays configuration information about the default inspect parameter map.
global	Displays configuration information about the global inspect parameter map.
protocol-info	Displays configuration information about the protocol-specific inspect parameter map.
regex	Displays configuration information about the regex inspect parameter map.
protocol-info-name	Displays configuration information about a specific protocol.
policy-map *policy-map-name*	Displays the policy maps configured on the router.
protocol-name	Displays the protocols configured for the policy map.
zone	Displays configuration information about the zones configured on the router.
self	(Optional) Displays configuration information about the system-defined zone.
zone-pair	Displays configuration information about each zone-pair.
zone-pair-name	Security zone-pair name.
platform	Displays firewall platform information.

standby	Displays platform standby information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(1)T	This command was introduced.
Cisco IOS XE Release 3.14S	This command was modified. The *zone-pair-name* argument was added.

Usage Guidelines

Use this command to display a summary of the firewall configuration on the device.

Examples

The following is the sample output from the **show policy-firewall config all** command. The field descriptions are self-explanatory.

```
Device# show policy-firewall config all

Zone: self
  Description: System defined zone
Parameter-map Config:
 Global:
  alert on
  sessions maximum 2147483647
  waas disabled
  l2-transparent dhcp-passthrough disabled
  dropped-packets disabled
  log summary disabled
  max-incomplete low 2147483647
  max-incomplete high 2147483647
  one-minute low 2147483647
  one-minute high 2147483647
 Default:
  audit-trail off
  alert on
  max-incomplete low 2147483647
  max-incomplete high 2147483647
  one-minute low 2147483647
  one-minute high 2147483647
  udp idle-time 30
  icmp idle-time 10
  dns-timeout 5
  tcp idle-time 3600
  tcp finwait-time 5
  tcp synwait-time 30
  tcp max-incomplete host 4294967295 block-time 0
  sessions maximum 2147483647
```

The following is the sample output from the **show policy-firewall config all** command when a zone-pair is configured. The field descriptions are self-explanatory.

```
Device# show policy-firewall config all

Zone-pair              : z1-z2
Source Zone            : z1
  Member Interfaces:
    GigabitEthernet0/0/0
```

```
Destination Zone       : z2
  Member Interfaces:
    GigabitEthernet0/0/1
Service-policy inspect : pmap
  Class-map : cmap (match-all)
   Match protocol tcp
  Action : inspect
   Parameter-map : Default
  Class-map : class-default (match-any)
   Match any
  Action : drop log
   Parameter-map : Default
---------------------------
Parameter-map Configuration:
  Parameter-map type inspect: pmap
  -------------------------
   alert messages                 : on
   all application inspection     : on
   audit trailing                 : off
   logging dropped-packets        : off
   icmp session idle-time         : 10 sec, ageout-time: 10 sec
   dns session idle-time          : 5 sec
   tcp session half-open          : on, half-close: on, idle: on
   tcp session idle-time          : 3600 sec, ageout-time: 3600 sec
   tcp session FIN wait-time      : 1 sec, FIN ageout-time: 1 sec
   tcp session SYN wait-time      : 30 sec, SYN ageout-time: 30 sec
   tcp loose window scaling enforcement: off
   tcp max-half-open connections/host  : unlimited block-time: 0 min
   udp half-open session idle-time: 30000 ms, ageout-time: 30000 ms
   udp session idle-time          : 30 sec, ageout-time: 30 sec
   sessions, connections/min threshold (low) : unlimited
   sessions, connections/min threshold (high): unlimited
   sessions, connection rate threshold (low) : unlimited
   sessions, connection rate threshold (high): unlimited
   sessions, max-incomplete threshold (low)  : unlimited
   sessions, max-incomplete threshold (high) : unlimited
   sessions, maximum no. of inspect sessions : unlimited
   total number of packets per flow          : default
   zone mismatch drop option           : off
```

The following is the sample output from the **show policy-firewall config zone-pair** *zone-pair-name* command. The field descriptions are self-explanatory.

```
Device# show policy-firewall config zone-pair z1-z2

Zone-pair              : z1-z2
Source Zone            : z1
  Member Interfaces:
    GigabitEthernet0/0/0
Destination Zone       : z2
  Member Interfaces:
    GigabitEthernet0/0/1
Service-policy inspect : pmap
  Class-map : cmap (match-all)
   Match protocol tcp
  Action : inspect
   Parameter-map : Default
  Class-map : class-default (match-any)
   Match any
  Action : drop log
   Parameter-map : Default
```

The following example is a sample output from the **show policy-firewall config class-map** command:

```
Device# show policy-firewall config class-map c1

Class Map type inspect match-all c1 (id 1)
   Match access-group  101
   Match protocol http
```

The following example shows output related to user-defined parameter map:

```
Device# show policy-firewall config parameter-map params1

parameter-map type inspect params1
  audit-trail off
  alert on
  max-incomplete low 2147483647
  max-incomplete high 2147483647
  one-minute low 2147483647
  one-minute high 2147483647
  udp idle-time 30
  icmp idle-time 10
  dns-timeout 5
  tcp idle-time 3600
  tcp finwait-time 5
  tcp synwait-time 30
  tcp max-incomplete host 4294967295 block-time 0
  sessions maximum 2147483647
```

The following example shows output related default parameter map:

```
Device# show policy-firewall config parameter-map default

  audit-trail off
  alert on
  max-incomplete low 2147483647
  max-incomplete high 2147483647
  one-minute low 2147483647
  one-minute high 2147483647
  udp idle-time 30
  icmp idle-time 10
  dns-timeout 5
  tcp idle-time 3600
  tcp finwait-time 5
  tcp synwait-time 30
  tcp max-incomplete host 4294967295 block-time 0
  sessions maximum 2147483647
```

The following example shows output related to global parameter map:

```
Device# show policy-firewall config parameter-map global

  alert on
  sessions maximum 2147483647
  waas disabled
  l2-transparent dhcp-passthrough disabled
  log dropped-packets disabled
  log summary disabled
  max-incomplete low 2147483647
  max-incomplete high 2147483647
  one-minute low 2147483647
  one-minute high 2147483647
```

show policy-firewall mib

To display connection statistics of the firewall policy on the router, use the **show policy-firewall mib** command in privileged EXEC mode.

show policy-firewall mib connection-statistics {**global** | **policy** *policy-name* **zone-pair** *name* | **L4-Protocol** | **L7-Protocol**} {*name* | **all**}

Syntax Description

connection-statistics	Displays the statistics for one of the following selected options.
global	Displays the global connection statistics.
policy *policy-name*	Displays statistics for a specific firewall policy.
zone-pair *name*	Displays statistics for a zone pair in a specific firewall policy.
L4-Protocol *name*	Displays statistics for a specific Layer 4 protocol.
L7-Protocol *name*	Displays statistics for a specific Layer 7 protocol.
all	Displays statistics for all Layer 4 or Layer 7 protocols.

Command Default

Privileged EXEC (#)

Command History

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

Usage Guidelines

Use this command to display the global connection statistics and the statistics per protocol in Layer 4 or Layer 7 for each policy or zone pair. Use the **debug policy-firewall mib** command to toggle on or off the support for MIBs in zone-based policy firewalls.

Examples

The following is sample output from five versios of the **show policy-firewall mib**command:

```
Router# show policy-firewall mib connection-statistics global
-------------------------------------------------
Connections Attempted                           26
Connections Setup Aborted                       0
Connections Policy Declined                     0
Connections Resource Declined                   0
Connections Half Open                           0
Connections Active                              0
Connections Expired                             25
Connections Aborted                             0
Connections Embryonic                           0
Connections 1-min Setup Count                   0
Connections 5-min Setup Count                   0
Router# show policy-firewall mib connection-statistics L4-Protocol all
-------------------------------------------------
Protocol             udp
Connections Attempted                           1
Connections Setup Aborted                       0
```

```
Connections Policy Declined                       0
Connections Resource Declined                     0
Connections Half Open                             0
Connections Active                                0
Connections Aborted                               0
Connections Embryonic                             0
Connections 1-min Setup Count                     0
Connections 5-min Setup Count                     0
-------------------------------------------------
Protocol             tcp
Connections Attempted                            25
Connections Setup Aborted                         0
Connections Policy Declined                       0
Connections Resource Declined                     0
Connections Half Open                             0
Connections Active                                0
Connections Aborted                               0
Connections Embryonic                             0
Connections 1-min Setup Count                     0
Connections 5-min Setup Count                     0
Router# show policy-firewall mib connection-statistics L7-Protocol all
-------------------------------------------------
Protocol             http
Connections Attempted                            14
Connections Setup Aborted                         0
Connections Policy Declined                       0
Connections Resource Declined                     0
Connections Half Open                             0
Connections Active                                0
Connections Aborted                               0
Connections Embryonic                             0
Connections 1-min Setup Count                     0
Connections 5-min Setup Count                     0
-------------------------------------------------
Protocol             tacacs
Connections Attempted                            12
Connections Setup Aborted                         0
Connections Policy Declined                       0
Connections Resource Declined                     0
Connections Half Open                             0
Connections Active                                0
Connections Aborted                               0
Connections Embryonic                             0
Connections 1-min Setup Count                     0
Connections 5-min Setup Count                     0
Router# show policy-firewall mib connection-statistics policy inout-policy zone-pair inout
 L4-Protocol all
-------------------------------------------------
Policy            inout-policy
Zone-pair            inout
-------------------------------------------------
Protocol             udp
Connections Attempted                             1
Connections Setup Aborted                         0
Connections Policy Declined                       0
Connections Resource Declined                     0
Connections Half Open                             0
Connections Active                                0
Connections Aborted                               0
-------------------------------------------------
Protocol             tcp
Connections Attempted                            11
Connections Setup Aborted                         0
Connections Policy Declined                       0
```

```
Connections Resource Declined                    0
Connections Half Open                            0
Connections Active                               0
Connections Aborted                              0
Router# show policy-firewall mib connection-statistics policy inout-policy zone-pair inout
 L7-Protocol all
-------------------------------------------------
Policy            inout-policy
Zone-pair            inout
-------------------------------------------------
Protocol             tacacs
Connections Attempted                           12
Connections Setup Aborted                        0
Connections Policy Declined                      0
Connections Resource Declined                    0
Connections Half Open                            0
Connections Active                               0
Connections Aborted                              0
```

The table below describes the significant fields shown in the displays.

Table 27: show policy-firewall mib Field Descriptions

Field	Description
Connections Attempted	The total number of connection attempts sent to the firewall. This is a cumulative value.
Connections Policy Declined	The number of connection attempts that were declined due to a firewall security policy. This is a cumulative value.
Connections Resource Declined	The number of connection attempts that were declined due to firewall resource constraints. This is a cumulative value.
Connections Half Open	The number of connections that are being established with the firewall. This is a reflection of the current state of the system.
Connections Active	The number of connections that are currently active. This is a reflection of the current state of the system.
Connections Expired	The number of connections that were active and terminated. This is a cumulative value.
Connections Aborted	The number of connections that were abnormally terminated after a successful connection. This is a cumulative value.
Connections Embryonic	The number of embryonic application layer connections. This is a reflection of the current state of the system.
Connections 1-min Setup Count	The number of connections that the firewall attempts to establish per second averaged over the last 60 seconds. This is a reflection of the current state of the system.
Connections 5-min Setup Count	The number of connections that the firewall attempts to establish per second, averaged over the last 300 seconds. This is a reflection of the current state of the system.

Related Commands

Command	Description
debug policy-firewall mib	Toggles on or off the MIB support.

show policy-firewall session

To display the session details of a firewall policy, use the **show policy-firewall session** command in privileged EXEC mode.

show policy-firewall session [**msrpc** | **ha** | **zone-pair** [**ha**]]

Syntax Description

msrpc	(Optional) Displays the Microsoft Remote Procedure Call (MSRPC) sessions.
ha	(Optional) Displays high availability (HA) sessions pertaining to zone pairs.
zone-pair	(Optional) Displays the sessions pertaining to zone pairs.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
15.1(1)T	This command was introduced.
15.1(4)M	This command was modified. The **msrpc** keyword was added.
15.2(3)T	This command was modified. The **ha** keyword was added.

Usage Guidelines

Use the **show policy-firewall session** command to display session details. Session details can be either global, zone pair-specific, or MSRPC-specific. Global session details incorporate information about all sessions created by the firewall, and zone pair-specific details that pertain to each zone pair.

Examples

The following is sample output from the **show policy-firewall session** command:

```
Router# show policy-firewall session zone-pair

Zone-pair: zone-pair-source2destination
  Service-policy inspect : policy-test
    Class-map: class-test (match-any)
   Inspect
      Number of Established Sessions = 100
      Established Sessions
        Session 3F4DF38 (10.0.0.148:13686)=>(10.0.0.33:80) http:tcp SIS_OPEN
          Created 00:00:02, Last heard 00:00:01
          Bytes sent (initiator:responder) [257:10494]
        Session 43F0F58 (10.0.0.149:13687)=>(10.0.0.33:80) http:tcp SIS_OPEN
          Created 00:00:02, Last heard 00:00:01
          Bytes sent (initiator:responder) [274:10494]
        Session 3F3BD98 (10.0.0.98:13770)=>(10.0.0.33:80) http:tcp SIS_OPEN
          Created 00:00:02, Last heard 00:00:02
          Bytes sent (initiator:responder) [251:0]
        Session 3F2E498 (10.0.0.104:13774)=>(10.0.0.33:80) http:tcp SIS_OPEN
          Created 00:00:02, Last heard 00:00:01
          Bytes sent (initiator:responder) [277:10220]
        Session 3F3B008 (10.0.0.105:13775)=>(10.0.0.33:80) http:tcp SIS_OPEN
          Created 00:00:02, Last heard 00:00:01
```

```
          Bytes sent (initiator:responder) [264:10220]
        Session 3F31AD8 (10.0.0.108:13776)=>(10.0.0.33:80) http:tcp SIS_OPEN
          Created 00:00:02, Last heard 00:00:01
          Bytes sent (initiator:responder) [265:10220]
        Session 2F91030 (10.0.0.113:13780)=>(10.0.0.33:80) http:tcp SIS_OPEN
          Created 00:00:02, Last heard 00:00:01
          Bytes sent (initiator:responder) [257:10220]
        Session 3F35308 (10.0.0.229:13966)=>(10.0.0.33:80) http:tcp SIS_OPEN
          Created 00:00:00, Last heard 00:00:00
          Bytes sent (initiator:responder) [278:10494]
        Session 3F30B58 (10.0.0.231:13968)=>(10.0.0.33:80) http:tcp SIS_OPEN
          Created 00:00:00, Last heard 00:00:00
          Bytes sent (initiator:responder) [257:10494]
        Session 3F30588 (10.0.0.234:13969)=>(10.0.0.33:80) http:tcp SIS_OPEN
          Created 00:00:00, Last heard 00:00:00
          Bytes sent (initiator:responder) [259:10494]
      Number of Half-open Sessions = 8
      Half-open Sessions
        Session 3F32298 (10.0.0.99:13068)=>(10.0.0.33:80) http:tcp SIS_OPENING
          Created 00:00:06, Last heard 00:00:06
          Bytes sent (initiator:responder) [0:0]
        Session 2F8F510 (10.0.0.123:13428)=>(10.0.0.33:80) http:tcp SIS_OPENING
          Created 00:00:04, Last heard 00:00:04
          Bytes sent (initiator:responder) [0:0]
        Session 3F4E128 (10.0.0.125:13430)=>(10.0.0.33:80) http:tcp SIS_OPENING
          Created 00:00:04, Last heard 00:00:04
          Bytes sent (initiator:responder) [0:0]
        Session 3F4E318 (10.0.0.126:13431)=>(10.0.0.33:80) http:tcp SIS_OPENING
          Created 00:00:04, Last heard 00:00:04
          Bytes sent (initiator:responder) [0:0]
        Session 3F4E6F8 (10.0.0.127:13432)=>(10.0.0.33:80) http:tcp SIS_OPENING
          Created 00:00:04, Last heard 00:00:04
          Bytes sent (initiator:responder) [0:0]
        Session 43ECF68 (10.0.0.138:13561)=>(10.0.0.33:80) http:tcp SIS_OPENING
          Created 00:00:03, Last heard 00:00:03
          Bytes sent (initiator:responder) [0:0]
        Session 3F4D968 (10.0.0.130:13674)=>(10.0.0.33:80) http:tcp SIS_OPENING
          Created 00:00:02, Last heard 00:00:02
          Bytes sent (initiator:responder) [0:0]
        Session 3F4DB58 (10.0.0.147:13685)=>(10.0.0.33:80) http:tcp SIS_OPENING
          Created 00:00:02, Last heard 00:00:02
          Bytes sent (initiator:responder) [0:0]

      Number of Terminating Sessions = 3
      Terminating Sessions
        Session 2F9DD90 (10.0.0.203:13603)=>(10.0.0.33:80) http:tcp SIS_CLOSING
          Created 00:00:03, Last heard 00:00:02
          Bytes sent (initiator:responder) [268:10494]
        Session 3F3AA38 (10.0.0.209:13844)=>(10.0.0.33:80) http:tcp SIS_CLOSING
          Created 00:00:01, Last heard 00:00:01
          Bytes sent (initiator:responder) [251:2301]
        Session 43F20C8 (10.0.0.224:14070)=>(10.0.0.33:80) http:tcp SIS_CLOSING
          Created 00:00:00, Last heard 00:00:00
          Bytes sent (initiator:responder) [264:2301]
Zone-pair: zone-pair-destination2source
  Service-policy inspect : policy-test
    Class-map: class-test (match-any)
   Inspect
```

The table below describes the significant fields shown in the display.

Table 28: show policy-firewall session Field Descriptions

Field	Description
Number of Established Sessions	Number of established sessions. A session is established when traffic flows between the sessions.
Number of Half-open Sessions	Number of half-opened sessions. A TCP session that has not yet reached the established state is called a half-opened session.
Number of Terminating Sessions	A link or session between a pair of devices that get closed. The terminating side waits for a timeout and closes the connection between the devices. After the connection is closed, the local port of the terminating side will not be available for new connections.

The following is sample output from the **show policy-firewall session zone-pair ha** command:

```
Router# show policy-firewall session zone-pair ha

Session 3FAF888 (192.168.1.2:14401)=>(10.99.75.1:80) http:tcp SIS_OPEN/TCP_ESTAB
Created 00:00:00, Last heard 00:00:00
Bytes sent (initiator:responder) [252:2301]
HA State: ACTIVE, RG: rg_foo id 1
Session 3FAF888 (192.168.1.3:14401)=>(10.99.175.1:80) http:tcp SIS_OPEN/TCP_ESTAB
Created 00:00:00, Last heard 00:00:00
Bytes sent (initiator:responder) [252:2301]
HA State: STANDBY, RG: rg_fzooid 2
```

show policy-firewall stats

To display the statistics of the firewall activity on the router, use the **show policy-firewall stats** command in privileged EXEC mode.

show policy-firewall stats [**all** | **drop-counters** | **zone-pair** [**name**]]

Syntax Description

all	(Optional) Displays all firewall statistics on the router.
drop-counters	(Optional) Displays the number of packets dropped for each error code.
zone-pair *name*	(Optional) Displays statistics pertaining to zone-pair.

Command Default

Privileged EXEC (#)

Command History

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

Usage Guidelines

This command provides the statistics of all the firewall activity on the router. The command displays the box-wide statistics or the statistics for each zone pair. To get all statistics, use the **all** keyword. Use the **drop-counters** keyword to display the packets dropped and grouped by their error codes. The output displays only the error codes for which the drop counter is greater than zero. If the number of packets dropped is similar for multiple error codes, the error codes are sorted in alphabetical order.

Examples

The following is sample output from the **show policy-firewall stats** command. The field descriptions are self-explanatory.

```
Router# show policy-firewall stats drop-counters
REASON                PACKETS DROPPED
    Invalid Header length               39
    policy match failure               38
    Police rate limiting               37
    Session limiting              36
    Bidirectional traffic disabled              35
    SYN with data or with PSH/URG flags               34
    Segment matching no TCP connection              33
    Invalid Segment               32
    Invalid Seq#              31
    Invalid Ack (or no Ack)               30
    Invalid Flags               29
    Invalid Checksum               28
    SYN inside current window               27
    RST inside current window               26
    Out-Of-Order Segment              25
    Retransmitted Segment               24
    Retransmitted Segment with Invalid Flags              23
    Stray Segment              22
    Internal Error               21
    Invalid Window scale option               20
    Invalid TCP options              19
    No zone-pair between zones               18
    One of the interfaces not being configured for zoning 17
```

```
Policy not present on zone-pair              16
DROP action found in policy-map               15
```

show policy-firewall stats vrf

To display VPN routing and forwarding (VRF)-level policy firewall statistics, use the **show policy-firewall stats vrf** command in user EXEC or privileged EXEC mode.

show policy-firewall stats vrf [*vrf-pmap-name*]

Syntax Description

vrf-pmap-name	(Optional) VRF name.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.3S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was modified. The command output was modified to display UDP and Internet Control Message Protocol (ICMP) half-opened session counts.

Examples

The following is sample output from the **show policy-firewall stats vrf** command:

```
Router# show policy-firewall stats vrf vrf-default

  VRF: default, Parameter-Map: vrf-default
  Interface reference count: 1
       Total Session Count(estab + half-open): 0, Exceed: 0
       Total Session Aggressive Aging Period Off, Event Count: 0

                Half Open
       Protocol Session Cnt     Exceed
       -------- -----------     ------
       All      0               0
       UDP      0               0
       ICMP     0               0
       TCP      0               0

       TCP Syn Flood Half Open Count: 0, Exceed: 0
       Half Open Aggressive Aging Period Off, Event Count: 0
```

The table below describes the significant fields shown in the display.

Table 29: show policy-firewall stats vrf Field Descriptions

Field	Description
Total Session Count	Total session count.
Exceed	Number of sessions that exceeded the configured session count.
Total Session Aggressive Aging Period Off	Indicates whether aggressive aging is enabled (On) or disabled (Off).

Field	Description
Event Count	The number of times the event has been enabled in the past.
TCP Syn Flood Half Open Count	Number of half-open synchronization (SYN) packets that exceeded the configured SYN flood rate limit.
Half Open Aggressive Aging Period Off	Aggressive aging of half-opened sessions is not configured.

Related Commands

Command	Description
clear policy-firewall stats vrf	Clears the policy firewall statistics counter at a VRF level.

show policy-firewall stats vrf global

To display global VPN Routing and Forwarding (VRF) firewall policy statistics, use the **show policy-firewall stats vrf global**command in user EXEC or privileged EXEC mode.

show policy-firewall stats vrf global

Syntax Description

This command has no arguments or keywords.

Command Default

This command has no default settings.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.3S	This command was introduced.

Examples

The following is sample output from the **show policy-firewall stats vrf global** command:

```
Router# show policy-firewall stats vrf global

Global table statistics
       total_session_cnt: 0
       exceed_cnt:        0
       tcp_half_open_cnt: 0
       syn_exceed_cnt:    0
```

The table below describes the fields shown in the display.

Table 30: show policy-firewall stats vrf global Field Descriptions

Field	Description
total_session_cnt	Total session count.
exceed_cnt	Number of sessions that exceeded the configured session count.
tcp_half_open_cnt	TCP half-open sessions configured at a global VRF level. When the configured session limit is reached, the TCP synchronization (SYN) cookie verifies the source of the half-open TCP sessions before creating more sessions. A TCP half-open session is a session that has not reached the established state.
syn_exceed_cnt	Number of SYN packets that exceeded the configured SYN flood rate limit.

Related Commands

Command	Description
clear policy-firewall stats vrf global	Clears the global VRF policy firewall statistics.

show policy-firewall stats zone

To display policy firewall statistics at a zone level, use the **show policy-firewall stats zone** command in user EXEC or privileged EXEC mode.

show policy-firewall stats zone [*zone-name*]

Syntax Description

zone-name	(Optional) Zone name.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.3S	This command was introduced.
Cisco IOS XE Release 3.4S	This command was modified. The command output was modified to display threat detection statistics.

Examples

The following is sample output from the **show policy-firewall stats zone** command:

```
Router# show policy-firewall stats zone zone02

Zone: zone02
 Parameter-map: zonepmap
 TCP SYN packet conform limit: 0
 TCP SYN packet exceed limit: 0

 Threat Detection Statistics:
                      Average(eps)   Current(eps)  Threat   Total events
  10-min Basic FW Drop:    0              0           0          20
  10-min Inspection Drop:  0              0           0          70
  10-min Syn Attack:       0              0           0          0
```

The table below describes the significant fields shown in the display.

Table 31: show policy-firewall stats zone Field Descriptions

Field	Description
Zone	Name of the zone.
Parameter-map	Name of the configured zone-type parameter map.
TCP SYN packet conform limit	Number of TCP synchronization (SYN) packets that are within the configured limit.
TCP SYN packet exceed limit	Number of TCP SYN packets that exceeded the configured SYN packet rate limit.

Field	Description
Basic FW Drop	Threat detection rate for firewall drop events.
Inspection Drop	Threat detection rate for firewall inspection-based drop events.
Syn Attack	Threat detection rate for SYN cookie attack events.

Related Commands

Command	Description
clear policy-firewall stats zone	Clears the policy firewall statistics counter at a zone level.
tcp syn-flood limit	Configures a limit to the number of TCP half-open sessions before triggering SYN cookie processing for new SYN packets.
threat-detection	Configures basic threat detection.

show policy-firewall summary-log

To display summary logs, use the **show policy-firewall summary log** command in privileged EXEC mode.

show policy-firewall summary-log

Syntax Description

This command has no arguments or keywords.

Command Default

Summary logs are not displayed.

Command Modes

Privileged EXEC(#)

Command History

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

Usage Guidelines

Use this command to display the summary logs captured as follows:

- Configured flow
- Configured flow value
- Number of flows

Note When the number of flows for the log summary reaches the configured flow value, some flows are not summarized.

Examples

The following is sample output from the **show policy-firewall summary-log**. The field descriptions are self-explanatory.

```
Router# show policy-firewall summary-log
*Apr 1 12:38:29.103: %FW-6-LOG_SUMMARY: 10 http packets were dropped from
10.0.0.1:1024 => 20.0.0.1:23 (target: class)-(z1toz2:C1)
```

Related Commands

Command	Description
clear policy-firewall	Clears the information collected by the firewall.

show policy-map type inspect

To display a specified policy map, use the **show policy-map type inspect** command in privileged EXEC mode.

show policy-map type inspect [*policy-map-name*] [**class** *class-map-name*]

Syntax Description

policy-map-name	(Optional) Name of the policy map.
class *class-map-name*	(Optional) Name of the class map.

Command Default

If a policy-map name is not specified, all Level 7 policy maps are displayed.

Command Modes

Privileged EXEC

Command History

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

Examples

The following example displays the policy map for policy map p1:

```
Router # show policy-map type inspect p1

 Policy Map type inspect p1
  Class c1
   Inspect
```

The following example shows sample command output:

```
Router# show policy-map type inspect p_inside

Policy Map type inspect p_inside
 Description: Policy map with inspect action
 Class c_permit
  Pass
 Class c_test
 Class class-default
```

The table below describes the significant fields shown in the display.

Table 32: show policy-map type inspect Field Descriptions

Field	Description
p_inside	Name of the policy map.
Description	Description of the policy map.
Class	Name of the class map.
Pass	Allows packets to be sent to the router without being inspected.

show policy-map type inspect urlfilter

To display the details of a URL filtering policy map, use the **show policy-map type inspect urlfilter** command in privileged EXEC mode.

show policy-map type inspect urlfilter [*policy-map-name*]

Syntax Description

policy-map-name	(Optional) Name of the policy map for which details are displayed.

Command Default

The details of all URL filtering policy maps are displayed.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

Use the **show policy-map type inspect urlfilter**command to display the details of all URL filtering policy maps. To display the details of a particular URL filtering policy map, specify the name of the policy map.

The output of the **show ip urlfilter cache** command displays the pages cached by a device.

Examples

The following is sample output from the **show policy-map type inspect urlfilter** command for a policy map named websense-policy:

```
Router# show policy-map type inspect urlfilter websense-policy

policy-map type inspect urlfilter url-websense-policy
  parameter-map urlfpolicy websense websense-parameter-map
  class type urlfilter trusted-domain-lists
   allow
  class type urlfilter untrusted-domain-lists
   reset
  class type urlfilter block-url-keyword-lists
   reset
  class type urlfilter websense websense-map
   server-specified-action
```

show policy-map type inspect zone-pair

To display runtime inspect type policy map statistics and other information such as sessions existing on a specified zone pair, use the **show policy-map type inspect zone-pair** command in privileged EXEC mode.

show policy-map type inspect zone-pair[*zone-pair-name*[**sessions**]] [**sessions**]
ipv6 | {**destination** *destination-ip* [**source***source-ip*] | **source***source-ip*[**destination** *destination-ip*]}
destination *destination-ip*[**source***source-ip*]
source*source-ip*[**destination** *destination-ip*]

Syntax Description

zone-pair-name	(Optional) Zone pair for which the system displays the runtime inspect type policy-map statistics.
sessions	(Optional) Displays stateful packet inspection sessions created because a policy map is applied on the specified zone pair.
ipv6	(Optional) Displays information about the IPv6 session.
destination *destination-ip*	(Optional) Displays information about the destination IPv4 or IPv6 address of the session.
source *source-ip*	(Optional) Displays information about the source IPv4 or IPv6 address of the session.

Command Default

Information about policy maps for all zone pairs is displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.4(9)T	This command was modified. The output was enhanced to display the police action configuration.
12.4(15)XZ	This command was integrated into Cisco IOS Release 12.4(15)XZ and implemented on the following platforms: Cisco 881 and Cisco 888.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.
Cisco IOS XE Release 3.4S	This command was modified. The output was enhanced to display the General Packet Radio Service (GPRS) Tunneling Protocol (GTP) configuration.
Cisco IOS XE Release 3.6S	This command was modified. The output was enhanced to display both IPv4 and IPv6 firewall sessions.
Cisco IOS XE Release 3.9S	This command was modified. The **destination**, **ipv6**, and **source** keywords and the*destination-ip* and *source-ip* arguments were added.

Usage Guidelines

If you do not specify a zone-pair name, policy maps on all zone pairs are displayed.

When packets are matched to an access group (**match access-group**), a protocol (**match protocol**), or a class map (**match class-map**), a traffic rate is generated for these packets. In a zone-based firewall policy, only the first packet that creates a session matches the policy. Subsequent packets in this flow do not match the filters in the configured policy, but instead match the session directly. The statistics related to subsequent packets are shown as part of the "inspect" action and are displayed using the **show policy-map type inspect zone-pair sessions** command.

Command Limitations

The cumulative counters in the **show policy-map type inspect zone-pair** command output do not increment for **match** statements in a nested class map configuration in Cisco IOS Releases 12.4(15)T and 12.4(20)T. The problem with the counters exists regardless of whether the top-level class map uses the **match-any** or **match-all** keyword.

The following configuration example shows the match counter problem:

```
class-map type inspect match-any y
 match protocol tcp
 match protocol icmp
class-map type inspect match-all x
 match class y
```

The following sample output from the **show policy-map type inspect zone-pair** command displays cumulative counters for the above configuration (if the class map matches any class map):

```
Device# show policy-map type inspect zone-pair sessions

policy exists on zp
 Zone-pair: zp
  Service-policy inspect : fw
    Class-map: x (match-any)
      Match: class-map match-any y
        2 packets, 48 bytes   <======== Cumulative class map counters are incrementing.
        30 second rate 0 bps
        Match: protocol tcp
          0 packets, 0 bytes     <===== The match for the protocol is not incrementing.
          30 second rate 0 bps
        Match: protocol icmp
          0 packets, 0 bytes
          30 second rate 0 bps
   Inspect
      Number of Established Sessions = 1
      Established Sessions
        Session 53105C0 (10.1.1.2:19180)=>(10.2.1.2:23) tacacs:tcp SIS_OPEN
          Created 00:00:02, Last heard 00:00:02
          Bytes sent (initiator:responder) [30:69]
    Class-map: class-default (match-any)
      Match: any
      Drop
        0 packets, 0 bytes
```

Examples

The following sample output from the **show policy-map type inspect zone-pair** command shows information about zone pairs zp and trusted-untrusted:

```
Device# show policy-map type inspect zone-pair zp

 Zone-pair: zp
  Service-policy : p1
```

```
   Class-map: c1 (match-all)
    Match: protocol tcp
    Inspect
     Session creations since subsystem startup or last reset 0
     Current session counts (estab/half-open/terminating) [0:0:0]
     Maxever session counts (estab/half-open/terminating) [0:0:0]
     Last session created never
     Last statistic reset never
     Last session creation rate 0
     half-open session total 0
   Class-map: c2 (match-all)
    Match: protocol udp
    Pass
     0 packets, 0 bytes
   Class-map: class-default (match-any)
    Match: any
    Drop
     0 packets, 0 bytes
```

```
Device# show policy-map type inspect zone-pair trusted-untrusted

 Zone-pair: trusted-untrusted
  Service-policy inspect : firewall-policy
Class-map: class_4 (match-any)
      Match: protocol dbcontrol-agent
      Match: protocol ddns-v3
      Match: protocol dhcp-failover
      Match: protocol discard
      Match: protocol dns
      Match: protocol dnsix
      Match: protocol echo
      Match: protocol entrust-svc-handler
      Inspect
        Packet inspection statistics [process switch:fast switch]
        dns packets: [0:28949015]
        Session creations since subsystem startup or last reset 4
        Current session counts (estab/half-open/terminating) [0:0:0]
        Maxever session counts (estab/half-open/terminating) [1:0:0]
        Last session created 00:06:16
        Last statistic reset never
        Last session creation rate 0
        Last half-open session total 0
```

Note Only some protocols that undergo Layer 7 inspections have dedicated statistics; others are grouped into either TCP statistics or UDP statistics.

The following is sample output from the **show policy-map type inspect zone-pair** command for a GTP configuration:

```
Device# show policy-map type inspect zone-pair zp

Zone-pair: zp
  Service-policy inspect : L4-Policy

    Class-map: L4-Class (match-all)
      Match:  protocol gtpv0
      Inspect
        Session creations since subsystem startup or last reset 0
        Current session counts (estab/half-open/terminating) [0:0:0]
```

```
      Maxever session counts (estab/half-open/terminating) [0:0:0]
      Last session created never
      Last statistic reset never
      Last session creation rate 0
      Last half-open session total 0
    Service-policy inspect gtpv0 : L7-Policy

      Class-map: L7-Class (match-any)
        0 packets, 0 bytes
        30 second offered rate 0000 bps, drop rate 0000 bps
        Match:   match mcc 772 mnc 331

      Class-map: class-default (match-any)
        0 packets, 0 bytes
        30 second offered rate 0000 bps, drop rate 0000 bps
        Match:  any

  Class-map: class-default (match-any)
    Match:  any
    Drop (default action)
      0 packets, 0 bytes
```

The following is sample output from the **show policy-map type inspect zone-pair sessions** command:

```
Device# show policy-map type inspect zone-pair sessions

Zone-pair: hi2int
  Service-policy inspect : pg1
    Class-map: c1 (match-any)
      Match: protocol ftp
      Match: protocol telnet
      Match: protocol smtp
      Match: protocol http
      Match: protocol tacacs
      Match: protocol dns
      Match: protocol sql-net
      Match: protocol https
      Match: protocol tftp
      Match: protocol gopher
      Match: protocol finger
      Match: protocol kerberos
      Match: protocol pop3
      Match: protocol sunrpc
      Match: protocol msrpc
      Match: protocol icmp
      Inspect
        Established Sessions
         Session 10E28550 (10.1.1.1:50536)=>(172.16.1.1:111) sunrpc SIS_OPEN
          Created 00:09:44, Last heard 00:09:18
          Bytes sent (initiator:responder) [108:0]
         Session 10E28550 (10.1.1.1:39377)=>(172.16.1.1:150) sql-net SIS_CLOSED
          Created 00:03:01, Last heard 00:03:01
          Bytes sent (initiator:responder) [0:0]
         Session 10E2859C (10.1.1.1:39377)=>(172.16.1.1:110) pop3 SIS_CLOSED
          Created 00:02:59, Last heard 00:02:59
          Bytes sent (initiator:responder) [0:0]
         Session 10E285E8 (10.1.1.1:39377)=>(172.16.1.1:443) https SIS_CLOSED
          Created 00:03:33, Last heard 00:03:33
          Bytes sent (initiator:responder) [0:0]
    Class-map: class-default (match-any)
      Match: any
      Drop (default action)
        147127 packets, 8485742 bytes
```

Note In the preceding sample output, the information displayed below the Class-map field is the traffic rate (bits-per-second) of the traffic belonging to only the connection-initiating traffic. Unless the connection setup rate is significantly high and sustained for multiple intervals over which the rate is computed, no significant data is shown for the connection.

The following sample output from the **show policy-map type inspect zone-pair sessions** command displays IPv6 firewall sessions:

```
Device# show policy-map type inspect zone-pair sessions

Zone-pair: hi2int
  Service-policy inspect : pg1

    Class-map: c1 (match-any)
      Match: protocol ftp
      Match: protocol telnet
      Match: protocol icmp

      Inspect
        Established Sessions
         Session 10E28550 ([2001:DB8::1]:50536)=>( [2001:DB8:2::1]:111) sunrpc SIS_OPEN
          Created 00:09:44, Last heard 00:09:18
          Bytes sent (initiator:responder) [108:0]
        Session 10E28550 ([2001:DB8::1]:39377)=>([2001:DB8:2::1]:150)  sql-net IS_CLOSED
          Created 00:03:01, Last heard 00:03:01
          Bytes sent (initiator:responder) [0:0]

    Class-map: class-default (match-any)
      Match: any
      Drop (default action)
        147127 packets, 8485742 bytes
```

The following sample output from the **show policy-map type inspect zone-pair** command displays the police action configuration:

```
Device# show policy-map type inspect zone-pair

Zone-pair: zp
Service-policy inspect : test-udp
  Class-map: check-udp (match-all)
   Match: protocol udp
   Inspect
    Packet inspection statistics [process switch:fast switch]
    udp packets: [3:4454]
    Session creations since subsystem startup or last reset 92
    Current session counts (estab/half-open/terminating) [5:33:0]
    Maxever session counts (estab/half-open/terminating) [5:59:0]
    Last session created 00:00:06
    Last statistic reset never
    Last session creation rate 61
    Last half-open session total 33
   Class-map: class-default (match-any)
   Match: any
   Drop (default action)
   0 packets, 0 bytes
```

The table below describes the significant fields shown in the display:

Table 33: show parameter-map type inspect zone-pair Field Descriptions

Field	Description
Zone-pair	Name of the configured security zone pair.
Service-policy inspect	Name of the service policy that was inspected.
Class-map	Name of the configured class map and the configured match criterion.
Match	Protocols that were configured as match criteria.
Inspect	Session details such as packets received, current session count, and total session count.

Related Commands

Command	Description
match access-group	Configures the match criteria for a class map on the basis of the specified ACL.
match class-map	Uses a traffic class as a classification policy.
match protocol	Configures the match criterion for a class map on the basis of a specified protocol.
policy-map type inspect	Creates a Layer 3 and Layer 4 or a Layer 7 (protocol-specific) inspect-type policy map.

show policy-map type inspect zone-pair urlfilter

To display the details of a URL filtering policy map--URL filter state, URL filter statistics, and URL filter server details--use the **show policy-map type inspect zone-pair urlfilter** command in privileged EXEC mode.

show policy-map type inspect zone-pair [*zone-pair-name*] **urlfilter cache** [**detail**]

Syntax Description

zone-pair-name	(Optional) Zone pair for which the system will display the runtime inspect type policy-map statistics. Default: The requested information is shown for all zone pairs.
cache	Displays information about the URL filter cache.
detail	(Optional) Displays each entry in the cache. Because cache entries can be long, only the first few bytes are displayed.

Command Default

The URL filter information for all zone pairs is displayed. Details about the URL filtering cache are not displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(6)T	This command was introduced.
12.4(15)XZ	This command was implemented on the following platforms: Cisco 881 and Cisco 888. The **detail** keyword was added to show more information about the URL filtering cache.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T. The **detail** keyword was added to show more information about the URL filtering cache.

Examples

The following example shows sample output for a Websense URL filtering server:

```
Router# show policy-map type inspect zone-pair urlfilter cache

Zone-pair: zp
 Urlfilter
 Websense URL Filtering is ENABLED

 Websense Primary server: 10.3.3.3(port : 15868)
 recount: 0
 Current packet buffer count(in use): 0
 Current cache entry count: 0
 Maxever request count: 0
 Maxever packet buffer count: 0
 Maxever cache entry count: 0
 Total requests sent to URL Filter Server :0
 Total responses received from URL Filter Server :0
 Total requests allowed: 0
 Total requests blocked: 0
Drop (default action)
```

```
 packets, 0 bytes
 Service-policy inspect : test
  Class-map: test (match-all)
   Match: protocol http
  Class-map: class-default (match-any)
   Match: any
```

The following example shows sample output for a Trend Micro URL filtering server, including the cache details:

```
Router# show policy-map type inspect zone-pair urlfilter cache detail

policy exists on zp zp_in
 Zone-pair: zp_in
 Service-policy inspect : trend-global-policy
  Class-map: http-class (match-all)
   Match: protocol http
   Match: access-group 101
 Inspect
   Packet inspection statistics [process switch:fast switch]
   tcp packets: [3353:0]
   Session creations since subsystem startup or last reset 21
   Current session counts (estab/half-open/terminating) [3:0:0]
   Maxever session counts (estab/half-open/terminating) [4:1:1]
   Last session created 00:00:22
   Last statistic reset never
   Last session creation rate 7
   Maxever session creation rate 14
   Last half-open session total 0
   Maximum number of bytes in cache: 131072000
   Time to live for eache cache entry (in hrs): 1
   Total number of bytes used by cache: 442
   Number of bytes used by domain type cache: 442
   Number of bytes used by directory type cache: 0
   ------------------------------------------------------------
   URL                                  Age   Access #/  Cat::Rep
   (Directory cache end with /)   (day:h:m:s)    Idle Time
   ------------------------------------------------------------
   example.com             0:00:00:23      28   58::100

   example1.com            0:00:00:25       1   56::100

   example.example2.com    0:00:00:34       1   56::100

  Class-map: class-default (match-any)
   Match: any
   Drop
     0 packets, 0 bytes

policy exists on zp zp_out
 Zone-pair: zp_out

 Service-policy inspect : icmp_permit

  Class-map: icmp_permit (match-all)
   Match: access-group 110
   Pass
    0 packets, 0 bytes

  Class-map: class-default (match-any)
   Match: any
   Drop
    0 packets, 0 bytes
```

show port-security

To display information about the port-security setting in EXEC command mode, use the **show port-security** command.

show port-security [**interface** *interface interface-number*]
show port-security [**interface** *interface interface-number*] {**address** | **vlan**}

Syntax Description

interface *interface*	(Optional) Specifies the interface type; possible valid values are **ethernet**, **fastethernet**, **gigabitethernet**, and **longreachethernet**.
interface-number	Interface number. Valid values are 1 to 6.
address	Displays all the secure MAC addresses that are configured on all the switch interfaces or on a specified interface with aging information for each address.
vlan	Virtual LAN.

Command Default

This command has no default settings.

Command Modes

EXEC

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(18)SXE	The **address** keyword was added to display the maximum number of MAC addresses configured per VLAN on a trunk port on the Supervisor Engine 720 only.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.

Usage Guidelines

The **vlan** keyword is supported on trunk ports only and displays per-Vlan maximums set on a trunk port.

The *interface-number* argument designates the module and port number. Valid values for *interface-number* depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48.

Examples

This example shows the output from the **show port-security** command when you do not enter any options:

```
Router# show port-security
Secure Port      MaxSecureAddr  CurrentAddr  SecurityViolation  Security
Action
                    (Count)        (Count)      (Count)
-------------------------------------------------------------------------------
```

```
     Fa5/1           11            11            0            Shutdown
     Fa5/5           15            5             0            Restrict
     Fa5/11          5             4             0            Protect
------------------------------------------------------------------------------

Total Addresses in System: 21
Max Addresses limit in System: 128
Router#
```

This example shows how to display port-security information for a specified interface:

```
Router# show port-security interface fastethernet 5/1
Port Security: Enabled
Port status: SecureUp
Violation mode: Shutdown
Maximum MAC Addresses: 11
Total MAC Addresses: 11
Configured MAC Addresses: 3
Aging time: 20 mins
Aging type: Inactivity
SecureStatic address aging: Enabled
Security Violation count: 0
Router#
```

This example show how to display all the secure MAC addresses that are configured on all the switch interfaces or on a specified interface with aging information for each address:

```
Router# show port-security address
Default maximum: 10
VLAN Maximum Current
1    5       3
2    4       4
3    6       4
Router#
```

Related Commands

Command	Description
clear port-security	Deletes configured secure MAC addresses and sticky MAC addresses from the MAC address table.

show ppp queues

To monitor the number of requests processed by each authentication, authorization, and accounting (AAA) background process, use the **show ppp queues**command inprivilegedEXEC mode.

show ppp queues

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3(2)AA	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **show ppp queues** command to display the number of requests handled by each AAA background process, the average amount of time it takes to complete each request, and the requests still pending in the work queue. This information can help you balance the data load between the network access server and the AAA server.

This command displays information about the background processes configured by the **aaa processes** global configuration command. Each line in the display contains information about one of the background processes. If there are AAA requests in the queue when you enter this command, the requests will be printed as well as the background process data.

Examples

The following example shows output from the **show ppp queues** command:

```
Router# show ppp queues
Proc #0   pid=73  authens=59   avg. rtt=118s. authors=160  avg. rtt=94s.
Proc #1   pid=74  authens=52   avg. rtt=119s. authors=127  avg. rtt=115s.
Proc #2   pid=75  authens=69   avg. rtt=130s. authors=80   avg. rtt=122s.
Proc #3   pid=76  authens=44   avg. rtt=114s. authors=55   avg. rtt=106s.
Proc #4   pid=77  authens=70   avg. rtt=141s. authors=76   avg. rtt=118s.
Proc #5   pid=78  authens=64   avg. rtt=131s. authors=97   avg. rtt=113s.
Proc #6   pid=79  authens=56   avg. rtt=121s. authors=57   avg. rtt=117s.
Proc #7   pid=80  authens=43   avg. rtt=126s. authors=54   avg. rtt=105s.
Proc #8   pid=81  authens=139  avg. rtt=141s. authors=120  avg. rtt=122s.
Proc #9   pid=82  authens=63   avg. rtt=128s. authors=199  avg. rtt=80s.
queue len=0 max len=499
```

The table below describes the fields shown in the example.

Table 34: show ppp queues Field Descriptions

Field	Description
Proc #	Identifies the background process allocated by the **aaa processes** command to handle AAA requests for PPP. All of the data in this row relates to this process.
pid=	Identification number of the background process.
authens=	Number of authentication requests the process has performed.
avg. rtt=	Average delay (in seconds) until the authentication request was completed.
authors=	Number of authorization requests the process has performed.
avg. rtt=	Average delay (in seconds) until the authorization request was completed.
queue len=	Current queue length.
max len=	Maximum length the queue ever reached.

Related Commands

Command	Description
aaa processes	Allocates a specific number of background processes to be used to process AAA authentication and authorization requests for PPP.

show pppoe session

To display information about currently active PPP over Ethernet (PPPoE) sessions, use the **show pppoe session** in privileged EXEC mode.

show pppoe session [**all** | **interface** *type number* | **packets** [**all** | **interface** *type number* | **ipv6**]]

Syntax Description

all	(Optional) Displays detailed information about the PPPoE session.
interface *type number*	(Optional) Displays information about the interface on which the PPPoE session is active.
packets	(Optional) Displays packet statistics for the PPPoE session.
ipv6	(Optional) Displays PPPoE session packet statistics for IPv6 traffic

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(4)YG	This command was introduced on the Cisco SOHO 76, 77, and 77H routers.
12.3(4)T	This command was integrated into Cisco IOS Release 12.3(4)T and was enhanced to display information about relayed PPPoE Active Discovery (PAD) messages.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB and support was added for the Cisco 7200, 7301, 7600, and 10000 series platforms.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2 and the output following the use of the **all** keyword was modified to indicate if a session is Interworking Functionality (IWF)-specific or if the **tag ppp-max-payload** tag is in the discovery frame and accepted.
12.4(15)XF	The output was modified to display Virtual Multipoint Interface (VMI) and PPPoE process-level values.
12.4(15)T	This command was integrated into Cisco IOS Release 12.4(15)T to support VMIs in Mobile Ad Hoc Router-to-Radio Networks (MANETs).
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
Cisco IOS XE Release 2.5	This command was implemented on Cisco ASR 1000 series routers.
Cisco IOS XE Release 3.5S	This command was modified. The **ipv6** keyword was added.

Single Session: Example

The following is sample output from the show pppoe session command:

```
Router# show pppoe session
     1 session  in FORWARDED (FWDED) State
     1 session  total
```

Uniq ID	PPPoE SID	RemMAC	Port	VT	VA	State	LocMAC	VA-st
26	19	0001.96da.a2c0	Et0/0.1	5	N/A	RELFWD	000c.8670.1006	VLAN:3434

PPPoE Session with IWF and ppp-max-payload Tag Example

The following is sample output from the **show pppoe session** command when there is an IWF session and the ppp-max-payload tag is accepted in the discovery frame (available in Cisco IOS Release 12.2(31)SB2):

```
Router# show pppoe session

     1 session  in LOCALLY_TERMINATED (PTA) State
     1 session  total.  1 session of it is IWF type
```

Uniq ID	PPPoE SID	RemMAC	Port	VT	VA	State	LocMAC	VA-st	Type
26	21	0001.c9f2.a81e	Et1/2	1	Vi2.1	PTA	0006.52a4.901e	UP	IWF

The table below describes the significant fields shown in the displays.

Table 35: show pppoe session Field Descriptions

Field	Description
Uniq ID	Unique identifier for the PPPoE session.
PPPoE SID	PPPoE session identifier.
RemMAC	Remote MAC address.
Port	Port type and number.
VT	Virtual-template interface.
VA	Virtual access interface.

Field	Description
State	Displays the state of the session, which will be one of the following: • FORWARDED • FORWARDING • LCP_NEGOTIATION • LOCALLY_TERMINATED • PPP_START • PTA • RELFWD (a PPPoE session was forwarded for which the Active discovery messages were relayed) • SHUTTING_DOWN • VACCESS_REQUESTED
LocMAC	Local MAC address.

show pppoe session all: Example

The following example shows information per session for the **show pppoe session all** command.

```
Router# show pppoe session all

Total PPPoE sessions 1
session id: 21
local MAC address: 0006.52a4.901e, remote MAC address: 0001.c9f2.a81e
virtual access interface: Vi2.1, outgoing interface: Et1/2, IWF
PPP-Max-Payload tag: 1500
    15942 packets sent, 15924 received
    224561 bytes sent, 222948 received
```

PPPoE Session Including Credit Flow Statistics: Example

The following example shows the output from the **show pppoe session all** command. This version of the display includes PPPoE credit flow statistics for the session.

```
Router# show pppoe session all
Total PPPoE sessions 1
session id: 1
local MAC address: aabb.cc00.0100, remote MAC address: aabb.cc00.0200
virtual access interface: Vi2, outgoing interface: Et0/0
17 packets sent, 24 received
1459 bytes sent, 2561 received
PPPoE Flow Control Stats
Local Credits: 65504 Peer Credits: 65478
Credit Grant Threshold: 28000 Max Credits per grant: 65534
PADG Seq Num: 7 PADG Timer index: 0
PADG last rcvd Seq Num: 7
PADG last nonzero Seq Num: 0
```

```
PADG last nonzero rcvd amount: 0
PADG Timers: [0]-1000 [1]-2000 [2]-3000 [3]-4000
PADG xmit: 7 rcvd: 7
PADC xmit: 7 rcvd: 7
PADQ xmit: 0 rcvd: 0
```

show pppoe session packet ipv6: Example

The following is sample output form the **show pppoe session packet ipv6** command. The output field descriptions are self-explanatory.

```
Device# show pppoe session packet ipv6

SID     Pkts -In         Pkts-Out        Bytes-In        Bytes-Out
1       2800            9               2721600         770
```

Related Commands

Command	Description
clear pppoe relay context	Clears PPPoE relay contexts created for relaying PAD messages.
show pppoe relay context all	Displays PPPoE relay contexts created for relaying PAD messages.

show private-hosts access-lists

To display the access lists for your Private Hosts configuration, use the **show private-hosts access-lists** command in privileged EXEC mode.

show private-hosts access-lists

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

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

Examples

The following example shows how to display the Private Hosts access lists for your configuration:

```
Router# s
how private-hosts access-lists

Promiscuous ACLs
Action Permit   Sequence # 010
    Source:0000.1111.4001 0000.0000.0000 Destination:0000.0000.0000 ffff.ffff.ffff
Action Deny     Sequence # 020
    Source:0000.0000.0000 ffff.ffff.ffff Destination:0000.0000.0000 ffff.ffff.ffff
Isolated ACLs
Action Deny     Sequence # 010
    Source:0000.1111.4001 0000.0000.0000 Destination:0000.0000.0000 ffff.ffff.ffff
Action Permit   Sequence # 020
    Source:0000.0000.0000 ffff.ffff.ffff Destination:0000.1111.4001 0000.0000.0000 Action
Redirect Sequence # 030 Redirect index 6
    Source:0000.0000.0000 ffff.ffff.ffff Destination:ffff.ffff.ffff 0000.0000.0000
Action Permit   Sequence # 040
    Source:0000.0000.0000 ffff.ffff.ffff Destination:0100.5e00.0000 0000.007f.ffff
    Source:0000.0000.0000 ffff.ffff.ffff Destination:3333.0000.0000 0000.ffff.ffff
Action Deny     Sequence # 050
    Source:0000.0000.0000 ffff.ffff.ffff Destination:0000.0000.0000 ffff.ffff.ffff
Mixed ACLs
Action Permit   Sequence # 010
    Source:0000.1111.4001 0000.0000.0000 Destination:ffff.ffff.ffff 0000.0000.0000 Action
Redirect Sequence # 020 Redirect index 6
    Source:0000.0000.0000 ffff.ffff.ffff Destination:ffff.ffff.ffff 0000.0000.0000
Action Permit   Sequence # 030
    Source:0000.1111.4001 0000.0000.0000 Destination:0000.0000.0000 ffff.ffff.ffff
Action Permit   Sequence # 040
    Source:0000.0000.0000 ffff.ffff.ffff Destination:0000.1111.4001 0000.0000.0000
Action Deny     Sequence # 050
    Source:0000.0000.0000 ffff.ffff.ffff Destination:0000.0000.0000 ffff.ffff.ffff
```

Related Commands

Command	Description
show fm private-hosts	Displays information about the Private Hosts feature manager.
show private-hosts configuration	Displays Private Hosts configuration information for the networking device.
show **private-hosts interface configuration**	Displays Private Hosts configuration information for individual interfaces.

show private-hosts configuration

To display information about the Private Hosts configuration on the router, use the **show private-hosts configuration** command in privileged EXEC mode.

show private-hosts configuration

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

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

Examples

The following example shows sample command output:

```
Router# show private-hosts configuration

Private hosts enabled. BR INDEX 6 State 0000000F
Privated hosts vlans lists:
200
Privated promiscuous MAC configuration:
A '*' mark behind the mac list indicates non-existent mac-list
-------------------------------------------------------------------------------
MAC-list                       VLAN list
-------------------------------------------------------------------------------
bras-list                     *** Uses the isolated vlans (if any) ***
```

The following example shows sample command output:

```
Router# show private-hosts configuration
Private-hosts enabled
Isolated vlan-list 10,12,15,200-300
Promiscuous MAC configuration:
-------------------------------------------------------------------------------
MAC-List               VLAN List
-------------------------------------------------------------------------------
Bras_list              10,12,15,200-300
Mcast_server_list      10,12,15
Router#
```

Related Commands

Command	Description
private-hosts	Enables or configures the Private Hosts feature.
private-hosts mode	Sets the switchport mode.
show fm **private-hosts interface configuration**	Displays the FM-related Private Hosts information.

Command	Description
show **private-hosts interface configuration**	Displays Private Hosts configuration information for individual interfaces.

show private-hosts interface configuration

To display information about the Private Hosts configuration on individual interfaces (ports), use the **show private-hosts interface configuration** command in privileged EXEC mode.

show private-hosts interface configuration

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
12.2(33)SXH	This command was integrated in Cisco IOS Release 12.2(33)SXH.

Examples

The following example shows sample command output:

```
Router# show private-hosts interface configuration

Private hosts enabled
Debug Events: 0 Acl: 0 API: 0
Promiscuous interface list
--------------------------
GigabitEthernet1/1 promiscuous connected Facing BRAS Jupiter
Isolated interface list
-------------------------
FastEthernet3/1-14 isolated connected Facing DSLAM AB-125-1
Mixed mode interface list
-------------------------
GigabitEthernet1/4-5 mixed connected Facing Server Mars
Router#
```

Related Commands

Command	Description
private-hosts	Enables or configures the Private Hosts feature.
private-hosts mode	Sets the switchport mode.
show fm **private-hosts**	Displays the FM-related Private Hosts information.
show private-hosts configuration	Displays Private Hosts configuration information for the router.

show private-hosts mac-list

To display the contents of the MAC address lists defined for Private Hosts, use the **show private-hosts mac-list** command in privileged EXEC mode.

show private-hosts mac-list [*list-name*]

Syntax Description

list-name	(Optional) The name of the MAC address list whose contents you want to display.

Command Modes

Privileged EXEC (#)

Command History

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

Examples

The following example shows sample command output:

```
Router# show private-hosts mac-list

MAC-List: bras-list
-----------------------------------------------------------------
MAC address    Description
-----------------------------------------------------------------
0000.1111.1111 BRAS-SERVER
```

Related Commands

Command	Description
private-hosts mac-list	Creates a MAC address list that identifies a content server that is being used to provide broadband services to isolated hosts.

show privilege

To display your current level of privilege, use the **show privilege** command in EXEC mode.

show privilege

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
10.3	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Examples

The following example shows sample output from the **show privilege** command. The current privilege level is 15.

```
Router# show privilege
Current privilege level is 15
```

Related Commands

Command	Description
enable password	Sets a local password to control access to various privilege levels.
enable secret	Specifies an additional layer of security over the **enable password** command.

show radius local-server statistics

To display the statistics for the local authentication server, use the **show radius local-server statistics**command in privileged EXEC mode.

show radius local-server statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

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

Examples

The following output displays statistics for the local authentication server.

```
Router# show radius local-server statistics
Successes              : 11262       Unknown usernames      : 0
Client blocks          : 0           Invalid passwords      : 8
Unknown NAS            : 0           Invalid packet from NAS: 0
NAS : 10.0.0.1
Successes              : 11262       Unknown usernames      : 0
Client blocks          : 0           Invalid passwords      : 8
Corrupted packet       : 0           Unknown RADIUS message : 0
No username attribute  : 0           Missing auth attribute : 0
Shared key mismatch    : 0           Invalid state attribute: 0
Unknown EAP message    : 0           Unknown EAP auth type  : 0
PAC refresh            : 0           Invalid PAC received   : 0
Maximum number of configurable users: 50, current user count: 11
Username                   Successes  Failures  Blocks
vayu-ap-1                       2235         0       0
vayu-ap-2                       2235         0       0
vayu-ap-3                       2246         0       0
vayu-ap-4                       2247         0       0
vayu-ap-5                       2247         0       0
vayu-11                            3         0       0
vayu-12                            5         0       0
vayu-13                            5         0       0
vayu-14                           30         0       0
vayu-15                            3         0       0
scm-test                           1         8       0
```

The first section of statistics lists cumulative statistics from the local authenticator.

The second section lists statistics for each access point (NAS) authorized to use the local authenticator. The EAP-FAST statistics in this section include the following:

- Auto provision success--the number of PACs generated automatically

- Auto provision failure--the number of PACs not generated because of an invalid handshake packet or invalid username or password
- PAC refresh--the number of PACs renewed by clients
- Invalid PAC received--the number of PACs received that were expired, that the authenticator could not decrypt, or that were assigned to a client username not in the authenticator's database

The third section lists stats for individual users. If a user is blocked and the lockout time is set to infinite, blocked appears at the end of the stat line for that user. If the lockout time is not infinite, Unblocked in x seconds appears at the end of the stat line for that user.

Use the **clear radius local-server statistics** command in privileged EXEC mode to reset local authenticator statistics to zero.

Related Commands

Command	Description
block count	Configures the parameters for locking out members of a group to help protect against unauthorized attacks.
clear radius local-server	Clears the statistics display or unblocks a user.
debug radius local-server	Displays the debug information for the local server.
group	Enters user group configuration mode and configures shared setting for a user group.
nas	Adds an access point or router to the list of devices that use the local authentication server.
radius-server host	Specifies the remote RADIUS server host.
radius-server local	Enables the access point or router to be a local authentication server and enters into configuration mode for the authenticator.
reauthentication time	Specifies the time (in seconds) after which access points or wireless-aware routers must reauthenticate the members of a group.
ssid	Specifies up to 20 SSIDs to be used by a user group.
user	Authorizes a user to authenticate using the local authentication server.
vlan	Specifies a VLAN to be used by members of a user group.

show radius server-group

To display properties for the RADIUS server group, use the **show radius server-group** command in user EXEC or privileged EXEC mode.

show radius server-group
{**server-group-name** | **all***123*}

Syntax Description

server-group-name	Displays properties for the server group named. The character string used to name the group of servers must be defined using the **aaa group server radius**command.
all	Displays properties for all the server group.
server	Displays properties for a specific server or servers in the group.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.2(2)T	This command was introduced.
12.2(33)SRA	The *server* argument was introduced.

Usage Guidelines

Use the **show radius server-group** command to display the server groups that you defined by using the **aaa group server radius** command.

Examples

The following **show radius server-group** command output displays properties for the server group "rad_sg":

```
Router# show radius server-group rad_sg
server group rad-sg
 Sharecount = 1  sg_unconfigured = FALSE
 Type = standard  Memlocks = 1
```

The following **show radius server-group** command output displays the properties for two server groups, 123 and 456, respectively. Using the **aaa group server radius** command, the configuration of each server group is also shown.

```
Router(config)# aaa new-model
!
!
Router(config)# aaa group server radius 123
 server 10.9.8.1 auth-port 1645 acct-port 1646
!
Router(config)# aaa group server radius 456
 server 10.9.8.2 auth-port 1645 acct-port 1646
Router(config)# exit
Router# show radius server-group all
Server group 123
```

```
 Sharecount = 1  sg_unconfigured = FALSE
 Type = standard
Server group 456
 Sharecount = 1  sg_unconfigured = FALSE
 Type = standard
Router# show radius server-group 123
Server group 123
 Sharecount = 1  sg_unconfigured = FALSE
 Type = standard
```

The table below describes the significant fields shown in the display.

Table 36: show radius server-group command Field Descriptions

Field	Description
Server group	Name of the server group.
Sharecount	Number of method lists that are sharing this server group. For example, if one method list uses a particular server group, the sharecount would be 1. If two method lists use the same server group, the sharecount would be 2.
sg_unconfigured	Server group has been unconfigured.
Type	The type can be either "standard" or "nonstandard". The type indicates whether the servers in the group accept nonstandard attributes. If all servers within the group are configured with the nonstandard option, the type will be shown as "nonstandard".
Memlocks	An internal reference count for the server-group structure that is in memory. The number represents how many internal data structure packets or transactions are holding references to this server group. Memlocks is used internally for memory management purposes.

Related Commands

Command	Description
aaa group server radius	Groups different RADIUS server hosts into distinct lists and distinct methods.
show aaa servers	Displays information about the number of packets sent to and received from AAA servers.
show radius statistics	Displays the RADIUS statistics for accounting and authentication packets.

show radius statistics

To display the RADIUS statistics for accounting and authentication packets, use the **show radius statistics** command in user EXEC or privileged EXEC mode.

show radius statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.1(3)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(1)S	This command was integrated into Cisco IOS Release 15.1(1)S. Support for the CISCO-RADIUS-EXT-MIB was added.
15.1(4)M	This command was modified. Support for the CISCO-RADIUS-EXT-MIB was added.

Usage Guidelines

The values in queue related fields (Maximum inQ length:, Maximum waitQ length:, and Maximum doneQ length:) of the **show radius statistics** command is shown as NA in vEWLC, as these queue related information is applicable only in IOS.

Examples

The following is sample output from the **show radius statistics** command:

```
Router# show radius statistics
                                Auth.      Acct.       Both
Maximum inQ length:              NA         NA         1
Maximum waitQ length:            NA         NA         2
Maximum doneQ length:            NA         NA         1
Total responses seen:            33         67         100
Packets with responses:          33         67         100
Packets without responses:       0          0          0
Access Rejects           :       0
Average response delay(ms) :     1331       124        523
Maximum response delay(ms):      5720       4800       5720
Number of Radius timeouts:       8          2          10
Duplicate ID detects:            0          0           0
Buffer Allocation Failures:      0          0           0
Maximum Buffer Size (bytes):     156        327         327
Malformed Responses        :     0          0           0
Bad Authenticators         :     0          0           0
Source Port Range: (2 ports only)
1645 - 1646
Last used Source Port/Identifier:
```

```
1645/33
1646/69
```

The table below describes significant fields shown in the display.

Table 37: show radius statistics Field Descriptions

Field	Description
Auth.	Statistics for authentication packets.
Acct.	Statistics for accounting packets.
Both	Combined statistics for authentication and accounting packets.
Maximum inQ length	Maximum number of entries allowed in the queue that holds the RADIUS messages not yet sent.
Maximum waitQ length	Maximum number of entries allowed in the queue that holds the RADIUS messages that have been sent and are waiting for a response.
Maximum doneQ length	Maximum number of entries allowed in the queue that holds the messages that have received a response and will be forwarded to the code that is waiting for the messages.
Total responses seen	Number of RADIUS responses seen from the server. In addition to the expected packets, the number includes repeated packets and packets that do not have a matching message in the waitQ.
Packets with responses	Number of packets that received a response from the RADIUS server.
Packets without responses	Number of packets that never received a response from any RADIUS server.
Access Rejects	Number of times access requests have been rejected by a RADIUS server.
Average response delay	Average time, in milliseconds (ms), from when the packet was first transmitted to when it received a response. If the response timed out and the packet was sent again, this value includes the timeout. If the packet never received a response, this value is not included in the average.
Maximum response delay	Maximum delay, in ms, observed while gathering the average response delay information.
Number of RADIUS timeouts	Number of times a server did not respond and the RADIUS server re-sent the packet.
Duplicate ID detects	RADIUS has a maximum of 255 unique IDs. In some instances, there can be more than 255 outstanding packets. When a packet is received, the doneQ is searched from the oldest entry to the youngest. If the IDs are the same, further techniques are used to see if this response matches this entry. If this response does not match, the duplicate ID detect counter is increased.
Buffer Allocation Failures	Number of times the buffer failed to get allocated.

Field	Description
Maximum Buffer Size (bytes)	Displays the maximum size of the buffer.
Malformed Responses	Number of corrupted responses, mostly due to bad authenticators.
Bad Authenticators	Number of authentication failures due to shared secret mismatches.
Source Port Range: (2 ports only)	Displays the port numbers.
Last used Source Port/Identifier	Ports that were last used by the RADIUS server for authentication.

The fields in the output are mapped to Simple Network Management Protocol (SNMP) objects in the CISCO-RADIUS-EXT-MIB and are used in SNMP reporting. The first line of the report is mapped to the CISCO-RADIUS-EXT-MIB as follows:

- Maximum inQ length maps to creClientTotalMaxInQLength
- Maximum waitQ length maps to creClientTotalMaxWaitQLength
- Maximum doneQ length maps to creClientTotalMaxDoneQLength

The field "Both" in the output can be derived from the authentication and accounting MIB objects. The calculation formula for each field, as displayed in the output, is given in the table below.

Table 38: Calculation Formula for the Both field in show radius statistics Command Output

show radius statistics Command Output Data	Calculation Formula for the Both Field
Maximum inQ length	creClientTotalMaxInQLength
Maximum waitQ length	creClientTotalWaitQLength
Maximum doneQ length	creClientDoneQLength
Total responses seen	creAuthClientTotalResponses + creAcctClientTotalResponses
Packets with responses	creAuthClientTotalPacketsWithResponses + creAcctClientTotalPacketsWithResponses
Packets without responses	creAuthClientTotalPacketsWithoutResponses + creAcctClientTotalPacketsWithoutResponses
Access Rejects	creClientTotalAccessRejects
Average response delay	creClientAverageResponseDelay
Maximum response delay	MAX(creAuthClientMaxResponseDelay, creAcctClientMaxResponseDelay)
Number of RADIUS timeouts	creAuthClientTimeouts + creAcctClientTimeouts
Duplicate ID detects	creAuthClientDupIDs + creAcctClientDupIDs

show radius statistics Command Output Data	Calculation Formula for the Both Field
Buffer Allocation Failures	creAuthClientBufferAllocFailures + creAcctClientBufferAllocFailures
Maximum Buffer Size (bytes)	MAX(creAuthClientMaxBufferSize, creAcctClientMaxBufferSize)
Malformed Responses	creAuthClientMalformedResponses + creAcctClientMalformedResponses
Bad Authenticators	creAuthClientBadAuthenticators + creAcctClientBadAuthenticators

Mapping the following set of objects listed in the CISCO-RADIUS-EXT-MIB map to fields displayed by the **show radius statistics**command is straightforward. For example, the creClientLastUsedSourcePort field corresponds to the Last used Source Port/Identifier portion of the report, creAuthClientBufferAllocFailures corresponds to the Buffer Allocation Failures for authentication packets, creAcctClientBufferAllocFailure corresponds to the Buffer Allocation Failures for accounting packets, and so on.

- creClientTotalMaxInQLength
- creClientTotalMaxWaitQLength
- creClientTotalMaxDoneQLength
- creClientTotalAccessRejects
- creClientTotalAverageResponseDelay
- creClientSourcePortRangeStart
- creClientSourcePortRangeEnd
- creClientLastUsedSourcePort
- creClientLastUsedSourceId
- creAuthClientBadAuthenticators
- creAuthClientUnknownResponses
- creAuthClientTotalPacketsWithResponses
- creAuthClientBufferAllocFailures
- creAuthClientTotalResponses
- creAuthClientTotalPacketsWithoutResponses
- creAuthClientAverageResponseDelay
- creAuthClientMaxResponseDelay
- creAuthClientMaxBufferSize
- creAuthClientTimeouts

- creAuthClientDupIDs
- creAuthClientMalformedResponses
- creAuthClientLastUsedSourceId
- creAcctClientBadAuthenticators
- creAcctClientUnknownResponses
- creAcctClientTotalPacketsWithResponses
- creAcctClientBufferAllocFailures
- creAcctClientTotalResponses
- creAcctClientTotalPacketsWithoutResponses
- creAcctClientAverageResponseDelay
- creAcctClientMaxResponseDelay
- creAcctClientMaxBufferSize
- creAcctClientTimeouts
- creAcctClientDupIDs
- creAcctClientMalformedResponses
- creAcctClientLastUsedSourceId

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs .

Related Commands

Command	Description
radius-server host	Specifies a RADIUS server host.
radius-server retransmit	Specifies how many times the Cisco IOS software searches the list of RADIUS server hosts before giving up.
radius-server timeout	Sets the interval for which a router waits for a server host to reply.

show radius table attributes

To display a list of all attributes supported by the RADIUS subsystem, use the **show radius table attributes** command in user EXEC or privileged EXEC mode.

show radius table attributes

Syntax Description

This command has no arguments or keywords.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

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

Usage Guidelines

This command enables you to verify that a required RADIUS attribute is supported in a specific release.

Examples

The following example displays the complete table attribute list from the **show radius table attributes** command.

```
Router# show radius table attributes

IETF ATTRIBUTE LIST:
    Name User-Name                      Format String
    Name User-Password                  Format Binary
    Name CHAP-Password                  Format Binary
    Name NAS-IP-Address                 Format IPv4 Address
    Name NAS-Port                       Format Ulong
    Name Service-Type                   Format Enum
    Name Framed-Protocol                Format Enum
    Name Framed-IP-Address              Format IPv4 Address
    Name Framed-IP-Netmask              Format IPv4 Address
    Name Framed-Routing                 Format Ulong
    Name Filter-Id                      Format Binary
    Name Framed-MTU                     Format Ulong
    Name Framed-Compression             Format Enum
    Name login-ip-addr-host             Format IPv4 Address
    Name Login-Service                  Format Enum
    Name login-tcp-port                 Format Ulong
    Name Reply-Message                  Format Binary
    Name Callback-Number                Format String
    Name Framed-Route                   Format String
    Name Framed-IPX-Network             Format IPv4 Address
    Name State                          Format Binary
    Name Class                          Format Binary
    Name Vendor-Specific                Format Binary
    Name Session-Timeout                Format Ulong
    Name Idle-Timeout                   Format Ulong
    Name Termination-Action             Format Boolean
    Name Called-Station-Id              Format String
    Name Calling-Station-Id             Format String
    Name Nas-Identifier                 Format String
    Name Acct-Status-Type               Format Enum
```

```
    Name Acct-Delay-Time                Format Ulong
    Name Acct-Input-Octets              Format Ulong
    Name Acct-Output-Octets             Format Ulong
    Name Acct-Session-Id                Format String
    Name Acct-Authentic                 Format Enum
    Name Acct-Session-Time              Format Ulong
    Name Acct-Input-Packets             Format Ulong
    Name Acct-Output-Packets            Format Ulong
    Name Acct-Terminate-Cause           Format Enum
    Name Multilink-Session-ID           Format String
    Name Acct-Link-Count                Format Ulong
    Name Acct-Input-Giga-Words          Format Ulong
    Name Acct-Output-Giga-Words         Format Ulong
    Name Event-Timestamp                Format Ulong
    Name CHAP-Challenge                 Format Binary
    Name NAS-Port-Type                  Format Enum
    Name Port-Limit                     Format Ulong
    Name Tunnel-Type                    Format Enum
    Name Tunnel-Medium-Type             Format Enum
    Name Tunnel-Client-Endpoint         Format String
    Name Tunnel-Server-Endpoint         Format String
    Name Acct-Tunnel-Connection         Format String
    Name Tunnel-Password                Format Binary
    Name Prompt                         Format Enum
    Name Connect-Info                   Format String
    Name EAP-Message                    Format Binary
    Name Message-Authenticator          Format Binary
    Name Tunnel-Private-Group-Id        Format String
    Name Tunnel-Assignment-Id           Format String
    Name Tunnel-Preference              Format Ulong
    Name Acct-Interim-Interval          Format Ulong
    Name Tunnel-Packets-Lost            Format Ulong
    Name NAS-Port-Id                    Format String
    Name Tunnel-Client-Auth-ID          Format String
    Name Tunnel-Server-Auth-ID          Format String
    Name Framed-Interface-Id            Format Binary
    Name Framed-IPv6-Prefix             Format Binary
    Name login-ip-addr-host             Format Binary
    Name Framed-IPv6-Route              Format String
    Name Framed-IPv6-Pool               Format String
    Name Dynamic-Author-Error-Cause     Format Enum
Non Standard ATTRIBUTE LIST:
    Name Old-Password                   Format Binary
    Name Ascend-Filter-Required         Format Enum
    Name Ascend-Cache-Refresh           Format Enum
    Name Ascend-Cache-Time              Format Ulong
    Name Ascend-Auth-Type               Format Ulong
    Name Ascend-Redirect-Number         Format String
    Name Ascend-Private-Route           Format String
    Name Ascend-Shared-Profile-Enable   Format Boolean
    Name Ascend-Client-Primary-DNS      Format IPv4 Address
    Name Ascend-Client-Secondary-DNS    Format IPv4 Address
    Name Ascend-Client-Assign-DNS       Format Ulong
    Name Ascend-Session-Svr-Key         Format String
    Name Ascend-Multicast-Rate-Limit    Format Ulong
    Name Ascend-Multicast-Client        Format Ulong
    Name Ascend-Multilink-Session-ID    Format Ulong
    Name Ascend-Num-In-Multilink        Format Ulong
    Name Ascend-Presession-Octets-In    Format Ulong
    Name Ascend-Presession-Octets-Out   Format Ulong
    Name Ascend-Presession-Packets-In   Format Ulong
    Name Ascend-Presession-Packets-Out  Format Ulong
    Name Ascend-Max-Time                Format Ulong
    Name Ascend-Disconnect-Cause        Format Enum
```

```
    Name Ascend-Connection-Progress     Format Enum
    Name Ascend-Data-Rate               Format Ulong
    Name Ascend-Presession-Time         Format Ulong
    Name Ascend-Require-Auth            Format Ulong
    Name Ascend-PW-Liftime              Format Ulong
    Name Ascend-IP-Direct               Format IPv4 Address
    Name Ascend-PPP-VJ-Slot-Comp        Format Boolean
    Name Ascend-Asyncmap                Format Ulong
    Name Ascend-Send-Secret             Format Binary
    Name ascend_pool_definition         Format String
    Name Ascend-IP-Pool                 Format Ulong
    Name Ascend-Dial-Number             Format String
    Name Ascend-Route-IP                Format Boolean
    Name Ascend-Send-Auth               Format Enum
    Name Ascend-Link-Compression        Format Enum
    Name Ascend-Target-Util             Format Ulong
    Name Ascend-Max-Channels            Format Ulong
    Name Ascend-Data-Filter             Format Binary
    Name Ascend-Call-Filter             Format Binary
    Name Ascend-Idle-Limit              Format Ulong
    Name Ascend-Data-Service            Format Ulong
    Name Ascend-Force-56                Format Ulong
    Name Ascend-Xmit-Rate               Format Ulong
Cisco VSA ATTRIBUTE LIST:
    Name Cisco AVpair                   Format String
    Name cisco-nas-port                 Format String
    Name fax_account_id_origin          Format String
    Name fax_msg_id                     Format String
    Name fax_pages                      Format String
    Name fax_modem_time                 Format String
    Name fax_connect_speed              Format String
    Name fax_mdn_address                Format String
    Name fax_mdn_flag                   Format String
    Name fax_auth_status                Format String
    Name email_server_address           Format String
    Name email_server_ack_flag          Format String
    Name gateway_id                     Format String
    Name call_type                      Format String
    Name port_used                      Format String
    Name abort_cause                    Format String
    Name h323-remote-address            Format String
    Name Conf-Id                        Format String
    Name h323-setup-time                Format String
    Name h323-call-origin               Format String
    Name h323-call-type                 Format String
    Name h323-connect-time              Format String
    Name h323-disconnect-time           Format String
    Name h323-disconnect-cause          Format String
    Name h323-voice-quality             Format String
    Name h323-gw-id                     Format String
    Name Cisco AVpair                   Format Binary
    Name Cisco encrypted string vsa     Format String
    Name Sub_Policy_In                  Format String
    Name Sub_Policy_Out                 Format String
    Name h323-credit-amount             Format String
    Name h323-credit-time               Format String
    Name h323-return-code               Format String
    Name h323-prompt-id                 Format String
    Name h323-time-and-day              Format String
    Name h323-redirect-number           Format String
    Name h323-preferred-lang            Format String
    Name h323-redirect-ip-address       Format String
    Name h323-billing-model             Format String
    Name h323-currency                  Format String
```

```
    Name ssg-account-info               Format String
    Name ssg-service-info               Format String
    Name ssg-command-code               Format Binary
    Name ssg-control-info               Format String
Microsoft VSA ATTRIBUTE LIST:
    Name MS-CHAP-Response               Format Binary
    Name MS-CHAP-ERROR                  Format Binary
    Name MS-CHAP-CPW-1                  Format Binary
    Name MS-CHAP-CPW-2                  Format Binary
    Name MS-CHAP-LM-Enc-PW              Format Binary
    Name MS-CHAP-NT-Enc-PW              Format Binary
    Name MS-MPPE-Enc-Policy             Format Binary
    Name MS-MPPE-Enc-Type               Format Binary
    Name MS-RAS-Vendor                  Format String
    Name MS-CHAP-DOMAIN                 Format String
    Name MSCHAP_Challenge               Format Binary
    Name MS-CHAP-MPPE-Keys              Format Binary
    Name MS-BAP-Usage                   Format Binary
    Name MS-Link-Util-Thresh            Format Binary
    Name MS-Link-Drop-Time-Limit        Format Binary
    Name MS-MPPE-Send-Key               Format Binary
    Name MS-MPPE-Recv-Key               Format Binary
    Name MS-RAS-Version                 Format String
    Name MS-Old-ARAP-Password           Format Binary
    Name New-ARAP-Password              Format Binary
    Name MS-ARAP-PW-Change-Reason       Format Binary
    Name MS-Filter                      Format Binary
    Name MS-Acct-Auth-Type              Format Binary
    Name MS-MPPE-EAP-Type               Format Binary
    Name MS-CHAP-V2-Response            Format Binary
    Name MS-CHAP-V2-Success             Format String
    Name MS-CHAP-CPW-2                  Format Binary
    Name MS-Primary-DNS                 Format IPv4 Address
    Name MS-Secondary-DNS               Format IPv4 Address
    Name MS-1st-NBNS-Server             Format IPv4 Address
    Name MS-2nd-NBNS-Server             Format IPv4 Address
    Name MS-ARAP-Challenge              Format Binary
3GPP VSA ATTRIBUTE LIST:
    Name Charging-ID                    Format Ulong
    Name PDP Type                       Format Enum
    Name Charging-Gateway-Address       Format IPv4 Address
    Name GPRS-QoS-Profile               Format String
    Name SGSN-Address                   Format IPv4 Address
    Name GGSN-Address                   Format IPv4 Address
    Name IMSI-MCC-MNC                   Format String
    Name GGSN-MCC-MNC                   Format String
    Name NSAPI                          Format String
    Name Session-Stop-Ind               Format Binary
    Name Selection-Mode                 Format String
    Name Charging-Characteristics       Format String
3GPP2 VSA ATTRIBUTE LIST:
    Name cdma-reverse-tnl-spec          Format Ulong
    Name cdma-diff-svc-class-opt        Format Ulong
    Name cdma-container                 Format String
    Name cdma-ha-ip-addr                Format IPv4 Address
    Name cdma-pcf-ip-addr               Format IPv4 Address
    Name cdma-bs-msc-addr               Format String
    Name cdma-user-id                   Format Ulong
    Name cdma-forward-mux               Format Ulong
    Name cdma-reverse-mux               Format Ulong
    Name cdma-forward-rate              Format Ulong
    Name cdma-reverse-rate              Format Ulong
    Name cdma-service-option            Format Ulong
    Name cdma-forward-type              Format Ulong
```

```
    Name cdma-reverse-type              Format Ulong
    Name cdma-frame-size                Format Ulong
    Name cdma-forward-rc                Format Ulong
    Name cdma-reverse-rc                Format Ulong
    Name cdma-ip-tech                   Format Ulong
    Name cdma-comp-flag                 Format Enum
    Name cdma-reason-ind                Format Enum
    Name cdma-bad-frame-count           Format Ulong
    Name cdma-num-active                Format Ulong
    Name cdma-sdb-input-octets          Format Ulong
    Name cdma-sdb-output-octets         Format Ulong
    Name cdma-numsdb-input              Format Ulong
    Name cdma-numsdb-output             Format Ulong
    Name cdma-ip-qos                    Format Ulong
    Name cdma-airlink-qos               Format Ulong
    Name cdma-rp-session-id             Format Ulong
    Name cdma-hdlc-layer-bytes-in       Format Ulong
    Name cdma-correlation-id            Format String
    Name cdma-moip-inbound              Format Ulong
    Name cdma-moip-outbound             Format Ulong
    Name cdma-session-continue          Format Ulong
    Name cdma-active-time               Format Ulong
    Name cdma-frame-size                Format Ulong
    Name cdma-esn                       Format String
    Name cdma-mn-ha-spi                 Format Ulong
    Name cdma-mn-ha-shared-key          Format Binary
    Name cdma-sess-term-capability      Format Ulong
    Name cdma-disconnect-reason         Format Ulong
Verizon VSA ATTRIBUTE LIST:
    Name mip-key-data                   Format Binary
    Name aaa-authenticator              Format Binary
    Name public-key-invalid             Format Binary
```

The table below describes the significant fields shown in the display.

Table 39: show radius table attributes Field Descriptions

Field	Description
User-Name	The name of the user on the system. The format is String.
User-Password	The password of the user on the system. The format is Binary.
CHAP-Password	Challenge Handshake Authentication Protocol (CHAP) password. The format is Binary.
NAS-IP-Address	Network-Attached Storage (NAS) IP address. The format is IPv4 Address.
NAS-Port	The RADIUS Attribute 5 (NAS-Port) format specified on a per-server group level. The format is Ulong.
Service-Type	Sets the service type. The format is Enum.
Framed-Protocol	Indicates the framing to be used for framed access. It may be used in both Access-Request and Access-Accept packets. The format is Enum.
Framed-IP-Address	Indicates the address to be configured for the user. It may be used in Access-Accept packets. The format is IPv4 Address.

Field	Description
Framed-IP-Netmask	Indicates the IP netmask to be configured for the user when the user is a router to a network. The format is IPv4 Address.
Framed-Routing	Indicates the routing method for the user when the user is a router to a network. The format is Ulong.
Filter-Id	To disable, enable, get, or set a filter, the filter ID must be valid. The format is Binary.
Framed-MTU	Indicates the maximum transmission unit to be configured for the user, when it is not negotiated by some other means (such as PPP). The format is Ulong.
Framed-Compression	Indicates a compression protocol to be used for the link. The format is Enum.
login-ip-addr-host	Indicates the host to which the user will connect when the Login-Service attribute is included. The format is IPv4 Address.
Login-Service	The Login-IP-Host AVP (AVP Code 14) is of type Address and contains the system with which to connect the user, when the Login-Service AVP is included. The format is Enum.
login-tcp-port	The Login-TCP-Port AVP (AVP Code 16) is of type Integer32 and contains the TCP port with which the user is to be connected, when the Login-Service AVP is also present. The format is Ulong.
Reply-Message	Indicates text that may be displayed to the user. The format is Binary.
Callback-Number	Indicates a dialing string to be used for callback. The format is String.
Framed-Route	Provides routing information to be configured for the user on the NAS. The format is String.
Framed-IPX-Network	The Framed-IPX-Network AVP (AVP Code 23) is of type Unsigned32, and contains the IPX Network number to be configured for the user. The format is Pv4 Address.
State	Is available to be sent by the server to the client in an Access-Challenge and must be sent unmodified from the client to the server in the new Access-Request reply to that challenge, if any. The format is Binary.
Class	Is available to be sent by the server to the client in an Access-Accept and should be sent unmodified by the client to the accounting server as part of the Accounting-Request packet if accounting is supported. The format is Binary.
Vendor-Specific	Is available to allow vendors to support their own extended attributes not suitable for general usage. The format is Binary.
Session-Timeout	Sets the maximum number of seconds of service to be provided to the user before termination of the session or prompt. The format is Ulong.

Field	Description
Idle-Timeout	Sets the maximum number of consecutive seconds of idle connection allowed to the user before termination of the session or prompt. The format is Ulong.
Termination-Action	Indicates what action the NAS should take when the specified service is completed. The format is Boolean.
Called-Station-Id	The Called-Station-Id AVP (AVP Code 30) is of type String and allows the NAS to send in the request the phone number that the user called, using Dialed Number Identification (DNIS) or a similar technology. The format is String.
Calling-Station-Id	The Calling-Station-Id AVP (AVP Code 31) is of type String and allows the NAS to send in the request the phone number that the call came from, using Automatic Number Identification (ANI) or a similar technology. The format is String.
Nas-Identifier	Contains a string identifying the NAS originating the access request. The format is String.
Acct-Status-Type	Indicates whether this Accounting-Request marks the beginning of the user service (Start) or the end (Stop). The format is Enum.
Acct-Delay-Time	Indicates how many seconds the client has been trying to send this record for, and can be subtracted from the time of arrival on the server to find the approximate time of the event generating this Accounting-Request. (Network transit time is ignored.) The format is Ulong.
Acct-Input-Octets	Indicates how many octets have been received from the port over the course of this service being provided, and can only be present in Accounting-Request records where Acct-Status-Type is set to Stop. The format is Ulong.
Acct-Output-Octets	Indicates how many octets have been sent to the port in the course of delivering this service, and can only be present in Accounting-Request records where Acct-Status-Type is set to Stop. The format is Ulong.
Acct-Session-Id	Is a unique accounting ID to make it easy to match start and stop records in a log file. The format is String.
Acct-Authentic	Indicate how the user was authenticated, whether by Radius, the NAS itself, or another remote authentication protocol. It may be included in an Accounting-Request. The format is Enum.
Acct-Session-Time	Indicates how many seconds the user has received service for, and can only be present in Accounting-Request records where Acct-Status-Type is set to Stop. The format is Ulong.
Acct-Input-Packets	Indicates how many packets have been received from the port over the course of this service being provided to a framed user, and can only be present in Accounting-Request records where Acct-Status-Type is set to Stop. The format is Ulong.

Field	Description
Acct-Output-Packets	Indicates how many packets have been sent to the port in the course of delivering this service to a framed user, and can only be present in Accounting-Request records where Acct-Status-Type is set to Stop. The format is Ulong.
Acct-Terminate-Cause	Indicates how the session was terminated, and can only be present in Accounting-Request records where Acct-Status-Type is set to Stop. The format is Enum.
Multilink-Session-ID	Indicates the service to use to connect the user to the login host. It is only used in Access-Accept packets. The format is String.
Acct-Link-Count	Gives the count of links which are known to have been in a given multilink session at the time the accounting record is generated. The format is Ulong.
Acct-Input-Giga-Words	Indicates how many times the Acct-Input-Octets counter has wrapped around 2^32 over the course of this service being provided, and can only be present in Accounting-Request records where the Acct-Status-Type is set to Stop or Interim-Update. The format is Ulong.
Acct-Output-Giga-Words	Indicates how many times the Acct-Output-Octets counter has wrapped around 2^32 in the course of delivering this service, and can only be present in Accounting-Request records where the Acct-Status-Type is set to Stop or Interim-Update. The format is Ulong.
Event-Timestamp	Use to include the Event-Timestamp attribute in Acct-Start or Acct-Stop messages. The format is Ulong.
CHAP-Challenge	The CHAP is used to verify periodically the identity of the peer using a 3-way handshake. The format is Binary.
NAS-Port-Type	Indicates the physical port number of the NAS which is authenticating the user. The format is Enum.
Port-Limit	Sets the maximum number of ports to be provided to the user by the NAS. The format is Ulong.
Tunnel-Type	Indicates the tunneling protocol(s) to be used (in the case of a tunnel initiator) or the the tunneling protocol in use (in the case of a tunnel terminator). The format is Enum.
Tunnel-Medium-Type	Indicates which transport medium to use when creating a tunnel for those protocols (such as L2TP) that can operate over multiple transports. The format is Enum.
Tunnel-Client-Endpoint	Contains the address of the initiator end of the tunnel. The format is String.
Tunnel-Server-Endpoint	Indicates the address of the server end of the tunnel. The format is String.
Acct-Tunnel-Connection	Indicates the identifier assigned to the tunnel session. The format is String.

Field	Description
Tunnel-Password	Can contain a password to be used to authenticate to a remote server. The format is Binary.
Prompt	Used only in Access-Challenge packets, and indicates to the NAS whether it should echo the user's response as it is entered, or not echo it. The format is Enum.
Connect-Info	Is sent from the NAS to indicate the nature of the user's connection. The format is String.
EAP-Message	Encapsulates Extensible Authentication Protocol packets so as to allow the NAS to authenticate dial-in users via EAP without having to understand the protocol. The format is Binary.
Message-Authenticator	Can be used to authenticate and integrity-protect Access-Requests in order to prevent spoofing. The format is Binary.
Tunnel-Private-Group-Id	Indicates the group ID for a particular tunneled session. The format is String.
Tunnel-Assignment-Id	Used to indicate to the tunnel initiator the particular tunnel to which a session is to be assigned. The format is String.
Tunnel-Preference	Should be included in each set to indicate the relative preference assigned to each tunnel if more than one set of tunneling attributes is returned by the RADIUS server to the tunnel initiator. The format is Ulong.
Acct-Interim-Interval	Indicates the number of seconds between each interim update in seconds for this specific session. The format is Ulong.
Tunnel-Packets-Lost	Indicates the number of packets lost on a given link. The format is Ulong.
NAS-Port-Id	Used to identify the IEEE 802.1X Authenticator port which authenticates the Supplicant. The format is String.
Tunnel-Client-Auth-ID	Specifies the name used by the tunnel initiator during the authentication phase of tunnel establishment. The format is String.
Tunnel-Server-Auth-ID	Specifies the name used by the tunnel terminator during the authentication phase of tunnel establishment. The format is String.
Framed-Interface-Id	Indicates the IPv6 interface identifier to be configured for the user. The format is Binary.
Framed-IPv6-Prefix	Indicates an IPv6 prefix (and corresponding route) to be configured for the user. The format is Binary.
Framed-IPv6-Route	Provides routing information to be configured for the user on the NAS. The format is String.
Framed-IPv6-Pool	Contains the name of an assigned pool that should be used to assign an IPv6 prefix for the user. The format is String.

Field	Description
Dynamic-Author-Error-Cause	Specifies the error causes associated with dynamic authorization. The format is Enum.
Old-Password	Is 16 octets in length. It contains the encrypted Lan Manager hash of the old password. The format is Binary.
Ascend-Filter-Required	Specifies whether the call should be permitted if the specified filter is not found. If present, this attribute will be applied after any authentication, authorization, and accounting (AAA) filter method-list. The format is Enum.
Ascend-Cache-Refresh	Specifies whether cache entries should be refreshed each time an entry is referenced by a new session. This attribute corresponds to the **cache refresh** command. The format is Enum.
Ascend-Cache-Time	Specifies the idle time out, in minutes, for cache entries. This attribute corresponds to the **cache clear age** command. The format is Ulong.
Ascend-Auth-Type	Indicates the type of name and password (PPP) authorization to use. The format Ulong.
Ascend-Redirect-Number	Indicates the original number in the information sent to the authentication server when the number dialed by a device is redirected to another number for authentication. The format is String.
Ascend-Private-Route	Specifies whether IP routing is allowed for the user profile. The format is String.
Ascend-Shared-Profile-Enable	Specifies whether multiple incoming callers can share a single RADIUS user profile. The format is Boolean.
Ascend-Client-Primary-DNS	Specifies a primary DNS server address to send to any client connecting to the MAX TNT. The format is IPv4 Address.
Ascend-Client-Secondary-DNS	Specifies a secondary DNS server address to send to any client connecting to the MAX TNT. The format is IPv4 Address.
Ascend-Client-Assign-DNS	Specifies whether or not the MAX TNT sends the Ascend-Client-Primary-DNS and Ascend-Client-Secondary-DNS values during connection negotiation. The format is Ulong.
Ascend-Session-Svr-Key	Specifies the session key that identifies the user session. You can specify up to 16 characters. The default value is null. The format is String.
Ascend-Multicast-Rate-Limit	Specifies how many seconds the MAX waits before accepting another packet from the multicast client. The format is Ulong.
Ascend-Multicast-Client	Specifies whether the user is a multicast client of the MAX. The format is Ulong.
Ascend-Multilink-Session-ID	Specifies the ID number of the Multilink bundle when the session closes. A Multilink bundle is a multichannel MP or MP+ call. The format is Ulong.

Field	Description
Ascend-Num-In-Multilink	Indicates the number of sessions remaining in a Multilink bundle when the session closes. A Multilink bundle is a multichannel MP or MP+ call. The format is Ulong.
Ascend-Presession-Octets-In	Reports the number of octets received before authentication. The value reflects only the data delivered by PPP or other encapsulation. It does not include the header or other protocol-dependent components of the packet. The format is Ulong.
Ascend-Presession-Octets-Out	Reports the number of octets transmitted before authentication. The value reflects only the data delivered by PPP or other encapsulation. It does not include the header or other protocol-dependent components of the packet. The format is Ulong.
Ascend-Presession-Packets-In	Reports the number of packets received before authentication. The packets are counted before the encapsulation is removed. The attribute's value does not include maintenance packets, such as keepalive or management packets. The format is Ulong.
Ascend-Presession-Packets-Out	Reports the number of packets transmitted before authentication. The packets are counted before the encapsulation is removed. The attribute's value does not include maintenance packets, such as keepalive or management packets. The format is Ulong.
Ascend-Max-Time	Specifies the maximum length of time in seconds that any session can remain online. Once a session reaches the time limit, its connection goes offline. The format is Ulong.
Ascend-Disconnect-Cause	Indicates the reason a connection went offline. The format is Enum.
Ascend-Connection-Progress	Indicates the state of the connection before it disconnects. The format is Enum.
Ascend-Data-Rate	Specifies the rate of data received on the connection in bits per second. The format is Ulong.
Ascend-Presession-Time	Reports the length of time in seconds from when a call connected to when it completes authentication. The format is Ulong.
Ascend-Require-Auth	Specifies whether the MAX TNT requires additional authentication after Calling-Line ID (CLID) or called-number authentication. The format is Ulong.
Ascend-PW-Liftime	Specifies the number of days that a password is valid. The format is Ulong.
Ascend-IP-Direct	Specifies the IP address to which the MAX TNT redirects packets from the user. When you include this attribute in a user profile, the MAX TNT bypasses all internal routing tables, and simply sends all packets it receives on the connection's WAN interface to the specified IP address. The format is IPv4 Address.

Field	Description
Ascend-PPP-VJ-Slot-Comp	Instructs the MAX TNT to not use slot compression when sending VJ-compressed packets. The format is Boolean.
Ascend-Asyncmap	The format is Ulong.
Ascend-Send-Secret	Specifies the password that the RADIUS server sends to the remote end of a connection on an outgoing call. It is encrypted when passed between the RADIUS server and the MAX TNT. The format is Binary.
Ascend_pool_definition	Specifies all the addresses in the pool. The format is String.
Ascend-IP-Pool	Specifies the first address in an IP address pool, as well as the number of addresses in the pool. The format is Ulong.
Ascend-Dial-Number	Specifies the phone number the MAX TNT dials to reach the router or node at the remote end of the link. The format is String.
Ascend-Route-IP	Specifies whether IP routing is allowed for the user profile. The format is Boolean.
Ascend-Send-Auth	Specifies the authentication protocol that the MAX TNT requests when initiating a PPP or MP+ connection. The answering side of the connection determines which authentication protocol, if any, the connection uses. The format is Enum.
Ascend-Link-Compression	Turns data compression on or off for a PPP link. The format is Enum.
Ascend-Target-Util	Specifies the percentage of bandwidth use at which the MAX TNT adds or subtracts bandwidth. The format is Ulong.
Ascend-Max-Channels	Specifies the maximum number of channels allowed on an MP+ call. The format is Ulong.
Ascend-Data-Filter	Specifies the characteristics of a data filter in a RADIUS user profile. The MAX TNT uses the filter only when it places or receives a call associated with the profile that includes the filter definition. The format is Binary.
Ascend-Call-Filter	Specifies the characteristics of a call filter in a RADIUS user profile. The MAX TNT uses the filter only when it places a call or receives a call associated with the profile that includes the filter definition. The format is Binary.
Ascend-Idle-Limit	Specifies the number of seconds the MAX TNT waits before clearing a call when a session is inactive. The format is Ulong.
Ascend-Data-Service	Specifies the type of data service the link uses for outgoing calls. The format is Ulong.
Ascend-Force-56	Indicates whether the MAX uses only the 56-kbps portion of a channel, even when all 64-kbps appear to be available. The format is Ulong.

Field	Description
Ascend-Xmit-Rate	Specifies the rate of data transmitted on the connection in bits per second. For ISDN calls, Ascend-Xmit-Rate indicates the transmit data rate. For analog calls, it indicates the modem baud rate at the time of the initial connection. The format is Ulong.
Cisco AVpair	The Cisco RADIUS implementation supports one vendor-specific option using the format recommended in the specification. Cisco's vendor-ID is 9, and the supported option has vendor-type 1, which is named "cisco-avpair". The format is String.
cisco-nas-port	Enables the display of physical interface information and parent interface details as part of the of the cisco-nas-port vendor-specific attribute (VSA) for login calls. The format is String.
fax_account_id_origin	Indicates the account ID origin as defined by system administrator for the **mmoip aaa receive-id** or the **mmoip aaa send-id** command. The format is String.
fax_msg_id	Indicates a unique fax message identification number assigned by Store and Forward Fax. The format is String.
fax_pages	Indicates the number of pages transmitted or received during this fax session. This page count includes cover pages. The format is String.
fax_modem_time	Indicates the amount of time in seconds the modem sent fax data (x) and the amount of time in seconds of the total fax session (y), which includes both fax-mail and PSTN time, in the form x/y. For example, 10/15 means that the transfer time took 10 seconds, and the total fax session took 15 seconds. The format is String.
fax_connect_speed	Indicates the modem speed at which this fax-mail was initially transmitted or received. Possible values are 1200, 4800, 9600, and 14400. The format is String.
fax_mdn_address	Indicates the address to which message delivery notifications (MDNs) will be sent. The format is String.
fax_mdn_flag	Indicates whether or not MDNs has been enabled. True indicates that MDN had been enabled; false means that MDN had not been enabled. The format is String.
fax_auth_status	Indicates whether or not authentication for this fax session was successful. Possible values for this field are success, failed, bypassed, or unknown. The format is String.
email_server_address	Indicates the IP address of the e-mail server handling the on-ramp fax-mail message. The format is String.
email_server_ack_flag	Indicates that the on-ramp gateway has received a positive acknowledgment from the e-mail server accepting the fax-mail message. The format is String.

Field	Description
gateway_id	Indicates the name of the gateway that processed the fax session. The name appears in the following format: hostname.domain-name. The format is String.
call_type	Describes the type of fax activity: fax receive or fax send. The format is String.
port_used	Indicates the slot/port number of the Cisco AS5300 used to either transmit or receive this fax-mail. The format is String.
abort_cause	If the fax session terminates, it indicates the system component that signaled the termination. Examples of system components that could trigger a termination are FAP (Fax Application Process), TIFF (the TIFF reader or the TIFF writer), fax-mail client, fax-mail server, ESMTP client, or ESMTP server. The format is String.
h323-remote-address	Indicates the IP address of the remote gateway. The format is String.
Conf-Id	Indicates a unique call identifier generated by the gateway. Used to identify the separate billable events (calls) within a single calling session. The format is String.
h323-setup-time	Indicates the setup time in NTP format: hour, minutes, seconds, microseconds, time_zone, day, month, day_of_month, year. The format is String.
h323-call-origin	Indicates the gateway's behavior in relation to the connection that is active for this leg. The format is String.
h323-call-type	Indicates the protocol type or family used on this leg of the call. The format is String.
h323-connect-time	Indicates the connect time in Network Time Protocol (NTP) format: hour, minutes, seconds, microseconds, time_zone, day, month, day_of_month, and year. The format is String.
h323-disconnect-time	Indicates the disconnect time in NTP format: hour, minutes, seconds, microseconds, time_zone, day, month, day_of_month, year. The format is String.
h323-disconnect-cause	Indicates the Q.931 disconnect cause code retrieved from CCAPI. The source of the code is the disconnect location such as a PSTN, terminating gateway, or SIP. The format is String.
h323-voice-quality	Indicates the ICPIF of the voice quality. The format is String.
h323-gw-id	Indicate the name of the tenor. The format is String.
Cisco AVpair	The Cisco RADIUS implementation supports one vendor-specific option using the format recommended in the specification. Cisco's vendor-ID is 9, and the supported option has vendor-type 1, which is named "cisco-avpair". The format is String.

Field	Description
Cisco encrypted string vsa	Cisco allows several forms of sub-attribute encryption. The only method supported is the Cisco Encrypted String VSA Format also supported by an IETF draft for Salt-Encryption of RADIUS attributes. The format is String.
Sub_Policy_In	Defines the service policy input. The format is String.
Sub_Policy_Out	Defines the service policy output. The format is String.
h323-credit-amount	Indicates the amount of credit (in currency) that the account contains. The format is String.
h323-credit-time	Indicates the number of seconds for which the call is authorized. The format is String.
h323-return-code	Return codes are instructions from the RADIUS server to the voice gateway. The format is String.
h323-prompt-id	Indexes into an array that selects prompt files used at the gateway. The format is String.
h323-time-and-day	Indicates the time of day at the dialed number or at the remote gateway in the format: hour, minutes, seconds. The format is String.
h323-redirect-number	Indicates the phone number to which the call is redirected; for example, to a toll-free number or a customer service number. The format is String.
h323-preferred-lang	Indicates the language to use when playing the audio prompt specified by the h323-prompt-id. The format is String.
h323-redirect-ip-address	Indicates the IP address for an alternate or redirected call. The format is String.
h323-billing-model	Indicates the type of billing service for a specific call. The format is String.
h323-currency	Indicates the currency to use with h323-credit-amount. The format is String.
ssg-account-info	Subscribes the subscriber to the specified service and indicates that the subscriber should be automatically connected to this service after successful logon. The format is String.
ssg-service-info	SSG redirects the user's HTTP traffic to a server in the specified server group. All the service features (such as quality of service (QoS) and prepaid billing) are applied to the HTTP traffic. The format is String.
ssg-command-code	Specifies account logon and logoff, session query, and service activate and deactivate information. The format is Binary.
ssg-control-info	Indicates the control-info code for prepaid quota. The format is String.
MS-CHAP-Response	This attribute contains the response value provided by a PPP Microsoft Challenge-Handshake Authentication Protocol (MS-CHAP) user in response to the challenge. The format is Binary.

Field	Description
MS-CHAP-ERROR	Contains error data related to the preceding MS-CHAP exchange. The format is Binary.
MS-CHAP-CPW-1	Allows the user to change their password if it has expired. The format is Binary.
MS-CHAP-CPW-2	Allows the user to change their password if it has expired. The format is Binary.
MS-CHAP-LM-Enc-PW	Contains the new Windows NT password encrypted with the old LAN Manager password hash. The format is Binary.
MS-CHAP-NT-Enc-PW	Contains the new Windows NT password encrypted with the old Windows NT password hash. The format is Binary.
MS-MPPE-Enc-Policy	The MS-MPPE-Encryption-Policy attribute may be used to signify whether the use of encryption is allowed or required. The format is Binary.
MS-MPPE-Enc-Type	The MS-MPPE-Encryption-Types attribute is used to signify the types of encryption available for use with Microsoft Point-to-Point Encryption (MPPE). The format is Binary.
MS-RAS-Vendor	Used to indicate the manufacturer of the RADIUS client machine. The format is Binary.
MS-CHAP-DOMAIN	Indicates the Windows NT domain in which the user was authenticated. The format is Binary.
MSCHAP_Challenge	Contains the challenge sent by a NAS to a MS-CHAP user. The format is Binary.
MS-CHAP-MPPE-Keys	Contains two session keys for use by the MPPE. The format is Binary.
MS-BAP-Usage	Describes whether the use of Bandwidth Allocation Protocol (BAP) is allowed, disallowed or required on new multilink calls. The format is Binary.
MS-Link-Util-Thresh	Represents the percentage of available bandwidth utilization below which the link must fall before the link is eligible for termination. The format is Binary.
MS-Link-Drop-Time-Limit	Indicates the length of time (in seconds) that a link must be underutilized before it is dropped. The format is Binary.
MS-MPPE-Send-Key	Contains a session key for use by the MPPE. The format is Binary.
MS-MPPE-Recv-Key	Contains a session key for use by the MPPE. The format is Binary.
MS-RAS-Version	Used to indicate the version of the RADIUS client software. The format is Binary.
MS-Old-ARAP-Password	Used to transmit the old Apple Remote Access Protocol (ARAP) password during an ARAP password change operation. The format is Binary.

Field	Description
New-ARAP-Password	Used to transmit the new ARAP password during an ARAP password change operation. The format is Binary.
MS-ARAP-PW-Change-Reason	Used to indicate reason for a server-initiated password change. The format is Binary.
MS-Filter	Used to transmit traffic filters. The format is Binary.
MS-Acct-Auth-Type	Used to represent the method used to authenticate the dial-up user. The format is Binary.
MS-MPPE-EAP-Type	Used to represent the EAP type used to authenticate the dial-up user. The format is Binary.
MS-CHAP-V2-Response	This attribute is identical in format to the standard CHAP Response packet. The format is Binary.
MS-CHAP-V2-Success	Contains a 42-octet authenticator response string and must be included in the Message field packet sent from the NAS to the peer. The format is Binary.
MS-CHAP-CPW-2	Allows the user to change their password if it has expired. The format is Binary.
MS-Primary-DNS	Used to indicate the address of the primary DNS server to be used by the PPP peer. The format is IPv4 Address.
MS-Secondary-DNS	Used to indicate the address of the secondary DNS server to be used by the PPP peer. The format is IPv4 Address.
MS-1st-NBNS-Server	Used to indicate the address of the primary NetBIOS Name Server (NBNS) server to be used by the PPP peer. The format is IPv4 Address.
MS-2nd-NBNS-Server	Used to indicate the address of the secondary NBNS server to be used by the PPP peer. The format is IPv4 Address.
MS-ARAP-Challenge	Only present in an Access-Request packet containing a Framed-Protocol Attribute with the value 3 (ARAP). The format is Binary.
Charging-ID	Generated for each activated context. It is a unique four octet value generated by the GGSN when a PDP Context is activated. The format is Ulong.
PDP Type	Indicates the Packet Data Protocol (PDP) is to be used by the mobile for a certain service. The format is Enum.
Charging-Gateway-Address	The IP address of the recommended Charging Gateway Functionality to which the SGSN should transfer the Charging Detail Records (CDR) for this PDP Context. The format is IPv4 Address.
GPRS-QoS-Profile	Controls the QoS negotiated values. The format is String.
SGSN-Address	This is the IP address of the SGSN that is used by the GTP control plane for handling control messages. The format is IPv4 Address.

Field	Description
GGSN-Address	IP address of the GGSN that is used by the GTP control plane for the context establishment. This address is the same as the GGSN IP address used in G-CDRs. The format is IPv4 Address.
IMSI-MCC-MNC	The MCC and MNC extracted from the user's IMSI number (the first 5 or 6 digits depending on the IMSI). The format is String.
GGSN-MCC-MNC	The MCC and MNC of the network to which the GGSN belongs. The format is String.
NSAPI	Identifies a particular PDP context for the associated PDN and MSISDN/IMSI from creation to deletion. The format is String.
Session-Stop-Ind	Indicates to the AAA server that the last PDP context of a session is released and that the PDP session has been terminated. The format is Binary
Selection-Mode	Contains the selection mode for this PDP Context received in the Create PDP Context Request Message. The format is String.
Charging-Characteristics	Contains the charging characteristics for this PDP Context received in the Create PDP Context Request Message (only available in R99 and later releases). The format is String.
cdma-reverse-tnl-spec	Indicates the style of reverse tunneling that is required, and optionally appears in a RADIUS Access-Accept message. The format is Ulong.
cdma-diff-svc-class-opt	This attribute is deprecated and is replaced by the Allowed Differentiated Services Marking attribute. The Home RADIUS server authorizes differentiated services via the Differentiated Services Class Options attribute, and optionally appears in a RADIUS Access-Accept message. The format is Ulong.
cdma-container	Contains embedded 3GPP2 VSAs and/or RADIUS accounting attributes. The format is String.
cdma-ha-ip-addr	A Home Agent (HA) IP address used during a MIP session by the user as defined in IETF RFC 2002. The format is IPv4 Address.
cdma-pcf-ip-addr	The IP address of the serving PCF (the PCF in the serving RN). The format is IPv4 Address.
cdma-bs-msc-addr	The Base Station (BS) Mobile Switching Center (MSC) address. The format is String.
cdma-user-id	The name of the user on the system. The format is Ulong.
cdma-forward-mux	Forwards FCH multiplex option. The format is Ulong.
cdma-reverse-mux	Reverses FCH multiplex option. The format is Ulong.

Field	Description
cdma-forward-rate	The format and structure of the radio channel in the forward Dedicated Control Channel. A set of forward transmission formats that are characterized by data rates, modulation characterized, and spreading rates. The format is Ulong.
cdma-reverse-rate	The format and structure of the radio channel in the reverse Dedicated Control Channel. A set of reverse transmission formats that are characterized by data rates, modulation characterized, and spreading rates. The format is Ulong.
cdma-service-option	Code Division Multiple Access (CDMA) service option as received from the RN. The format is Ulong.
cdma-forward-type	Forward direction traffic type. It is either Primary or Secondary. The format is Ulong.
cdma-reverse-type	Reverse direction traffic type. It is either Primary or Secondary. The format is Ulong.
cdma-frame-size	Specifies the Fundamental Channel (FCH) frame size. The format is Ulong.
cdma-forward-rc	The format and structure of the radio channel in the forward FCH. A set of forward transmission formats that are characterized by data rates, modulation characterized, and spreading rates. The format is Ulong.
cdma-reverse-rc	The format and structure of the radio channel in the reverse FCH. A set of reverse transmission formats that are characterized by data rates, modulation characterized, and spreading rates. The format is Ulong.
cdma-ip-tech	Identifies the IP technology to use for the call: Simple IP or Mobile IP. The format is Ulong.
cdma-comp-flag	Indicates the type of compulsory tunnel. The format is Ulong.
cdma-reason-ind	Indicates the reasons for a stop record. The format is Ulong.
cdma-bad-frame-count	The total number of PPP frames from the MS dropped by the Packet Data Serving Node (PDSN) due to uncorrectable errors. The format is Ulong.
cdma-num-active	The number of active transitions. The format is Ulong.
cdma-sdb-input-octets	This is the Short Data Burst (SDB) octet count reported by the RN in the SDB Airlink Record. The format is Ulong.
cdma-sdb-output-octets	The SDB octet count reported by the RN in the SDB Airlink Record. The format is Ulong.
cdma-numsdb-input	The number of terminating SDBs. The format is Ulong.
cdma-numsdb-output	The number of originating SDBs. The format is Ulong.
cdma-ip-qos	Indicates the IP Quality of Service (QoS). The format is Ulong.

Field	Description
cdma-airlink-qos	Identifies Airlink Priority associated with the user. This is the user's priority associated with the packet data service. The format is Ulong.
cdma-rp-session-id	Identifies the resource reservation protocol type session identifier. The format is Ulong.
cdma-hdlc-layer-bytes-in	The count of all octets received in the reverse direction by the High-Level Data Link Control (HDLC) layer in the PDSN. The format is Ulong.
cdma-correlation-id	Indicates a unique accounting ID created by the Serving PDSN for each packet data session that allows multiple accounting events for each associated R-P connection or P-P connection to be correlated.The format is String.
cdma-moip-inbound	This is the total number of octets in registration requests and solicitations sent by the MS. The format is Ulong.
cdma-moip-outbound	This is the total number of octets in registration replies and agent advertisements, sent to the MS. The format is Ulong.
cdma-session-continue	This attribute when set to "true" means it is not the end of a Session and an Accounting Stop is immediately followed by an Account Start Record. "False" means end of a session. The format is Ulong.
cdma-active-time	The total active connection time on traffic channel in seconds. The format is Ulong.
cdma-frame-size	Specifies the FSH frame size. The format is Ulong.
cdma-esn	Indicates the Electronic Serial Number (ESN). The format is String.
cdma-mn-ha-spi	The SPI for the MN-HA shared key that optionally appears in a RADIUS Access-Request message. It is used to request an MN-HA shared key. The format is Ulong.
cdma-mn-ha-shared-key	A shared key for MN-HA that may appear in a RADIUS Access-Accept message. The MN-HA shared key is encrypted using a method based on the RSA Message Digest Algorithm MD5 [RFC 1321] as described in Section 3.5 of RFC 2868. The format is Binary.
cdma-sess-term-capability	The value shall be bitmap encoded rather than a raw integer. This attribute shall be included in a RADIUS Access-Request message to the Home RADIUS server and shall contain the value 3 to indicate that the PDSN and HA support both Dynamic authorization with RADIUS and Registration Revocation for Mobile IPv4. The attribute shall also be included in the RADIUS Access-Accept message and shall contain the preferred resource management mechanism by the home network, which shall be used for the session and may include values 1 to 3. The format is Ulong.
cdma-disconnect-reason	Indicates the reason for disconnecting the user. This attribute may be included in a RADIUS Disconnect-Request message from Home RADIUS server to the PDSN. The format is Ulong.

Field	Description
mip-key-data	This is the key data payload containing the encrypted MN_AAA key, MN_HA key, CHAP key, MN_Authenticator, and AAA_Authenticator. The format is Binary.
aaa-authenticator	This is the 64-bit AAA_Authenticator value decrypted by the Home RADIUS AAA Server. The format is Binary.
public-key-invalid	The home RADIUS AAA Server includes this attribute to indicate that the Public key used by the MN is not valid. The format is Binary.

Related Commands

Command	Description
show radius	Displays information about the RADIUS servers that are configured in the system.

show redundancy application asymmetric-routing

To display asymmetric routing information for a redundancy group, use the **show redundancy application asymmetric-routing** command in user EXEC or privileged EXEC mode.

show redundancy application asymmetric-routing {**interface** | **tunnel**} **group** *id*

Syntax Description

interface	Displays asymmetric routing interface information.
tunnel	Displays asymmetric routing tunnel information.
group *id*	Displays information about the redundancy group.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
15.2(3)T	This command was introduced.

Examples

The following is sample output from the **show redundancy application asymmetric-routing interface group** command:

```
Device# show redundancy application asymmetric-routing interface group 1

AR Group ID:1 interface Ethernet1/1
neighbor 10.3.3.2,
  transport context:
    my ip 10.9.9.1, my port 53000
    peer ip 10.9.9.2, peer port 53000
```

The following is sample output from the **show redundancy application asymmetric-routing tunnel group** command:

```
Device# show redundancy application asymmetric-routing tunnel group 1

Group ID:1
  rii  1000, idb Ethernet1/2
        packet sent: 0, packet received: 0
        byte sent:   0, byte recv:       0
        encap: length 32
         IP :45 00 00 00 00 00 00 00 FF 11 00 00 09 09 09 01 09 09 09 02
         UDP:CF 08 CF 08 00 00 00 00
         AR :00 01 03 E8
```

The following table describes the significant fields shown in the displays.

Table 40: show redundancy application asymmetric-routing Field Descriptions

Field	Description
AR Group ID	The identifier for the asymmetric routing redundancy group.

Field	Description
interface	The interface type and number.
neighbor	The IP address of the peer redundancy group's control interface.
transport context:	The IP address of the asymmetric routing interface and the IP address of the peer asymmetric routing interface are displayed under the transport context.
Group ID	The identifier for the asymmetric routing redundancy group.
rii	The redundancy interface identifier.

Related Commands

Command	Description
redundancy application asymmetric-routing	Associates a redundancy group with an interface that is used for asymmetric routing.

show redundancy application control-interface group

To display control interface information for a redundancy group, use the **show redundancy application control-interface group** command in privileged EXEC mode.

show redundancy application control-interface group [*group-id*]

Syntax Description

group-id	(Optional) Redundancy group ID. Valid values are 1 and 2.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

The **show redundancy application control-interface**command shows information for the redundancy group control interfaces.

Examples

The following is sample output from the **show redundancy application control-interface** command:

```
Router# show redundancy application control-interface group 2
The control interface for rg[2] is GigabitEthernet0/1/0
Interface is Control interface associated with the following protocols: 2 1
BFD Enabled
Interface Neighbors:
```

Related Commands

Command	Description
show redundancy application faults	Displays fault-specific information for a redundancy group.
show redundancy application group	Displays redundancy group information.
show redundancy application if-mgr	Displays if-mgr information for a redundancy group.
show redundancy application protocol	Displays protocol-specific information for a redundancy group.

show redundancy application data-interface

To display data interface-specific information, use the **show redundancy application data-interface**command in privileged EXEC mode.

show redundancy application data-interface group [*group-id*]

Syntax Description

group	Specifies the redundancy group.
group-id	(Optional) Redundancy group ID. Valid values are 1 and 2.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

The **show redundancy application data-interface** command displays information about the redundancy group data interfaces.

Examples

The following is sample output from the **show redundancy application data-interface** command:

```
Router# show redundancy application data-interface group 1
The data interface for rg[1] is GigabitEthernet0/1/1
```

Related Commands

Command	Description
show redundancy application control-interface	Displays control interface information for a redundancy group.
show redundancy application faults	Displays fault-specific information for a redundancy group.
show redundancy application group	Displays redundancy group information.
show redundancy application if-mgr	Displays if-mgr information for a redundancy group.
show redundancy application protocol	Displays protocol-specific information for a redundancy group.

show redundancy application faults group

To display fault-specific information for a redundancy group, use the **show redundancy application faults group**command in privileged EXEC mode.

show redundancy application faults group [*group-id*]

Syntax Description

group-id	(Optional) Redundancy group ID. Valid values are 1 and 2.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

The **show redundancy application faults**command shows information returned by redundancy group faults.

Examples

The following is sample output from the **show redundancy application faults** command:

```
Router# show redundancy application faults group 2
Faults states Group 2 info:
        Runtime priority: [150]
                RG Faults RG State: Up.
                        Total # of switchovers due to faults:           2
                        Total # of down/up state changes due to faults: 2
```

Related Commands

Command	Description
show redundancy application control-interface	Displays control interface information for a redundancy group.
show redundancy application group	Displays redundancy group information.
show redundancy application if-mgr	Displays if-mgr information for a redundancy group.
show redundancy application protocol	Displays protocol-specific information for a redundancy group.

show redundancy application group

To display the redundancy group information, use the **show redundancy application group** command in privileged EXEC mode.

show redundancy application group [*group-id* | **all**]

Syntax Description

group-id	(Optional) Redundancy group ID. Valid values are 1 and 2.
all	(Optional) Display information about all redundancy groups.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.1S	This command was introduced.
15.3(2)T	This command was integrated into Cisco IOS Release 15.3(2)T.

Usage Guidelines

Use the **show redundancy application group** command to display the current state of each interbox redundancy group on the device and the peer device.

Examples

The following is sample output from the **show redundancy application group all** command:

```
Device# show redundancy application group all

Faults states Group 1 info:
        Runtime priority: [200]
                RG Faults RG State: Up.
                        Total # of switchovers due to faults:           3
                        Total # of down/up state changes due to faults: 2
Group ID:1
Group Name:grp2
Administrative State: No Shutdown
Aggregate operational state : Up
My Role: ACTIVE
Peer Role: UNKNOWN
Peer Presence: No
Peer Comm: No
Peer Progression Started: No
RF Domain: btob-one
         RF state: ACTIVE
         Peer RF state: DISABLED
RG Protocol RG 1
------------------
        Role: Active
        Negotiation: Enabled
        Priority: 200
        Protocol state: Active
        Ctrl Intf(s) state: Down
        Active Peer: Local
        Standby Peer: Not exist
        Log counters:
```

```
                role change to active: 2
                role change to standby: 0
                disable events: rg down state 1, rg shut 0
                ctrl intf events: up 0, down 2, admin_down 1
                reload events: local request 3, peer request 0
RG Media Context for RG 1
--------------------------
        Ctx State: Active
        Protocol ID: 1
        Media type: Default
        Control Interface: GigabitEthernet0/1/0
        Hello timer: 5000
        Effective Hello timer: 5000, Effective Hold timer: 15000
         LAPT values: 0, 0
        Stats:
                Pkts 0, Bytes 0, HA Seq 0, Seq Number 0, Pkt Loss 0
                Authentication not configured
                Authentication Failure: 0
                Reload Peer: TX 0, RX 0
                Resign: TX 1, RX 0
        Standby Peer: Not Present.
Faults states Group 2 info:
        Runtime priority: [150]
                RG Faults RG State: Up.
                        Total # of switchovers due to faults:           2
                        Total # of down/up state changes due to faults: 2
Group ID:2
Group Name:name1
Administrative State: No Shutdown
Aggregate operational state : Up
My Role: ACTIVE
Peer Role: UNKNOWN
Peer Presence: No
Peer Comm: No
Peer Progression Started: No
RF Domain: btob-two
         RF state: ACTIVE
         Peer RF state: DISABLED
RG Protocol RG 2
------------------
        Role: Active
        Negotiation: Enabled
        Priority: 150
        Protocol state: Active
        Ctrl Intf(s) state: Down
        Active Peer: Local
        Standby Peer: Not exist
        Log counters:
                role change to active: 1
                role change to standby: 0
                disable events: rg down state 1, rg shut 0
                ctrl intf events: up 0, down 2, admin_down 1
                reload events: local request 2, peer request 0
RG Media Context for RG 2
--------------------------
        Ctx State: Active
        Protocol ID: 2
        Media type: Default
        Control Interface: GigabitEthernet0/1/0
        Hello timer: 5000
        Effective Hello timer: 5000, Effective Hold timer: 15000
         LAPT values: 0, 0
        Stats:
                Pkts 0, Bytes 0, HA Seq 0, Seq Number 0, Pkt Loss 0
```

```
            Authentication not configured
            Authentication Failure: 0
            Reload Peer: TX 0, RX 0
            Resign: TX 0, RX 0
    Standby Peer: Not Present.
```

The table below describes the significant fields shown in the display.

Table 41: show redundancy application group all Field Descriptions

Field	Description
Faults states Group 1 info	Redundancy group faults information for Group 1.
Runtime priority	Current priority of the redundancy group.
RG Faults RG State	Redundancy group state returned by redundancy group faults.
Total # of switchovers due to faults	Number of switchovers triggered by redundancy group fault events.
Total # of down/up state changes due to faults	Number of down and up state changes triggered by redundancy group fault events.
Group ID	Redundancy group ID.
Group Name	Redundancy group name.
Administrative State	Redundancy group state configured by users.
Aggregate operational state	Current redundancy group state.
My Role	Current role of the device.
Peer Role	Current role of the peer device.
Peer Presence	Indicates if the peer device is detected or not.
Peer Comm	Indicates the communication state with the peer device.
Peer Progression Started	Indicates if the peer device has started Redundancy Framework (RF) progression.
RF Domain	Name of the RF domain for the redundancy group.

Related Commands

Command	Description
show redundancy application control-interface	Displays control interface information for a redundancy group.
show redundancy application faults	Displays fault-specific information for a redundancy group.
show redundancy application if-mgr	Displays if-mgr information for a redundancy group.

Command	Description
show redundancy application protocol	Displays protocol-specific information for a redundancy group.

show redundancy application if-mgr

To display interface manager information for a redundancy group, use the **show redundancy application if-mgr** command in privileged EXEC mode.

show redundancy application if-mgr group [*group-id*]

Syntax Description

group	Specifies the redundancy group.
group-id	(Optional) Redundancy group ID. Valid values are 1 to 2.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

The **show redundancy application if-mgr** command shows information of traffic interfaces protected by redundancy groups. When a traffic interface is functioning with the redundancy group, the state is no shut on the active device, and shut on the standby device. On the other hand, it is always shut on the standby device.

Examples

The following is sample output from the **show redundancy application if-mgr** command:

```
Router# show redundancy application if-mgr group 2
RG ID: 2
 Interface       VIP         VMAC        Shut   Decrement
 ============================================================
 GigabitEthernet0/1/7 10.1.1.3 0007.b422.0016  no shut    50
 GigabitEthernet0/3/1 11.1.1.3 0007.b422.0017  no shut    50
```

The table below describes the significant fields shown in the display.

Table 42: show redundancy application if-mgr Field Descriptions

Field	Description
RG ID	Redundancy group ID.
Interface	Interface name.
VIP	Virtual IP address for this traffic interface.
VMAC	Virtual MAC address for this traffic interface.
Shut	The state of this interface. **Note** It is always “shut” on the standby box.
Decrement	The decrement value for this interface. When this interface goes down, the runtime priority of its redundancy group decreases.

Related Commands

Command	Description
show redundancy application control-interface	Displays control interface information for a redundancy group.
show redundancy application faults	Displays fault-specific information for a redundancy group.
show redundancy application group	Displays redundancy group information.
show redundancy application protocol	Displays protocol-specific information for a redundancy group

show redundancy application protocol

To display protocol-specific information for a redundancy group, use the **show redundancy application protocol**command in privileged EXEC mode.

show redundancy application protocol {*protocol-id* | **group** [*group-id*] }

Syntax Description

protocol-id	Protocol ID. The range is from 1 to 8.
group	Specifies the redundancy group.
group-id	(Optional) Redundancy group ID. Valid values are 1 and 2.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

The **show redundancy application protocol**command shows information returned by redundancy group protocol.

Examples

The following is sample output from the **show redundancy application protocol** command:

```
Router# show redundancy application protocol 3

Protocol id: 3, name:
 BFD: ENABLE
 Hello timer in msecs: 0
 Hold timer in msecs: 0
```

The table below describes the significant fields shown in the display.

Table 43: show redundancy application protocol Field Descriptions

Field	Description
Protocol id	Redundancy group protocol ID.
BFD	Indicates whether the BFD protocol is enabled for the redundancy group protocol.
Hello timer in msecs	Redundancy group hello timer, in milliseconds, for the redundancy group protocol. The default is 3000 msecs.
Hold timer in msecs	Redundancy group hold timer, in milliseconds, for the redundancy group protocol. The default is 10000 msecs.

Related Commands

Command	Description
show redundancy application group	Displays redundancy group information.
show redundancy application control-interface	Displays control interface information for a redundancy group.
show redundancy application faults	Displays fault-specific information for a redundancy group.
show redundancy application if-mgr	Displays if-mgr information for a redundancy group.

show redundancy application transport

To display transport-specific information for a redundancy group, use the **show redundancy application transport**command in privileged EXEC mode.

show redundancy application transport {**client** | **group** [*group-id*]}

Syntax Description

client	Displays transport client-specific information.
group	Displays the redundancy group name.
group-id	(Optional) Redundancy group ID. Valid values are 1 and 2.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

The **show redundancy application transport** command shows information for redundancy group transport.

Examples

The following is sample output from the **show redundancy application transport group** command:

```
Router# show redundancy application transport group 1
Transport Information for RG (1)
```

Related Commands

Command	Description
show redundancy application control-interface	Displays control interface information for a redundancy group.
show redundancy application faults	Displays fault-specific information for a redundancy group.
show redundancy application group	Displays redundancy group information.
show redundancy application if-mgr	Displays if-mgr information for a redundancy group.
show redundancy application protocol	Displays protocol-specific information for a redundancy group.

show redundancy linecard-group

To display the components of a Blade Failure Group, use the **show redundancy linecard-group** command in privileged EXEC mode.

show redundancy linecard-group *group-id*

Syntax Description

group-id	Group ID.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)SXE2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

The following example shows the components of a Blade Failure Group:

```
Router# show redundancy linecard-group

1
Line Card Redundancy Group:1 Mode:feature-card
Class:load-sharing
Cards:
Slot:3 Subslot:0
Slot:5 Subslot:0
```

Related Commands

Command	Description
linecard-group feature card	Assigns a group ID to a Blade Failure Group.

show running-config

To display the contents of the current running configuration file or the configuration for a specific module, Layer 2 VLAN, class map, interface, map class, policy map, or virtual circuit (VC) class, use the **show running-config** command in privileged EXEC mode.

show running-config [*options*]

Syntax Description

options	(Optional) Keywords used to customize output. You can enter more than one keyword. • **all** --Expands the output to include the commands that are configured with default parameters. If the **all** keyword is not used, the output does not display commands configured with default parameters. • **brief** --Displays the configuration without certification data and encrypted filter details. The **brief** keyword can be used with the **linenum** keyword. • **class-map** [*name*][**linenum**]--Displays class map information. The **linenum** keyword can be used with the **class-map** *name* option. • **control-plane** [**cef-exception**| **host**| **transit**]--Displays control-plane information. The **cef-exception**, **host**, and **transit** keywords can be used with the **control-plane** option. • **flow** {**exporter** | **monitor** | **record**}--Displays global flow configuration commands. The **exporter**, **monitor**, and **record**keywords can be used with the **flow** option. • **full** --Displays the full configuration. • **interface** *type number* -- Displays interface-specific configuration information. If you use the **interface** keyword, you must specify the interface type and the interface number (for example, **interface ethernet 0**). Keywords for common interfaces include **async**, **ethernet**, **fastEthernet**, **group-async**, **loopback**, **null**, **serial**, and **virtual-template**. Use the **show run interface ?**command to determine the interfaces available on your system. • **linenum** --Displays line numbers in the output. The **brief** or **full** keyword can be used with the **linenum** keyword. The **linenum**keyword can be used with the **class-map**, **interface**, **map-class**, **policy-map**, and **vc-class** keywords. • **map-class** [**atm** | **dialer** | **frame-relay**] [**name**] [**linenum**]--Displays map class information. This option is described separately; see the **show running-config map-class** command page.
	• **partition types** -- Displays the configuration corresponding to a partition. The **types** keyword can be used with the **partition**option. • **policy-map** [*name*][**linenum**]--Displays policy map information. The **linenum** keyword can be used with the **policy-map** *name* option. • **vc-class** [*name*] [**linenum**]--Displays VC-class information (the display is available only on certain devices such as the Cisco 7500 series devices). The **linenum** keyword can be used with the **vc-class** *name* option.

	• **view full** --Enables the display of a full running configuration. This is for view-based users who typically can only view the configuration commands that they are entitled to access for that particular view. • **vrf** *name* --Displays the Virtual routing and forwarding (VRF)-aware configuration module number . • **vlan** [*vlan-id*]--Displays the specific VLAN information ; valid values are from 1 to 4094.

Command Default

The default syntax, **show running-config**, displays the contents of the running configuration file, except commands configured using the default parameters.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.0	This command was introduced.
12.0	This command was replaced by the **more system:running-config** command.
12.0(1)T	This command was integrated into Cisco IOS Release 12.0(1)T, and the output modifier (|) was added.
12.2(4)T	This command was modified. The **linenum** keyword was added.
12.3(8)T	This command was modified. The **view full**option was added.
12.2(14)SX	This command was integrated into Cisco IOS Release 12.2(14)SX. The **module** *number* and **vlan** *vlan-id* keywords and arguments were added for the Supervisor Engine 720.
12.2(17d)SXB	This command was integrated into Release 12.2(17d)SXB and implemented on the Supervisor Engine 2.
12.2(33)SXH	This command was modified. The **all**keyword was added.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2. This command was enhanced to display the configuration information for traffic shaping overhead accounting for ATM and was implemented on the Cisco 10000 series device for the PRE3.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.2(33)SB	This command was modified. Support for the Cisco 7300 series device was added.
12.4(24)T	This command was modified in a release earlier than Cisco IOS Release 12.4(24)T. The **partition** and **vrf** keywords were added. The **module** and **vlan** keywords were removed.
15.0(1)M	This command was modified. The output was modified to include encrypted filter information.
12.2(33)SXI	This command was modified. The output was modified to display Access Control List (ACL) information.

Usage Guidelines

The **show running-config** command is technically a command alias (substitute or replacement syntax) of the **more system:running-config** command. Although the use of more commands is recommended (because of

their uniform structure across platforms and their expandable syntax), the **show running-config** command remains enabled to accommodate its widespread use, and to allow typing shortcuts such as **show run**.

The **show running-config interface** command is useful when there are multiple interfaces and you want to look at the configuration of a specific interface.

The **linenum** keyword causes line numbers to be displayed in the output. This option is useful for identifying a particular portion of a very large configuration.

You can enter additional output modifiers in the command syntax by including a pipe character (|) after the optional keyword. For example, **show running-config interface serial 2/1 linenum | begin 3**. To display the output modifiers that are available for a keyword, enter **| ?** after the keyword. Depending on the platform you are using, the keywords and the arguments for the *options* argument may vary.

Prior to Cisco IOS Release 12.2(33)SXH, the **show running-config**command output omitted configuration commands set with default values. Effective with Cisco IOS Release 12.2(33)SXH, the **show running-config all** command displays complete configuration information, including the default settings and values. For example, if the Cisco Discovery Protocol (abbreviated as CDP in the output) hold-time value is set to its default of 180:

- The **show running-config** command does not display this value.
- The **show running-config all** displays the following output: cdp holdtime 180.

If the Cisco Discovery Protocol holdtime is changed to a nondefault value (for example, 100), the output of the **show running-config** and **show running-config all**commands is the same; that is, the configured parameter is displayed.

Note In Cisco IOS Release 12.2(33)SXH, the **all**keyword expands the output to include some of the commands that are configured with default values. In subsequent Cisco IOS releases, additional configuration commands that are configured with default values will be added to the output of the **show running-config all**command.

Effective with Cisco IOS Release 12.2(33)SXI, the **show running-config** command displays ACL information. To exclude ACL information from the output, use the **show running** | **section exclude ip access** | **access list**command.

Cisco 7600 Series Device

In some cases, you might see a difference in the duplex mode that is displayed between the **show interfaces** command and the **show running-config** command. The duplex mode that is displayed in the **show interfaces** command is the actual duplex mode that the interface is running. The **show interfaces** command displays the operating mode of an interface, and the **show running-config** command displays the configured mode of the interface.

The **show running-config** command output for an interface might display the duplex mode but no configuration for the speed. This output indicates that the interface speed is configured as auto and that the duplex mode that is displayed becomes the operational setting once the speed is configured to something other than auto. With this configuration, it is possible that the operating duplex mode for that interface does not match the duplex mode that is displayed with the **show running-config** command.

Examples

The following example shows the configuration for serial interface 1. The fields are self-explanatory.

```
Device# show running-config interface serial 1
```

```
Building configuration...
Current configuration:
!
interface Serial1
 no ip address
 no ip directed-broadcast
 no ip route-cache
 no ip mroute-cache
 shutdown
end
```

The following example shows the configuration for Ethernet interface 0/0. Line numbers are displayed in the output. The fields are self-explanatory.

```
Device# show running-config interface ethernet 0/0 linenum
Building configuration...
Current configuration : 104 bytes
 1 : !
 2 : interface Ethernet0/0
 3 :  ip address 10.4.2.63 255.255.255.0
 4 :  no ip route-cache
 5 :  no ip mroute-cache
 6 : end
```

The following example shows how to set line numbers in the command output and then use the output modifier to start the display at line 10. The fields are self-explanatory.

```
Device# show running-config linenum | begin 10

   10 : boot-start-marker
   11 : boot-end-marker
   12 : !
   13 : no logging buffered
   14 : enable password #####
   15 : !
   16 : spe 1/0 1/7
   17 :  firmware location bootflash:mica-modem-pw.172.16.0.0.bin
   18 : !
   19 : !
   20 : resource-pool disable
   21 : !
   22 : no aaa new-model
   23 : ip subnet-zero
   24 : ip domain name cisco.com
   25 : ip name-server 172.16.11.48
   26 : ip name-server 172.16.2.133
   27 : !
   28 : !
   29 : isdn switch-type primary-5ess
   30 : !
   .
   .
   .
   126 : end
```

The following example shows how to display the module and status configuration for all modules on a Cisco 7600 series device. The fields are self-explanatory.

```
Device#
show running-config
Building configuration...
Current configuration:
```

```
!
version 12.0
service timestamps debug datetime localtime
service timestamps log datetime localtime
no service password-encryption
!
hostname device
!
boot buffersize 126968
boot system flash slot0:7600r
boot bootldr bootflash:c6msfc-boot-mz.120-6.5T.XE1.0.83.bin
enable password lab
!
clock timezone Pacific -8
clock summer-time Daylight recurring
redundancy
 main-cpu
  auto-sync standard
!
ip subnet-zero
!
ip multicast-routing
ip dvmrp route-limit 20000
ip cef
mls flow ip destination
mls flow ipx destination
cns event-service server
!
spanning-tree portfast bpdu-guard
spanning-tree uplinkfast
spanning-tree vlan 200 forward-time 21
port-channel load-balance sdip
!
!
!
 shutdown
!
!
.
.
.
```

In the following sample output from the **show running-config** command, the **shape average**command indicates that the traffic shaping overhead accounting for ATM is enabled. The BRAS-DSLAM encapsulation type is qinq and the subscriber line encapsulation type is snap-rbe based on the ATM adaptation layer 5 (AAL5) service. The fields are self-explanatory

```
Device# show running-config
.
.
.
subscriber policy recording rules limit 64
no mpls traffic-eng auto-bw timers frequency 0
call rsvp-sync
!
controller T1 2/0
framing sf
linecode ami
!
controller T1 2/1
framing sf
linecode ami
!
```

```
!
policy-map unit-test
class class-default
shape average percent 10 account qinq aal5 snap-rbe
!
```

The following is sample output from the **show running-config class-map** command. The fields in the display are self-explanatory.

```
Device# show running-config class-map
Building configuration...
Current configuration : 2910 bytes
!
class-map type stack match-all ip_tcp_stack
 match field IP protocol eq 0x6 next TCP
class-map type access-control match-all my
 match field UDP dest-port eq 1111
 match encrypted
  filter-version 0.1, Dummy Filter 2
  filter-id      123
  filter-hash    DE0EB7D3C4AFDD990038174A472E4789
  algorithm      aes256cbc
  cipherkey      realm-cisco.sym
  ciphervalue    #
oeahb4L6JK+XuC0q8k9AqXvBeQWzVfdg8WV67WEXbiWdXGQs6BEXqQeb4Pfow570zM4eDw0gxlp/Er8w
/lXsmolSgYpYuxFMYb1KX/H2iCXvA76VX7w5TElb/+6ekgbfP/d5ms6DEzKa8DlOpl+Q95lP194PsIlU
wCyfVCwLS+T8p3RDLi8dKBgQMcDW4Dha1ObBJTpV4zpwhEdMvJDu5PATtEQhFjhN/UYeyQiPRthjbkJn
LzT8hQFxwYwVW8PCjkyqEwYrr+R+mFG/C7tFRiooaW9MU9PCpFd95FARvlU=#
  exit
class-map type stack match-all ip_udp_stack
 match field IP protocol eq 0x11 next UDP
class-map type access-control match-all psirt1
 match encrypted
  filter-version 0.0_DummyVersion_20090101_1830
  filter-id      cisco-sa-20090101-dummy_ddts_001
  filter-hash    FC50BED10521002B8A170F29AF059C53
  algorithm      aes256cbc
  cipherkey      realm-cisco.sym
  ciphervalue    #
DkGbVq0FPAsVJKguU15lQPDfZyTcHUXWsj8+tD+dCSYW9cjkRU9jyST4vO4u69/L62QlbyQuKdyQmb10
6sAeY5vDsDfDV05k4o5eD+j8cMt78iZT0Qg7uGiBSYBbak3kKn/5w2gDd1vnivyQ7g4Ltd9+XM+GP6XL
27RrXeP5A5iGbzC7KI9t6riZXk0gmR/vFw1a5wck0D/iQHIlFa/yRPoKMSFlqfIlLTe5NM7JArSTKET2
pu7wZammTz4FF6rY#
  exit
 match start TCP payload-start offset 0 size 10 regex "abc.*def"
 match field TCP source-port eq 1234
class-map type access-control match-all psirt2
 match encrypted
  filter-version 0.0_DummyVersion_20090711_1830
  filter-id      cisco-sa-20090711-dummy_ddts_002
  filter-hash    DE0EB7D3C4AFDD990038174A472E4789
  algorithm      aes256cbc
  cipherkey      realm-cisco.sym
```

The following example shows that the teletype (tty) line 2 is reserved for communicating with the 2nd core:

```
Device# show running
Building configuration...

Current configuration:
!
```

```
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname device
!
enable password lab
!
no ip subnet-zero
!
!
!
interface Ethernet0
 ip address 172.25.213.150 255.255.255.128
 no ip directed-broadcast
 no logging event link-status
!
interface Serial0
 no ip address
 no ip directed-broadcast
 no ip mroute-cache
 shutdown
 no fair-queue
!
interface Serial1
 no ip address
 no ip directed-broadcast
 shutdown
!
ip default-gateway 172.25.213.129
ip classless
ip route 0.0.0.0 0.0.0.0 172.25.213.129
!
!
line con 0
 transport input none
line 1 6
 no exec
 transport input all
line 7
 no exec
 exec-timeout 300 0
 transport input all
line 8 9
 no exec
 transport input all
line 10
 no exec
 transport input all
 stopbits 1
line 11 12
 no exec
 transport input all
line 13
 no exec
 transport input all
 speed 115200
line 14 16
 no exec
 transport input all
line aux 0
line vty 0 4
 password cisco
```

```
 login
!
end
```

Related Commands

Command	Description
bandwidth	Specifies or modifies the bandwidth allocated for a class belonging to a policy map, and enables ATM overhead accounting.
boot config	Specifies the device and filename of the configuration file from which the device configures itself during initialization (startup).
configure terminal	Enters global configuration mode.
copy running-config startup-config	Copies the running configuration to the startup configuration. (Command alias for the **copy system:running-config nvram:startup-config** command.)
shape	Shapes traffic to the indicated bit rate according to the algorithm specified, and enables ATM overhead accounting.
show interfaces	Displays statistics for all interfaces configured on the device or access server.
show policy-map	Displays the configuration of all classes for a specified service policy map or all classes for all existing policy maps, and displays ATM overhead accounting information, if configured.
show startup-config	Displays the contents of NVRAM (if present and valid) or displays the configuration file pointed to by the CONFIG_FILE environment variable. (Command alias for the **more:nvram startup-config** command.)

show running-config vrf

To display the subset of the running configuration of a router that is linked to a specific VPN routing and forwarding (VRF) instance or linked to all VRFs configured on the router, use the **show running-config vrf** command in privileged EXEC mode.

show running-config vrf [*vrf-name*]

Syntax Description

vrf-name	(Optional) Name of the VRF configuration that you want to display.

Command Default

If you do not specify the name of a VRF configuration, the running configurations of all VRFs on the router are displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(28)SB	This command was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.
Cisco IOS XE Release 3.5S	This command was modified. The output of the command was modified to display the Network Address Translation (NAT) configuration.

Usage Guidelines

Use the **show running-config vrf** command to display a specific VRF configuration or to display all VRF configurations on the router. To display the configuration of a specific VRF, specify the name of the VRF.

This command displays the following elements of the VRF configuration:

- The VRF submode configuration.
- The routing protocol and static routing configurations associated with the VRF.
- The configuration of interfaces in the VRF, which includes the configuration of any owning controller and physical interface for a subinterface.

Examples

The following is sample output from the **show running-config vrf** command. It includes a base VRF configuration for VRF vpn3 and Border Gateway Protocol (BGP) and Open Shortest Path First (OSPF) configurations associated with VRF vpn3.

```
Router# show running-config vrf vpn3

Building configuration...

Current configuration : 720 bytes
```

```
ip vrf vpn3
 rd 100:1
 route-target export 100:1
 route-target import 100:1
!
!
interface GigabitEthernet0/0/1
 description connected to nat44-1ru-ce1 g0/0/0
 ip vrf forwarding vpn3
 ip address 172.17.0.1 255.0.0.0
 ip nat inside
 shutdown
 negotiation auto
!
interface GigabitEthernet0/0/3
 no ip address
 negotiation auto
!
interface GigabitEthernet0/0/3.2
 encapsulation dot1Q 2
 ip vrf forwarding vpn3
 ip address 10.0.0.1 255.255.255.0
 ip nat inside
!
router bgp 100
 !
 address-family ipv4 vrf vpn3
  redistribute connected
  redistribute static
 exit-address-family
ip nat inside source route-map rm-vpn3 pool shared-pool vrf vpn3 match-in-vrf overload
ip nat pool shared-pool 10.0.0.2 10.0.0.254 prefix-length 24
!
router ospf 101 vrf vpn3
 log-adjacency-changes
 area 1 sham-link 10.43.43.43 10.23.23.23 cost 10
 network 172.17.0.0 0.255.255.255 area 1
.
.
.
end
```

The table below describes the significant fields shown in the display.

Table 44: show running-config vrf Field Descriptions

Field	Description
Current configuration: 720 bytes	Indicates the number of bytes (720) in the VRF vpn3 configuration.
ip vrf vpn3	Indicates the name of the VRF (vpn3) for which the configuration is displayed.
rd 100:1	Identifies the route distinguisher (100:1) for VRF vpn3.
route-target export 100:1 route-target import 100:1	Specifies the route-target extended community for VRF vpn3. • Routes tagged with route-target export 100:1 are exported from VRF vpn3. • Routes tagged with the route-target import 100:1 are imported into VRF vpn3.

Field	Description
interface GigabitEthernet0/0/1	Specifies the interface associated with VRF vpn3.
ip vrf forwarding vpn3	Associates VRF vpn3 with the named interface.
ip address 172.17.0.1 255.0.0.0	Configures the IP address of the Gigabit Ethernet interface.
ip nat inside	Enables NAT of inside addresses.
router bgp 100	Sets up a BGP routing process for the router with the autonomous system number as 100.
address-family ipv4 vrf vpn3	Sets up a routing session for VRF vpn3 using the standard IPv4 address prefixes.
redistribute connected	Redistributes routes that are automatically established by the IP on an interface into the BGP routing domain.
ip nat pool	Defines a pool of IP addresses for NAT.
router ospf 101 vrf vpn3	Sets up an OSPF routing process and associates VRF vpn3 with OSPF VRF processes.
area 1 sham-link 10.43.43.43 10.23.23.23 cost 10	Configures a sham-link interface on a provider edge (PE) router in a Multiprotocol Label Switching (MPLS) VPN backbone. • 1 is the ID number of the OSPF area assigned to the sham-link. • 10.43.43.43 is the IP address of the source PE router. • 10.23.23.23 is the IP address of the destination PE router. • 10 is the OSPF cost to send IP packets over the sham-link interface.
network 172.17.0.0 0.255.255.255 area 1	Defines the interfaces on which OSPF runs and defines the area ID for those interfaces.

Related Commands

Command	Description
ip vrf	Configures a VRF routing table.
show ip interface	Displays the usability status of interfaces configured for IP.
show ip vrf	Displays the set of defined VRFs and associated interfaces.
show running-config interface	Displays the configuration for a specific interface.

show sasl

To display Simple Authentication and Security Layer (SASL) information, use the **show sasl** command in user EXEC or privileged EXEC mode.

show sasl {**all** | **context** | **mechanisms** | **profile** {*profile-name* | **all**}}

Syntax Description

all	Displays detailed information for all SASL profiles.
context	Displays context information for SASL profiles.
mechanisms	Displays the mechanisms applied for all SASL profiles.
profile *profile-name*	Displays detailed information for the specified SASL profile.
profile all	Displays all configured profiles.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
12.3(1)	This command was introduced.
12.2(33)SRC	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SRC.
12.2(33)SXI	This command was integrated into a release earlier than Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1.

Examples

The following is sample output from the **show sasl profile all** command:

```
Router# show sasl profile all
SASL profile 'sgw_sasl' Refs:0 Mechs:0x2
    client:  <NONE>/<NONE>
    servers: ravi/ravi

SASL profile 'sgw_1' Refs:0 Mechs:0x1
    client:  us1/pw1
    servers: server1/user
```

The table below describes the significant fields shown in the display.

Table 45: show sasl profile all Field Descriptions

Field	Description
SASL profile	Indicates the name of the SASL profile.

Field	Description
Refs	Indicates the number of active sessions.
Mechs	Indicates the profile mechanisms configured.
client	Indicates the SASL client configured for the specified profile.
servers	Indicates the SASL server configured for the specified profile.

Related Commands

Command	Description
sasl	Configures SASL.

show secure bootset

To display the status of Cisco IOS image and configuration resilience, use the **show secure**command in privileged EXEC mode.

show secure bootset

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

Use the **show secure bootset**command, instead of the Cisco IOS directory listing **dir** command, to verify the existence of an image archive. This command also displays output that specifies whether the image or configuration archive is ready for an upgrade.

Examples

The following is sample output from the **show secure bootset** command. The field descriptions are self-explanatory:

```
Router# show secure bootset
%IOS image and configuration resilience is not active
Router# show secure bootset
IOS resilience router id JMX0704L5GH
IOS image resilience version 12.3 activated at 08:16:51 UTC Sun Jun 16 2002
Secure archive slot0:c3745-js2-mz type is image (elf) []
  file size is 25469248 bytes, run size is 25634900 bytes
  Runnable image, entry point 0x80008000, run from ram
IOS configuration resilience version 12.3 activated at 08:17:02 UTC Sun Jun 16 2002
Secure archive slot0:.runcfg-20020616-081702.ar type is config
configuration archive size 1059 bytes
```

Related Commands

Command	Description
dir	Displays a list of files on a file system.
secure boot-config	Saves a secure copy of the router running configuration in persistent storage.
secure boot-image	Enables Cisco IOS image resilience.

show smm

To display string matching module (SMM) information, use the **show smm** command in privileged EXEC mode.

show smm {**counters** | **timing** | **tree** [*tree-index* | **details**]}

Syntax Description

counters	Displays information about SMM counters.
timing	Displays timing information about the SMM.
tree	Displays the AVL tree containing the string information.
tree-index	(Optional) Specifies the tree index.
details	(Optional) Displays detailed information about the AVL tree.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.0(1)	This command was introduced in a release earlier than Cisco IOS Release 15.0(1) on Cisco 3845 series routers.

Examples

The following is sample output from the **show smm counters** command. Fields in the output are self-explanatory.

```
Router# show smm counters

Number of non-matching packets processed   - 0
Number of cache hits                       - 0
Number of cache misses                     - 0
Cache full instances                       - 0
Number of matching packets processed       - 0
Number of matches for Stage0               - 0
Number of matches for Stage1               - 0
Number of matches for Stage2               - 0
Number of matches for Stage3               - 0
Number of signatures in signature database - 0
```

The following is sample output from the **show smm timing** command:

```
Router# show smm timing
Packet processing stats (in microseconds) :
-------------------------------------------
Minimum processing time per packet - 0
Maximum processing time per packet - 0
Average processing time for non-matching packets - 0
Average processing time for matching packets     - 0
```

Related Commands

Command	Description
action string match	Returns 1 to the $_string_result, if the string matches the pattern when an EEM applet is triggered.

show snmp mib nhrp status

To display status information about the Next Hop Resolution Protocol (NHRP) MIB, use the **show snmp mib nhrp** status command in privileged EXEC mode.

show snmp mib nhrp status

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

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

Usage Guidelines

This command is used to display the status of the MIB for NHRP and whether the NHRP MIB is enabled or disabled.

Examples

The following output is from the show snmp mib nhrp status command:

```
Spoke_103# show snmp mib nhrp status
NHRP-SNMP Agent Feature: Enabled
NHRP-SNMP Tree State: Good
ListEnqueue Count = 0 Node Malloc Counts = 1
Spoke_103#
```

Table 1 describes the significant fields shown in the display.

Table 46: show snmp mib nhrp status Field Descriptions

Field	Description
NHRP-SNMP Agent Feature:	Shows the status of the NHRP MIB. "Enabled" indicates that the NHRP MIB is enabled. If the NHRP MIB was disabled, it would display "Disabled".
ListEnqueue Count	Indicates how many nodes have been queued for freeing.
Node Malloc Counts	Indicates how many nodes are allocated.

Related Commands

Command	Description
show snmp mib	Displays a list of the MIB OIDs registered on the system.

show ssh

To display the status of Secure Shell (SSH) server connections on the router, use the **show ssh** command in user EXEC or privileged EXEC mode.

show ssh vty [*ssh-number*]

Syntax Description

vty	Displays virtual terminal line (VTY) connection details.
ssh-number	(Optional) The number of SSH server connections on the router. Range is from 0 to 1510. The default value is 0.

Command Modes

User Exec (>)
Privileged EXEC (#)

Command History

Release	Modification
12.1(15)T	This command was introduced.
12.2(33)SRA	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXI	This command was modified. It was integrated into Cisco IOS Release 12.2(33)SXI.
Cisco IOS XE Release 2.1	This command was modified. It was integrated into Cisco IOS XE Release 2.1.

Usage Guidelines

Use the **show ssh** command to display the status of the SSH connections on your router. This command does not display any SSH configuration data. Use the **show ip ssh** command for SSH configuration information such as timeouts and retries.

Examples

The following is sample output from the **show ssh** command with SSH enabled:

```
Router# show ssh
Connection     Version      Encryption     State                Username
0               1.5         3DES           Session Started       guest
```

The table below describes the significant fields shown in the display.

Table 47: show ssh Field Descriptions

Field	Description
Connection	Number of SSH connections on the router.
Version	Version number of the SSH terminal.
Encryption	Type of transport encryption.

Field	Description
State	The status of SSH connection to indicate if the session has started or stopped.
Username	Uesrname to log in to the SSH.

Related Commands

Command	Description
show ip ssh	Displays version and configuration data for SSH.

show ssl-proxy module state

To display the spanning-tree state for the specified VLAN, enter the **showssl-proxymodulestate** command in user EXEC mode.

show ssl-proxy module *mod* **state**

Syntax Description

mod	Module number.

Command Modes

User EXEC (>)

Command History

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

Usage Guidelines

This command is supported on Cisco 7600 series routers that are configured with a Secure Sockets Layer (SSL) Services Module only.

Examples

This example shows how to verify that the VLAN information displayed matches the VLAN configuration. The fields shown in the display are self-explanatory.

```
Router# show ssl-proxy module 6 state
SSL-services module 6 data-port:
 Switchport:Enabled
Administrative Mode:trunk
Operational Mode:trunk
Administrative Trunking Encapsulation:dot1q
Operational Trunking Encapsulation:dot1q
Negotiation of Trunking:Off
Access Mode VLAN:1 (default)
Trunking Native Mode VLAN:1 (default)
Trunking VLANs Enabled:100
Pruning VLANs Enabled:2-1001
Vlans allowed on trunk:100
Vlans allowed and active in management domain:100
Vlans in spanning tree forwarding state and not pruned:
100
Allowed-vlan :100
Router#
```

Related Commands

Command	Description
ssl-proxy module allowed-vlan	Adds the VLANs allowed over the trunk to the SSL Services Module.

show tacacs

To display statistics for a TACACS+ server, use the **show tacacs** command in privileged EXEC mode.

show tacacs [**private** | **public**]

Syntax Description

private	(Optional) Displays private tacacs+ server statistics.
public	(Optional) Displays public tacacs+ server statistics.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
11.2	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.3	This command was integrated into Cisco IOS XE Release 2.3. The **private** and **public** keywords were added.

Examples

The following example is sample output for the **show tacacs** command:

```
Router# show tacacs

Tacacs+ Server            : 172.19.192.80/49
              Socket opens:          3
             Socket closes:          3
             Socket aborts:          0
             Socket errors:          0
          Socket Timeouts:           0
   Failed Connect Attempts:          0
        Total Packets Sent:          7
        Total Packets Recv:          7
          Expected Replies:          0
  No current connection
```

he following is sample output from the **show tacacs** command for the private IP address 192.168.0.0:

```
Router# show tacacs private 192.168.0.0
Tacacs+ Server -  private  :  192.168.0.0
              Socket opens:          0
             Socket closes:          0
             Socket aborts:          0
             Socket errors:          0
          Socket Timeouts:           0
   Failed Connect Attempts:          0
```

```
        Total Packets Sent:          0
        Total Packets Recv:          0
```

The following is sample output from the **show tacacs** command for the public IP address 209.165.200.224:

```
Router# show tacacs public 209.165.200.224
Tacacs+ Server -  public  :  209.165.200.224
              Socket opens:          0
             Socket closes:          0
             Socket aborts:          0
             Socket errors:          0
          Socket Timeouts:           0
   Failed Connect Attempts:          0
        Total Packets Sent:          0
        Total Packets Recv:          0
```

The table below describes the significant fields shown in the display.

Table 48: show tacacs Field Descriptions

Field	Description
Tacacs+ Server	IP address of the TACACS+ server.
Socket opens	Number of successful TCP socket connections to the TACACS+ server.
Socket closes	Number of successfully closed TCP socket attempts.
Socket aborts	Number of premature TCP socket closures to the TACACS+ server; That is, the peer did not wait for a reply from the server after a the peer sent its request.
Socket errors	Any other socket read or write errors, such as incorrect packet format and length.
Failed Connect Attempts	Number of failed TCP socket connections to the TACACS+ server.
Total Packets Sent	Number of packets sent to the TACACS+ server.
Total Packets Recv	Number of packets received from the TACACS+ server.
Tacacs+ Server	IP address of the TACACS+ server.

Related Commands

Command	Description
tacacs-server host	Specifies a TACACS+ host.

show tcp intercept connections

To display TCP incomplete and established connections, use the **show tcp intercept connections**command in EXEC mode.

show tcp intercept connections

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.2 F	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **show tcp intercept connections** command to display TCP incomplete and established connections.

Examples

The following is sample output from the **show tcp intercept connections** command:

```
Router# show tcp intercept connections

Incomplete:
Client                Server                State    Create   Timeout  Mode
172.19.160.17:58190   10.1.1.30:23          SYNRCVD  00:00:09 00:00:05 I
172.19.160.17:57934   10.1.1.30:23          SYNRCVD  00:00:09 00:00:05 I

Established:
Client                Server                State    Create   Timeout  Mode
172.16.232.23:1045    10.1.1.30:23          ESTAB    00:00:08 23:59:54 I
```

The table below describes significant fields shown in the display.

Table 49: show tcp intercept connections Field Descriptions

Field	Description
Incomplete:	Rows of information under "Incomplete" indicate connections that are not yet established.
Client	IP address and port of the client.
Server	IP address and port of the server being protected by TCP intercept.
State	SYNRCVD--establishing with client. SYNSENT--establishing with server. ESTAB--established with both, passing data.

Field	Description
Create	Hours:minutes:seconds since the connection was created.
Timeout	Hours:minutes:seconds until the retransmission timeout.
Mode	I--intercept mode. W--watch mode.
Established:	Rows of information under "Established" indicate connections that are established. The fields are the same as those under "Incomplete" except for the Timeout field described below.
Timeout	Hours:minutes:seconds until the connection will timeout, unless the software sees a FIN exchange, in which case this indicates the hours:minutes:seconds until the FIN or RESET timeout.

Related Commands

Command	Description
ip tcp intercept connection-timeout	Changes how long a TCP connection will be managed by the TCP intercept after no activity.
ip tcp intercept finrst-timeout	Changes how long after receipt of a reset or FIN-exchange the software ceases to manage the connection.
ip tcp intercept list	Enables TCP intercept.
show tcp intercept statistics	Displays TCP intercept statistics.

show tcp intercept statistics

To display TCP intercept statistics, use the **show tcp intercept statistics**command in EXEC mode.

show tcp intercept statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

Release	Modification
11.2 F	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS release 12.(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Use the **show tcp intercept statistics**command to display TCP intercept statistics.

Examples

The following is sample output from the **show tcp intercept statistics** command:

```
Router# show tcp intercept statistics
intercepting new connections using access-list 101
2 incomplete, 1 established connections (total 3)
1 minute connection request rate 2 requests/sec
```

Related Commands

Command	Description
ip tcp intercept connection-timeout	Changes how long a TCP connection will be managed by the TCP intercept after no activity.
ip tcp intercept finrst-timeout	Changes how long after receipt of a reset or FIN-exchange the software ceases to manage the connection.
ip tcp intercept list	Enables TCP intercept.
show tcp intercept connections	Displays TCP incomplete and established connections.

show tech-support alg

To display application layer gateway (ALG)-specific information to assist in troubleshooting, use the **show tech-support alg** command in privileged EXEC mode.

show tech-support alg platform

Syntax Description

platform	Displays platform-specific ALG information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.9S	This command was introduced.

Usage Guidelines

The **show tech-support alg** command is useful for collecting a large amount of information about ALGs for troubleshooting purposes. The output of this command can be provided to technical support representatives when reporting a problem. The command output displays the output of a number of **show** commands at once. The output from this command varies depending on your platform and configuration.

Examples

The following is sample output from the **show tech-support alg platform** command:

```
Device# show tech-support alg platform

show platform hardware qfp active feature alg memory

Pool information:
Pool-Name                Num-Entries  Entry-Limit  Size(bytes)  Num-Additions
-----------------------------------------------------------------------------
FTP pool                 640          0            41376        0
SCCP pool                160          0            8096         0
SIP pool                 640          0            348576       0
SIP pkt pool             160          0            18336        0
SIP msg pool             320          0            26016        0
RTSP pool                160          0            10656        0
H323 info pool           100          5000         61216        0
H323 fs olc pool         100          5000         3616         0
H323 pkt sb pool         100          5000         3616         0
H323 indus pool          1000         2000         4112416      0
H323 tl olc pool         100          5000         3616         0
H323 msg info pool       100          5000         8416         0
DNS pool                 1024         0            82336        0
LDAP pool                128          5000         4512         0
LDAP pkt info pool       32           160          670624       0
RCMD pool                160          5000         5536         0
HTTP info pool           2400         1048576      192416       0
HTTP req ctxt pool       6400         2097152      1638816      0
HTTP resp ctxt pool      6400         2097152      1331616      0
HTTP hdr fld pool        6400         2097152      307616       0
HTTP MIME ctxt pool      6400         2097152      819616       0
NetBIOS L7 data pool     1024         5000         33184        0
Act token pool           640          0            143776       0
Ext state pool           160          0            5536         0
ALG HA ntuple hdr pool   10000        0            640416       0
```

```
Sun RPC info pool        1024         7168         33184        0
MS RPC info pool         1024         7168         49568        0
MS RPC extended toke...  1024         7168         82336        0
SMTP l7 info pool        2400         524288       1075616      0
SMTP command pool        6400         1048576      307616       0
SMTP log filter pool     6400         1048576      307616       0
SMTP mask pool           6400         1048576      307616       0
IMAP info pool           2400         524288       154016       0
POP3 info pool           2400         524288       154016       0
GTP AIC ctxt pool        2400         1048576      154016       0
GTP request response...  2400         524288       154016       0
GTP hash info pool       2400         2097152      192416       0
GTP master pdp pool      2400         524288       1421216      0
GTP secondary pdp pool   2400         524288       269216       0
GTP req_resp hash en...  2400         1048576      192416       0

Table information:
Ha hash table: Num-Entries: 10000, Size(bytes): 40000

show platform hardware qfp active feature td datapath memory
==VTCP ucode info==
info alloc 0, free 0, fail 0
pkt buf alloc 0, free 0, fail 0
buf size alloc 0, free 0
rx drop 0, tx drop 0, tcp drop 0, alg csum 0
sending: rx ack 0, rst 0, hold rst 0 tx payload: seg 0, rexmit 0
vtcp_info_chunk 0x8d54fcb0, totalfree: 2048, allocated: 0
vtcp_pkt_pool 0x8d5d80c0, total: 1048240, free: 1048240
vtcp_timer_wheel 0x8d6d84d0, vtcp_init 1
td_internal debug 0x0
td_global td_init 0x2
alg_debug_vtcp 0x0

show platform hardware qfp active feature alg statistics
ALG counters:
ALG         Cntrl-Pkt        Parser-Err&Drop  Parser-No-Act
FTP         0                0                0
SIP         0                0                0
SKINNY      0                0                0
H225        0                0                0
H245        0                0                0
H225ras     0                0                0
RTSP        0                0                0
DNS         0                0                0
LDAP        0                0                0
TFTP        0                0                0
HTTP        0                0                0
SHELL       0                0                0
LOGIN       0                0                0
NETBIOS-NS  0                0                0
NETBIOS-SSN 0                0                0

ALG chunk pool:
Pool-Name                   Used-Entries     Free-Entries
FTP pool                    0                640
SCCP pool                   0                160
SIP pool                    0                640
SIP pkt pool                0                160
SIP msg pool                0                320
RTSP pool                   0                160
H323 info pool              0                100
H323 fs olc pool            0                100
H323 pkt sb pool            0                100
H323 indus pool             50               950
```

```
H323 tl olc pool            0               100
H323 msg info pool          0               100
DNS pool                    0               1024
LDAP pool                   0               128
LDAP pkt info pool          0               32
HTTP info pool              0               0
HTTP req ctxt pool          0               0
HTTP resp ctxt pool         0               0
HTTP hdr fld pool           0               0
HTTP MIME ctxt pool         0               0
NetBIOS L7 data pool        0               1024

Common ALG chunk pool:
Pool-Name                   Used-Entries    Free-Entries
Act Token Pool              0               640
Ext State Pool              0               160
HA ntuple hdr Pool          0               10000
Sun RPC info pool           0               1024
MS RPC info pool            0               1024
SMTP l7 info pool           0               0
SMTP command pool           0               0
SMTP log filter pool        0               0
SMTP mask pool              0               0
IMAP info pool              0               0
POP3 info pool              0               0
GTP AIC ctxt pool           0               0
GTP Req/Res pool            0               0
GTP hash info pool          0               0
GTP master pdp pool         0               0
GTP secondary pdp pool      0               0
GTP req_res hash entry pool 0               0
.
.
.
```

The table below describes the significant fields shown in the display.

Table 50: show tech-support alg platform Field Descriptions

Field	Description
Pool information	Detailed information about ALG pools.
Pool-Name	Name of the ALG pool.
Num-Entries	Number of pool entries.
Entry-Limit	Configured limit for the number of packets that can access the pool.
info alloc	Virtual TCP (vTCP) allocated counts.
pak buf alloc	Allocated packet buffer.
buf siz alloc	Allocated buffer size.

Related Commands

Command	Description
show platform hardware qfp feature alg	Displays ALG-specific information in the QFP.

show tech-support ipsec

To display IPsec information to assist in troubleshooting, use the **show tech-support ipsec** command in privileged EXEC mode.

show tech-support ipsec [**peer** *ipv4-address* | **vrf** *vrf-name* | **platform**]

Syntax Description

peer *ipv4-address*	(Optional) Displays information about the specified IPv4 peer.
vrf *vrf-name*	(Optional) Displays information about the specified VPN routing and forwarding (VRF) instance.
platform	(Optional) Displays platform specific information about the IPsec flow.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(20)T	This command was introduced.
Cisco IOS XE Release 2.4	This command was implemented on the Cisco ASR 1000 Series Aggregation Service Routers.
Cisco IOS XE Release 3.7S	This command was modified. The **platform** keyword was added. The output was enhanced to display platform specific information about the IPsec flow.

Usage Guidelines

The **show tech-support ipsec** command simplifies the collection of IPsec-related information if you are troubleshooting a problem.

The **show tech-support ipsec** command without any keywords displays the output from the following **show** commands, as listed in the order below:

- **show version**
- **show running-config**
- **show crypto isakmp sa count**
- **show crypto ipsec sa count**
- **show crypto session summary**
- **show crypto session detail**
- **show crypto isakmp sa detail**
- **show crypto ipsec sa detail**
- **show crypto isakmp peers**
- **show crypto ruleset detail**
- **show processes memory | include Crypto IKMP**

- **show processes cpu | include Crypto IKMP**
- **show crypto eli**
- **show crypto engine accelerator statistic**

The **show tech-support ipsec** command with the **peer** keyword and the *ipv4-address* argument displays the output from the following **show** commands, as listed in the order below:

- **show version**
- **show running-config**
- **show crypto session remote** *ipv4address* **detail**
- **show crypto isakmp sa peer** *ipv4address* **detail**
- **show crypto ipsec sa peer** *ipv4address* **detail**
- **show crypto isakmp peers** *ipv4address*
- **show crypto ruleset detail**
- **show processes memory** | **include Crypto IKMP**
- **show processes cpu** | **include Crypto IKMP**
- **show crypto eli**
- **show crypto engine accelerator statistic**

The **show tech-support ipsec** command with the **vrf** *vrf-name* keyword and argument displays the output from the following **show** commands as listed in the order below:

- **show version**
- **show running-config**
- **show crypto isakmp sa count vrf** *vrf-name*
- **show crypto ipsec sa count vrf** *vrf-name*
- **show crypto session ivrf** *ivrf-name* **detail**
- **show crypto session fvrf** *fvrf-name* **detail**
- **show crypto isakmp sa vrf** *vrf-name* **detail**
- **show crypto ipsec sa vrf** *vrf-name* **detail**
- **show crypto ruleset detail**
- **show processes memory** | **include Crypto IKMP**
- **show processes cpu** | **include Crypto IKMP**
- **show crypto eli**
- **show crypto engine accelerator statistic**

The **show tech-support ipsec platform** command displays the output from the following **show** commands, as listed in the order below:

- **show clock**
- **show version**
- **show running-config**
- **show crypto tech-support**
- **show crypto isakmp sa count**
- **show crypto ipsec sa count**
- **show crypto isakmp sa detail**
- **show crypto ipsec sa detail**
- **show crypto session summary**
- **show crypto session detail**
- **show crypto isakmp peers**
- **show crypto ruleset detail**
- **show processes memory**
- **show processes cpu**
- **show crypto eli**
- **show crypto engine accelerator statistic**
- **show crypto isakmp diagnose error**
- **show crypto isakmp diagnose error count**
- **show crypto call admission statistics**

Related Commands

Command	Description
show tech-support	Displays information about the device when the device reports a problem.

show tech-support pki

To display public key infrastructure (PKI)-specific information to assist in troubleshooting, use the **show tech-support pki** command in privileged EXEC mode.

show tech-support pki

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.8.1	This command was introduced.
Cisco IOS XE Fuji 16.9.1	This command was modified to display the clock, version and other configuration details.

Usage Guidelines

The **show tech-support pki** command is useful for collecting the complete set of PKI-related information for troubleshooting purposes. The output of this command can be provided to technical support representatives when reporting a problem.

Examples

The following is sample output from the **show tech-support pki** command:

```
Device# show tech-support pki

------------------ show clock ------------------


07:07:35.291 IST Sun Jun 3 2018

------------------ show version ------------------

Cisco IOS XE Software, Version 2018-05-31_14.33_sudsirig
Cisco IOS Software [Fuji], IOS-XE Virtual XE Software (X86_64_LINUX_IOSD-UNIVERSALK9-M),
Experimental Version 16.10.20180531:085308
[polaris_dev-/nobackup/sudsirig/poldev_cflow_devtest 105]
Copyright (c) 1986-2018 by Cisco Systems, Inc.
Compiled Thu 31-May-18 14:26 by sudsirig


Cisco IOS-XE software, Copyright (c) 2005-2018 by cisco Systems, Inc.
All rights reserved.  Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0.  The
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY.  You can redistribute and/or modify such
GPL code under the terms of GPL Version 2.0.  For more details, see the
documentation or "License Notice" file accompanying the IOS-XE software,
or the applicable URL provided on the flyer accompanying the IOS-XE
software.


ROM: IOS-XE ROMMON

pki_a uptime is 6 hours, 53 minutes
```

```
Uptime for this control processor is 6 hours, 54 minutes
System returned to ROM by reload
System restarted at 00:14:18 IST Sun Jun 3 2018
System image file is "cdrom0:packages.conf"
Last reload reason: reload



This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.

License Level: ax
License Type: Default. No valid license found.
Next reload license Level: ax

cisco CSR1000V (VXE) processor (revision VXE) with 2372442K/3075K bytes of memory.
Processor board ID 9VJK6T4IQMT
4 Gigabit Ethernet interfaces
32768K bytes of non-volatile configuration memory.
8113356K bytes of physical memory.
16162815K bytes of virtual hard disk at bootflash:.
0K bytes of WebUI ODM Files at webui:.

Configuration register is 0x2102


------------------ show running-config ------------------


Building configuration...

Current configuration : 6003 bytes
!
! Last configuration change at 07:07:18 IST Sun Jun 3 2018
!
version 16.10
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
platform qfp utilization monitor load 80
no platform punt-keepalive disable-kernel-core
platform console serial
!
hostname pki_a
!
boot-start-marker
boot-end-marker
!
!
logging buffered 1000000
no logging console
!
no aaa new-model
```

```
clock timezone IST 5 30
clock calendar-valid
!
!
ip admission watch-list expiry-time 0
!
subscriber templating
!
multilink bundle-name authenticated
!
crypto pki server rootca
no database archive
issuer-name CN=RCA1 C=pki
grant auto
hash sha512
lifetime certificate 364
lifetime ca-certificate 364
!
crypto pki trustpoint TP-self-signed-777972883
enrollment selfsigned
subject-name cn=IOS-Self-Signed-Certificate-777972883
revocation-check none
rsakeypair TP-self-signed-777972883
!
crypto pki trustpoint rootca
revocation-check none
rsakeypair rootca 1024
hash sha512
!
crypto pki trustpoint test
enrollment url http://9.45.3.241:80
usage ike
subject-name CN=R1 C=pki
revocation-check crl
rsakeypair test 1024
auto-enroll 3
hash sha512
!
!
crypto pki certificate chain TP-self-signed-777972883
crypto pki certificate chain rootca
certificate ca 02
  30820203 3082016C A0030201 02020102 300D0609 2A864886 F70D0101 0D050030
  15311330 11060355 0403130A 52434131 20433D70 6B69301E 170D3138 30363033
  30313334 35365A17 0D313930 36303230 31333435 365A3015 31133011 06035504
  03130A52 43413120 433D706B 6930819F 300D0609 2A864886 F70D0101 01050003
  818D0030 81890281 8100AD12 BD3E2CA7 3B3F1C19 A18CD53B DF618277 00512357
  A95C141E 4DE7B147 EF4FC9DC C0EB8B7D A81D20E3 25A4B53C 87D19F61 F63AE52A
  82724182 F3DE33AE A59ABB7B 9C6F4D9D F944B0AB 789F635C 740CC101 73CE3043
  7EA692F4 DCFAB15B 99782B0C 0143EFA4 BA4242CD E20F77DD B968C0C8 B5EF2A3F
  D3313C6F 49D93E12 D98D0203 010001A3 63306130 0F060355 1D130101 FF040530
  030101FF 300E0603 551D0F01 01FF0404 03020186 301F0603 551D2304 18301680
  1446E428 7A45971E 1904AB57 D78E8249 54FF9C1F 90301D06 03551D0E 04160414
  46E4287A 45971E19 04AB57D7 8E824954 FF9C1F90 300D0609 2A864886 F70D0101
  0D050003 8181005A CC810010 60BB1DD5 6847F3CE AAE871C9 6E214C60 FD5C56C1
  05A15C67 99CB7464 B518897E 2FE96C87 5FF54631 1224BCE2 AEF599DB 61CB0576
  A70757E6 183A3238 863E54FB 959333C8 562150DE F6FA68D8 DE2526D6 8F41BE72
  26C30292 042D16D3 ADA81A98 CC1D94CD ED06A9EA 6B2BE946 82760C7F A7146306
  D95D07A6 F1ADF6
            quit
crypto pki certificate chain test
certificate 04
  30820203 3082016C A0030201 02020104 300D0609 2A864886 F70D0101 0D050030
  15311330 11060355 0403130A 52434131 20433D70 6B69301E 170D3138 30363033
```

```
  30313336 31395A17 0D313930 36303230 31333435 365A3029 3111300F 06035504
  03130852 3120433D 706B6931 14301206 092A8648 86F70D01 09021605 706B695F
  6130819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281 8100CDB7
  98AF2475 DF4A4DD5 26C602CD C27358F2 D90A4BE7 FA58F5AB 2E5495C7 EEB55513
  A357339C 319392CD FD28F607 BDBDBB77 21261F94 A623B694 A966F9F6 0327582B
  6A6CA0EE C0E8AD8E 7715FFB5 01BCBE7D 2DE0ECD2 D985A524 BFDEAA21 47D7D45A
  19820585 B314EAA7 E939AC85 2A2385AF F9DE5871 3C9A41DF 683BAFD5 D2D30203
  010001A3 4F304D30 0B060355 1D0F0404 030205A0 301F0603 551D2304 18301680
  1446E428 7A45971E 1904AB57 D78E8249 54FF9C1F 90301D06 03551D0E 04160414
  EFBBABD1 EECCC80E 3CAE59B0 C6AC6333 91070AC1 300D0609 2A864886 F70D0101
  0D050003 81810086 59F8185A 5B769128 C37F1C7B 1A32D024 438BC872 1AC6AD50
  F1E9E96F C8DC9413 9ACDFA82 4858F4FA 829F7BAC 09A040AF 5A5A53AB AC6EA5E6
  EADC2BFC BFB33036 C4295B18 C5CC141D A3BCE791 6E25123F 4ABC5746 E569F072
  51AC1E71 0E872A09 8012E547 820E229E F73D8C0E 8818BB5C 8F9E49D6 22EE9BF3
  028A40BB D0EAE0
        quit
certificate ca 02
  30820203 3082016C A0030201 02020102 300D0609 2A864886 F70D0101 0D050030
  15311330 11060355 0403130A 52434131 20433D70 6B69301E 170D3138 30363033
  30313334 35365A17 0D313930 36303230 31333435 365A3015 31133011 06035504
  03130A52 43413120 433D706B 6930819F 300D0609 2A864886 F70D0101 01050003
  818D0030 81890281 8100AD12 BD3E2CA7 3B3F1C19 A18CD53B DF618277 00512357
  A95C141E 4DE7B147 EF4FC9DC C0EB8B7D A81D20E3 25A4B53C 87D19F61 F63AE52A
  82724182 F3DE33AE A59ABB7B 9C6F4D9D F944B0AB 789F635C 740CC101 73CE3043
  7EA692F4 DCFAB15B 99782B0C 0143EFA4 BA4242CD E20F77DD B968C0C8 B5EF2A3F
  D3313C6F 49D93E12 D98D0203 010001A3 63306130 0F060355 1D130101 FF040530
  030101FF 300E0603 551D0F01 01FF0404 03020186 301F0603 551D2304 18301680
  1446E428 7A45971E 1904AB57 D78E8249 54FF9C1F 90301D06 03551D0E 04160414
  46E4287A 45971E19 04AB57D7 8E824954 FF9C1F90 300D0609 2A864886 F70D0101
  0D050003 8181005A CC810010 60BB1DD5 6847F3CE AAE871C9 6E214C60 FD5C56C1
  05A15C67 99CB7464 B518897E 2FE96C87 5FF54631 1224BCE2 AEF599DB 61CB0576
  A70757E6 183A3238 863E54FB 959333C8 562150DE F6FA68D8 DE2526D6 8F41BE72
  26C30292 042D16D3 ADA81A98 CC1D94CD ED06A9EA 6B2BE946 82760C7F A7146306
  D95D07A6 F1ADF6
        quit
!
license udi pid CSR1000V sn 9VJK6T4IQMT
no license smart enable
diagnostic bootup level minimal
!
spanning-tree extend system-id
!
redundancy
!
interface GigabitEthernet1
no ip address
shutdown
negotiation auto
no mop enabled
no mop sysid
!
interface GigabitEthernet2
ip address 9.45.3.241 255.255.0.0
negotiation auto
no mop enabled
no mop sysid
!
interface GigabitEthernet3
no ip address
shutdown
negotiation auto
no mop enabled
no mop sysid
!
```

```
interface GigabitEthernet4
ip address 33.33.33.1 255.255.0.0
negotiation auto
no mop enabled
no mop sysid
!
ip forward-protocol nd
ip http server
ip http secure-server
ip tftp source-interface GigabitEthernet2
ip route 202.153.0.0 255.255.0.0 9.45.0.1
!
control-plane
!
line con 0
exec-timeout 0 0
stopbits 1
line vty 0 4
login
!
end


------------------ show crypto pki certificate verbose ------------------

Certificate
  Status: Available
  Version: 3
  Certificate Serial Number (hex): 04
  Certificate Usage: General Purpose
  Issuer:
    cn=RCA1 C=pki
  Subject:
    Name: pki_a
    hostname=pki_a
    cn=R1 C=pki
  Validity Date:
    start date: 07:06:19 IST Jun 3 2018
    end   date: 07:04:56 IST Jun 2 2019
  Subject Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (1024 bit)
  Signature Algorithm: SHA512 with RSA Encryption
  Fingerprint MD5: 11BC5664 377EEEDC 665FD807 FC9FB976
  Fingerprint SHA1: 5DE8E5B9 EDD3F73B 37A0FF8B E4F6397E 19B6B124
  X509v3 extensions:
    X509v3 Key Usage: A0000000
      Digital Signature
      Key Encipherment
    X509v3 Subject Key ID: EFBBABD1 EECCC80E 3CAE59B0 C6AC6333 91070AC1
    X509v3 Authority Key ID: 46E4287A 45971E19 04AB57D7 8E824954 FF9C1F90
    Authority Info Access:
  Associated Trustpoints: test
  Key Label: test

CA Certificate
  Status: Available
  Version: 3
  Certificate Serial Number (hex): 02
  Certificate Usage: Signature
  Issuer:
    cn=RCA1 C=pki
  Subject:
    cn=RCA1 C=pki
```

```
  Validity Date:
    start date: 07:04:56 IST Jun 3 2018
    end   date: 07:04:56 IST Jun 2 2019
  Subject Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (1024 bit)
  Signature Algorithm: SHA512 with RSA Encryption
  Fingerprint MD5: 0C61C633 C72CE9EC 45E86045 03611E16
  Fingerprint SHA1: 3737DC2B 576D41F5 86ABCD44 F8D05B95 FC2661DF
  X509v3 extensions:
    X509v3 Key Usage: 86000000
      Digital Signature
      Key Cert Sign
      CRL Signature
    X509v3 Subject Key ID: 46E4287A 45971E19 04AB57D7 8E824954 FF9C1F90
    X509v3 Basic Constraints:
        CA: TRUE
    X509v3 Authority Key ID: 46E4287A 45971E19 04AB57D7 8E824954 FF9C1F90
    Authority Info Access:
  Associated Trustpoints: test rootca



------------------ show clock detail ------------------


07:07:35.514 IST Sun Jun 3 2018
Time source is user configuration

------------------ show crypto pki timers detail ------------------

PKI Timers
|        1:44.647  (2018-06-03T07:09:19Z)
  |        1:44.647  (2018-06-03T07:09:19Z) SHADOW test
  |       11:11.420  (2018-06-03T07:18:46Z) SESSION CLEANUP
Expiry Alert Timers
|303d23:57:20.646  (2019-04-03T07:04:55Z)
  |303d23:57:20.646  (2019-04-03T07:04:55Z) ID(test)
  |303d23:57:21.325  (2019-04-03T07:04:56Z) CS(test)
Trustpool Timers
|3693d22:22:24.339  (2028-07-14T05:29:59Z)
  |3693d22:22:24.339  (2028-07-14T05:29:59Z) TRUSTPOOL
CS Timers
|     5:57:21.277  (2018-06-03T13:04:56Z)
  |     5:57:21.277  (2018-06-03T13:04:56Z) CS CRL UPDATE
  |363d23:57:20.995  (2019-06-02T07:04:55Z) CS CERT EXPIRE

------------------ show crypto pki trustpoint ------------------


Trustpoint TP-self-signed-777972883:
    Subject Name:
    cn=IOS-Self-Signed-Certificate-777972883
          Serial Number (hex): 01
    Persistent self-signed certificate trust point
    Using key label TP-self-signed-777972883


Trustpoint rootca:
    Subject Name:
    cn=RCA1 C=pki
          Serial Number (hex): 02
    Certificate configured.
```

```
Trustpoint test:
    Subject Name:
    cn=RCA1 C=pki
          Serial Number (hex): 02
    Certificate configured.
    SCEP URL: http://9.45.3.241:80/cgi-bin


------------------ show crypto pki counters ------------------


PKI Sessions Started: 9
PKI Sessions Ended: 9
PKI Sessions Active: 0
Successful Validations: 1
Failed Validations: 0
Bypassed Validations: 0
Pending Validations: 0
CRLs checked: 0
CRL - fetch attempts: 0
CRL - failed attempts: 0
CRL - rejected busy fetching: 0
AAA authorizations: 0

------------------ show crypto pki crls ------------------


------------------ show crypto pki sessions ------------------


------------------ show crypto key mypubkey all ------------------


% Key pair was generated at: 03:41:10 IST Jun 3 2018
Key name: rootca#
Key type: RSA KEYS
Storage Device: not specified
Usage: General Purpose Key
Key is not exportable.
Key Data:
  30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00B2A2CB
  981220AC 5148C520 B3758EF2 FD00534D E8ECFAA1 C22F9680 C184C785 7FAB0DA1
  505FFB68 E66BD1B6 2560849E 071A3AA8 77B2CA36 00DB9F0A 6DEF0067 C7F95031
  41825E0F C0000417 28A31029 0E0AEF25 BF3C3425 DB03E4D0 7C338411 41873EC7
  044A9EF0 FEB11A07 484F0B26 6BF83C80 21D89FB2 85B2CFD4 3C571D2C D7020301
  0001
% Key pair was generated at: 07:04:56 IST Jun 3 2018
Key name: rootca
Key type: RSA KEYS
Storage Device: not specified
Usage: General Purpose Key
Key is not exportable. Redundancy enabled.
Key Data:
  30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00AD12BD
  3E2CA73B 3F1C19A1 8CD53BDF 61827700 512357A9 5C141E4D E7B147EF 4FC9DCC0
  EB8B7DA8 1D20E325 A4B53C87 D19F61F6 3AE52A82 724182F3 DE33AEA5 9ABB7B9C
  6F4D9DF9 44B0AB78 9F635C74 0CC10173 CE30437E A692F4DC FAB15B99 782B0C01
  43EFA4BA 4242CDE2 0F77DDB9 68C0C8B5 EF2A3FD3 313C6F49 D93E12D9 8D020301
  0001
% Key pair was generated at: 07:04:56 IST Jun 3 2018
```

```
Key name: rootca.server
Key type: RSA KEYS
Temporary key
Usage: Encryption Key
Key is not exportable.
Key Data:
  307C300D 06092A86 4886F70D 01010105 00036B00 30680261 00DB008C C1220131
  2ABB976F 1210B31D 0F84E5AE 24840A01 7A459228 7BB785C4 98DABB13 A8FCE70D
  13A38E40 0FFAC835 A294348C FAC36445 5D128775 8526BE2F D68539C6 91584899
  915BDB10 E963CB56 2FBCFAF1 76CA6C42 C004D778 81A5C614 AD020301 0001
% Key pair was generated at: 07:06:03 IST Jun 3 2018
Key name: client
Key type: RSA KEYS
Storage Device: not specified
Usage: General Purpose Key
Key is not exportable. Redundancy enabled.
Key Data:
  30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 009E6F1C
  B3748AFA 5679B076 A7D3F692 C9F560BB BD61BE66 4DD01B53 9EB5B633 96BC6E63
  A5485193 B9651CA6 09CF2E07 F4841313 E5191B54 011C10DC A639093E 55A015CA
  15B73B31 829D6E55 A69A93E6 9BF321AB 06A2A3C8 547A7F25 DFDF0421 0F9F53B5
  7AFB72BB D65CB226 50515468 23E0D057 7F9675EA 30845D72 F1BB2BB0 85020301
  0001
% Key pair was generated at: 07:06:19 IST Jun 3 2018
Key name: test
Key type: RSA KEYS
Storage Device: not specified
Usage: General Purpose Key
Key is not exportable. Redundancy enabled.
Key Data:
  30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00CDB798
  AF2475DF 4A4DD526 C602CDC2 7358F2D9 0A4BE7FA 58F5AB2E 5495C7EE B55513A3
  57339C31 9392CDFD 28F607BD BDBB7721 261F94A6 23B694A9 66F9F603 27582B6A
  6CA0EEC0 E8AD8E77 15FFB501 BCBE7D2D E0ECD2D9 85A524BF DEAA2147 D7D45A19
  820585B3 14EAA7E9 39AC852A 2385AFF9 DE58713C 9A41DF68 3BAFD5D2 D3020301
  0001

------------------ show crypto pki certificate storage ------------------

Trustpool - certificates will be stored in nvram:
TP-self-signed-777972883 - certificates will be stored in nvram:
rootca - certificates will be stored in nvram:
test - certificates will be stored in nvram:


------------------ show crypto pki certificate pem ------------------


------Trustpoint: TP-self-signed-777972883------
% The specified trustpoint is not enrolled (TP-self-signed-777972883).
% Only export the CA certificate in PEM format.
% Error: failed to get CA cert.
------Trustpoint: rootca------
% The specified trustpoint is not enrolled (rootca).
% Only export the CA certificate in PEM format.
% CA certificate:
-----BEGIN CERTIFICATE-----
MIICAzCCAWygAwIBAgIBAjANBgkqhkiG9w0BAQ0FADAVMRMwEQYDVQQDEwpSQ0Ex
IEM9cGtpMB4XDTE4MDYwMzAxMzQ1NloXDTE5MDYwMjAxMzQ1NlowFTETMBEGA1UE
AxMKUkNBMSBDPXBraTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEArRK9Piyn
Oz8cGaGM1TvfYYJ3AFEjV6lcFB5N57FH70/J3MDri32oHSDjJaS1PIfRn2H2OuUq
gnJBgvPeM66lmrt7nG9NnflEsKt4n2NcdAzBAXPOMEN+ppL03PqxW5l4KwwBQ++k
ukJCzeIPd925aMDIte8qP9MxPG9J2T4S2Y0CAwEAAaNjMGEwDwYDVR0TAQH/BAUw
AwEB/zAOBgNVHQ8BAf8EBAMCAYYwHwYDVR0jBBgwFoAURuQoekWXHhkEq1fXjoJJ
```

```
VP+cH5AwHQYDVR0OBBYEFEbkKHpFlx4ZBKtX146CSVT/nB+QMA0GCSqGSIb3DQEB
DQUAA4GBAFrMgQAQYLsd1WhH886q6HHJbiFMYP1cVsEFoVxnmct0ZLUYiX4v6WyH
X/VGMRIkvOKu9ZnbYcsFdqcHV+YYOjI4hj5U+5WTM8hWIVDe9vpo2N4lJtaPQb5y
JsMCkgQtFtOtqBqYzB2Uze0GqeprK+lGgnYMf6cUYwbZXQem8a32
-----END CERTIFICATE-----

------Trustpoint: test------
% CA certificate:
-----BEGIN CERTIFICATE-----
MIICAzCCAWygAwIBAgIBAjANBgkqhkiG9w0BAQ0FADAVMRMwEQYDVQQDEwpSQ0Ex
IEM9cGtpMB4XDTE4MDYwMzAxMzQ1NloXDTE5MDYwMjAxMzQ1NlowFTETMBEGA1UE
AxMKUkNBMSBDPXBraTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEArRK9Piyn
Oz8cGaGM1TvfYYJ3AFEjV6lcFB5N57FH70/J3MDri32oHSDjJaS1PIfRn2H2OuUq
gnJBgvPeM66lmrt7nG9NnflEsKt4n2NcdAzBAXPOMEN+ppL03PqxW5l4KwwBQ++k
ukJCzeIPd925aMDIte8qP9MxPG9J2T4S2Y0CAwEAAaNjMGEwDwYDVR0TAQH/BAUw
AwEB/zAOBgNVHQ8BAf8EBAMCAYYwHwYDVR0jBBgwFoAURuQoekWXHhkEq1fXjoJJ
VP+cH5AwHQYDVR0OBBYEFEbkKHpFlx4ZBKtX146CSVT/nB+QMA0GCSqGSIb3DQEB
DQUAA4GBAFrMgQAQYLsd1WhH886q6HHJbiFMYP1cVsEFoVxnmct0ZLUYiX4v6WyH
X/VGMRIkvOKu9ZnbYcsFdqcHV+YYOjI4hj5U+5WTM8hWIVDe9vpo2N4lJtaPQb5y
JsMCkgQtFtOtqBqYzB2Uze0GqeprK+lGgnYMf6cUYwbZXQem8a32
-----END CERTIFICATE-----

% General Purpose Certificate:
-----BEGIN CERTIFICATE-----
MIICAzCCAWygAwIBAgIBBDANBgkqhkiG9w0BAQ0FADAVMRMwEQYDVQQDEwpSQ0Ex
IEM9cGtpMB4XDTE4MDYwMzAxMzYxOVoXDTE5MDYwMjAxMzQ1NlowKTERMA8GA1UE
AxMIUjEgQz1wa2kxFDASBgkqhkiG9w0BCQIWBXBraV9hMIGfMA0GCSqGSIb3DQEB
AQUAA4GNADCBiQKBgQDNt5ivJHXfSk3VJsYCzcJzWPLZCkvn+lj1qy5UlcfutVUT
o1cznDGTks39KPYHvb27dyEmH5SmI7aUqWb59gMnWCtqbKDuwOitjncV/7UBvL59
LeDs0tmFpSS/3qohR9fUWhmCBYWzFOqn6TmshSojha/53lhxPJpB32g7r9XS0wID
AQABo08wTTALBgNVHQ8EBAMCBaAwHwYDVR0jBBgwFoAURuQoekWXHhkEq1fXjoJJ
VP+cH5AwHQYDVR0OBBYEFO+7q9HuzMgOPK5ZsMasYzORBwrBMA0GCSqGSIb3DQEB
DQUAA4GBAIZZ+BhaW3aRKMN/HHsaMtAkQ4vIchrGrVDx6elvyNyUE5rN+oJIWPT6
gp97rAmgQK9aWlOrrG6l5urcK/y/szA2xClbGMXMFB2jvOeRbiUSP0q8V0blafBy
UawecQ6HKgmAEuVHgg4invc9jA6IGLtcj55J1iLum/MCikC70Org
-----END CERTIFICATE-----


------------------ show crypto pki server ------------------


Certificate Server rootca:
    Status: enabled
    State: enabled
    Server's configuration is locked  (enter "shut" to unlock it)
    Issuer name: CN=RCA1 C=pki
    CA cert fingerprint: 0C61C633 C72CE9EC 45E86045 03611E16
    Granting mode is: auto
    Last certificate issued serial number (hex): 4
    CA certificate expiration timer: 07:04:56 IST Jun 2 2019
    CRL NextUpdate timer: 13:04:56 IST Jun 3 2018
    Current primary storage dir: nvram:
    Database Level: Minimum - no cert data written to storage

------------------ show crypto pki server rootca certificates ------------------

Serial Issued date              Expire date               Subject Name
1       <cert file not accessible>
2       <cert file not accessible>
3       <cert file not accessible>
4       <cert file not accessible>


------------------ show crypto pki server rootca crl ------------------
```

```
Certificate Revocation List:
    Issuer: cn=RCA1 C=pki
    This Update: 07:04:56 IST Jun 3 2018
    Next Update: 13:04:56 IST Jun 3 2018
    Number of CRL entries: 0
    CRL size: 220 bytes


------------------ show crypto pki server rootca requests ------------------

The Enrollment Request Database is empty.
```

Related Commands

Command	Description
show tech-support	Displays information about the device when the device reports a problem.

show tunnel endpoints

To display the contents of the tunnel endpoint database that is used for tunnel endpoint address resolution, when running a tunnel in multipoint generic routing encapsulation (mGRE) mode, use the **show tunnel endpoints**command in privileged EXEC mode.

show tunnel endpoints [**tunnel** *tunnel-number*]

Syntax Description

tunnel	(Optional) Specifies the tunnel interface. If a tunnel is specified, only the endpoint database for that tunnel is displayed. If a tunnel is not specified, endpoint databases for all tunnels are displayed.
tunnel-number	(Optional) Tunnel interface number. The range is from 0 to 2147483647.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.0(27)S	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.(33)SRA.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
Cisco IOS XE Release 2.1	This command was implemented on the Cisco ASR 1000 series routers.

Usage Guidelines

The output of **show tunnel endpoints** command displays the tunnel destination and transport address together with any overlay or virtual private network (VPN) address that resolves to it.

Examples

The following example shows that there are two tunnel endpoints in the database that are associated with tunnel 1 (192.0.2.0 and 192.0.2.1). Through these endpoints, VPN destination 192.0.2.3 is reachable by tunneling to endpoint 192.0.2.0 and VPN destination 192.0.2.2 is reachable by tunneling to endpoint 192.0.2.1.

```
Router# show tunnel endpoints
Tunnel0 running in multi-GRE/IP mode

 Endpoint transport 20.20.20.20 Refcount 4 Base 0x55BCC5E8 Create Time 00:01:08
   overlay ::FFFF:20.20.20.20 Refcount 2 Parent 0x55BCC5E8 Create Time 00:01:08
   overlay 20.20.20.20 Refcount 2 Parent 0x55BCC5E8 Create Time 00:01:08
```

The table below describes the significant fields shown in the display..

Table 51: show tunnel endpoints Field Descriptions

Field	Description
Transport	Displays the transport address.
Refcount	Number of overlay addresses that are resolving through the destination address.
Base	Displays the base address.
Overlay	Displays the overlay address.
Parent	Reference to the tunnel endpoint.

Related Commands

Command	Description
tunnel mode	Sets the encapsulation mode for the tunnel interface.
tunnel protection	Associates a tunnel interface with an IPSec profile.

show usb controllers

To display USB host controller information, use the **show usb controllers**command in privileged EXEC mode.

show usb controllers [*controller-number*]

Syntax Description

controller-number	(Optional) Displays information only for the specified controller.

Command Default

Information about all controllers on the system are displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(11)T	This command was integrated into the Cisco 7200VXR NPE-G2 platform.

Usage Guidelines

Use the **show usb controllers**command to display content such as controller register specific information, current asynchronous buffer addresses, and period scheduling information. You can also use this command to verify that copy operations are occurring successfully onto a USB flash module.

Examples

The following example is sample output from the **show usb controllers** command:

```
Router# show usb controllers
Name:1362HCD
Controller ID:1
Controller Specific Information:
    Revision:0x11
    Control:0x80
    Command Status:0x0
    Hardware Interrupt Status:0x24
    Hardware Interrupt Enable:0x80000040
    Hardware Interrupt Disable:0x80000040
    Frame Interval:0x27782EDF
    Frame Remaining:0x13C1
    Frame Number:0xDA4C
    LSThreshold:0x628
    RhDescriptorA:0x19000202
    RhDescriptorB:0x0
    RhStatus:0x0
    RhPort1Status:0x100103
    RhPort2Status:0x100303
    Hardware Configuration:0x3029
    DMA Configuration:0x0
    Transfer Counter:0x1
    Interrupt:0x9
    Interrupt Enable:0x196
    Chip ID:0x3630
    Buffer Status:0x0
    Direct Address Length:0x80A00
    ATL Buffer Size:0x600
```

```
    ATL Buffer Port:0x0
    ATL Block Size:0x100
    ATL PTD Skip Map:0xFFFFFFFF
    ATL PTD Last:0x20
    ATL Current Active PTD:0x0
    ATL Threshold Count:0x1
    ATL Threshold Timeout:0xFF
Int Level:1
Transfer Completion Codes:
         Success              :920             CRC              :0
         Bit Stuff            :0               Stall            :0
         No Response          :0               Overrun          :0
         Underrun             :0               Other            :0
         Buffer Overrun       :0               Buffer Underrun :0
Transfer Errors:
         Canceled Transfers   :2               Control Timeout :0
Transfer Failures:
         Interrupt Transfer   :0               Bulk Transfer   :0
         Isochronous Transfer :0               Control Transfer:0
Transfer Successes:
         Interrupt Transfer   :0               Bulk Transfer   :26
         Isochronous Transfer :0               Control Transfer:894
USBD Failures:
         Enumeration Failures :0               No Class Driver Found:0
         Power Budget Exceeded:0
USB MSCD SCSI Class Driver Counters:
         Good Status Failures :3               Command Fail    :0
         Good Status Timed out:0               Device not Found:0
         Device Never Opened  :0               Drive Init Fail :0
         Illegal App Handle   :0               Bad API Command :0
         Invalid Unit Number  :0               Invalid Argument:0
         Application Overflow :0               Device in use   :0
         Control Pipe Stall   :0               Malloc Error    :0
         Device Stalled       :0               Bad Command Code:0
         Device Detached      :0               Unknown Error   :0
         Invalid Logic Unit Num:0
USB Aladdin Token Driver Counters:
         Token Inserted       :1               Token Removed   :0
         Send Insert Msg Fail :0               Response Txns   :434
         Dev Entry Add Fail   :0               Request Txns    :434
         Dev Entry Remove Fail:0               Request Txn Fail:0
         Response Txn Fail    :0               Command Txn Fail:0
         Txn Invalid Dev Handle:0
USB Flash File System Counters:
         Flash Disconnected   :0               Flash Connected :1
         Flash Device Fail    :0               Flash Ok        :1
         Flash startstop Fail :0               Flash FS Fail   :0
USB Secure Token File System Counters:
         Token Inserted       :1               Token Detached  :0
         Token FS success     :1               Token FS Fail   :0
         Token Max Inserted   :0               Create Talker Failures:0
         Token Event          :0               Destroy Talker Failures:0
         Watched Boolean Create Failures:0
```

show usb device

To display USB device information, use the **show usb device**command in privileged EXEC mode.

show usb device [*controller-ID* [*device-address*]]

Syntax Description

controller-ID	(Optional) Displays information only for the devices under the specified controller.
device-address	(Optional) Displays information only for the device with the specified address.

Command Default

Information for all devices attached to the system are displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(11)T	This command was integrated into the Cisco 7200VXR NPE-G2 platform.

Usage Guidelines

Use the **show usb device** command to display information for either a USB flash drive or a USB eToken, as appropriate.

Examples

The following example is sample output from the **show usb device** command:

```
Router# show usb device

Host Controller:1
Address:0x1
Device Configured:YES
Device Supported:YES
Description:DiskOnKey
Manufacturer:M-Sys
Version:2.0
Serial Number:0750D84030316868
Device Handle:0x1000000
USB Version Compliance:2.0
Class Code:0x0
Subclass Code:0x0
Protocol:0x0
Vendor ID:0x8EC
Product ID:0x15
Max. Packet Size of Endpoint Zero:64
Number of Configurations:1
Speed:Full
Selected Configuration:1
Selected Interface:0
Configuration:
    Number:1
    Number of Interfaces:1
    Description:
    Attributes:None
    Max Power:140 mA
    Interface:
```

```
        Number:0
        Description:
        Class Code:8
        Subclass:6
        Protocol:80
        Number of Endpoints:2
        Endpoint:
            Number:1
            Transfer Type:BULK
            Transfer Direction:Device to Host
            Max Packet:64
            Interval:0
        Endpoint:
            Number:2
            Transfer Type:BULK
            Transfer Direction:Host to Device
            Max Packet:64
            Interval:0
Host Controller:1
Address:0x11
Device Configured:YES
Device Supported:YES
Description:eToken Pro 4254
Manufacturer:AKS
Version:1.0
Serial Number:
Device Handle:0x1010000
USB Version Compliance:1.0
Class Code:0xFF
Subclass Code:0x0
Protocol:0x0
Vendor ID:0x529
Product ID:0x514
Max. Packet Size of Endpoint Zero:8
Number of Configurations:1
Speed:Low
Selected Configuration:1
Selected Interface:0
Configuration:
    Number:1
    Number of Interfaces:1
    Description:
    Attributes:None
    Max Power:60 mA
    Interface:
        Number:0
        Description:
        Class Code:255
        Subclass:0
        Protocol:0
        Number of Endpoints:0
```

The following table describes the significant fields shown in the display.

Table 52: show usb device Field Descriptions

Field	Description
Device handle	Internal memory handle allocated to the device.

Field	Description
Device Class code	The class code supported by the device. This number is allocated by the USB-IF. If this field is reset to 0, each interface within a configuration specifies its own class information, and the various interfaces operate independently. If this field is set to a value between 1 and FEH, the device supports different class specifications on different interfaces, and the interfaces may not operate independently. This value identifies the class definition used for the aggregate interfaces. If this field is set to FFH, the device class is vendor-specific.
Device Subclass code	The subclass code supported by the device. This number is allocated by the USB-IF.
Device Protocol	The protocol supported by the device. If this field is set to 0, the device does not use class-specific protocols on a device basis. If this field is set to 0xFF, the device uses a vendor-specific protocol on a device basis.
Interface Class code	The class code supported by the interface. If the value is set to 0xFF, the interface class is vendor specific. All other values are allocated by the USB-IF.
Interface Subclass code	The subclass code supported by the interface. All values are allocated by the USB-IF.
Interface Protocol	The protocol code supported by the interface. If this field is set to 0, the device does not use a class-specific protocol on this interface. If this field is set to 0xFF, the device uses a vendor-specific protocol for this interface.
Max Packet	Maximum data packet size, in bytes.

show usb driver

To display information about registered USB class drivers and vendor-specific drivers, use the **show usb driver**command in privileged EXEC mode.

show usb driver [*index*]

Syntax Description

index	(Optional) Displays information only for drivers on the specified index.

Command Default

Information about all drivers is displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(11)T	This command was integrated into the Cisco 7200VXR NPE-G2 platform.
Cisco IOS XE Release 3.6	This command was integrated into Cisco IOS XE Release 3.6.

Examples

The following example is sample output for the **show usb driver** command:

```
Router# show usb driver

Index:0
Owner Mask:0x6
Class Code:0x0
Subclass Code:0x0
Protocol:0x0
Interface Class Code:0x8
Interface Subclass Code:0x6
Interface Protocol Code:0x50
Product ID:0x655BD598
Vendor ID:0x64E90000
Attached Devices:
    Controller ID:1, Device Address:1
Index:1
Owner Mask:0x1
Class Code:0x0
Subclass Code:0x0
Protocol:0x0
Interface Class Code:0x0
Interface Subclass Code:0x0
Interface Protocol Code:0x0
Product ID:0x514
Vendor ID:0x529
Attached Devices:
    Controller ID:1, Device Address:17
Index:2
Owner Mask:0x5
Class Code:0x9
Subclass Code:0x6249BD58
Protocol:0x2
```

```
Interface Class Code:0x5DC0
Interface Subclass Code:0x5
Interface Protocol Code:0xFFFFFFFF
Product ID:0x2
Vendor ID:0x1
Attached Devices:
    None
Index:3
Owner Mask:0x10
Class Code:0x0
Subclass Code:0x0
Protocol:0x0
Interface Class Code:0x0
Interface Subclass Code:0x0
Interface Protocol Code:0x0
Product ID:0x0
Vendor ID:0x0
Attached Devices:
    None
```

The following table describes the significant field shown in the display.

Table 53: show usb driver Field Descriptions

Field	Description
Owner Mask	Indicates the fields that are used in enumeration comparison. The driver can own different devices on the basis of their product or vendor IDs and device or interface class, subclass, and protocol codes.

show usb port

To sisplay USB root hub port information, use the **show usb port**command in privileged EXEC mode.

show usb port [*port-number*]

Syntax Description

port-number	(Optional) Displays information only for a specified. If the *port-number* is not issued, information for all root ports will be displayed.

Command Modes

Privileged EXEC

Command History

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

Examples

The following sample from the **show usb port** command shows the status of the port 1 on the router:

```
Router# show usb port
Port Number:0
Status:Enabled
Connection State:Connected
Speed:Full
Power State:ON
Port Number:1
Status:Enabled
Connection State:Connected
Speed:Low
Power State:ON
```

show usb-devices summary

To display USB device summary information for all USB devices attached to the router, use the **show usb-devices summary**command in privileged EXEC mode.

show usb-devices summary

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 3.6	This command was integrated into Cisco IOS XE Release 3.6.

Usage Guidelines

Use the **show usb-devices summary** command to display information for either a USB flash drive or a USB eToken, as appropriate.

Examples

The following example is sample output from the **show usb-devices summary** command, which shows that a USB token device is supported by Cisco (see the text in bold).:

```
Router# show usb-devices summary

USB Device: OHCI Host Controller
Bus: 03 Port: 00 Cnt: 00 Speed: 12
Vendor: 1d6b ProdID: 0001 Rev: 2.06
Serial Number: 0001:01:11.1

USB Device: OHCI Host Controller
Bus: 02 Port: 00 Cnt: 00 Speed: 12
Vendor: 1d6b ProdID: 0001 Rev: 2.06
Serial Number: 0001:01:11.0

USB Device: Token 4.28.1.1 2.7.195
Bus: 02 Port: 00 Cnt: 01 Speed: 12
Vendor: 0529 ProdID: 0600 Rev: 1.00
Serial Number:

USB Device: EHCI Host Controller
Bus: 01 Port: 00 Cnt: 00 Speed: 480
Vendor: 1d6b ProdID: 0002 Rev: 2.06
Serial Number: 0001:01:11.2

USB Device: eUSB
Bus: 01 Port: 03 Cnt: 01 Speed: 480
Vendor: 0e39 ProdID: 2b00 Rev: b9.00
Serial Number: 1E884812183636210510
```

show usb tree

To display information about the port state and all attached devices, use the **show usb tree**command in privileged EXEC mode.

show usb tree

Syntax Description

This command has no arguments or keywords.

Command Modes

EXEC

Command History

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

Examples

The following example is sample output from the **show usb tree** command. This output shows that both a USB flash module and a USB eToken are currently enabled.

```
Router# show usb tree

[Host Id:1, Host Type:1362HCD, Number of RH-Port:2]
<Root Port0:Power=ON      Current State=Enabled>
  Port0:(DiskOnKey) Addr:0x1 VID:0x08EC PID:0x0015 Configured (0x1000000)
<Root Port1:Power=ON      Current State=Enabled>
  Port1:(eToken Pro 4254) Addr:0x11 VID:0x0529 PID:0x0514 Configured (0x1010000)
```

show usbtoken

To display information about the USB eToken (such as the eToken ID), use the **show usbtoken**command in privileged EXEC mode.

show usbtoken [**0-9**]**:** {**all***filesystem*}

Syntax Description

0-9	(Optional) One of the ten available flash drives you can choose from; valid values: 0-9. If you do not specify a number, 0 is used by default
all	(Optional) All configuration files stored on the eToken.
filesystem	(Optional) Name of a configuration file.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(11)T	This command was integrated into the Cisco 7200VXR NPE-G2 platform.
Cisco IOS XE Release 3.6	This command was integrated into Cisco IOS XE Release 3.6.

Usage Guidelines

Use the **show usbtoken** command to verify whether a USB eToken is inserted in the router.

Examples

The following example is sample output from the **show usbtoken** command:

```
Router# show usbtoken0
Token ID           :43353334
Token device name  : token0
Vendor name        : Vendor34
Product Name       :Etoken Pro
Serial number      : 22273a334353
Firmware version   :   4.1.3.2
Total memory size  : 32 KB
Free memory size   : 16 KB
FIPS version       :  Yes/No
Token state        :  "Active" | "User locked" | "Admin locked" | "System Error" | "Uknown"
ATR (Answer To Reset) :"3B F2 98 0  FF C1 10 31 FE 55 C8 3"
```

The following table describes the significant fields shown in the display.

Table 54: show usbtoken Field Descriptions

Field	Description
Token ID	Token identifier.
Token device name	A unique name derived by the token driver.
ATR (Answer to Reset)	Information replied by Smart cards when a reset command is issued.

show user-group

To display information about user groups, use the **show user-group**command in privileged EXEC mode.

show user-group [*group-name* | **count**]

Syntax Description

group-name	(Optional) Name of the user-group.
count	(Optional) Displays the total number of user groups, the names of the user groups, and the number of members in each.

Command Modes

Privileged EXEC (#)

Command History

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

Examples

The following is sample output from the show user-group command when the auth_proxy_ug user group is specified.

```
Router# show user-group auth_proxy_ug
!
Usergroup: auth_proxy_ug
------------------------------------------------------------
User Name     Type  Interface   Learn   Age (min)
------------------------------------------------------------
192.168.101.131     IPv4  Vlan333   Dynamic   0
```

!

The following is sample output from the show user-group command when the **count** keyword is used.

```
Router# show user-group count
!
Total Usergroup: 2
--------------------------
User Group    Members
--------------------------
auth_proxy_ug    1
eng_group_ug    1
!
```

The table below describes the significant fields shown in the displays.

Table 55: show user-group Field Descriptions

Field	Description
User Name	IP address of the user-group.
Learn	Describes how the mapping of source IP addresses to user groups is learned.

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
user-group	Defines the user-group associated with the identity policy.

show users

To displa y information about the active lines on the router, use the **show users**command in user EXEC or privileged EXEC mode.

show users [[**all**] [**wide**] | **slot** {*slot-number* | **all**} | **summary**] [**lawful-intercept**]

Syntax Description

all	(Optional) Specifies that all lines be displayed, regardless of whether anyone is using them.
wide	(Optional) Specifies that the wide format be used.
slot	(Optional) Displays information about remote logins to other processes in the chassis.
slot-number	(Optional) The slot number.
summary	(Optional) Displays a summary of user sessions.
lawful-intercept	(Optional) Displays lawful-intercept users.

Command Modes

User EXEC (>)
Privileged EXEC (#)

Command History

Release	Modification
10.0	This command was introduced.
12.3(2)T	The **summary** keyword was introduced.
12.3(7)T	The **lawful-intercept** keyword was introduced.
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRB.
12.2(33)SXI	This command was modified in a release earlier than Cisco IOS Release 12.2(33)SXI. The **slot** keyword and *slot-number* argument were added.
Cisco IOS XE Release 2.1	This command was implemented on the Cisco ASR 1000 Series Aggregation Sevices Routers.

Usage Guidelines

This command displays the line number, connection name, idle time, hosts (including virtual access interfaces), and terminal location. An asterisk (*) indicates the current terminal session.

If the **lawful-intercept** keyword is issued, the names of all users who have access to a configured lawful intercept view will be displayed. To access the **show users lawful-intercept** command, you must be an authorized lawful-intercept-view user.

When an idle timeout is configured on a full virtual access interface and a subvirtual access interface, the **show users** command displays the idle time for both the interfaces. However, if the idle timeout is not configured on both the interfaces, then the **show users** command will display the idle time for the full virtual access interface only.

Examples

The following is sample output from the **show users** command:

```
Router# show users
      Line           User            Host(s)        Idle Location
      0 con 0                        idle
*     2 vty 0        user1           idle            0   SERVICE1.CISCO.COM
```

The following is sample output identifying an active virtual access interface:

```
Router# show users
Line         User      Host(s)                Idle    Location
*  0 con 0             idle                   01:58
  10 vty 0             Virtual-Access2         0      1212321
```

The following is sample output from the **show users all** command:

```
Router# show users all
    Line       User          Host(s)      Idle  Location
*   0 vty 0    user1         idle         0    SERVICE1.CISCO.COM
    1 vty 1
    2 con 0
    3 aux 0
    4 vty 2
```

The table below describes the significant fields shown in the displays.

Table 56: show users Field Descriptions

Field	Description
Line	Contains three subfields: • The first subfield (0 in the sample output) is the absolute line number. • The second subfield (vty in the sample output) indicates the type of line. Possible values follow: aux--auxiliary port con--console tty--asynchronous terminal port vty--virtual terminal • The third subfield (0 in the * sample output) indicates the relative line number within the type.
User	User using the line. If no user is listed in this field, no one is using the line.
Host(s)	Host to which the user is connected (outgoing connection). A value of idle means that there is no outgoing connection to a host.
Idle	Interval (in minutes) since the user has entered something.
Location	Either the hard-wired location for the line or, if there is an incoming connection, the host from which the incoming connection came.

The following sample output from the **show users lawful intercept**command shows three LI-View users on the system--li_admin, li-user1, and li-user2:

```
Router# show users lawful-intercept

li_admin
li-user1
li-user2
Router#
```

Related Commands

Command	Description
line	Identifies a specific line for configuration and starts the line configuration command collection mode.
li-view	Initializes a lawful intercept view.
show line	Displays the parameters of a terminal line.
username	Establishes a username-based authentication system.