Troubleshooting Commands

clear ip nat statistics

To clear the NAT datapath map and session information, use the **clear ip nat statistics** command in privileged EXEC mode.

clear ip nat statistics

Syntax Description

This command has no arguments or keywords.

Command Default None

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.8.1a	This command is supported for Cisco Catalyst SD-WAN.

Usage Guidelines Use the **ip nat clear statistics** command to clear the NAT datapath map and session information.

Examples The following is a sample output from the **ip nat clear statistics** command:

```
Device# ip nat clear statistics
```

clear sdwan app-fwd cflowd flow-all

To clear the cflowd flows in all VPNs, use the **clear sdwan app-fwd cflowd flow-all** command in privileged exec mode.

clear sdwan app-fwd cflowd flow-all

Syntax Description This command has no keywords or arguments.

Command Default None

Command Modes Privileged exec (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines This command can be used to clear all the cflowd flows from all VPNs in a Cisco IOS XE Catalyst SD-WAN device.

Example

The following example shows how to clear the cflowd flows from all VPNs from a Cisco IOS XE Catalyst SD-WAN device.

```
Device# clear sdwan app-fwd cflowd flow-all
```

Related Commands

Command	Description
clear sdwan app-fwd cflowd statistics	Clears all cflowd statistics from a Cisco IOS XE Catalyst SD-WAN device.

clear sdwan app-fwd cflowd statistics

To clear the cflowd packet statistics, use the **clear sdwan app-fwd cflowd statistics** command in privileged EXEC mode.

clear sdwan app-fwd cflowd statistics

Syntax Description This command has no keywords or arguments.

Command Default None

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines This command can be used to clear the cflowd packet statistics from a Cisco IOS XE Catalyst SD-WAN device.

Example

The following example shows how to clear the cflowd packet statistics from a Cisco IOS XE Catalyst SD-WAN device.

```
Device# clear sdwan app-fwd cflowd statistics
```

Related Commands

Command	Description
clear sdwan app-fwd cflowd flow-all	Clears all cflowd flows from a Cisco IOS XE Catalyst SD-WAN device.

clear sdwan app-route statistics

To clear the app-route statistics from a Cisco IOS XE Catalyst SD-WAN device, use the **clear sdwan app-route statistics** command in privileged EXEC mode.

clear sdwan app-route statistics

Syntax Description This command has no keywords or arguments.

Command Default None

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

This command can be used to clear the application aware routing statistics from a Cisco IOS XE Catalyst SD-WAN device.

Example

The following example shows how to clear the app-route statistics from a Cisco IOS XE Catalyst SD-WAN device.

```
Device# clear sdwan app-route statistics
```

clear sdwan appqoe dreopt

To clear DRE cache and restart DRE service, use the **clear sdwan appqoe dreopt cache** command in privileged EXEC mode.

clear sdwan appqoe dreopt { **cache** | **statistics** [**peer**] [**peer-no** *peer-id*] | **auto-bypass** [**server** *server-ip server-port*] }

Syntax Description

cache	Clears DREOPT cache.
statistics	Clears global DRE statistics.
peer	(Optional) Clears DREOPT peer statistics table.
peer-no *peer-id*	(Optional) Clears DREOPT statistics using peer-no for the specified peer ID.
auto-bypass	Clears DRE auto-bypass table.
server *server-ipserver-port*	Clears DRE auto-bypass entries for the specified server IP address and server port.

Command Default

This command has no default behavior.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	This command can be used in SD-WAN controller mode.

Example

The following example shows how to clear DRE cache.

```
Device# clear sdwan appqoe dreopt cache

DRE cache successfully cleared
```

clear sdwan bfd transitions

To clear all Bidirectional Forwarding Detection (BFD) transition counters from a Cisco IOS XE Catalyst SD-WAN device, use the **clear sdwan bfd transitions** command in privileged EXEC mode.

clear sdwan bfd transitions

Syntax Description This command has no keywords or arguments.

Command Default None

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI te

Usage Guidelines The BFD protocol detects link failures as part of the Cisco SD-WAN high availability solution and by default, it is enabled on all Cisco IOS XE Catalyst SD-WAN devices. You cannot disable this protocol. The BFD protocol functionalities include path liveliness and quality measurement.

This command is used to clear all BFD transitions counters from a Cisco IOS XE Catalyst SD-WAN device.

Example

The following example clears all BFD transition counters from a Cisco IOS XE Catalyst SD-WAN device.

```
Device# clear sdwan bfd transitions
```

Related Commands

Command	Description
show sdwan bfd sessions	Displays information about the BFD sessions.
show sdwan bfd history	Displays the history of the BFD sessions.

clear sdwan control connection-history

To erase the connection history on a Cisco IOS XE Catalyst SD-WAN device, use the **clear sdwan control connection-history** command in privileged EXEC mode.

clear sdwan control connection-history

Syntax Description This command has no keywords or arguments.

Command Default None

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines Cisco IOS XE SD-WAN devices establish control plane connection with Cisco SD-WAN Controllers (Cisco SD-WAN Manager, Cisco Catalyst SD-WAN Controller, and Cisco Catalyst SD-WAN Validator), and maintains these connections with Cisco Catalyst SD-WAN Controller and Cisco SD-WAN Manager.

This command can be used to erase all the connection history information from the Cisco IOS XE Catalyst SD-WAN devices.

Example

The following example erases the connection history information from a Cisco IOS XE Catalyst SD-WAN device:

```
Device# clear sdwan control connections-history
```

Related Commands

Command	Description
clear control connections	Resets the DTLS connections from a local device to all Cisco IOS XE Catalyst SD-WAN devices.
show sdwan control connection-history	Displays control connection history.

clear sdwan control connections

To reset the DTLS connections from a Cisco IOS XE Catalyst SD-WAN device to the SD-WAN controllers, use the **clear sdwan control connections** command in privileged EXEC mode.

clear sdwan control connections

Syntax Description This command has no keywords or arguments.

Command Default None

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

Cisco IOS XE SD-WAN devices establish control plane connection with Cisco SD-WAN Controllers (Cisco SD-WAN Manager, Cisco Catalyst SD-WAN Controller, and Cisco Catalyst SD-WAN Validator), and maintains these connections with Cisco Catalyst SD-WAN Controller and Cisco SD-WAN Manager.

This command can be used to reset the DTLS connections from a Cisco IOS XE Catalyst SD-WAN device to the Cisco SD-WAN Controllers.

Example

The following example shows how to reset the DTLS connections.

```
Device# clear sdwan control connections
```

Related Commands

Command	Description
clear control connections-history	Erases the connection history on a Cisco IOS XE Catalyst SD-WAN device.
show sdwan control connections	Displays information about control connections.
show sdwan control connection-history	Displays information about control connections history.

clear sdwan control port-index

To reset port-hop back to the base port on Cisco IOS XE Catalyst SD-WAN devices, use the **clear sdwan control port-index** command in privileged EXEC mode.

clear sdwan control port-index

Syntax Description

This command has no keywords or arguments.

Command Default

This command has no default behavior.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	This command was introduced.

Usage Guidelines

Use the **clear sdwan control port-index** command to reach back to 12346 base port on all the WAN interfaces.

Examples

The following example shows how to clear SD-WAN control port-index:

```
Device# clear sdwan control port-index
```

clear sdwan dns app-fwd cflowd flow-all

To clear the DNS cache for all cflowd flows, use the **clear sdwan dns app-fwd cflowd flow-all** command in privileged EXEC mode.

clear sdwan dns app-fwd cflowd flow-all

Syntax Description This command has no keywords or arguments.

Command Default None

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines This command can be used to clear the DNS cache for all cflowd flows in a Cisco IOS XE Catalyst SD-WAN device.

Example

The following example shows how to clear the DNS cache for all cflowd flows in a Cisco IOS XE Catalyst SD-WAN device.

```
Device# clear sdwan dns app-fwd cflowd flow-all
```

Related Commands

Command	Description
clear control connections-history	Erases the connection history on a Cisco IOS XE Catalyst SD-WAN device.
clear sdwan dns app-fwd cflowd flow-all	Clears all cflowd flows.

clear sdwan dns app-fwd cflowd statistics

To clear the cflowd statistics from a Cisco IOS XE Catalyst SD-WAN device, use the **clear sdwan dns app-fwd cflowd statistics** command in privileged EXEC mode.

clear sdwan dns app-fwd cflowd statistics

Syntax Description This command has no keywords or arguments.

Command Default None

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI te

Usage Guidelines

This command can be used to clear the cflowd statistics from a Cisco IOS XE Catalyst SD-WAN device.

Example

The following example shows how to clear the cflowd statistics from a Cisco IOS XE Catalyst SD-WAN device.

```
Device# clear sdwan dns app-fwd cflowd statistics
```

Related Commands

Command	Description
clear sdwan dns app-fwd cflowd flow-all	Clears all cflowd flows from a Cisco IOS XE Catalyst SD-WAN device.

clear sdwan dns app-fwd dpi flow-all

To clear the DNS Deep Packet Inspection (DPI) flows from a Cisco IOS XE Catalyst SD-WAN device, use the **clear sdwan dns app-fwd dpi flow-all** command in privileged exec mode.

clear sdwan dns app-fwd dpi flow-all

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Privileged exec (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI ten

Usage Guidelines

This command can be used to clear the DNS DPI flows from a Cisco IOS XE Catalyst SD-WAN device.

Example

The following example shows how to clear the dpi flows from a Cisco IOS XE Catalyst SD-WAN device.

```
Device# clear sdwan dns app-fwd dpi flow-all
```

Related Commands

Command	Description
clear sdwan dns app-fwd dpi summary	Clears all DPI statistics.

clear sdwan dns app-fwd dpi summary

To clear all known dpi statistics for all related app information, use the **clear sdwan dns app-fwd dpi summary** command in privileged EXEC mode. This command does not have a **no** form.

clear sdwan dns app-fwd dpi summary

Syntax Description This command has no keywords or arguments.

Command Default None

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines Use this command to clear out any dpi statistics for all related app information.

Example

The following example clears the dpi statistics for all related app information.

```
Device#clear sdwan dns app-fwd dpi summary
```

Table 1: Related Commands

Commands	Description
clear sdwan dns app-fwd dpi flow-all	Clears all dpi flows in the entire system.

clear sdwan dns app-route statistics

To clear all app-route statistics, use the **clear sdwan dns app-route statistics** command in privileged EXEC mode. This command does not have a **no** form.

clear sdwan dns app-route statistics

Syntax Description This command has no keywords or arguments.

Command Default None

Command Modes Privileged EXEC(#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

Use this command to clear all app route related statistics from the system.

Example

The following example clears all app route statistics from the router.

```
Device# clear sdwan dns app-route statistics
```

clear sdwan dns cache

To clear the cache of DNS entries on a Cisco IOS XE Catalyst SD-WAN device, use the **clear sdwan dns cache** command in privileged EXEC mode.

clear sdwan dns cache

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN

Usage Guidelines

The DNS cache is populated when a Cisco IOS XE Catalyst SD-WAN device establishes a connection with the Cisco Catalyst SD-WAN Validator. For a Cisco IOS XE Catalyst SD-WAN device, this connection is transient, and the DNS cache is cleared when the connection to the Cisco Catalyst SD-WAN Validator is closed.

This command can be used to clear the DNS cache from a Cisco IOS XE Catalyst SD-WAN device.

Example

The following example shows how to clear the DNS cache from a Cisco IOS XE Catalyst SD-WAN device.

```
Device# clear sdwan dns cache
```

Command	Description
show sdwan control local-properties	Displays control plane local properties, including entries in the DNS cache.

clear sdwan installed-certificates

To clear all the installed certificates from a Cisco IOS XE Catalyst SD-WAN device, use the **clear sdwan installed-certificates** command in privileged EXEC mode.

clear sdwan installed-certificates

Syntax Description This command has no keywords or arguments.

Command Default None

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines This command can be used to clear all the installed certificates from a Cisco IOS XE Catalyst SD-WAN device, including the public and private keys, and the root certificate. After clearing all certificates from a device, the command resets the device to factory default.

Example

The following example shows how to clear all the installed certificates from a Cisco IOS XE Catalyst SD-WAN device.

```
Device# clear sdwan installed-certificates
```

Related Commands

Command	Description
show sdwan control local-properties	Displays control plane local properties, including entries in the DNS cache.

clear sdwan notification stream viptela

To clear the SD-WAN notification stream viptela, use the **clear sdwan notification stream viptela** command in privileged EXEC mode.

clear sdwan notification stream viptela

Syntax Description This command has no keywords or arguments.

Command Default None

Command Modes Privileged EXEC(#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

Use this command to clear the sdwan notification stream viptela.

Example

The following example shows how to clear the sdwan notification stream viptela.

```
Device#clear sdwan notification stream viptela
```

clear sdwan omp

To clear Cisco SD-WAN Overlay Management Protocol (OMP) peers, routes,and TLOCs, use the **clear sdwan omp** command in privileged exec mode.

clear sdwan omp { **all** | **peer** [*ipv4 address*] | **routes** | **tlocs** }

Syntax Description

all	Clears all OMP peering sessions with all OMP peers.
peer	Clears the OMP peering sessions with a specific peer.
ipv4 address	(Optional) Specifies an IPv4 address of the OMP peer
routes	Clears OMP routes.
tlocs	Clears OMP TLOCs.

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Privileged exec (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

By default, all Cisco IOS XE Catalyst SD-WAN Edge devices establishes OMP peering with Cisco Catalyst SD-WAN Controllers.

This command can be used to clear Cisco SD-WAN OMP peers, routes, and TLOCs that it learns from the Cisco Catalyst SD-WAN Controller.

Example

The following example shows how to reset OMP peering sessions.

```
Device# clear sdwan omp all
```

The following example shows how to clear OMP peering session with a specific peer.

```
Device# clear sdwan omp peer 10.10.10.10
```

The following example shows how to clear OMP routes.

```
Device# clear sdwan omp routes
```

Related Commands

Command	Description
show sdwan omp peers	Displays information about all OMP peering sessions.
show sdwan omp routes	Displays information about OMP routes.
show sdwan omp tlocs	Displays information learned from the TLOC routes advertised using OMP sessions.

clear sdwan policy

To reset counters for IPv6 access lists, route policies, or data policies, use the **clear sdwan policy** command in privileged EXEC mode.

clear sdwan policy { **access-list** [*acl-name*] | **app-route-policy** [*policy-name*] | **ipv6-access-list** [*access-list-name*] | **data-policy** [*policy-name*] }

Syntax Description

acl-name	(Optional) Clears the counters associated with the specified access list.
policy-name	(Optional) Clears the counters associated with the specified application-aware routing policy.
access-list-name	(Optional) Clears Cisco SD-WAN policy IPv6 access-list counters.
policy-name	(Optional) Clears the counters associated with the specified data policy.

Command Default

None

Command Modes

Privileged exec (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager C

Usage Guidelines

The SD-WAN centralized policies comes from the Cisco Catalyst SD-WAN Controller to Cisco IOS XE Catalyst SD-WAN devices.

This command can be used to clear counters for IPv6 access lists, data policies, or route policies.

Example

The following example shows how to clear all access lists.

```
Device# clear sdwan policy access-list
```

The following example shows how to clear all app-route-policy.

```
Device# clear sdwan policy app-route-policy
```

The following example shows how to clear all IPv6 access lists.

```
Device# clear sdwan policy ipv6-access-list
```

Related Commands

Command	Description
show sdwan policy from-vsmart	Displays Cisco SD-WAN centralized policies from Cisco Catalyst SD-WAN Controller.

clear sdwan reverse-proxy context

To clear the signed certificate installed for authentication with a reverse proxy device and reset the control connections to the reverse proxy device, use the **clear sdwan reverse-proxy context** command in privileged EXEC mode.

clear sdwan reverse-proxy context

Syntax Description This command has no keywords or arguments

Command Default None

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 17.6.1a	Command introduced.

Example

```
Device# clear sdwan reverse-proxy context
```

clear sdwan tunnel gre-keepalive

To clear the GRE tunnel keepalives, use the **clear sdwan tunnel gre-keepalive** command in privileged EXEC mode.

clear sdwan tunnel gre-keepalive

Syntax Description This command has no keywords or arguments.

Command Default None

Command Modes Privileged EXEC(#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines Use **clear sdwan tunnel gre-keepalive** command to clear the SD-WAN tunnel gre-keepalives.

Example

The following example shows how to clear the SD-WAN tunnel gre keepalives.

```
Device# clear sdwan tunnel gre-keepalive
```

Table 2: Related Commands

Commands	Description
clear sdwan tunnel statistics	Clears SD-WAN tunnel statistics.

clear sdwan tunnel statistics

To reset the information about the packets received on the IPsec connections for the Cisco IOS XE Catalyst SD-WAN devices, use the **clear sdwan tunnel statistics** command in privileged EXEC mode.

clear sdwan tunnel statistics

Syntax Description This command has no keywords or arguments.

Command Default None

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines This command can be used to reset the information about the packets transmitted and received on the IPsec connections that originate on Cisco IOS XE Catalyst SD-WAN devices.

Example

The following example shows how to reset the information about the packets transmitted and received on the IPsec connections.

```
Device# clear sdwan tunnel statistics
```

Related Commands

Command	Description
show sdwan tunnel statistics	Displays information about the packets transmitted and received on the IPsec connections.

clear sdwan umbrella dp-stats

To clear the umbrella dp-stats, use the **clear sdwan umbrella dp-stats** command in privileged EXEC mode. This command does not have a **no** form.

clear sdwan umbrella dp-stats

Syntax Description This command has no keywords or arguments.

Command Default None

Command Modes Privileged EXEC(#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines Use **clear sdwan umbrella dp-stats** command to clear the SD-WAN umbrella datapath stats.

Example

The following example shows how to clear the SD-WAN umbrella data path stats.

```
Device# clear sdwan umbrella dp-stats
```

clear sdwan utd engine standard logging events

To clear SD-WAN UTD engine logging events, use the **clear sdwan utd engine standard logging events** command in privileged EXEC mode.

clear sdwan utd engine standard logging events

Syntax Description This command has no keywords or arguments.

Command Default None

Command Modes Privileged EXEC(#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines Use **clear sdwan utd engine standard logging events** command to clear the SD-WAN UTD engine logging events.

Example

The following example shows how to clear the SD-WAN UTD engine logging events.

```
Device# clear sdwan utd engine standard logging events
```

clear sdwan utd engine standard statistics daq vrf

To clear SD-WAN UTD engine statistics for all VRFs or a specific VRF, use the **clear sdwan utd engine standard statistics daq vrf** command in privileged EXEC mode. This command does not have a **no** form.

clear sdwan utd engine standard statistics daq vrf { **global** | *name* }

Syntax Description

global	Clears SD-WAN UTD engine standard statistics for all VRFs.
name	Clears SD-WAN UTD engine standard statistics for a specific VRF.

Command Default None

Command Modes Privileged EXEC(#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines Use this command to clear the SD-WAN UTD engine standard statistics for all VRFs or a specific VRF.

Example

The following example shows how to clear the SD-WAN UTD engine statistics for all VRFs.

```
Device# clear sdwan utd engine standard statistics daq vrf global
```

clear sdwan utd engine standard statistics url-filtering vrf

To clear SD-WAN UTD engine url-filtering statistics all VRFs or for a specific VRF, use the **clear sdwan utd engine standard statistics url-filtering vrf** command in privileged EXEC mode. This command does not have a **no** form.

clear sdwan utd engine standard statistics url-filtering vrf { **global** | *name* }

Syntax Description

global	Clears SD-WAN UTD engine standard statistics for all VRFs.

name	Clears SD-WAN UTD engine standard statistics for a specific VRF.

Command Default

None

Command Modes

Privileged EXEC(#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

Use this command to clear the SD-WAN UTD engine standard url-filtering statistics for all VRFs or for a specific VRF.

Example

The following example shows how to clear the SD-WAN UTD engine url filtering statistics for all VRFs.

```
Device# clear sdwan utd engine standard statistics url-filter vrf global
```

clear sdwan utd statistics

To clear SD-WAN UTD statistics, use the **clear sdwan utd statistics** command in privileged EXEC mode. This command does not have a **no** form.

clear sdwan utd statistics { **channel** [*service* | *threat-defense*] | **default** [**channel** | **context** | **policy** | **tls-decrypt** | **vrf**] | **divert** | **drop** | **general** | **policy** [*all*] | **sn** | **summary** | **tls-decrypt** | **vrf** [**default** | **global** | *id* | *name*] }

Syntax Description

channel	Clears channel-specific UTD dataplane statistics.
service	Clears UTD dataplane stats for service channel.
threat-defense	Clears UTD dataplane stats for threat-defense channel.
default	Clears SD-WAN UTD statistics default.
context	Clears SD-WAN UTD statistics default context.
policy	Clears UTD dataplane policy statistics.
tls-decrypt	Clears SD-WAN UTD statistics tls-decrypt.
vrf	Clears SD-WAN UTD statistics VRF.
divert	Clears SD-WAN UTD statistics divert.
drop	Clears SD-WAN UTD statistics drop.

general	Clears SD-WAN UTD statistics general.
policy	Clears UTD dataplane policy statistics.
all	Clears UTD dataplane policy statistics all.
sn	Clears SD-WAN UTD statistics sn.
summary	Clears SD-WAN UTD statistics summary.
vrf	Clears SD-WAN UTD statistics VRF.
default	Clears SD-WAN UTD statistics VRF default.
global	Clears SD-WAN UTD statistics VRF global.
id	Clears SD-WAN UTD statistics VRF ID.
name	Clears SD-WAN UTD statistics VRF name.

Command Default None

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines Use this command to clear SD-WAN UTD statistics.

Example

The following example shows how to clear the SD-WAN UTD statistics from the default VRF.

```
Device# clear sdwan utd statistics vrf default
```

clear sdwan zbfw statistics drop

To clear SD-WAN ZBFW drop statistics, use the **clear sdwan zbfw statistics drop** command in privileged EXEC mode. This command does not have a **no** form.

clear sdwan zbfw statistics drop

Syntax Description This command has no keywords or arguments.

Command Default None

Command Modes Privileged EXEC(#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

Use **clear sdwan zbfw statistics drop** command to clear the SD-WAN ZBFW drop statistics.

Example

The following example shows how to clear the SD-WAN ZBFW drop statistics.

```
Device# clear sdwan zbfw statistics drop
```

debug packet-trace condition

To enable packet tracing on edge devices, use the **debug packet-trace condition** command in privileged EXEC mode.

debug packet-trace condition [**start** | **stop**] [**bidirectional**] [**circular**] [**destination-ip** *ip-address*] [**ingress-if** *interface*] [**logging**] [**source-ip** *ip-address*] [**vpn-id** *vpn-id*]

Syntax Description

bidirectional	(Optional) Enables bidirectional flow debugging for source IP and destination IP.
circular	(Optional) Enables circular packet tracing. In this mode, the 1024 packets in the buffer are continuously overwritten.
clear	(Optional) Clears all the debug configurations and packet tracer memory.
destination-ip	(Optional) Specifies the destination IPv4 address.
ingress-if	(Optional) Specifies the ingress interface name. Note: It is must to choose VPN to configure the interface.
logging	(Optional) Enables the packet tracer debug logging.
source-ip	(Optional) Specifies the source IP address.
start	(Optional) Starts the conditional debugging.
stop	(Optional) Stops the conditional debugging.
vpn-id	(Optional) Enables the packet tracing for the specified VPN.

Command Default

None

Command Modes

Privileged EXEC (#)

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.8.1a	This command was introduced.

Usage Guidelines

The parameters after the keywords **start** and **stop** can be configured in any order.

Example

The following example shows how to configure conditions for packet tracing:

```
Device# debug packet-trace condition source-ip 10.0.0.1
Device# debug packet-trace condition vpn-id 0
Device# debug packet-trace condition interface ge0/1
Device# debug packet-trace condition stop
```

debug platform condition match

To filter IPv4 and IPv6 debugging output for certain **debug** commands on the basis of specified conditions, use the **debug platform condition match protocol** command in privileged EXEC mode. To remove the specified condition, use the **no** form of this command.

debug platform condition interface *interface name* **match** [{ **ipv4 | ipv6** }] **protocol** [{ **tcp** | **udp** | **protocol_id** }] [{ **src ip** | **src ip mask** | **src port** | **destination ip** | **destination ip mask** | **destination port** }] [{ **both** | **ingress** | **egress** }] [**bidirectional**]
no debug platform condition match protocol

Syntax Description

interface *interface*	Filters the output on the basis of the interface specified.
match	Enables conditional debugging for matching packets.
IPv4	(Optional) Filters the output on the basis of the specified IPv4 address.
Ipv6	(Optional) Filters the output on the basis of the specified IPv6 address.
protocol	Filters the output on the basis of the specified protocol.
tcp	(Optional) Specifies TCP to filter the output on the basis of the TCP.
udp	(Optional) Specifies UDP to filter the output on the basis of the UDP.
protocol_id	(Optional) Specifies protocol ID to filter the output on the basis of the protocol ID.
src ip	(Optional) Specifies the source IP address to filter the output on the basis of the source IP.
src ip mask	(Optional) Specifies the source IP subnet mask to filter the output on the basis of the source IP subnet mask.
destination ip	(Optional) Specifies the destination IP address to filter output on the basis of the destination IP address.
destination ip mask	(Optional) Specifies the destination IP address to filter output on the basis of the destination IP subnet mask.
destination port	(Optional) Specifies the destination port address to filter output on the basis of the destination port.

both	(Optional) Filters output on the basis of both incoming and outgoing packets.
ingress	(Optional) Filters output on the basis of incoming packets.
egress	(Optional) Filters output on the basis of outgoing packets.
bidirectional	(Optional) Filters output in both the directions.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.8.1a	This command was introduced.

The following example shows how to create the equivalent bidirectional Access Control List (ACL) to match the packet flow in both directions.

```
Device# debug packet-trace condition source-ip 10.0.0.1
Device# debug packet-trace condition destination-ip 10.0.0.2
Device# debug platform condition match ipv4 host 10.0.0.1 host 10.0.0.2 both bidirectional
Device# debug packet-trace condition stop
```

debug platform condition start

To start conditional debugging on a system, use the **debug platform condition start** command in privileged EXEC mode.

debug platform condition start

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.8.1a	This command was introduced.

The following example shows how to start conditional debugging on a system:

```
Device# debug platform condition interface Gi0/0/1 efp-id 100 access-list 700
Device# debug platform feature evc dataplane
Device# debug platform condition start
```

debug platform condition stop

To stop conditional debugging on a system, use the **debug platform condition stop** command in privileged EXEC mode.

debug platform condition stop

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.8.1a	This command was introduced.

The following example shows how to stop conditional debugging on a system.

```
Device# debug platform condition interface Gi0/0/1 efp-id 100 access-list 700
Device# debug platform feature evc dataplane
Device# debug platform condition start
Device# debug platform condition stop
```

debug platform condition feature sdwan controlplane bfd

To start conditional debugging on a system for BFD sessions on a control plane, use the **debug platform condition feature sdwan controlplane bfd** command in privileged EXEC mode.

debug platform condition feature sdwan controlplane bfd

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.15.1a	This command was introduced.

Examples

The following example shows how to enable debugging mode for BFD sessions on a control plane:

```
Device# debug platform condition feature sdwan controlplane bfd
  ld         BFD LD
  tloc-pair  BFD tloc pair

Device# debug platform condition feature sdwan controlplane bfd ld 20008
Device# debug platform condition
Device# debug platform condition start

Device# debug platform condition feature sdwan controlplane bfd tloc-pair
encap ipsec local-color mpls remote-color mpls system-ip 172.16.255.1
```

```
debug platfom condition start
```

debug platform software sdwan fpm

To enable debugging mode for Forwarding Policy Manager, use the **debug platform software sdwan fpm** command in privileged EXEC mode. To disable debugging mode for Forwarding Policy Manager, use the **undebug** form of the command.

debug platform software sdwan fpm { **all** | **config** | **dpi** | **policy** | **ttm** }
undebug platform software sdwan fpm { **all** | **config** | **dpi** | **policy** | **ttm** }

Syntax Description

all	Controls the debugging of events related to the forwarding policy manager, including configuration changes, application-aware routing events, and communication with the tunnel table manager.
config	Controls the debugging of messages that are logged as a result of a policy configuration change made either directly on the router or because the changes have been pushed from the Cisco vSmart controller to the router.
dpi	Controls the debugging of all application-aware routing (deep packet inspection) events.
policy	Controls the debugging of messages that are logged as the result of policy programming events.
ttm	Controls the debugging of communication between the forwarding policy manager and the tunnel table manager.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

Use the **debug platform software sdwan fpm** command to enable debugging mode for Forwarding Policy Manager. Debug output is placed in the *bootflash:/tracelogs* folder on the local device.

Examples

The following example shows how to enable debugging mode for Forwarding Policy Manager. After the information is collected, you can disable it, using the undebug form of the command:

```
Device# debug debug platform software sdwan fpm all
Device# undebug debug platform software sdwan fpm all
```

debug vdaemon

To enable and disable debugging mode for vdaemon software function on Cisco SD-WAN controllers. The debug output is saved to the /var/log/tmplog/vdebug file on the local device.

debug vdaemon { **all** | **cert** | **confd** | **error** | **events** | **ftm** | **hello** | **misc** | **mts** | **ncs** | **packets** | **peer** *sess-id logging module verbosity level* | **rtm** | **ssl** | **ttm** }
no debug vdaemon { **all** | **cert** | **confd** | **error** | **events** | **ftm** | **hello** | **misc** | **mts** | **ncs** | **packets** | **peer** *sess-id logging module verbosity level* | **rtm** | **ssl** | **ttm** }

Syntax Description

all	Enables the display of debugging output for all vdaemon processes.
cert	Enables the display of debugging output for vdaemon certificate functions.
confd	Enables the display of debugging output for vdaemon process CLI functions.
error	Enables the display of debugging output errors for vdaemon actions.
events	Enables the display of debugging output for vdaemon process events.
ftm	Enables the display of debugging output for vdaemon ftm actions.
hello	Enables the display of debugging output for vdaemon hello packets.
misc	Enables the display of debugging output for miscellaneous vdaemon process events.
mt	Enables the display of debugging output for vdaemon multi-tenant actions.
ncs	Enables the display of debugging output for vdaemon networked control system (NCS) actions.
packets	Enables the display of debugging output for all vdaemon process packets.
peer *sess-id logging module verbosity level*	Enables the display of debugging output for communication between peer sessions. *logging module*: verifies the logs for the peer. *verbosity level*: Enables verbose logs for the module specified only of the peer whose session id is provided.
rtm	Enables the display of debugging output for communication between the Cloud OnRamp for SaaS and the route table manager.
ssl	Enables the display of debugging output for vdaemon SSL actions.
ttm	Enables the display of debugging output for communication between the Cloud OnRamp for SaaS and the tunnel table manager.

Command Default

None

Command Modes Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Release 17.3.1a	This command was introduced.
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	The following new keywords are added: • ftm • mt • ncs • rtm • ssl • ttm • peer *sess-id logging module verbosity level*

Examples The following is a sample output for **debug vdaemon peer** command.

```
Device# debug vdaemon peer sess-ID 22
Sess ID: 0000000012
Sess ID: 0000000022


Device# debug vdaemon ttm ?

Possible completions:
  debug     Debug logs
  error     Error logs
  notice    Notice logs
  verbose   Verbose logs
  |         Output modifiers
  <cr>

Device# debug vdaemon ttmverbose
```

debug platform software sdwan vdaemon

To enable debugging mode for vdaemon peer on Cisco SD-WAN Controllers, use the **debug platform software sdwan vdaemon peer** command in privileged EXEC mode. To disable debugging mode, use the **no** form of the command.

debug platform software sdwan vdaemon *session-id*

no debug platform software sdwan vdaemon peer *session-id*

Syntax Description

peer	Specifies the peer name.

session-id	Specifies the session ID.

Command Default None

Command Modes Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	This command was introduced.

Example

```
Device# debug platform software sdwan vdaemon peer
session-id
Device#  no debug platform software sdwan vdaemon peer
session-id
```

set platform software trace

To configure the binary trace level for one or all modules of a Cisco SD-WAN process on a specific hardware slot, issue the command **set platform software trace** in the Privileged EXEC mode.

set platform software trace *process slot module level*

Syntax Description

process	Specify a Cisco SD-WAN process. For the list of Cisco SD-WAN processes for which binary trace is supported see the table 'Supported Cisco SD-WAN Daemons' under 'Usage Guidelines'.
level	Hardware slot from which process messages must be logged.
module	Configure the trace level for one or all the modules of the process.

slot	Select one of the following trace levels: • debug: Debug messages • emergency: Emergency possible message • error: Error messages • info: Informational messages • noise: Maximum possible message • notice: Notice messages • verbose: Verbose debug messages • warning: Warning messages

Command Default

Notice level

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command support introduced for select Cisco SD-WAN processes. See the table 'Supported Cisco SD-WAN Daemons' under 'Usage Guidelines'.
Cisco IOS XE Catalyst SD-WAN Release 17.11.1a	New parameters are introduced for better binary configuration.

Usage Guidelines

Table 3: Supported Cisco SD-WAN Daemons

Cisco SD-WAN Daemons	Supported from Release
• fpmd • ftm • ompd • vdaemon • cfgmgr	Cisco IOS XE Catalyst SD-WAN Release 17.4.1a

Example

In the following example, the binary trace level for the 'config' module of the 'fpmd' process on the 'RP active' FRU is set to 'debug'.

```
Device# set platform software trace fpmd RP active config debug
```

set platform software trace vdaemon

To set the trace level for a specific module within a process on Cisco SD-WAN Controllers, use the **set platform software trace** command in privileged EXEC mode. The tracing functionality logs internal events. Trace files are automatically created and saved to the tracelogs subdirectory.

set platform software trace vdaemon *R0 RP verbose*

Syntax Description

R0	Specifies the route processor with slot 0.
RP	Specifies the route processor.
verbose	(Optional) Displays verbose information, meaning all information that can be displayed on the console during the process will be displayed.

Command Default

Trace levels are not set.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	This command was introduced.
Cisco IOS XE Release 17.12.1a	The following new modules are added: • vdaemon-cert • vdaemon-ftm • vdaemon-mt • vdaemon-ncs • vdaemon-rtm • vdaemon-ssl • vdaemon-ttm

Example

This example shows the trace level verbose for all the modules in the route processor with slot 0:

```
Device# set platform software trace vdaemon R0 vdaemon verbose
vdaemon-affinity  vdaemon-cert  vdaemon-confd  vdaemon-err
vdaemon-event     vdaemon-ftm   vdaemon-hello  vdaemon-misc
vdaemon-mt        vdaemon-ncs   vdaemon-pkt    vdaemon-pwk
vdaemon-rtm       vdaemon-ssl   vdaemon-ttm
```

This example shows the trace level verbose for all the modules in the route processor:

```
Device#  set platform software trace vdaemon RP active vdaemon verbose
```

```
vdaemon-affinity  vdaemon-cert   vdaemon-cfgdb  vdaemon-confd
vdaemon-err       vdaemon-event  vdaemon-ftm    vdaemon-hello
vdaemon-misc      vdaemon-mt     vdaemon-ncs    vdaemon-pkt
vdaemon-pwk       vdaemon-rtm    vdaemon-ssl    vdaemon-ttm
```

show sdwan control connections

To display the information about active control connections and control plane connections on Cisco IOS XE SD-WAN devices, use the **show sdwan control connections** command in privileged EXEC mode.

show sdwan control connections [**detail**]

Syntax Description

detail	(Optional) Displays detailed information about active control plane connections.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	This command was introduced.
Cisco IOS XE Catalyst SD-WAN Release 17.12.1a	Added the peer-session-id details in the control connection summary display.

Example

```
Device# show sdwan control connections detail

----------------------------------------------------------------------
LOCAL-COLOR- lte SYSTEM-IP- 172.16.255.19   PEER-PERSONALITY- vsmart
----------------------------------------------------------------------
site-id             100
domain-id           1
protocol            tl
sprivate-ip          10.0.5.19
private-port        23556
public-ip           10.0.5.19
public-port         23556
org-name            Cisco Systems Regression
state               up [Local Err: NO_ERROR] [Remote Err: NO_ERROR]
uptime              0:00:00:42
hello interval      1000
hello tolerance     12000
controller-grp-id   0
shared-region-id-set N/A
peer-session-id      0x004ff14166
```

monitor capture (access list/class map)

To configure a monitor capture specifying an access list or a class map as the core filter for the packet capture, use the **monitor capture** command in privileged EXEC mode. To disable the monitor capture with the specified access list or class map as the core filter, use the **no** form of this command.

monitor capture *capture-name* { **access-list** *access-list-name* | **class-map** *class-map-name* }
no monitor capture *capture-name* { **access-list** *access-list-name* | **class-map** *class-map-name* }

Syntax Description

capture-name	Specify the name of the capture.
access-list *access-list-name*	Specify an access list with the specified name.
class-map *class-map-name*	Specify a class map with the specified name.

Command Default

A monitor capture with the specified access list or a class map as the core filter for the packet capture is not configured.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	This command was introduced.

Usage Guidelines

Configure the access list using the **ip access-list** command or the class map using the **class-map** command before using the **monitor capture** command. You can specify a class map, or an access list, or an explicit inline filter as the core filter. If you have already specified the filter when you entered the **monitor capture match** command, the command replaces the existing filter.

Examples

The following example shows how to define a core system filter using an existing access control list:

```
Device> enable
Device# configure terminal
Device(config)# ip access-list standard acl1
Device(config-std-nacl)# permit any
Device(config-std-nacl)# exit
Device(config)# exit
Device# monitor capture mycap access-list acl1
Device# end
```

The following example shows how to define a core system filter using an existing class map:

```
Device> enable
Device# configure terminal
Device(config)# ip access-list standard acl1
Device(config-std-nacl)# permit any
Device(config-std-nacl)# exit
Device(config)# class-map match-all cmap
Device(config-cmap)# match access-group name acl
Device(config-cmap)# exit
Device(config)# exit
```

```
Device# monitor capture mycap class-map classmap1
Device# end
```

Related Commands

Command	Description
class-map	Configures a class map.
ip access-list	Configures an access list.
match access-group	Configures the match criteria for a class map on the basis of the specified ACL.
monitor capture (interface/control plane)	Specifies attachment points with direction.
monitor capture match	Defines an explicit inline core filter.
permit	Sets conditions in a named IP access list.
show monitor capture	Displays packet capture details.

monitor capture (interface/control plane)

To configure monitor capture specifying an attachment point and the packet flow direction, use the **monitor capture** command in privileged EXEC mode. To disable the monitor capture with the specified attachment point and the packet flow direction, use the **no** form of this command.

monitor capture *capture-name* {**interface** *type number* | **control-plane**} {**in** | **out** | **both**}
no monitor capture *capture-name* {**interface** *type number* | **control-plane**} {**in** | **out** | **both**}

Syntax Description

capture-name	Specify the name of the capture.
interface *type number*	Specify an interface with the specified type and number as an attachment point.
control-plane	Specify a control plane as an attachment point.
in	Specifies the inbound traffic direction.
out	Specifies the outbound traffic direction.
both	Specifies both inbound and outbound traffic directions.

Command Default

The monitor packet capture filter specifying is not configured.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	This command was introduced.

Usage Guidelines

Repeat the **monitor capture** command as many times as required to add multiple attachment points.

Examples

The following example shows how to add an attachment point to an interface:

```
Device> enable
Device# monitor capture mycap interface GigabitEthernet 2 in
Device# end
```

The following example shows how to add an attachment point to a control plane:

```
Device> enable
Device# monitor capture mycap control-plane out
Device# end
```

Related Commands

Command	Description
access-list	Configures an access list.
class-map	Configures a class map.
monitor capture match	Defines an explicit in-line core filter.
monitor capture (access list/class map)	Specifies an access list or class map as the core filter during packet capture.
show monitor capture	Displays packet capture details.

monitor capture match ipv4

To define a core filter for monitoring packet capture for IPv4 packets, use the **monitor capture match ipv4** command in privileged EXEC mode. To remove this filter, use the **no** form of this command.

monitor capture *capture-name* **match ipv4** *source-prefix/length destination-prefix/length* [**bidirectional**]

no monitor capture *capture-name* [**match**]

Syntax Description

capture-name	Name of the capture.
source-prefix/length	Network prefix and length of the IPv4 source address.
destination-prefix/length	Network prefix and length of the IPv4 destination address.
bidirectional	(Optional) Captures bidirectional packets.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command is supported for Cisco Catalyst SD-WAN.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE `monitor capture match` command.

Examples

The following example shows how to define a core filter for monitoring packet capture for IPv4 packets:

```
Device# monitor capture match CISCO ipv4 198.51.100.0/24 192.0.2.0/24 bidirectional
```

monitor capture match ipv6

To define a core filter for monitoring packet capture for IPv6 packets, use the **monitor capture match ipv6** command in privileged EXEC mode. To remove this filter, use the **no** form of this command.

monitor capture *capture_name* **match ipv6** { { *ipv6-source-prefix/length* | **any** | **host** *ipv6-source-address* } { *ipv6-destination-prefix/length* | **any** | **host** *ipv6-destination-address* } | **protocol** { *protocol_num* | **tcp** | **udp** } { *ipv6-source-prefix/length* | **any** | **host** *ipv6-source-address* } [**eq** | **lt** | **gt** | **neg** | **range** *port-num*] { *ipv6-destination-prefix/length* | **any** | **host** *ipv6-destination-address* } [**eq** | **lt** | **gt** | **neg** | **range** *port-num*] } [**bidirectional**]
no monitor capture *capture_name*

Syntax Description

capture_name	Name of the capture.
interface_name	Specify GigabitEthernet IEEE 802.3z interface name.
interface_num	Specify the GigabitEthernet interface number. Range: 1 to 32.
match	Describes filters inline.
ipv6	IPv6 packets only.
ipv6-prefix/length	IPv6 source or destination prefix. Range for the Length value: 0 to 128.
host *ipv6-address*	Specifies a single source or destination IPv6 host.
protocol_num	Specifies an IP protocol number.
any	Specifies the network prefix and length of any IPv4 or IPv6 destination address.
TCP | **UDP**	Filter by TCP or UDP protocol.
eq	(Optional) Specifies that only packets with a port number that is equal to the port number associated with the IP address are matched.
lt	(Optional) Specifies that only packets with a port number that is lower than the port number associated with the IP address are matched.
gt	(Optional) Specifies that only packets with a port number that is greater than the port number associated with the IP address are matched.

neg	(Optional) Specifies that only packets with a port number that is not equal to the port number associated with the IP address are matched.
range *port-num*	(Optional) Specifies the range of port numbers. Range: 0 to 65535.
bidirectional	(Optional) Captures bidirectional packets.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	This command was introduced.

Usage Guidelines

Use the **monitor capture** command to specify the core filter as a class map, access list, or explicit inline filter. Any filter has already specified before you enter the **monitor capture match** command is replaced.

Examples

The following example shows how to set a filter for IPv6 source and destination traffic:

```
Device# monitor capture test match ipv6 protocol tcp host 2001:3c0:1::71 host 2001:380:1::71
 bidirectional
```

Related Commands

Command	Description
monitor capture match ipv4	Monitor filtering and capturing of IPv4 traffic.

privilege exec level

To set the privilege level for exec commands, use the **privilege exec level** command in global configuration mode. To reset the exec command to the default privilege level of 15, use the **no** form of this command.

privilege exec level *level command*
no privilege exec level *level command*

Syntax Description

level	Privilege level 0 - 15.
command	The exec command for which you want to set thes privilege level.

Command Default

The default exec privilege level is 15.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

Cisco Internetwork Operating System (IOS) currently has 16 privilege levels that range from 0 through 15. Users have access to limited commands at lower privilege levels compared to higher privilege levels. You can use this command to set the privilege level for exec commands.

Example

The following example shows how to set the exec command show logging to privilege level 1.

```
Device(config)# privilege exec level 1 show logging
```

request platform software sdwan admin-tech

To collect system status information in a compressed tar file for troubleshooting and diagnostics, use the **request platform software sdwan admin-tech** command in privileged EXEC mode.

request platform software sdwan admin-tech
{ **exclude-certs** | **exclude-cores** | **exclude-logs** | **exclude-tech** | **timeout** }

Syntax Description

exclude-certs	Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 17.15.1a Do not include any certificates in the compressed tar file. Certificates are stored in the /var/crash directory on a local Cisco IOS XE Catalyst SD-WAN device.
exclude-cores	Do not include any core files in the compressed tar file. Core files are stored in the /var/crash directory on a local Cisco IOS XE Catalyst SD-WAN device.
exclude-logs	Do not include any log files in the compressed tar file. Log files are stored in the /var/log directory on a local Cisco IOS XE Catalyst SD-WAN device.
exclude-tech	Do not include any process (daemon) and operational-related files in the compressed tar file. These files are stored in the /var/tech directory on a local Cisco IOS XE Catalyst SD-WAN device.
timeout	Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 17.15.1a admin-tech timeout value. When the admin-tech is truncated, you can provide custom timeout value for admin-tech. Default: 30 minutes.

Command Modes

Privileged EXEC mode (#)

Command History

Release	Modification
Cisco IOS XE SD-WAN 16.10.1	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.15.1a	Added the **exclude-certs** and **timeout** keywords.

Usage Guidelines

This command can be used to collect system status information in a compressed tar file for troubleshooting and diagnostics. This tar file, which is saved in the vmanage-admin's home directory, contains the output of various commands and the contents of various files on the local device, including syslog files, files for each process (daemon) running on the device, core files, and configuration rollback files. For aid in troubleshooting, send the file to Cisco SD-WAN customer support.

If your Cisco IOS XE Catalyst SD-WAN device contains a large number of crash log files, it might take a few minutes for the request admin-tech command to complete.

On a Cisco IOS XE Catalyst SD-WAN device, you can run only one request admin-tech command at a time. If a command is in progress, Cisco IOS XE Catalyst SD-WAN device does not let a second one start.

Example

The following example shows how to collect system status information in a compressed tar file for troubleshooting and diagnostics.

```
Device# request platform software sdwan admin-tech
Requested admin-tech initiated.
Created admin-tech file '/home/vmanage-admin/cEdge-20201115-110540-admin-tech.tar.gz'
IOS filename::  'bootflash:vmanage-admin/cEdge-20201115-110540-admin-tech.tar.gz'
```

Related Commands

Command	Description
admin-tech-on-failure	Collects system status information in a compressed tar file for troubleshooting and diagnostics.

request platform software sdwan auto-suspend reset

To bring all BFD sessions out of suspension, use the **request platform software sdwan auto-suspend reset** command in privileged EXEC mode.

request platform software sdwan auto-suspend reset { **local-sys-ip** *local-ip-address* **local-color** *local-color* **remote-sys-ip** *remote-ip-address* **remote-color** *remote-color* **encap** *encap-type* }

Syntax Description

local-sys-ip *local-ip-address*	Specifies the local system IP address.
local-color *local-color*	Identifier for the transport tunnel. The color specifies a specific WAN transport provider.
remote-sys-ip *remote-ip-address*	Specifies the IP address of the remote system.
remote-color *remote-color*	Specifies a WAN transport provider.
encap *encap-value*	Specifies the encapsulation type for the BFD session.

Command Default None

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	This command was introduced.

Usage Guidelines Use this command to bring all BFD sessions out of suspension.

Example

The following example shows how to reset a local color lte BFD session:

```
# request platform software sdwan auto-suspend reset local-color lte
```

The following example shows how to reset a BFD session with a local system IP, local color lte, and remote system IP with a remote color:

```
# request platform software sdwan auto-suspend reset local-sys-ip 172.16.12.255 local-color
 lte remote-sys-ip 10.10.1.1 remote-color 3g
```

The following example shows how to reset a BFD session with a local system IP, local color lte, remote system IP with a remote color, and an encapsulation type of IPsec:

```
# request platform software sdwan auto-suspend reset local-sys-ip 172.16.12.255 local-color
 lte remote-sys-ip 10.10.1.1 remote-color 3g encap ipsec
```

Related Commands

Command	Description
show sdwan bfd history	Displays Cisco SD-WAN BFD history.
show sdwan bfd sessions	Displays Cisco SD-WAN BFD sessions.
show sdwan bfd summary	Displays a Cisco SD-WAN BFD summary.
show sdwan bfd tloc-summary-list	Displays a Cisco SD-WAN BFD TLOC summary list.

request platform software sdwan certificate install

To install a certificate on the Cisco SD-WAN WAN Edge device, use the **request platform software sdwan certificate install** command in privileged EXEC mode.

request platform software sdwan certificate install *file-path* { **vpn** *vpn-id* }

Syntax Description

file-path	Path to the certificate file. Install the certificate in specified filename. *file-path* can be one of the following: • bootflash • flash • webui
vpn *vpn-id*	VPN in which the certificate file is located. When you include this option, one of the interfaces in the specified VPN is used to retrieve the file.

Command Default

None.

Command Modes

Privileged EXEC mode (#)

Command History

Release	Modification
Cisco IOS XE SD-WAN 16.10.1	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

This command can be used to install a certificate on a Cisco IOS XE Catalyst SD-WAN device. Certificates are used on Public Key Infrastructure (PKI) deployments.

Example

The command can be used to install a certificate on a Cisco IOS XE Catalyst SD-WAN device. Certificates are used on Public Key Infrastructure (PKI) deployments.

```
Device# request platform software sdwan certificate install bootflash:cert.csr
```

request platform software sdwan config reset

To clear the SD-WAN configuration from a Cisco IOS XE Catalyst SD-WAN device, use the **request platform software sdwan config reset** command in privileged EXEC mode.

request platform software sdwan config reset

Command Default

None

Command Modes

Privileged EXEC mode (#)

Command History

Release	Modification
Cisco IOS XE SD-WAN 16.10.1	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

This command can be used to clear the SD-WAN configuration from a Cisco IOS XE Catalyst SD-WAN device. This command is disruptive, since all the SD-WAN configurations of the Cisco IOS XE Catalyst SD-WAN device will be wiped out.

This may be needed in order to restart the PnP process.

Note In releases prior to Cisco IOS XE Catalyst SD-WAN Release 17.7.1a, the **request platform software sdwan config reset** command displayed a prompt requesting that you reload the Cisco IOS XE Catalyst SD-WAN device.

Starting from Cisco IOS XE Catalyst SD-WAN Release 17.7.1a, you no longer see the prompt requesting you to reload the Cisco IOS XE Catalyst SD-WAN device. The Cisco IOS XE Catalyst SD-WAN device reloads automatically with an appropriate message on the console.

When this command encounters a Virtual Teletype (VTY) line without autoboot, you need to change the `config-register` value so that the autoboot bit is set as `0xXXX2`.

You can check the value of `config-register` using the **show version** or **show bootvar** commands.

```
Device# show bootvar
BOOT variable = bootflash:packages.conf,1;bootflash:prev_packages.conf,1;
CONFIG_FILE variable does not exist
BOOTLDR variable does not exist
Configuration register is 0x2102
Standby not ready to show bootvar
```

You can change the value of `config-register` by pushing the configuration to the device using a CLI add-on template or by using the CLI.

```
config-transaction
config-register 0x2102
commit
```

Example

The following example shows how to clear the SD-WAN configuration from a Cisco IOS XE Catalyst SD-WAN device.

```
Device# request platform software sdwan config reset
```

request platform software sdwan csr upload

To upload a Certificate Signing Request (CSR) to a Cisco IOS XE Catalyst SD-WAN device, use the **request platform software sdwan csr upload** command in privileged EXEC mode.

request platform software sdwan csr upload *file-path*

Syntax Description

file-path	Path of the certificate file. Upload the CSR in the file at the specified path. *file-path* can be one of the following: • bootflash • flash • webui

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE SD-WAN 16.10.1	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

This command can be used to upload a CSR to a Cisco IOS XE Catalyst SD-WAN device. They are used on Public Key Infrastructure (PKI) deployments.

Example

The following example shows how to upload a CSR to a Cisco IOS XE Catalyst SD-WAN device.

```
Device# request platform software sdwan csr upload bootflash:cert.csr
Uploading CSR via VPN 0
Generating CSR on the hardware Router ..
Enter organization-unit name            : SDWAN-Org
Re-enter organization-unit name          : SDWAN-Org
Organization-unit name differs. Certificate will be deleted. Proceed? [yes,NO] Yes
```

request platform software sdwan port_hop color

To manually request the port hopping for TLOCs with a specific color, use the **request platform software sdwan port_hop color** command in privileged EXEC mode.

request platform software sdwan port_hop color *color*

Syntax Description

color	Color of an individual WAN transport interface. Values: 3g, biz-internet, blue, bronze, custom1, custom2, custom3, default, gold, green, lte, metro-ethernet, mpls, private1, private2, private3, private4, private5, private6, public-internet, red, and silver.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE SD-WAN 16.10.1	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

This command can be used when NAT entries become stale.

Manually rotate to the next OMP port in the group of preselected OMP port numbers when a connection cannot be established, and continue the port hopping until a connection can be established. Each connection attempt times out in about 60 seconds.

Example

The following example shows how to rotate to the next OMP port in the group of preselected OMP port numbers to the TLOC with color LTE.

```
Device# request platform software sdwan port_hop color lte
```

request platform software sdwan root-cert-chain install

To install a file containing the root certificate key chain, use the **request platform software sdwan root-cert-chain install** command in privileged EXEC mode.

request platform software sdwan root-cert-chain install *file-path* { **vpn** *vpn-id* }

Syntax Description

file-path	Install the specified file containing the root certificate chain. *file-path* can be one of the following: • bootflash • flash • webui
vpn *vpn-id*	VPN in which the certificate file is located. When you include this option, one of the interfaces in the specified VPN is used to retrieve the file.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE SD-WAN 16.10.1	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

This command can be used to install a file containing the root certificate key chain. It is used on Public Key Infrastructure (PKI) deployments.

Example

The following example shows how to install a file containing the root certificate key chain.

```
Device# request platform software sdwan root-cert-chain install bootflash:root-chain
```

Related Commands

Command	Description
request platform software sdwan root-cert-chain uninstall	Uninstalls a file containing the root certificate key chain.

request platform software sdwan root-cert-chain uninstall

To uninstall a file containing the root certificate key chain, use the **request platform software sdwan root-cert-chain uninstall** command in privileged EXEC mode.

request platform software sdwan root-cert-chain uninstall

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE SD-WAN 16.10.1	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

This command can be used to uninstall a file containing the root certificate key chain. It is used on Public Key Infrastructure (PKI) deployments.

Example

The following example shows how to uninstall a file containing the root certificate key chain.

```
Device# request platform software sdwan root-cert-chain uninstall
```

Related Commands

Command	Description
request platform software sdwan root-cert-chain install	Installs a file containing the root certificate key chain.

request platform software sdwan software activate

To activate a software image on a local Cisco IOS XE Catalyst SD-WAN device, use the **request platform software sdwan software activate** command in privileged EXEC mode.

request platform software sdwan software activate *build-number* { **clean** | **now** }

Syntax Description

build-number	Name of the software image to activate on the device.
clean	Activates the specified software image, but do not associate the existing configuration file, and do not associates any files that store information about the device history, such as log and trace files, with the newly activated software image. **Note** Beginning with Cisco IOS XE Catalyst SD-WAN Release 17.10.1a, this option is no longer supported.
now	Activates the specified software image immediately, with no prompt asking you to confirm that you want to activate. **Note** Beginning with Cisco IOS XE Catalyst SD-WAN Release 17.14.1a, this option is no longer supported.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE SD-WAN 16.10.1	This command was introduced.
Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	The **clean** option is no longer supported.
Cisco IOS XE Catalyst SD-WAN Release 17.14.1a	The **now** option is no longer supported.

Usage Guidelines

This command can be used to activate a software image on a local Cisco IOS XE Catalyst SD-WAN device through CLI. The Cisco IOS XE Catalyst SD-WAN device reloads when the activation is complete.

Example

The following example shows how to activate a software image on a local Cisco IOS XE Catalyst SD-WAN device through CLI.

```
Device# request platform software sdwan software activate 17.03.01a.0.354
```

Related Commands

Command	Description
show sdwan software	Verifies whether the software is activated.

request platform software sdwan software install

To install a software image on a Cisco IOS XE Catalyst SD-WAN device, use the **request platform software sdwan software install** command in privileged EXEC mode.

request platform software sdwan software install *file-path* { **vpn** *vpn-id* } { **reboot** { **no-sync** } } { **download-timeout** *minutes* }

Syntax Description

file-path	Installs the software image in the specified file system. The file system must be located on the local device. *file-path* can be one of the following: • bootflash • flash • webui
vpn *vpn-id*	VPN in which the image is located. When you include this option, one of the interfaces in the specified VPN is used to retrieve the software image.
reboot no-sync	Reboots the device after installation of the software image completes. By default, the device's current configuration is copied to the other hard-disk partition and is installed with the new software image. If you include the no-sync option, the software is installed in the other hard-disk partition, and it is installed with the factory-default configuration. The existing configuration and any files that store information about the device history, such as log and trace files, are not copied to the other partition. Effectively, the no-sync option restores the device to its initial factory configuration.
download-timeout *minutes*	Specifies the installation timeout value. How long to wait before cancelling requests to install software. The duration ranges from 1 through 1440 minutes (24 hours). The default time is 60 minutes.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE SD-WAN 16.10.1	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

This command can be used to install a software image on a Cisco IOS XE Catalyst SD-WAN device. Before the software is installed, the software image is verified to determine that it is valid and that it has been signed. If the verification process fails, the software image installation is not performed.

Example

The following example shows how to install a software image on a Cisco IOS XE Catalyst SD-WAN device.

```
Device# request platform software sdwan software install
bootflash:isr4300-universalk9.17.03.02.SPA.bin
```

request platform software sdwan software remove

To remove a software image from a local Cisco IOS XE Catalyst SD-WAN device, use the **request platform software sdwan software remove** command in privileged EXEC mode.

request platform software sdwan software remove *build-number*

Syntax Description

build-number	Name of the software image to delete from the device. You cannot delete the active image.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE SD-WAN 16.10.1	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

This command can be used to remove a software image from a local Cisco IOS XE Catalyst SD-WAN device. You cannot delete the active image.

Example

The following example shows how to remove a software image from a local Cisco IOS XE Catalyst SD-WAN device.

```
Device# request platform software sdwan software remove 17.03.01a.0.354
```

request platform software sdwan software secure-boot

To check and enforce the secure boot state of the system software images, use the **request platform software sdwan software secure-boot** command in privileged EXEC mode.

request platform software sdwan software secure-boot [**list** | **set** | **status**]

Syntax Description

list	Checks secure boot state and checks whether software images on the device are secure or not secure.
set	Removes insecure software images from the device and remove an insecure boot loader.
status	Displays the security status of the software images installed on the device.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	The command is deprecated.

request platform software sdwan software set-default

To set a software image as the default image on a Cisco IOS XE Catalyst SD-WAN device, use the **request platform software sdwan software set-default** command in privileged EXEC mode.

request platform software sdwan software set-default *build-number*

Syntax Description

build-number	Name of the software image to designate as the default image on a Cisco IOS XE Catalyst SD-WAN device.

Command Default

None.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE SD-WAN 16.10.1	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

This command can be used to set a software image to be the default image on a Cisco IOS XE Catalyst SD-WAN device. Performing this operation overwrites the factory-default software image, replacing it with an image of your choosing. It is recommended that you set a software image to be the default only after verifying that the software is operating as desired on a Cisco IOS XE Catalyst SD-WAN device and in your network.

Example

The following example shows how to set a software image to be the default image on a Cisco IOS XE Catalyst SD-WAN device.

```
Device# request platform software sdwan software set-default 17.03.01a.0.354
```

request platform software sdwan software upgrade-confirm

To confirm that the upgrade to a new software image is successful, use the **request platform software sdwan software upgrade-confirm** command in privileged EXEC mode.

request platform software sdwan software upgrade-confirm

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE SD-WAN 16.10.1	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

This command can be used to confirm that the upgrade to a new software image is successful. If the device configuration includes the **sdwan system upgrade-confirm** command, issuing the **request platform software sdwan software upgrade-confirm** command within the time limit configured in the **upgrade-confirm** command confirms that the upgrade to the new software image has been successful. If this command is not issued, the device reverts automatically to the previously running software image.

If you have initiated the software upgrade from Cisco SD-WAN Manager, Cisco SD-WAN Manager automatically issues the **request platform software sdwan software upgrade-confirm** command when the Cisco IOS XE Catalyst SD-WAN device finishes rebooting. If you have initiated the software upgrade

manually from the Cisco IOS XE Catalyst SD-WAN device, you issue the **request platform software sdwan software upgrade-confirm** command from the CLI.

Example

The following example shows how to confirm that the upgrade to a new software image is successful from the CLI and the device configuration includes the **sdwan system upgrade-confirm** command.

```
Device# request platform software sdwan software upgrade-confirm
```

set platform software trace

To configure the binary trace level for one or all modules of a Cisco SD-WAN process on a specific hardware slot, issue the command **set platform software trace** in the Privileged EXEC mode.

set platform software trace *process slot module trace-level*

Syntax Description	*process*

Specify a Cisco SD-WAN process.

- all: Specify all the processes
- backplaneswitch-manager: Backplane Switch Manager Process
- bt-logger: Binary-Tracing Logger Process
- btrace-manager: Btrace Manager Process
- cfgmgr: SDWAN Cfgmgr process
- chassis-manager: Chassis-Manager
- cli-agent: CLI Agent
- cxpd: SDWAN CXP process
- dbgd: SDWAN DBG process
- dbm: Database Manager
- dmiauthd: DMI Authentication Daemon
- emd: Environmental Monitoring
- flow-file-export: Flow file export
- forwarding-manager: Forwarding Manager
- fpmd: SDWAN FPM process
- ftmd: SDWAN FTM process
- host-manager: Host Manager
- htx: AppQoE HTX Process
- install-manager: Install Manager Process
- iomd: IOMD Process
- ios: IOS Process
- iox-manager: IOx Manager Process
- license-manager: License Manager Process
- logger: Logging Manager
- mdt-pubd: Model Defined Telemetry Publisher
- ncsshd_bp: NETCONF SSH Daemon BINOS Proxy Daemon
- ndbman: Netconf DataBase Manager
- nginx: Nginx Webserver Process
- ompd: SDWAN OMP process
- pluggable-services: Pluggable Services

- qfp-control-process: QFP Client Control Process
- qfp-driver: QFP Driver Process
- qfp-ha-server: QFP HA Server
- qfp-service-process: QFP Client Serivce Process
- replication-mgr: Replication Manager
- service-mgr: Service Manager Process
- shell-manager: Shell Manager
- smd: Session Manager Process
- system-integrity: system-integrity (pistisd) Process
- ttmd: SDWAN TTM process
- vdaemon: SDWAN vDaemon process
- virt-manager: Virtualization Manager

level	Hardware slot from which process messages must be logged.

module

Specify the trace level for one or all the modules of the process.

- all-modules: All trace modules
- aom: Asynchronous object manager
- backwalk: Backwalk
- bcrdu: Crimson Dynamic Update
- bcrft: Crimson Function Tracking
- bcrpgc: Crimson Profile Guided Compiling
- bidb: Interface descriptor blocks
- bipc: Inter-process communication
- bipc_tls: BIPC-TLS communication
- bso: BSO query
- btrace: Tracing
- btrace_ra: Tracing RA
- ccolib-api: CCOLIB_API
- cdllib: CLI
- chasfs: Chassis filesystem
- cond_debug: Conditional debug
- crimson-oper: Crimson operational data
- cxpd-analytics: cloudexpress analytics
- cxpd-app: cloudexpress app
- cxpd-config: cloudexpress config
- cxpd-dpi: cloudexpress dpi
- cxpd-ftm: cloudexpress ftm
- cxpd-misc: cloudexpress misc
- cxpd-omp: cloudexpress omp
- cxpd-oper: cloudexpress oper
- cxpd-rtm: cloudexpress rtm
- cxpd-telemetry: cloudexpress telemetry
- cxpd-ttm: cloudexpress ttm
- dassist: DB assist access layer
- dbal: DB access layer
- dbdm: DB dependency management

- dfs_user: DFS
- dns-resolver: DNS Resolver
- dnsclient: dnsclient library
- evlib: Event
- evutil: Event utility
- green-be: Green backend
- green-fe: Green frontend
- httpcon-curl: HTTPCON library, curl
- httpcon-main: HTTPCON library, main
- installer-api INSTALLER_API
- libmonitor: monitor library
- mqipc: Message queue
- oormon: Out of resource monitoring
- prelib: Preload
- scooby: Scooby
- serdes: Serdes
- service-dir: Service directory
- services: Services
- tdldb-assist: DB table assist library
- tdldbpersist: DB PERSISTENCE
- tdllib: Type management
- thpool: Thread Pool
- tl3_stm: TL3 software transactional memory
- ublock: Micro blocks
- uihandler: CLI command handlers
- uipeer User interface peer
- uistatus User interface peer status
- uswap: Crimson User land Swap
- vconfd: vconfd library
- vipcommon-http: common library, http
- vipcommon-misc: common library, misc
- vipcommon-mqipc: common library, mqipc

- vipcommon-msgq: common library, msgq
- vipcommon-pwk: common library, pwk
- vipcommon-rtmsg: common library, rtmsg
- vipcommon-sql: common library, sql

slot Select one of the following trace levels:

- debug: Debug messages
- emergency: Emergency possible message
- error: Error messages
- info: Informational messages
- noise: Maximum possible message
- notice: Notice messages
- verbose: Verbose debug messages
- warning: Warning messages

Command Default

The default tracing level for all modules is **notice**.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.11.1a	New keywords introduced: • cxpd-analytics: cloudexpress analytics • cxpd-app: cloudexpress app • cxpd-config: cloudexpress config • cxpd-dpi: cloudexpress dpi • cxpd-ftm: cloudexpress ftm • cxpd-misc: cloudexpress misc • cxpd-omp: cloudexpress omp • cxpd-oper: cloudexpress oper • cxpd-rtm: cloudexpress rtm • cxpd-telemetry: cloudexpress telemetry • cxpd-ttm: cloudexpress ttm
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Command support introduced for select Cisco SD-WAN processes. See the table 'Supported Cisco SD-WAN Daemons' under 'Usage Guidelines'.

Usage Guidelines

Table 4: Supported Cisco SD-WAN Daemons

Cisco SD-WAN Daemons	Supported from Release
• fpmd • ftm • ompd • vdaemon • cfgmgr	Cisco IOS XE Catalyst SD-WAN Release 17.4.1a

Example

In the following example, the binary trace level for the 'config' module of the 'fpmd' process on the 'R0' FRU is set to 'debug'.

```
Device# set platform software trace fpmd R0 config debug
```

show aaa servers

To display the status and number of packets that are sent to and received from all public and private authentication, authorization, and accounting (AAA) RADIUS servers as interpreted by the AAA Server MIB, use the **show aaa servers** command in user EXEC or privileged EXEC mode.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	This command was introduced.

Usage Guidelines

For more information about this command, see the Cisco IOS XE show aaa servers

Examples

The following is sample output from the **show aaa servers private** command. Only the first four lines of the display pertain to the status of private RADIUS servers, and the output fields in this part of the display are described in the table below.

```
Device# show aaa server private
RADIUS: id 24, priority 1, host 172.31.164.120, auth-port 1645, acct-port 1646
     State: current UP, duration 375742s, previous duration 0s
     Dead: total time 0s, count 0
     Quarantined: No
     Authen: request 5, timeouts 1, failover 0, retransmission 1
             Response: accept 4, reject 0, challenge 0
             Response: unexpected 0, server error 0, incorrect 0, time 14ms
             Transaction: success 4, failure 0
             Throttled: transaction 0, timeout 0, failure 0
     Author: request 0, timeouts 0, failover 0, retransmission 0
             Response: accept 0, reject 0, challenge 0
             Response: unexpected 0, server error 0, incorrect 0, time 0ms
             Transaction: success 0, failure 0
```

```
        Throttled: transaction 0, timeout 0, failure 0
Account: request 5, timeouts 0, failover 0, retransmission 0
        Request: start 3, interim 0, stop 2
        Response: start 3, interim 0, stop 2
        Response: unexpected 0, server error 0, incorrect 0, time 12ms
        Transaction: success 5, failure 0
        Throttled: transaction 0, timeout 0, failure 0
Elapsed time since counters last cleared: 4d8h22m
Estimated Outstanding Access Transactions: 0
Estimated Outstanding Accounting Transactions: 0
Estimated Throttled Access Transactions: 0
Estimated Throttled Accounting Transactions: 0
Maximum Throttled Transactions: access 0, accounting 0
Requests per minute past 24 hours:
        high - 8 hours, 22 minutes ago: 0
        low  - 8 hours, 22 minutes ago: 0
        average: 0
```

show autoip status

To display the status of automatic IP address detection for a device and display information that is detected, use the **show autoip status** command in privileged EXEC mode.

show autoip status

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Examples

The following is sample output from the **show autoip status** command when an available IP address has been detected:

```
Device# show autoip status

============================
AutoIP process is stopped
============================
Last status       :success
Finally in use    :
IP address        : 192.168.0.6
Gateway IP address: 192.168.0.3
Subnet            : 192.168.47.0
Subnet mask       : 255.255.255.0
DNS server1       : 8.8.8.8
DNS server 2      : 8.8.4.4
Interface         : GigabitEthernet0/0/0
```

The following is sample output from the **show autoip status** command when detection is in progress:

```
Device# show autoip status

============================
AutoIP process is running
============================
Last status       :fail
Currently in use  :
IP address        : 192.168.1.2
Gateway IP address: 192.168.1.1
Subnet            : 192.168.40.0
Subnet mask       : 255.255.255.0
DNS server1       : 8.8.8.8
DNS server 2      : 8.8.4.4
Interface         : GigabitEthernet0/0/0
```

show class map type inspect

To display Layer 3 and Layer 4 or Layer 7 (application-specific) inspect type class maps and their matching criteria, use the **show class map type inspect** command in privileged EXEC mode.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.11.1a	This command is supported in Cisco Catalyst SD-WAN

Usage Guidelines

For usage guidelines, see the Cisco IOS XE show class-map type inspect command.

Example

The following example displays the Layer 3 and Layer 4 or Layer 7 (application-specific) inspect type class maps and their matching criteria.

```
Device# show class-map type inspect
 Class Map type inspect match-all seq_1-seq-11-cm_ (id 2)
   Match access-group name seq_1-seq-Rule_3-acl_

 Class Map type inspect match-all seq_1-seq-1-cm_ (id 1)
   Match access-group name seq_1-seq-rule1-v6-acl_
```

show cellular

To display information about the Global Navigation Satellite System (GNSS) configuration, use the **show cellular** command in privileged EXEC (#) mode.

show cellular *slot_number*

Syntax Description

gps detail	Shows the GNSS details.

Command Default None

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.15.1a	This command is supported in Cisco Catalyst SD-WAN.

Examples

The following sample output displays the GNSS details such as feature status, mode, constellation configuration, GPS port selection, current GPS status, location coordinates, timestamp, and details of individual satellites such as GPS, GLONASS, Galileo, and BeiDou.

```
Device# show cellular 0/3/0 gps detail
GPS Feature = enabled
GPS Mode Configured = standalone
Current Constellation Configured = gnss
GPS Port Selected = Dedicated GPS port
GPS Status = GPS coordinates acquired
Last Location Fix Error = Offline [0x0]
Latitude = 37 Deg 25 Min 6.0448 Sec North
Longitude = 121 Deg 55 Min 9.6295 Sec West
Timestamp (GMT) = Fri Jul 12 16:11:30 2024

Fix type = 2D, Height = 20m
HDOP = 0.7, GPS Mode Used = standalone

Satellite Info
----------------
GPS:
Satellite #5, elevation 60, azimuth 108, SNR 31 *
Satellite #11, elevation 24, azimuth 50, SNR 34 *
Satellite #12, elevation 40, azimuth 163, SNR 33 *
Satellite #15, elevation 1, azimuth 151, SNR 19 *
Satellite #18, elevation 30, azimuth 248, SNR 33 *
Satellite #20, elevation 46, azimuth 59, SNR 36 *
Satellite #25, elevation 64, azimuth 206, SNR 35 *
Satellite #26, elevation 6, azimuth 320, SNR 27 *
Satellite #28, elevation 13, azimuth 274, SNR 33 *
Satellite #29, elevation 59, azimuth 327, SNR 37 *
Satellite #31, elevation 8, azimuth 305, SNR 27 *
Satellite #46, elevation 0, azimuth 0, SNR 34 **
Glonass:
Satellite #74, elevation 35, azimuth 312, SNR 34 *
Satellite #82, elevation 21, azimuth 52, SNR 35 *
Satellite #73, elevation 52, azimuth 248, SNR 41 *
Satellite #80, elevation 20, azimuth 187, SNR 34 *
Satellite #84, elevation 30, azimuth 278, SNR 22
Satellite #83, elevation 51, azimuth 9, SNR 27 *
Satellite #67, elevation 24, azimuth 61, SNR 36 *
Satellite #66, elevation 2, azimuth 16, SNR 0
Satellite #68, elevation 21, azimuth 115, SNR 0
Galileo:
Satellite #13, elevation 33, azimuth 247, SNR 38 *
Satellite #15, elevation 75, azimuth 330, SNR 39 *
Satellite #27, elevation 68, azimuth 271, SNR 37 *
Satellite #3, elevation 2, azimuth 118, SNR 0
Satellite #5, elevation 4, azimuth 71, SNR 0 *
Satellite #21, elevation 21, azimuth 316, SNR 0
Satellite #30, elevation 42, azimuth 164, SNR 0
Beidou:
```

```
Satellite #6, elevation 3, azimuth 322, SNR 30
Satellite #12, elevation 15, azimuth 274, SNR 30 *
Satellite #19, elevation 33, azimuth 108, SNR 0
Satellite #20, elevation 21, azimuth 54, SNR 0 *
Satellite #22, elevation 14, azimuth 161, SNR 0
Satellite #24, elevation 28, azimuth 295, SNR 0
Satellite #26, elevation 37, azimuth 232, SNR 0 *
Satellite #29, elevation 25, azimuth 73, SNR 0 *
```

show clock

To display view the system clock on a device, use the **show clock** command in privileged EXEC mode.

show clock

Command Default None

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	This command was introduced.

Examples The following sample output displays the system clock with the date and time.

```
Device# show clock
*00:42:53.470 UTC Tue Jul 26 2022
```

show configuration commit list

To display the configuration commit list, use the **show configuration commit list** command in global configuration mode.

show configuration commit list

Command Default None

Command Modes Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	This command was introduced.

Examples

The following sample output displays the configuration commit list.

```
Device(config)# show configuration commit list
2022-07-26 00:41:21

SNo. ID       User       Client      Time Stamp          Label       Comment

~~~~ ~~       ~~~~       ~~~~~~      ~~~~~~~~~~          ~~~~~       ~~~~~~~

0    10001    vmanage-ad netconf     2022-05-12 10:17:03

1    10014    vmanage-ad netconf     2022-04-04 06:36:45

2    10013    vmanage-ad netconf     2022-04-04 06:20:41

3    10012    vmanage-ad netconf     2022-04-04 06:20:38

4    10011    admin      cli         2022-03-27 21:02:40

5    10010    admin      cli         2022-03-27 20:14:42

6    10009    admin      cli         2022-03-27 20:12:57

7    10008    admin      cli         2022-03-27 20:11:21

8    10007    cfgmgr     system      2022-03-27 20:10:21

9    10006    system     system      2022-03-27 19:57:34

10   10005    system     system      2022-03-27 19:57:32

11   10004    system     system      2022-03-27 19:57:31

12   10003    system     system      2022-03-27 19:57:30

13   10002    system     system      2022-03-27 19:57:30

14   10001    system     system      2022-03-27 19:57:28

15   10000    dmidlib_sy system      2022-03-27 19:57:25
```

show crypto ipsec sa

To display the settings used by IPsec security associations (SAs), use the **show crypto ipsec sa** command in privileged EXEC mode.

Supported Parameters

active	(Optional) Displays high availability (HA)-enabled IPsec SAs that are in the active state.

address	(Optional) Displays all existing SAs. The SAs are sorted by the destination address (either the local address or the address of the IPsec remote peer) and then by protocol (Authentication Header [AH] or Encapsulation Security Protocol [ESP]).
detail	(Optional) Displays detailed information of all settings.
identity [**detail**]	(Optional) Displays only the flow information. The SA information isn't displayed.
interface *type number*	(Optional) Displays all SAs created for an interface type. The interface types are: **ATM**, **Dialer**, **GigabitEthernet**, **Loopback**, **Serial**, **Vlan**, **VirtualPortGroup**.
ipv6	(Optional) Displays IPv6 IPsec SA information.
detailed	(Optional) Displays detailed error counters.
platform	(Optional) Displays platform-specific information about the IPsec flow.
ipv4-address	(Optional) Displays IPsec SAs for an IPv4 peer.
ipv6-address	(Optional) Displays IPsec SAs for an IPv6 peer.
map *map-name* [**detail**]	(Optional) Displays any existing SAs that were created for the crypto map set using a value for the *map-name* argument.
peer [**detail** | [**vrf** *vrf*] [*ipv4-address* [**detail**] | *ipv6-address* [**detail** | **platform**]]]	(Optional) Displays all existing SAs with the peer IP address.
standby	(Optional) Displays HA-enabled IPsec SAs that are in the standby state.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Command qualified for use in Cisco vManage CLI templates and modified the display of current outbound SPI and SPI entries.

Usage Guidelines

For more information about this command, see the Cisco IOS XE show crypto ipsec sa command.

Examples

Example 1:

The following sample output from the **show crypto ipsec sa** command shows that the SPI values isn't valid or displayed for Cisco SD-WAN IPSec tunnels.

```
Device# show crypto ipsec sa
interface: Tunnel1
    Crypto map tag: Tunnel1-vesen-head-0, local addr 10.1.15.15

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (10.1.15.15/255.255.255.255/0/12346)
   remote ident (addr/mask/prot/port): (10.1.16.16/255.255.255.255/0/12366)
   current_peer 10.1.16.16 port 12366
     PERMIT, flags={origin_is_acl,}
```

```
    #pkts encaps: 449884, #pkts encrypt: 449884, #pkts digest: 449884
    #pkts decaps: 449874, #pkts decrypt: 449874, #pkts verify: 449874
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0

     local crypto endpt.: 10.1.15.15, remote crypto endpt.: 10.1.16.16
     plaintext mtu 1438, path mtu 1480, ip mtu 1480, ip mtu idb Tunnel1
     current outbound spi:  [Not Available]
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: [Not Available]
        transform: esp-gcm 256 ,
        in use settings ={Transport UDP-Encaps, esn}
        conn id: 2003, flow_id: CSR:3, sibling_flags FFFFFFFF80000008, crypto map:
Tunnel1-vesen-head-0
        sa timing: remaining key lifetime is not applicable
        Kilobyte Volume Rekey has been disabled
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

      inbound ah sas:

      inbound pcp sas:

      outbound esp sas:
       spi: [Not Available]
        transform: esp-gcm 256 ,
        in use settings ={{Transport UDP-Encaps, esn}
        conn id: 2003, flow_id: CSR:3, sibling_flags FFFFFFFF80000008, crypto map:
Tunnel1-vesen-head-0
        sa timing: remaining key lifetime is not applicable
        Kilobyte Volume Rekey has been disabled
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

      outbound ah sas:

      outbound pcp sas:
```

Example 2:

The following is a sample output from the **show crypto ipsec sa** command that shows an IKE-based IPSec tunnel.

```
Device# show crypto ipsec sa
interface: Tunnel100
    Crypto map tag: Tunnel100-head-0, local addr 192.168.70.11

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.70.11/255.255.255.255/47/0)
   remote ident (addr/mask/prot/port): (192.168.70.12/255.255.255.255/47/0)
   current_peer 192.168.70.12 port 500
     PERMIT, flags={origin_is_acl,}
    #pkts encaps: 2292, #pkts encrypt: 2292, #pkts digest: 2292
    #pkts decaps: 112, #pkts decrypt: 112, #pkts verify: 112
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 0, #recv errors 0
```

```
     local crypto endpt.: 192.168.70.11, remote crypto endpt.: 192.168.70.12
     plaintext mtu 1446, path mtu 1500, ip mtu 1500, ip mtu idb GigabitEthernet2
     current outbound spi: 0x19967EA7(429293223)
     PFS (Y/N): N, DH group: none

     inbound esp sas:
      spi: 0xB13A9E4F(2973408847)
       transform: esp-gcm 256 ,
        in use settings ={Tunnel, }
        conn id: 2003, flow_id: CSR:3, sibling_flags FFFFFFFF80000048, crypto map:
Tunnel100-head-0
        sa timing: remaining key lifetime 24 days, 23 hours, 41 mins
        Kilobyte Volume Rekey has been disabled
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x19967EA7(429293223)
        transform: esp-gcm 256 ,
        in use settings ={Tunnel, }
        conn id: 2004, flow_id: CSR:4, sibling_flags FFFFFFFF80000048, crypto map:
Tunnel100-head-0
        sa timing: remaining key lifetime 24 days, 23 hours, 41 mins
        Kilobyte Volume Rekey has been disabled
        IV size: 8 bytes
        replay detection support: Y
        Status: ACTIVE(ACTIVE)

     outbound ah sas:

     outbound pcp sas:
```

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

Table 5: show crypto ipsec sa Field Descriptions

Field	Description
interface	Interface on which the SA is created.
Crypto map tag	Policy tag for IPsec.
protected vrf	IVRF name that applies to the IPsec interface.
local ident (addr/mask/prot/port)	Local selector that is used for encryption and decryption.
remote ident (addr/mask/prot/port)	Remote selector that is used for encryption and decryption.
Group	Name of the GDOI group corresponding to the IPsec SA.
current_peer	Peer that communicates with the IPsec tunnel.
PERMIT, flags	Indicates that the IPsec SA is triggered by the access control list (ACL) permit action.

Field	Description
pkts encaps	Number of packets that were successfully encapsulated by IPsec.
pkts encrypt	Number of packets that were successfully encrypted by IPsec.
pkts digest	Number of packets that were successfully hash digested by IPsec.
pkts decaps	Number of packets that were successfully decapsulated by IPsec.
pkts decrypt	Number of packets that were successfully decrypted by IPsec.
pkts verify	Number of received packets that passed the hash digest check.
pkts compressed	Number of packets that were successfully compressed by IPsec.
pkts decompressed	Number of packets that were successfully decompressed by IPsec.
pkts not compressed	Number of outbound packets that weren’t compressed.
pkts compr. failed	Number of packets that failed compression by IPsec.
pkts not decompressed	Number of inbound packets that weren’t compressed.
pkts decompress failed	Number of packets that failed decompression by IPSec.
send errors	Number of outbound packets with errors.
recv errors	Number of inbound packets with errors.
local crypto endpt.	Local endpoint terminated by IPsec.
remote crypto endpt.	Remote endpoint terminated by IPsec.
path mtu	MTU size that is calculated based on the Internet Control Message Protocol (ICMP) unreachable packet, including the IPsec overhead, if any.
ip mtu	Interface MTU size that depends on the IPsec overhead.
ip mtu idb	Interface description block (IDB) that is used to determine the crypto IP MTU.
current outbound spi	Current outbound Security Parameters Index (SPI). This value isn't valid and is set to "Not Available".
inbound esp sas	Encapsulating Security Payload (ESP) for the SA for the inbound traffic.
spi	SPI for classifying the inbound packet. This value isn't valid and is set to "Not Available".
transform	Security algorithm that is used to provide authentication, integrity, and confidentiality.

Field	Description
in use settings	Transform that the SA uses (such as tunnel mode, transport mode, UDP-encapsulated tunnel mode, or UDP-encapsulated transport mode).
conn id	ID that is stored in the crypto engine to identify the IPsec/Internet Key Exchange (IKE) SA.
flow_id	SA identity.
crypto map	Policy for IPsec.
sa timing: remaining key lifetime (k/sec)	Seconds or kilobytes remaining before a rekey occurs.
HA last key lifetime sent (k)	Last stored kilobytes lifetime value for HA.
ike_cookies	ID that identifies the IKE SAs.
IV size	Size of the initialization vector (IV) that is used for the cryptographic synchronization data used to encrypt the payload.
replay detection support	Replay detection feature enabled by a specific SA.
Status	Indicates whether the SA is active.
inbound ah sas	Authentication algorithm for the SA for inbound traffic.
inbound pcp sas	Compression algorithm for the SA for inbound traffic.
outbound esp sas	Encapsulating security payload for the SA for outbound traffic.
outbound ah sas	Authentication algorithm for the SA for outbound traffic.
outbound pcp sas	Compression algorithm for the SA for outbound traffic.
DENY, flags	Indicates that the IPsec SA is triggered by the ACL deny action.
pkts decompress failed	Packets decompressed by IPsec that failed.
pkts no sa (send)	Outbound packets that couldn’t find the associated IPsec SA.
pkts invalid sa (rcv)	Received packets that failed the IPsec format check.
pkts invalid prot (recv)	Received packets that have the wrong protocol field.
pkts verify failed	Received packets that failed the hash digest check.
pkts invalid identity (recv)	Packets that couldn’t find the associated selector after decryption.
pkts invalid len (rcv)	Inbound packets that have an incorrect pad length for the software crypto engine.
pkts replay rollover (send)	Sent packets that failed the replay test check.

Field	Description
pkts replay rollover (rcv)	Received packets that failed the replay test check.
pkts internal err (send)	Sent packets that failed because of a software or hardware error.
pkts internal err (rcv)	Received packets that failed because of a software or hardware error.
protected vrf	IVRF name that applies to the IPsec interface.
pkts tagged (send)	Packets tagged with a Cisco TrustSec SGT in the outbound direction.
pkts untagged (rcv)	Packets not tagged with a Cisco TrustSec SGT in the inbound direction.

show cts environment-data

To display the TrustSec environment data, use the **show cts environment-data** command in user EXEC or privileged EXEC mode

show cts environment-data

Command Default

None

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	This command was introduced.

Examples

The following sample outputs displays the environment data.

```
Device# show cts environment-data

 CTS Environment Data

====================

Current state = START

Last status = In Progress

Environment data is empty

State Machine is running

Retry_timer (60 secs) is not running
```

show cts pac

To display the Protected Access Credentials (PACs), use the **show cts pacs** command in user EXEC or privileged EXEC mode

Command Default

None

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	This command was introduced.

Usage Guidelines

Use this command to identify the Network Device Admission Control (NDAC) authenticator and to verify NDAC completion.

Examples

The following sample output displays the Protected Access Credential (PAC) received from a Cisco ACS with the authenticator ID (A-ID–Info):

```
Device# show cts pac

 AID: 1100E046659D4275B644BF946EFA49CD
PAC-Info:
PAC-type = Cisco Trustsec
AID: 1100E046659D4275B644BF946EFA49CD
I-ID: device1
A-ID-Info: acs1
Credential Lifetime: 13:59:27 PDT Jun 5 2010
PAC-Opaque: 000200B000030001000400101100E046659D4275B644BF946EFA49CD0006009400
0301008285A14CB259CA096487096D68D5F34D000000014C09A6AA00093A808ACA80B39EB656AF0B
CA91F3564DF540447A11F9ECDFA4AEC3A193769B80066832495B8C40F6B5B46B685A68411B7DF049
A32F2B03F89ECF948AC4BB85CF855CA186BEF8E2A8C69A7C0BE1BDF6EC27D826896A31821A7BA523
C8BD90072CB8A8D0334F004D4B627D33001B0519D41738F7EDDF3A
Refresh timer is set for 00:01:24
```

show cts role-based counters

To display Security Group access control list (ACL) enforcement statistics, use the **show cts role-based counters** command in user EXEC and privileged EXEC mode.

show cts role-based counters { **default** | { **ipv4** | **ipv6** } } { { [**from** | [*sgt_number* | **unknown**] | { **ipv4** | **ipv6** | **to** | [*sgt_number* | **unknown**] | { **ipv4** | **ipv6** } }] } } { **to** | [*sgt_number* | **unknown**] | { **ipv4** | **ipv6** } } { **ipv4** | **ipv6** }

Syntax Description

default	Specifies default policy counters.
from	Specifies the source security group.

ipv4	Specifies security groups on IPv4 networks.
ipv6	Specifies security groups on IPv6 networks.
to	Specifies the destination security group.
sgt_num	Security Group Tag number. Valid values are from 0 to 65533.
unknown	Specifies all source groups.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	This command was introduced.

Usage Guidelines

Use the **show cts role-based counters** command to display the Security Group ACL (SGACL) enforcement statistics. Use the **clear cts role-based counters** to reset all or a range of statistics.

Specify the source SGT with the **from** keyword and the destination SGT with the **to** keyword. All statistics are displayed when both the **from** and **to** keywords are omitted.

The **default** keyword displays the statistics of the default unicast policy. When neither **ipv4** nor **ipv6** are specified this command displays only IPv4 counters.

Examples

The following sample output displays all enforcement statistics for IPv4 and IPv6 events:

```
Device# show cts role-based counters

 Role-based counters

From To SW-Denied HW-Denied SW-Permitted HW_Permitted
2 5 129 89762 421 7564328
3 5 37 123456 1325 12345678
3 7 0 65432 325 2345678
```

show cts role-based permissions

To display the Cisco TrustSec role-based access control list (RBACL) permissions, use the **show cts role-based permissions** command in privileged EXEC mode.

show cts role-based permissions { { **default** } | { **from** } | { **ipv4** } | { **ipv6** } | { **to** } } { **details** }

show cts role-based permissions { { **default** } | { **from** } | { **ipv4** } | { **to** } } { **details** }

Syntax Description

default	(Optional) Displays the default permission list.
from	(Optional) Displays the source group.

ipv4	(Optional) Displays the IPv4 RBACLs.
ipv6	(Optional) Displays the IPv6 RBACLs.
to	(Optional) Displays the destination group.
details	(Optional) Displays the attached access control list (ACL) details.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	This command was introduced.

Usage Guidelines

This show command displays the content of the RBACL permission matrix. You can specify the source SGT by using the **from** keyword and the destination SGT by using the **to** keyword. When both **from** and **to** are specified the RBACLs of a single cell are displayed. An entire column is displayed when only the **to** is used. An entire row is displayed when the **from** keyword is used.

The entire permission matrix is displayed when both the **from** clause and **to** keywords are omitted.

The command output is sorted by destination SGT as a primary key and the source SGT as a secondary key. The RBACLs for each cell is displayed in the same order they are defined in the configuration or acquired from Cisco ACS.

The **details** keyword is provided when a single cell is selected by specifying both **from** and **to** keywords. When the **details** keyword is specified the ACEs of the RBACLs of a single cell are displayed.

Examples

The following is sample output from the **show cts role-based permissions** command:

```
Device# show cts role-based permissions

 Role-based permissions from group 2 to group 5:
srb2
srb5
Role-based permissions from group 3 to group 5:
srb3
srb5
Role-based permissions from group 3 to group 7:
srb4
```

The following is sample output from the **show cts role-based permissions** command

```
Device# show cts role-based permissions

 Role-based permissions from group 2 to group 5:
srb2
srb5
```

show cts role-based sgt-map

To display the Security Group Tag (SGT) Exchange Protocol (SXP) source IP-to-SGT bindings table, use the **show cts role-based sgt-map** command in user EXEC or privileged EXEC mode.

show cts role-based sgt-map [*ipv4_dec ipv4_cidr ipv6_hex ipv6_cidr* | **all** | { **ipv4** | **ipv6** } | **host** | [*ipv4_decimal ipv6_dec*] | **summary** | { **ipv4** | **ipv6** } | **vrf** *instance_name* | [*ipv4_dec ipv4_cidr ipv6_dec ipv6_cidr* | **all** | [**ipv4** | **ipv6**] | **host** | [*ipv4_decimal ipv6_dec*] | **summary** | [**ipv4** | **ipv6**]]]

Syntax Description

ipv4_dec	IPv4 address in dot-decimal notation. For example (208.77.188.166)
ipv4_cidr	IPv4 address range in Classless Inter-Domain Routing (CIDR) For example, 10.0.0.0/8, where the /8 signifies that the 8 most significant bits identify the networks, and the 24 least-significant bits, the hosts.
ipv6_hex	IPv6 address in hexadecimal separated by colons. For example, 2001:db8:85a3::8a2e:370:7334.
ipv6_cidr	A range of IPv6 address in hexadecimal CIDR notation.
host*ipv4_decimalipv6_hex*	Specifies mappings for a specific IPv4 or IPv6 host. Use dot decimal and hex colon notation for IPv4 and IPv6 respectively.
all	Specifies all mappings to be displayed.
summary*ipv4ipv6*	Summary of IPv4 or IPv6 mappings. Displays both IPv4 and IPv6 if you do not specify a keyword.
vrf*instance_name*	Specifies a VPN routing and forwarding instance for mappings.

Command Default

None

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	This command was introduced.

Usage Guidelines

Use this command to verify that source IP addresses to the appropriate Security Group Tags bindings are correct. This command shows information about active IP-SGT bindings for the specified IP host address or subnet.

This command displays a single binding when host IP address is specified. It displays all the bindings for IP addresses within a given subnet if <network>/<length> is specified.

A summary of the active bindings by source is displayed at the end of the keyword all output and also if the keyword summary is entered.

Examples

The following sample output displays the bindings of IP address and SGT source names:

```
Device# show cts role-based sgt-map vrf 1 all

Active IPv4-SGT Bindings Information
IP Address SGT Source
============================================
10.1.1.1 500 CLI
10.2.2.2 600 SXP
IP-SGT Active Bindings Summary
============================================
Total number of CLI bindings = 1
Total number of SXP bindings = 1
Total number of active bindings = 2
```

show cts sxp connections

To display Cisco TrustSec Security Group Tag (SGT) Exchange Protocol (CTS-SXP) connection or source IP-to-SGT mapping information, use the **show cts sxp connections** command in user EXEC or privileged EXEC mode.

Supported Parameters

connections	Displays Cisco TrustSec SXP connections information.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	This command was introduced.

Usage Guidelines

For more information about this command, see the Cisco IOS XE show cts sxp

Examples

The following example displays the SXP connections using the **brief** keyword:

```
Device# show cts sxp connection brief

 SXP              : Enabled
 Default Password : Set
 Default Source IP: Not Set
Connection retry open period: 10 secs
Reconcile period: 120 secs
Retry open timer is not running
------------------------------------------------------------------------------
Peer_IP          Source_IP        Conn Status       Duration
------------------------------------------------------------------------------
10.10.10.1          10.10.10.2          On               0:00:02:14 (dd:hr:mm:sec)
10.10.2.1          10.10.2.2          On               0:00:02:14 (dd:hr:mm:sec)
Total num of SXP Connections = 2
```

The following example displays the CTS-SXP connections:

```
Device# show cts sxp connections

 SXP              : Enabled
 Default Password : Set
 Default Source IP: Not Set
Connection retry open period: 10 secs
Reconcile period: 120 secs
Retry open timer is not running
----------------------------------------------
Peer IP          : 10.10.10.1
Source IP        : 10.10.10.2
Set up           : Peer
Conn status      : On
Connection mode  : SXP Listener
Connection inst# : 1
TCP conn fd      : 1
TCP conn password: not set (using default SXP password)
Duration since last state change: 0:00:01:25 (dd:hr:mm:sec)
----------------------------------------------
Peer IP          : 10.10.2.1
Source IP        : 10.10.2.2
Set up           : Peer
Conn status      : On
Connection mode  : SXP Listener
TCP conn fd      : 2
TCP conn password: not set (using default SXP password)
Duration since last state change: 0:00:01:25 (dd:hr:mm:sec)
Total num of SXP Connections = 2
```

The following example displays the CTS-SXP connections for a bi-directional connection when the device is both the speaker and listener:

```
Device# show cts sxp connections

SXP : Enabled
Highest Version Supported: 4
Default Password : Set
Default Source IP: Not Set
Connection retry open period: 120 secs
Reconcile period: 120 secs
Retry open timer is running
----------------------------------------------
Peer IP : 2.0.0.2
Source IP : 1.0.0.2
Conn status : On (Speaker) :: On (Listener)
Conn version : 4
Local mode : Both
Connection inst# : 1
TCP conn fd : 1(Speaker) 3(Listener)
TCP conn password: default SXP password
Duration since last state change: 1:03:38:03 (dd:hr:mm:sec) :: 0:00:00:46 (dd:hr:mm:sec)
```

The following example displays output from a CTS-SXP listener with a torn down connection to the SXP speaker. Source IP-to-SGT mappings are held for 120 seconds, the default value of the Delete Hold Down timer.

```
Device# show cts sxp connections

 SXP              : Enabled
```

```
 Default Password : Set
 Default Source IP: Not Set
Connection retry open period: 10 secs
Reconcile period: 120 secs
Retry open timer is not running
----------------------------------------------
Peer IP          : 10.10.10.1
Source IP        : 10.10.10.2
Set up           : Peer
Conn status      : Delete_Hold_Down
Connection mode  : SXP Listener
Connection inst# : 1
TCP conn fd      : -1
TCP conn password: not set (using default SXP password)
Delete hold down timer is running
Duration since last state change: 0:00:00:16 (dd:hr:mm:sec)
----------------------------------------------
Peer IP          : 10.10.2.1
Source IP        : 10.10.2.2
Set up           : Peer
Conn status      : On
Connection inst# : 1
TCP conn fd      : 2
TCP conn password: not set (using default SXP password)
Duration since last state change: 0:00:05:49 (dd:hr:mm:sec)
Total num of SXP Connections = 2
```

show crypto key mypubkey rsa

To display the RSA public keys of your router, use the **show crypto key mypubkey rsa** command in privileged EXEC mode.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For more information about this command, see the Cisco IOS XE show crypto key mypubkey rsa command.

The following example shows the status information for all active crypto sessions:

```
Device#show crypto key mypubkey rsa
Key name: TRUST_POINT_100
Key type: RSA KEYS
 Storage Device: private-config
 Usage: General Purpose Key
 Key is not exportable. Redundancy enabled.
 Key Data:
  30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101
  00B4E83F ABAE87DC DB7ACBB2 844F5FD6 FF2E9E02 DE49A302 D3D7884F 0B26EE6A
  D3D56275 4D733A4F 5D974061 CE8FB520 54276D6D 3B132C82 EB8A3C24 115F77F5
  C38740CE 1BBD89DB 3F766728 649B63FC 2C40C3AD 251656A1 BAF8341E 1736F03D
  0A0D15AF 0E9D3E94 4E2074C7 BA572CA3 95B3D664 916ADA74 281CDE07 B3DD0B42
  13289610 32E611AB 2B3B4EB6 0A3573B1 F097AC2A 3720961C 97597201 3CE8171C
  F02B99B4 3B7B718F 83E221E1 E172554D C2BEA127 93882766 A28C5E8C 4B83BDC5
  A161597D 2C3D8E13 3BE00D8F 02D0AD55 962DF402 599580A6 F049DBF4 045D751B
  A8932156 10B29D9F 037AB33F C1FC463D E59E014C 27660223 546A8B3A E6997713
```

```
  CF020301 0001
% Key pair was generated at: 00:22:51 UTC Oct 27 2021
```

show crypto pki certificates

To display information about your certificate, the certification authority certificate (CA), and any registration authority (RA) certificates, use the **show crypto pki certificates** command in privileged EXEC mode.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For more information about this command, see the Cisco IOS XE show crypto pki certificates command

The following is sample output from the **show crypto pki certificates** command after you authenticated the CA by requesting the certificate of the CA and public key with the crypto pki authenticate command.

```
Device#show crypto pki certificates
CA Certificate
  Status: Available
  Certificate Serial Number: 3051DF7123BEE31B8341DFE4B3A338E5F
  Key Usage: Not Set
```

The CA certificate might show Key Usage as "Not Set."

The following is sample output from the **show crypto pki certificates** command, and it shows the certificate of the router and the certificate of the CA. In this example, a single, general-purpose Rivest, Shamir, and Adelman (RSA) key pair was previously generated, and a certificate was requested but not received for that key pair.

```
Device#show crypto pki certificates
Certificate
  Subject Name
    Name: myrouter.example.com
    IP Address: 10.0.0.1
    Serial Number: 04806682
  Status: Pending
  Key Usage: General Purpose
    Fingerprint: 428125BD A3419600 3F6C7831 6CD8FA95 00000000
CA Certificate
  Status: Available
  Certificate Serial Number: 3051DF7123BEE31B8341DFE4B3A338E5F
  Key Usage: Not Set
```

Note In the previous sample, the certificate status of the device shows "Pending." After the device receives its certificate from the CA, the Status field changes to "Available" in the show output.

The following is sample output from the **show crypto pki certificates** command, and it shows the certificates of two routers and the certificate of the CA. In this example, special-usage RSA key pairs were previously generated, and a certificate was requested and received for each key pair.

```
Device#show crypto pki certificates
Certificate
  Subject Name
    Name: myrouter.example.com
    IP Address: 10.0.0.1
  Status: Available
  Certificate Serial Number: 428125BDA34196003F6C78316CD8FA95
  Key Usage: Signature

Certificate
  Subject Name
    Name: myrouter.example.com
    IP Address: 10.0.0.1
  Status: Available
  Certificate Serial Number: AB352356AFCD0395E333CCFD7CD33897
  Key Usage: Encryption

CA Certificate
  Status: Available
  Certificate Serial Number: 3051DF7123BEE31B8341DFE4B3A338E5F
  Key Usage: Not Set
```

The following is sample output from the **show crypto pki certificates** command when the CA supports an RA. In this example, the CA and RA certificates were previously requested with the **crypto pki authenticate** command.

```
Device#show crypto pki certificates
CA Certificate
  Status: Available
  Certificate Serial Number: 3051DF7123BEE31B8341DFE4B3A338E5F
  Key Usage: Not Set
RA Signature Certificate
  Status: Available
  Certificate Serial Number: 34BCF8A0
  Key Usage: Signature

RA KeyEncipher Certificate
  Status: Available
  Certificate Serial Number: 34BCF89F
  Key Usage: Encryption
```

The following is sample output from the **show crypto pki certificates** using the optional trustpoint-name argument and verbose keyword. The output shows the certificate of a router and the certificate of the CA. In this example, general-purpose RSA key pairs were previously generated, and a certificate was requested and received for the key pair.

```
Device#show crypto pki certificates verbose TRUST_POINT_100
Certificate
  Status: Available
  Version: 3
  Certificate Serial Number (hex): 31
  Certificate Usage: General Purpose
  Issuer:
    o=CRDC
    ou=CRDC-Lab
    cn=vCisco-CA
```

```
  Subject:
    Name: ROUTER1
    cn=ROUTER1
    o=Internet Widgits Pty Ltd
    st=Some-State
    c=AU
  Validity Date:
    start date: 12:57:14 UTC Jul 24 2021
    end   date: 12:57:14 UTC Jul 22 2031
  Subject Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (2048 bit)
  Signature Algorithm: SHA1 with RSA Encryption
  Fingerprint MD5: D0AD3252 586C0DB8 9F4EFC15 1D81AC5F
  Fingerprint SHA1: 6824ED1A C1405149 577CF210 C0BC83D1 8741F0D1
  X509v3 extensions:
    X509v3 Subject Key ID: E806DCF5 89698C43 97795999 4440D7F1 16F9827C
    X509v3 Authority Key ID: 91C2776C 651DF253 08FA9614 D2082F99 BEBF0B00
    Authority Info Access:
  Cert install time: 08:29:26 UTC Oct 21 2021
  Associated Trustpoints: TRUST_POINT_100
  Storage: nvram:CRDC#31.cer
  Key Label: TRUST_POINT_100
  Key storage device: private config

CA Certificate
  Status: Available
  Version: 3
  Certificate Serial Number (hex): 01
  Certificate Usage: Signature
  Issuer:
    o=CRDC
    ou=CRDC-Lab
    cn=vCisco-CA
  Subject:
    o=CRDC
    ou=CRDC-Lab
    cn=vCisco-CA
  Validity Date:
    start date: 13:41:14 UTC Feb 9 2018
    end   date: 13:41:14 UTC Feb 9 2038
  Subject Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (4096 bit)
  Signature Algorithm: SHA1 with RSA Encryption
  Fingerprint MD5: 5ECA97DB 97FF1B95 DFEEB8FB DAB6656F
  Fingerprint SHA1: 73A7E91E 3AB12ABE 746348E4 A0E21BE3 8413130C
  X509v3 extensions:
    X509v3 Key Usage: 86000000
      Digital Signature
      Key Cert Sign
      CRL Signature
    X509v3 Subject Key ID: 91C2776C 651DF253 08FA9614 D2082F99 BEBF0B00
    X509v3 Basic Constraints:
        CA: TRUE
    X509v3 Authority Key ID: 91C2776C 651DF253 08FA9614 D2082F99 BEBF0B00
    Authority Info Access:
  Cert install time: 08:29:23 UTC Oct 21 2021
  Associated Trustpoints: TRUST_POINT_ex TRUST_POINT_100
  Storage: nvram:CRDC#1CA.cer
```

show crypto session

To display status information for active crypto sessions, use the **show crypto session** command in privileged EXEC mode.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For more information about this command, see the Cisco IOS XE show crypto session command.

The following example shows the status information for all active crypto sessions:

```
Device#show crypto session
Crypto session current status
Interface: Virtual-Access2
Username: cisco
Profile: prof
Group: easy
Assigned address: 10.3.3.4
Session status: UP-ACTIVE
Peer: 10.1.1.2 port 500
  IKE SA: local 10.1.1.1/500 remote 10.1.1.2/500 Active
  IKE SA: local 10.1.1.1/500 remote 10.1.1.2/500 Inactive
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 host 3.3.3.4
        Active SAs: 2, origin: crypto map
```

The following example shows the show crypto session detail command output.

```
Device#show crypto session detail
Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation
R - IKE Auto Reconnect, U - IKE Dynamic Route Update
S - SIP VPN

Interface: Tunnel100
Profile: cisco
Uptime: 03:59:01
Session status: UP-ACTIVE
Peer: 10.0.21.16 port 500 fvrf: (none) ivrf: 11
      Phase1_id: cn=ROUTER2,o=Internet Widgits Pty Ltd,st=Some-State,c=AU
      Desc: (none)
  Session ID: 1780
  IKEv2 SA: local 10.0.20.15/500 remote 10.0.21.16/500 Active
          Capabilities:U connid:1 lifetime:20:00:59
  IPSEC FLOW: permit 47 host 10.0.20.15 host 10.0.21.16
        Active SAs: 2, origin: crypto map
        Inbound:  #pkts dec'ed 1668 drop 0 life (KB/Sec) KB Vol Rekey Disabled/2294
        Outbound: #pkts enc'ed 1665 drop 0 life (KB/Sec) KB Vol Rekey Disabled/2294
```

show endpoint-tracker

To display individual tracker status, tracker group status, and tracker group configurations, use the **show endpoint-tracker** command in privileged EXEC mode.

show endpoint-tracker [**interface** *interface-type/number* | **records** | **static-route** | **tracker-group** | **sla-profile** | **sla-mode** | **sla-status** | **sla-statistics**]

Syntax Description

interface	Shows the endpoint tracker information on one interface.
records	Shows the endpoint tracker records.
static-route	Shows the static-route endpoint trackers.
tracker-group	Shows the endpoint tracker group.
sla-profile	Shows the endpoint tracker sla-profile.
sla-mode	Shows all the available SLA modes and the associated parameter values.
sla-status	Shows the endpoint tracker sla-status.
sla-statistics	Shows the endpoint tracker sla-statistics.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.
Cisco IOS XE Catalyst SD-WAN Release 17.14.1a	Added the following keywords: sla-profile, sla-mode, sla-status, and sla-statistics

Examples

The following is a sample output from the **show endpoint-tracker static-route** command:

```
Device# show endpoint-tracker static-route
Tracker Name      Status   RTT in msec     Probe ID
vm7-tcp-10001     UP           3               1
vm7-tcp-10002     UP           2               2
vm7-tcp-10003     UP           5               3
vm7-tcp-10004     UP           5               4
vm7-udp-10001     UP           1               5
vm7-udp-10002     UP           1               6
vm7-udp-10003     UP           1               7
vm7-udp-10004     UP           1               8
```

The following is a sample output from the **show endpoint-tracker tracker-group** command:

```
Device# show endpoint-tracker tracker-group
Tracker Name                    Element trackers name           Status          RTT in
msec   Probe ID
vm7-group-tcp-10001-udp-10002    vm7-tcp-10001, vm7-udp-10002     UP(UP AND UP)   5, 1
      9, 10
vm7-group-tcp-10003-udp-10004    vm7-tcp-10003, vm7-udp-10004     UP(UP AND UP)   5, 1
```

```
      13, 14
vm7-group-udp-10001-tcp-10002    vm7-tcp-10002, vm7-udp-10001     UP(UP OR UP)     4, 1
      11, 12
vm7-group-udp-10003-tcp-10004    vm7-tcp-10004, vm7-udp-10003     UP(UP OR UP)     4, 1
      15, 16
interface-tracker-group          tracker1, tracker2               UP(UP OR UP)     1,1
      53, 54
```

The following is a sample output from the **show endpoint-tracker records** command:

```
Device# show endpoint-tracker records
Record Name                    Endpoint                          EndPoint Type Threshold(ms)
 Multiplier Interval(s) Tracker-Type
vm7-group-tcp-10001-udp-10002    vm7-tcp-10001 AND vm7-udp-10002      N/A           N/A
        N/A        N/A      tracker-group
vm7-group-tcp-10003-udp-10004    vm7-tcp-10003 AND vm7-udp-10004      N/A           N/A
        N/A        N/A      tracker-group
vm7-group-udp-10001-tcp-10002    vm7-tcp-10002 OR vm7-udp-10001       N/A           N/A
        N/A        N/A      tracker-group
vm7-group-udp-10003-tcp-10004    vm7-tcp-10004 OR vm7-udp-10003       N/A           N/A
        N/A        N/A      tracker-group
vm7-tcp-10001                    10.0.0.1                             TCP           100
        1          20       static-route
vm7-tcp-10002                    10.0.0.2                             TCP           100
        1          20       static-route
vm7-udp-10001                    10.0.0.1                             UDP           100
        1          20       static-route
vm7-udp-10002                    10.0.0.2                             UDP           100
        1          20       static-route
group1                           tracker1 OR tracker2                 N/A           N/A
        N/A        N/A      tracker-group
group3                           tracker3 OR tracker4                 N/A           N/A
        N/A        N/A      tracker-group
tracker1                         198.168.20.2                         IP            300
        3          60       interface
tracker2                         198.168.20.3                         IP            300
        3          60       interface
tracker3                         www.diatracker.com                   DNS_NAME      300
        3          60       interface
tracker4                         www.newdiatracker.com                DNS_NAME      300
        3          60       interface
```

The following is a sample output from the **show endpoint-tracker interface** command:

```
Device# show endpoint-tracker interface GigabitEthernet1
Interface      Record Name     Status   RTT in msecs  Probe ID    Next Hop
track-static              1:172.16.1.2    UP        2              11        10.1.1.1
track-static-ro           DIA-Tracker     UP        8              21        172.16.11.1
track-static_static-ro    track-static    UP        1              9         10.1.1.1
GigabitEthernet1          tracker-t1      UP        2              1         10.1.16.13
```

The following is a sample output from the **show endpoint-tracker sla-mode** command:

```
Device# show endpoint-tracker sla-mode
SLA mode             Poll Interval(Secs)  Poll multiplier(buckets)     Dampening multiplier
      Dampening window(Secs)

==========================================================================================
Aggressive           60                   1                            1
       60
Moderate             120                  1                            2
       240
Conservative         300                  1                            3
       900
```

The following table below describes the significant fields shown in the sample output.

Table 6: show endpoint-tracker command Field Descriptions

Field	Description
Tracker Name	Displays names of the configured trackers.
Status	Displays the UP or DOWN status of the trackers, tracker group, and interfaces.
RTT in msecs	Displays the round-trip time of a tracker during which packets are sent to an endpoint and a response is received in ms.
Probe ID	Displays the IDs assigned to each active tracker. Two probe IDs are displayed for a tracker group, and one probe ID is displayed for an individual tracker.
Element Tracker Name	Displays the tracker names associated with the tracker group.
Record Name	Displays all the configured trackers or tracker group names.
Endpoint	Displays all the configured endpoints. Two types of endpoint trackers are supported—static-route tracker and interface tracker.
Endpoint Type	Displays the endpoint types configurations—IP address, DNS name, API URL, TCP/UDP.
Threshold (ms)	Displays wait time for the probe to return a response before declaring that the configured endpoint is down.
Multiplier	Displays the number of times probes are sent to the endpoints.
Interval (s)	Displays the time interval between which probes are sent to the endpoints.
Tracker Type	Displays the tracker type configured. Supported types are interface, static-route, and tracker-group.
Interface	Displays endpoint-tracker information for the specified interface.
Next Hop	Displays IPv4 addresses of the next hop.

show etherchannel load-balancing

To display information about EtherChannel load balancing, use the **show etherchannel load-balancing** command in privileged EXEC mode.

show etherchannel load-balancing

Command Default None

Command Modes Privileged EXEC (#))

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	This command was introduced.

Examples

The following sample output displays information about EtherChannel load balancing.

```
Device# show etherchannel load-balancing
EtherChannel Load-Balancing Method:
Global LB Method: vlan-manual

  Port-Channel:                       LB Method
    Port-channel1                   :  flow-based
```

show etherchannel summary

To display EtherChannel information, use the **show etherchannel summary** command in privileged EXEC mode.

show etherchannel summary

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	This command was introduced.

Examples

The following sample output displays the EtherChannel information.

```
Device# show etherchannel summary
Flags:  D - down        P/bndl - bundled in port-channel
        I - stand-alone s/susp - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator

        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1       Po1(RU)         LACP     Te0/3/0(bndl) Te0/3/1(hot-sby)
```

```
RU - L3 port-channel UP State
SU - L2 port-channel UP state
P/bndl -  Bundled
S/susp  - Suspended
```

show flow exporter

To view flow exporter status and statistics, use the **show flow exporter** command in privileged EXEC mode.

show flow exporter [*exporter-name*] [**templates**]

Syntax Description

exporter-name	(Optional) Name of a flow exporter that was previously configured.
templates	(Optional) Displays flow exporter template information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	This command can be used in controller mode to view flow exporter statistics for Cisco SD-WAN performance monitor.

The following is sample output from the **show flow exporter** command. The output displays the template format for exporters that are configured on the device. This output varies according to the flow record configured:

```
Device# show flow exporter CISCO-MONITOR templates

Flow Exporter CISCO-MONITOR:

  Client: Option options interface-table

  Exporter Format: IPFIX (Version 10)

  Template ID    : 256

  Source ID      : 6

  Record Size    : 102

  Template layout

  ____________________________________________________________________________

  |                 Field                   |    ID | Ent.ID | Offset |  Size |

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

  | INTERFACE INPUT SNMP                    |    10 |        |      0 |     4 |
```

```
| interface name short                    |    82 |        |      4 |    33 |
| interface name long                     |    83 |        |     37 |    65 |
-----------------------------------------------------------------------------


Client: Option options sampler-table
Exporter Format: IPFIX (Version 10)
Template ID    : 257
Source ID      : 6
Record Size    : 48
Template layout
_____________________________________________________________________________
|                Field                    |    ID | Ent.ID | Offset |  Size |
-----------------------------------------------------------------------------
| FLOW SAMPLER                            |    48 |        |      0 |     4 |
| flow sampler name                       |    84 |        |      4 |    41 |
| flow sampler algorithm export           |    49 |        |     45 |     1 |
| flow sampler interval                   |    50 |        |     46 |     2 |
-----------------------------------------------------------------------------


Client: Option options application-name
Exporter Format: IPFIX (Version 10)
Template ID    : 258
Source ID      : 6
Record Size    : 83
Template layout
_____________________________________________________________________________
|                Field                    |    ID | Ent.ID | Offset |  Size |
-----------------------------------------------------------------------------
| APPLICATION ID                          |    95 |        |      0 |     4 |
| application name                        |    96 |        |      4 |    24 |
| application description                 |    94 |        |     28 |    55 |
-----------------------------------------------------------------------------
```

```
Client: Option sub-application-table

Exporter Format: IPFIX (Version 10)

Template ID    : 259

Source ID      : 6

Record Size    : 168

Template layout

_____________________________________________________________________________

|                 Field                   |    ID | Ent.ID | Offset |  Size |

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

| APPLICATION ID                          |    95 |        |      0 |     4 |

| SUB APPLICATION TAG                     |    97 |        |      4 |     4 |

| sub application name                    |   109 |        |      8 |    80 |

| sub application description             |   110 |        |     88 |    80 |

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


Client: Option options application-attributes

Exporter Format: IPFIX (Version 10)

Template ID    : 260

Source ID      : 6

Record Size    : 258

Template layout

_____________________________________________________________________________

|                 Field                   |    ID | Ent.ID | Offset |  Size |

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

| APPLICATION ID                          |    95 |        |      0 |     4 |

| application category name               | 12232 |      9 |      4 |    32 |

| application sub category name           | 12233 |      9 |     36 |    32 |
| application group name                  | 12234 |      9 |     68 |    32 |

| application traffic-class               | 12243 |      9 |    100 |    32 |

| application business-relevance          | 12244 |      9 |    132 |    32 |

| p2p technology                          |   288 |        |    164 |    10 |

| tunnel technology                       |   289 |        |    174 |    10 |
```

```
| encrypted technology                    |   290 |        |    184 |    10 |
| application set name                    | 12231 |      9 |    194 |    32 |
| application family name                 | 12230 |      9 |    226 |    32 |
-------------------------------------------------------------------------------

  Client: Option options tunnel-tloc-table
  Exporter Format: IPFIX (Version 10)
  Template ID    : 261
  Source ID      : 6
  Record Size    : 52
  Template layout

_______________________________________________________________________________
|                 Field                   |    ID | Ent.ID | Offset |  Size |
-------------------------------------------------------------------------------
| TLOC TABLE OVERLAY SESSION ID           | 12435 |      9 |      0 |     4 |
| tloc local color                        | 12437 |      9 |      4 |    16 |
| tloc remote color                       | 12439 |      9 |     20 |    16 |
| tloc tunnel protocol                    | 12440 |      9 |     36 |     8 |
| tloc local system ip address            | 12436 |      9 |     44 |     4 |
| tloc remote system ip address           | 12438 |      9 |     48 |     4 |
-------------------------------------------------------------------------------

Client: Flow Monitor CISCO-MONITOR-art_ipv4
  Exporter Format: IPFIX (Version 10)
  Template ID    : 0
  Source ID      : 0
  Record Size    : 208
  Template layout

_______________________________________________________________________________
|                 Field                   |    ID | Ent.ID | Offset |  Size |
-------------------------------------------------------------------------------
| interface input snmp                    |    10 |        |      0 |     4 |
| connection client ipv4 address          | 12236 |      9 |      4 |     4 |
```

connection server ipv4 address	12237	9	8	4
ip dscp	195		12	1
ip protocol	4		13	1
ip ttl	192		14	1
connection server transport port	12241	9	15	2
connection initiator	239		17	1
timestamp absolute monitoring-interval	359		18	8
flow observation point	138		26	8
overlay session id input	12432	9	34	4
routing vrf service	12434	9	38	4
application id	95		42	4
interface output snmp	14		46	4
flow direction	61		50	1
flow sampler	48		51	1
overlay session id output	12433	9	52	4
timestamp absolute first	152		56	8
timestamp absolute last	153		64	8
connection new-connections	278		72	4
connection sum-duration	279		76	8
connection server counter bytes long	232		84	8
connection server counter packets long	299		92	8
connection client counter bytes long	231		100	8
connection client counter packets long	298		108	8
connection server counter bytes network	8337	9	116	8
connection client counter bytes network	8338	9	124	8
connection delay response to-server sum	9303	9	132	4
connection server counter responses	9292	9	136	4
connection delay response to-server his	9300	9	140	4
connection client counter packets retra	9268	9	144	4
connection delay application sum	9306	9	148	4
connection delay response client-to-ser	9309	9	152	4
connection transaction duration sum	9273	9	156	4

```
  | connection transaction duration min     |  9275 |      9 |    160 |      4 |
  | connection transaction duration max     |  9274 |      9 |    164 |      4 |
  | connection transaction counter complete |  9272 |      9 |    168 |      4 |
  | connection client counter bytes retrans |  9267 |      9 |    172 |      4 |
  | connection server counter bytes retrans |  9269 |      9 |    176 |      4 |
  | connection server counter packets retra |  9270 |      9 |    180 |      4 |
  | connection delay network long-lived to- |  9255 |      9 |    184 |      4 |
  | connection delay network to-client num- |  9259 |      9 |    188 |      4 |
  | connection delay network long-lived to- |  9254 |      9 |    192 |      4 |
  | connection delay network to-server num- |  9258 |      9 |    196 |      4 |
  | connection delay network long-lived cli |  9256 |      9 |    200 |      4 |
  | connection delay network client-to-serv |  9257 |      9 |    204 |      4 |
  ----------------------------------------------------------------------------


Client: Flow Monitor CISCO-MONITOR-media_ipv4
  Exporter Format: IPFIX (Version 10)
  Template ID    : 0
  Source ID      : 0
  Record Size    : 180
  Template layout
  ____________________________________________________________________________
  |                 Field                    |    ID | Ent.ID | Offset |  Size |
  ----------------------------------------------------------------------------
  | ipv4 source address                      |     8 |        |      0 |     4 |
  | ipv4 destination address                 |    12 |        |      4 |     4 |
  | interface input snmp                     |    10 |        |      8 |     4 |
  | ip dscp                                  |   195 |        |     12 |     1 |
  | ip protocol                              |     4 |        |     13 |     1 |
  | ip ttl                                   |   192 |        |     14 |     1 |
  | ipv6 source address                      |    27 |        |     15 |    16 |
  | ipv6 destination address                 |    28 |        |     31 |    16 |
  | transport source-port                    |     7 |        |     47 |     2 |
```

transport destination-port	11		49	2
connection initiator	239		51	1
timestamp absolute monitoring-interval	359		52	8
flow observation point	138		60	8
overlay session id input	12432	9	68	4
routing vrf service	12434	9	72	4
application id	95		76	4
routing forwarding-status	89		80	1
interface output snmp	14		81	4
flow direction	61		85	1
flow sampler	48		86	1
overlay session id output	12433	9	87	4
transport rtp ssrc	4254	9	91	4
transport rtp payload-type	4273	9	95	1
counter bytes long	1		96	8
counter packets	2		104	4
timestamp absolute first	152		108	8
timestamp absolute last	153		116	8
connection new-connections	278		124	4
transport packets expected counter	4246	9	128	4
transport packets lost counter	4251	9	132	4
transport packets lost rate	4253	9	136	4
transport rtp jitter mean	4255	9	140	4
transport rtp jitter minimum	4256	9	144	4
transport rtp jitter maximum	4257	9	148	4
counter bytes rate	4235	9	152	4
application media bytes counter	4236	9	156	4
application media bytes rate	4238	9	160	4
application media packets counter	4239	9	164	4
application media packets rate	4241	9	168	4
transport rtp jitter mean sum	4325	9	172	8

show flow monitor sdwan_flow_monitor cache

To ensure that Unified Logging is enabled successfully for security connection events, use the **show flow monitor sdwan_flow_monitor cache** command in privileged EXEC mode.

show flow monitor sdwan_flow_monitor cache

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

The following is sample output from the **show flow monitor sdwan_flow_monitor cache** command that displays Unified Logging status for the security connection events:

```
IPV4 SOURCE ADDRESS:                            104.193.88.123
IPV4 DESTINATION ADDRESS:                       192.168.20.200
TRNS SOURCE PORT:                               80
TRNS DESTINATION PORT:                          32964
IP VPN ID:                                      1000
IP PROTOCOL:                                    6
interface input:                                Tu2000000001
interface output:                               Gi3
counter bytes long:                             458
counter packets long:                           4
timestamp abs first:                            07:53:16.191
timestamp abs last:                             07:53:16.244
ulogging fw zp id:                              1
ulogging fw zone id array:                      1 2
ulogging fw class id:                           54049
ulogging fw policy id:                          29456
ulogging fw proto id:                           1
ulogging fw action:                             0
ulogging fw drop reason id:                     61
ulogging fw end flow reason:                    1
ulogging fw source ipv4 address translated:     10.1.1.1
ulogging fw destination ipv4 address translated: 20.1.1.1
ulogging fw source port translated:             0
ulogging fw destination port translated:        0
```

show flow record

To display FNF records, use the **show flow record** command in privileged EXEC mode.

show flow record

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.12.1a	This command is supported in Cisco SD-WAN.

The following is sample output from the **show flow record** command that displays FNF records for cflowd events:

```
Router# show flow record
```

IPv4 flow record:

```
flow record sdwan_flow_record-1666223692122679:
  Description:        flow and application visibility records
  No. of users:       1
  Total field space:  102 bytes
  Fields:
    match ipv4 protocol
    match ipv4 source address
    match ipv4 destination address
    match transport source-port
    match transport destination-port
    match routing vrf service
    collect ipv4 dscp
    collect transport tcp flags
    collect interface input
    collect interface output
    collect counter bytes long
    collect counter packets long
    collect timestamp absolute first
    collect timestamp absolute last
    collect application name
    collect flow end-reason
    collect connection initiator
    collect overlay session id input
    collect overlay session id output
    collect connection id long
    collect drop cause id
    collect counter bytes sdwan dropped long
    collect sdwan sla-not-met
    collect sdwan preferred-color-not-met
    collect sdwan qos-queue-id
collect counter packets sdwan dropped long
```

IPv6 flow format:

```
flow record sdwan_flow_record_ipv6-1667963213662363:
  Description:        flow and application visibility records
  No. of users:       1
  Total field space:  125 bytes
  Fields:
    match ipv6 protocol
    match ipv6 source address
    match ipv6 destination address
    match transport source-port
    match transport destination-port
    match routing vrf service
    collect ipv6 dscp
    collect transport tcp flags
    collect interface input
    collect interface output
    collect counter bytes long
    collect counter packets long
    collect timestamp absolute first
    collect timestamp absolute last
    collect application name
    collect flow end-reason
```

```
collect connection initiator
collect overlay session id input
collect overlay session id output
collect connection id long
collect drop cause id
collect counter bytes sdwan dropped long
collect sdwan sla-not-met
collect sdwan preferred-color-not-met
collect sdwan qos-queue-id
collect counter packets sdwan dropped long
```

show full-configuration probe-path load-balance-dia

To view the configured parameters for Cloud onRamp for SaaS load balancing, use the **show full-configuration probe-path load-balance-dia** command in configuration (config) mode.

show full-configuration probe-path load-balance-dia

Command Default

None

Command Modes

configuration (config)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	This command was introduced.

Example

```
Device(config)#show full-configuration probe-path load-balance-dia
probe-path load-balance-dia latency-variance 50
probe-path load-balance-dia loss-variance 30
probe-path load-balance-dia source-ip-hash false
```

show geo file-contents info

To show the geodatabase file contents copied on the device from the Cisco.com download, use the **show geo file-contents info** command in privileged EXEC mode.

show geo file-contents info [**bootflash:** | **crashinfo:** | **flash:** | **webui:**]

Syntax Description

info	View the geolocation database file within the following folders: • bootflash • crashinfo • flash • webui

Command Default No geolocation database file information is displayed.

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines File content is displayed for the nondefault database only.

Examples The following is example output from the **show geo file-contents info** command:

```
Device# show geo file-contents info bootflash:geo_ipv4_db
File version      : 2134.ajkdbnakjsdn
Number of entries : 415278
```

show geo status

To show the status of the geolocation database, use the **show geo status** command in privileged EXEC mode.

show geo status

Syntax Description This command has no arguments or keywords.

Command Default No geolocation database status information is displayed.

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines Use the **show geo status** command to determine if the geolocation database is enabled or not.

Examples The following are example outputs from the **show geo status** command:

```
Device# show geo status
Geo-Location Database is enabled
File in use       : Device default
```

```
Device# show geo status
Geo-Location Database has not been enabled.
```

show interfaces

To display statistics for all interfaces configured on the router, use the **show interfaces** command in privileged EXEC mode.

show interfaces [*type/number*] [**accounting** | **capabilities** | **counters** | **crb** | **dampening** | **debounce** | **description** | **etherchannel** | **flowcontrol** | **history** | **irb** | **mac-accounting** | **mpls-exp** | **mtu** | **precedence** | **private-vlan mapping** | **pruning** | **rate-limit** | **stats** | **status** | **summary** | **switch-port** | **transceiver** | **trunk**]

Syntax Description

None	Displays information for all interfaces.
type	(Optional) Interface type. Allowed values for type can be ACR, ATM-ACR, Analysis-Module, AppNav-Compress, AppNav-UnCompress, Async, Auto-Template, BD-VIF, BDI, BVI, Bluetooth, CDMA-Ix, CEM, CEM-ACR, CEM-PG, CTunnel, Container, Dialer, EsconPhy, Ethernet-Internal, Fcpa, Filter, Filtergroup, GMPLS, GigabitEthernet, IMA-ACR, LISP, LongReachEthernet, Loopback, Lspvif, MFR, Multilink, NVI, Null, Overlay, PROTECTION_GROUP, Port-channel, Portgroup, Pos-channel, SBC, SDH_ACR, SERIAL-ACR, SONET_ACR, SSLVPN-VIF, SYSCLOCK, Serial-PG, Service-Engine, TLS-VIF, Tunnel, Tunnel-tp, VPN, Vif, Vir-cem-ACR, Virtual-PPP, Virtual-Template, Virtual-TokenRing, Virtual-cem, VirtualPortGroup, Vlan, multiservice, nve, pseudowire, ucse, vasileft, vasiright, vmi, voaBypassIn, voaBypassOut, voaFilterIn, voaFilterOut, voaIn, voaOut.
number	(Optional) Port number on the selected interface.
accounting	(Optional) Displays the number of packets of each protocol type that have been sent through the interface.
capabilities	(Optional) Displays the interface capabilities for a module, an interface, or all interfaces.
counters	(Optional) Displays the current status of the protocol counters enabled.
crb	(Optional) Displays interface routing or bridging information.
dampening	(Optional) Displays interface dampening information.
debounce	(Optional) Displays the status and configuration for the debounce timer.
description	(Optional) Displays the interface description.
etherchannel	(Optional) Displays interface Ether Channel information.
flowcontrol	(Optional) Displays flow-control information.
history	(Optional) Displays histograms of interface utilization.
irb	(Optional) Displays interface routing or bridging information.

mac-accounting	(Optional) Displays interface MAC accounting information.
mpls-exp	(Optional) Displays interface Multiprotocol Label Switching (MPLS) experimental accounting information.
mtu	(Optional) Displays MTU information.
precedence	(Optional) Displays interface precedence accounting information.
private-vlan mapping	(Optional) Displays information about the private virtual local area network (PVLAN) mapping for VLAN SVIs.
pruning	(Optional) Displays the interface trunk VTP pruning information.
rate-limit	(Optional) Displays interface rate-limit information.
stats	(Optional) Displays interface packets and octets, in and out, by using switching path.
status	(Optional) Displays the interface status or a list of interfaces in an error-disabled state on local area network (LAN) ports only.
summary	(Optional) Displays interface summary.
switchport	(Optional) Displays the administrative and operational status of a switching (nonrouting) port.
transceiver	(Optional) Displays information about the optical transceivers that have digital optical monitoring (DOM) enabled.
trunk	(Optional) Displays the interface-trunk information.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE show interfaces command.

Example

The following example shows how to display interface information on all interfaces.

```
Device# show interfaces
GigabitEthernet0/0/0 is up, line protocol is up
  Hardware is ISR4331-3x1GE, address is 084f.f99b.267c (bia 084f.f99b.267c)
  Description: INET
  Internet address is 10.3.6.2/24
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
```

```
  Encapsulation ARPA, loopback not set
  Keepalive not supported
  Full Duplex, 1000Mbps, link type is auto, media type is RJ45
  output flow-control is off, input flow-control is off
  ARP type: ARPA, ARP Timeout 00:20:00
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 2000 bits/sec, 2 packets/sec
  5 minute output rate 1000 bits/sec, 1 packets/sec
     235182 packets input, 23708237 bytes, 0 no buffer
     Received 1 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 170048 multicast, 0 pause input
     71585 packets output, 12131971 bytes, 0 underruns
     Output 6 broadcasts (0 IP multicasts)
     0 output errors, 0 collisions, 1 interface resets
     1 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out
GigabitEthernet0/0/1 is up, line protocol is up
  Hardware is ISR4331-3x1GE, address is 084f.f99b.267d (bia 084f.f99b.267d)
  Description: Service
  Internet address is 10.3.13.2/24
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not supported
  Full Duplex, 1000Mbps, link type is auto, media type is RJ45
  output flow-control is off, input flow-control is off
  ARP type: ARPA, ARP Timeout 00:20:00
  Last input 00:00:00, output 00:00:14, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     144332 packets input, 13390830 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 144332 multicast, 0 pause input
     13613 packets output, 5135370 bytes, 0 underruns
     Output 1 broadcasts (0 IP multicasts)
     0 output errors, 0 collisions, 1 interface resets
     1 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 pause output
     0 output buffer failures, 0 output buffers swapped out
<output truncated>
```

The following example shows how to display interface information on Loopback 65528.

```
Device# show interfaces Loopback 65528
Loopback65528 is up, line protocol is up
  Hardware is Loopback
  Internet address is 192.168.1.1/32
  MTU 1514 bytes, BW 8000000 Kbit/sec, DLY 5000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation LOOPBACK, loopback not set
```

```
  Keepalive set (10 sec)
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/0 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 packets output, 0 bytes, 0 underruns
     Output 0 broadcasts (0 IP multicasts)
     0 output errors, 0 collisions, 0 interface resets
     0 unknown protocol drops
     0 output buffer failures, 0 output buffers swapped out
```

The following example shows how to display interface descriptions.

```
Device# show interfaces description
Interface                      Status         Protocol Description
Gi0/0/0                        up             up       INET
Gi0/0/1                        up             up       Service
Gi0/0/2                        down           down
Gi0                            admin down     down
Sdwan-intf                     up             up
Lo65528                        up             up
NV0                            up             up
Tu0                            up             up
```

The following example shows how to display the number of packets of each protocol type that have been sent through the interface.

```
Device# show interface accounting
GigabitEthernet0/0/0 INET
                Protocol    Pkts In   Chars In   Pkts Out  Chars Out
                   Other     169551   14869854      39712    6645521
                      IP      66732    8948821      32339    5548047
           Spanning Tree     259684   13763252          0          0
                     ARP      26188    1571280      26193    1571580
                     CDP       4818    2009106       4815    2123285
                    LLDP       8702    3498204       8704    2950656
GigabitEthernet0/0/1 Service
                Protocol    Pkts In   Chars In   Pkts Out  Chars Out
                   Other     143370   13301850      13521    5100639
           Spanning Tree     259682   13763146          0          0
                     ARP          0          0          1         60
                     CDP       4826    2012442       4817    2124153
                    LLDP       8702    3498204       8704    2976768
GigabitEthernet0/0/2
                Protocol    Pkts In   Chars In   Pkts Out  Chars Out
No traffic sent or received on this interface.
Interface GigabitEthernet0 is disabled
SDWAN System Intf IDB
                Protocol    Pkts In   Chars In   Pkts Out  Chars Out
No traffic sent or received on this interface.
Loopback65528
                Protocol    Pkts In   Chars In   Pkts Out  Chars Out
No traffic sent or received on this interface.
NVI0
                Protocol    Pkts In   Chars In   Pkts Out  Chars Out
No traffic sent or received on this interface.
Tunnel0
```

```
               Protocol    Pkts In   Chars In   Pkts Out  Chars Out
No traffic sent or received on this interface.
```

The following example shows how to display interfaces summary.

```
Device# show interface summary

 *: interface is up
 IHQ: pkts in input hold queue     IQD: pkts dropped from input queue
 OHQ: pkts in output hold queue    OQD: pkts dropped from output queue
 RXBS: rx rate (bits/sec)          RXPS: rx rate (pkts/sec)
 TXBS: tx rate (bits/sec)          TXPS: tx rate (pkts/sec)
 TRTL: throttle count

  Interface                   IHQ        IQD       OHQ       OQD      RXBS      RXPS
TXBS      TXPS      TRTL
------------------------------------------------------------------------------------------------------------
* GigabitEthernet0/0/0          0          0         0         0      4000         6
3000         3         0
* GigabitEthernet0/0/1          0          0         0         0         0         0
  0         0         0
  GigabitEthernet0/0/2          0          0         0         0         0         0
  0         0         0
  GigabitEthernet0              0          0         0         0         0         0
  0         0         0
* Sdwan-system-intf             0          0         0         0         0         0
  0         0         0
* Loopback65528                 0          0         0         0         0         0
  0         0         0
* NVI0                          0          0         0         0         0         0
  0         0         0
* Tunnel0                       0          0         0         4         0         0
  0         0         0
```

show interface port-channel

To display the general status of the port channel interface, use the **show interface port-channel** command in privileged EXEC mode.

show interface port-channel

Command Default

None

Command Modes

Privileged EXEC (>)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	This command was introduced.

Examples

The following sample output displays the status of port channel 10.

```
Device# show interface port-channel 10
 Port-channel10 is up, line protocol is up

  Hardware is 10GEChannel, address is a8b4.5606.ddc9 (bia a8b4.5606.ddc9)
```

```
MTU 1500 bytes, BW 20000000 Kbit/sec, DLY 10 usec,

   reliability 255/255, txload 1/255, rxload 1/255

Encapsulation ARPA, loopback not set

Keepalive set (10 sec)

ARP type: ARPA, ARP Timeout 04:00:00

  No. of active members in this channel: 2

      Member 0 : TenGigabitEthernet0/1/0 , Full-duplex, 10000Mb/s

      Member 1 : TenGigabitEthernet0/1/1 , Full-duplex, 10000Mb/s

  No. of PF_JUMBO supported members in this channel : 2

Last input never, output never, output hang never

Last clearing of "show interface" counters 00:39:12

Input queue: 0/750/0/0 (size/max/drops/flushes); Total output drops: 0

Queueing strategy: fifo

Output queue: 0/80 (size/max)

5 minute input rate 0 bits/sec, 0 packets/sec

5 minute output rate 0 bits/sec, 0 packets/sec

   0 packets input, 0 bytes, 0 no buffer

   Received 0 broadcasts (0 IP multicasts)

   0 runts, 0 giants, 0 throttles

   0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored

   0 watchdog, 0 multicast, 0 pause input

   0 packets output, 0 bytes, 0 underruns
   Output 0 broadcasts (0 IP multicasts)

   0 output errors, 0 collisions, 0 interface resets

   0 unknown protocol drops

   0 babbles, 0 late collision, 0 deferred

   0 lost carrier, 0 no carrier, 0 pause output

   0 output buffer failures, 0 output buffers swapped out
   0 carrier transitions
```

show interface port-channel etherchannel

To display information about a specific port channel interface, use the **show interface port-channel etherchannel** command in privileged EXEC mode.

show interface port-channel *channel-number* **etherchannel**

Command Default None

Command Modes Privileged EXEC (>)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	This command was introduced.

Examples The following sample output displays the information about port channel 10.

```
Device# show interface port-channel 10 etherchannel
Flags:  D - down        P/bndl - bundled in port-channel
        I - stand-alone s/susp - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        U - in use      f - failed to allocate aggregator

        M - not in use, minimum links not met
        u - unsuitable for bundling
        w - waiting to be aggregated
        d - default port


Number of channel-groups in use: 1
Number of aggregators:           1

Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------------
1       Po1(RU)         LACP     Te0/3/0(bndl) Te0/3/1(hot-sby)

RU - L3 port-channel UP State
SU - L2 port-channel UP state
P/bndl -  Bundled
S/susp  - Suspended
```

show inventory

To display the product inventory listing of all Cisco products installed in the networking device, use the **showinventory** command in privileged EXEC mode.

show inventory [*entity* | **fru** *entity* | **oid** *entity* | **raw** *entity*]

Syntax Description

entity	(Optional) Name of a Cisco entity (for example, chassis, backplane, module, or slot). A quoted string may be used to display a specific UDI information; for example “module 0” displays UDI information for slot 0 of an entity named module.
fru	(Optional) Retrieves information about all Field Replaceable Units (FRUs) installed in the Cisco networking device.

oid	(Optional) Retrieves information about the vendor-specific hardware registration identifier, referred to as object identifier (OID).
raw	(Optional) Retrieves information about all Cisco products referred to as entities installed in the Cisco networking device, even if the entities do not have a product ID (PID) value, a unique device identifier (UDI), or other physical identification.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

The **show inventory** command retrieves and displays inventory information about each Cisco product in the form of a UDI. The UDI is a combination of three separate data elements: a product identifier (PID), a version identifier (VID), and the serial number (SN).

The PID is the name by which the product can be ordered; it has been historically called the "Product Name" or "Part Number". This is the identifier that one would use to order an exact replacement part.

The VID is the version of the product. Whenever a product has been revised, the VID will be incremented. The VID is incremented according to a rigorous process derived from Telcordia GR-209-CORE, an industry guideline that governs product change notices.

The SN is the vendor-unique serialization of the product. Each manufactured product will carry a unique serial number assigned at the factory, which cannot be changed in the field. This is the means by which to identify an individual, specific instance of a product.

The UDI refers to each product as an entity. Some entities, such as a chassis, will have sub-entities like slots. Each entity will display on a separate line in a logically ordered presentation that is arranged hierarchically by Cisco entities.

Use the show inventory command without options to display a list of Cisco entities installed in the networking device that are assigned a PID.

Example

The following example shows how to display the inventory in the device.

```
Device# show inventory

++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
INFO: Please use "show license UDI" to get serial number for licensing.
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++

NAME: "Chassis", DESCR: "Cisco ISR4331 Chassis"
PID: ISR4331/K9        , VID: V05  , SN: SAMPLESN123
NAME: "Power Supply Module 0", DESCR: "250W AC Power Supply for Cisco ISR 4330"
PID: PWR-4330-AC       , VID: V03  , SN: SAMPLESN123
NAME: "Fan Tray", DESCR: "Cisco ISR4330 Fan Assembly"
PID: ACS-4330-FANASSY  , VID:      , SN:
NAME: "module 0", DESCR: "Cisco ISR4331 Built-In NIM controller"
PID: ISR4331/K9        , VID:      , SN:
```

```
NAME: "NIM subslot 0/0", DESCR: "Front Panel 3 ports Gigabitethernet Module"
PID: ISR4331-3x1GE     , VID: V01  , SN:
NAME: "module 1", DESCR: "Cisco ISR4331 Built-In SM controller"
PID: ISR4331/K9        , VID:      , SN:
NAME: "module R0", DESCR: "Cisco ISR4331 Route Processor"
PID: ISR4331/K9        , VID: V05  , SN: SAMPLESN123
NAME: "module F0", DESCR: "Cisco ISR4331 Forwarding Processor"
PID: ISR4331/K9        , VID:      , SN:
```

The following example shows how to display the inventory in the device with an entity argument value.

```
Device# show inventory "module 0"

++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
INFO: Please use "show license UDI" to get serial number for licensing.
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++

NAME: "module 0", DESCR: "Cisco ISR4331 Built-In NIM controller"
PID: ISR4331/K9        , VID:      , SN:
NAME: "NIM subslot 0/0", DESCR: "Front Panel 3 ports Gigabitethernet Module"
PID: ISR4331-3x1GE     , VID: V01  , SN:
```

The following example shows how to display the inventory in the device with oid argument value.

```
Device# show inventory oid

++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
INFO: Please use "show license UDI" to get serial number for licensing.
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
NAME: "Chassis", DESCR: "Cisco ISR4331 Chassis"
PID: ISR4331/K9        , VID: V05  , SN: SAMPLESN123
OID: 1.3.6.1.4.1.9.12.3.1.3.1544
NAME: "Power Supply Module 0", DESCR: "250W AC Power Supply for Cisco ISR 4330"
PID: PWR-4330-AC       , VID: V03  , SN: SAMPLESN123
OID: 1.3.6.1.4.1.9.12.3.1.6.442
NAME: "Fan Tray", DESCR: "Cisco ISR4330 Fan Assembly"
PID: ACS-4330-FANASSY  , VID:      , SN:
OID: 1.3.6.1.4.1.9.12.3.1.7.244
NAME: "module 0", DESCR: "Cisco ISR4331 Built-In NIM controller"
PID: ISR4331/K9        , VID:      , SN:
OID: 1.3.6.1.4.1.9.12.3.1.9.104.8
NAME: "NIM subslot 0/0", DESCR: "Front Panel 3 ports Gigabitethernet Module"
PID: ISR4331-3x1GE     , VID: V01  , SN:
OID: 1.3.6.1.4.1.9.12.3.1.9.104.5
NAME: "module 1", DESCR: "Cisco ISR4331 Built-In SM controller"
PID: ISR4331/K9        , VID:      , SN:
OID: 1.3.6.1.4.1.9.12.3.1.9.104.9
NAME: "module R0", DESCR: "Cisco ISR4331 Route Processor"
PID: ISR4331/K9        , VID: V05  , SN: SAMPLESN123
OID: 1.3.6.1.4.1.9.12.3.1.9.104.6
NAME: "module F0", DESCR: "Cisco ISR4331 Forwarding Processor"
PID: ISR4331/K9        , VID:      , SN:
OID: 1.3.6.1.4.1.9.12.3.1.9.104.7
```

Table 7: Related Commands

Commands	Description
show license udi	Shows license UDI information.

show idmgr pxgrid-status

To display the Identity Manager status for pxGrid connections, use the **show idmgr pxgrid-status** command in privileged EXEC mode.

show idmgr pxgrid-status

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	This command was introduced.

Examples

The following sample output displays the Identity Manager status for pxGrid connections.

```
Device# show idmgr pxgrid-status
idmgr pxgrid-status default
----------------------------------------
Identity Manager Tenant - default
----------------------------------------
State                          Connection and subscriptions successful
Current event                  EVT-None
Previous event                 SXP websocket create eveent
Session base URL
Session pubsub base URL
Session topic
UserGroups topic
Session Websocket status       ws-disconnected
SXP base URL                   https://ise-dc-21.mylabtme.local:8910/pxgrid/ise/sxp
SXP pubsub base URL            wss://ise-dc-21.mylabtme.local:8910/pxgrid/ise/pubsub
SXP topic                      /topic/com.cisco.ise.sxp.binding
SXP Websocket status           ws-connected
Last notification sent         Connection successful
Timestamp of recent session
```

Related Commands

Command	Description
show idmgr omp ip-user-bindings	Displays ip-user session bindings sent to OMP.
show idmgr omp user-usergroup-bindings	Displays user-usergroup bindings sent to OMP.
show idmgr user-sessions	Displays users essions learnt from Cisco ISE.

show idmgr omp ip-user-bindings

To display the ip-user session bindings sent to OMP, use the **show idmgr omp ip-user-bindings** command in privileged EXEC mode.

show idmgr omp ip-user-bindings

Command Default None

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	This command was introduced.

Examples

The following sample output displays the ip-user session bindings sent to OMP.

```
Device# show idmgr omp ip-user-bindings
IP                                                  OMP UPDATE
ADDRESS   USERNAME                                  STATE
------------------------------------------------------------
72.1.1.7  TestUser0@SDWAN-IDENTITY.CISCO.COM  omp-updated
```

Related Commands

Command	Description
show idmgr pxgrid-status	Displays Identity Manager status for pxGrid connections.
show idmgr omp user-usergroup-bindings	Displays user-usergroup bindings sent to OMP.
show idmgr user-sessions	Displays users sessions learned from Cisco ISE.

show idmgr omp user-usergroup-bindings

To display the user-usergroup bindings sent to OMP, use the **show idmgr omp user-usergroup-bindings** command in privileged EXEC mode.

show idmgr omp user-usergroup-bindings

Command Default None

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	This command was introduced.

Examples

The following sample output displays the user-usergroup bindings sent to OMP.

```
Device# show idmgr omp user-usergroup-bindings
idmgr omp user-usergroup-bindings TestUser0@SDWAN-IDENTITY.CISCO.COM
 user-groups      "Unknown sdwan-identity.cisco.com/S-1-5-32-545
S-1-5-21-787885371-2815506856-1818290038-513 SDWAN-IDENTITY.CISCO.COM/Builtin/Users
SDWAN-IDENTITY.CISCO.COM/Users/Domain Users "
```

```
 omp-update-state omp-updated
idmgr omp user-usergroup-bindings TestUser1@SDWAN-IDENTITY.CISCO.COM
 user-groups      "Unknown sdwan-identity.cisco.com/S-1-5-32-545
S-1-5-21-787885371-2815506856-1818290038-513 SDWAN-IDENTITY.CISCO.COM/Builtin/Users
SDWAN-IDENTITY.CISCO.COM/Users/Domain Users "
 omp-update-state omp-updated
idmgr omp user-usergroup-bindings adsclient
 user-groups      "User Identity Groups:Employee User Identity Groups:TestUserGroup-1 null
 null "
 omp-update-state omp-updated
```

Related Commands

Command	Description
show idmgr pxgrid-status	Displays Identity Manager status for pxGrid connections.
show idmgr omp ip-user-bindings	Displays the ip-user session bindings sent to OMP.
show idmgr user-sessions	Displays users sessions learned from Cisco ISE.

show idmgr user-sessions

To display the user sessions learned from Cisco ISE, use the **show idmgr user-sessions** command in privileged EXEC mode.

show idmgr user-sessions

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	This command was introduced.

Examples

The following sample output displays the user sessions learnt from ISE.

```
Device# show idmgr user-sessions

USERNAME                              ADDRESS   TIMESTAMP                      STATE

-------------------------------------------------------------------------------------------
TestUser0@SDWAN-IDENTITY.CISCO.COM  72.1.1.7  2022-02-18T13:00:54.372-05:00  Authenticated
```

Related Commands

Command	Description
show idmgr pxgrid-status	Displays Identity Manager status for pxGrid connections.
show idmgr omp ip-user-bindings	Displays the ip-user session bindings sent to OMP.
show idmgr omp user-usergroup-bindings	Displays the user-usergroup bindings sent to OMP.

show ip bgp ipv4

To display entries in the IP version 4 (IPv4) BGP unicast database-related information **show ip bgp ipv4 unicast** command in privileged EXEC mode.

show [**ip**] **bgp ipv4 unicast** [*command*]

Syntax Description

prefix-list	(Optional) Displays entries for the specified prefix.
commad	(Optional) Any multiprotocol BGP command unicast commands supported by the **show ip bgp ipv4 unicast** command.

Command Modes

Privileged EXEC (#)

Examples

The following is sample output from the **show ip bgp ipv4 unicast** command:

```
Device# show ip bgp ipv4 unicast

 BGP table version is 4, local router ID is 10.0.40.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 10.10.10.0/24   172.16.10.1              0             0  300 i
*> 10.10.20.0/24   172.16.10.1              0             0  300 i
*  10.20.10.0/24   172.16.10.1              0             0  300 i
```

The following is sample output from the **show ip bgp ipv4 multicast** command:

```
Device# show ip bgp ipv4 multicast

 BGP table version is 4, local router ID is 10.0.40.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*> 10.10.10.0/24   172.16.10.1              0             0  300 i
*> 10.10.20.0/24   172.16.10.1              0             0  300 i
*  10.20.10.0/24   172.16.10.1              0             0  300 i
```

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

Table 8: show ip bgp ipv4 unicast Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	IP address of the router.

Field	Description
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: • s—The table entry is suppressed. • d—The table entry is damped. • h—The table entry history. • *—The table entry is valid. • >—The table entry is the best entry to use for that network. • i—The table entry was learned via an Internal Border Gateway Protocol (IBGP) session.
Origin codes	Origin of the entry. The origin code is displayed at the end of each line in the table. It can be one of the following values: • i—Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. • e—Entry originated from an Exterior Gateway Protocol (EGP). • ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	IP address of a network entity.
Next Hop	IP address of the next system that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the router has some non-BGP routes to this network.
Metric	If shown, the value of the interautonomous system metric.
LocPrf	Local preference value as set with the **set local-preference** route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.

The following is sample output from the **show ip bgp ipv4 unicast** *prefix* command. The output indicates the imported path information from a VRF named vpn1.

```
Device# show ip bgp ipv4 unicast 192.168.1.0

BGP routing table entry for 10.1.1.0/24, version 2
Paths: (1 available, best #1, table default)
  Not advertised to any peer
  Refresh Epoch 1
  65002, imported path from 1:1:192.168.1.0/24 (vpn1)
    10.4.4.4 (metric 11) from 10.4.4.4 (10.4.4.4)
      Origin IGP, metric 0, localpref 100, valid, internal, best
      Extended Community: RT:1:1
```

```
      mpls labels in/out nolabel/16
```

The following is sample output from the **show ip bgp ipv4 unicast** *prefix* **best-path-reason** command. (The **best-path-reason** keyword was added in Cisco IOS XE Gibralter 16.10.1.)

Prior to running the command, the best path has already been determined. Each path is compared to the best path. The line that starts with **Best Path Evaluation:** shows the reason why this path is not the preferred path, compared to the best path. Possible reasons include: **Lower local preference**, and **Longer cluster length**. The best path shows the reason: **Overall best path**.

```
Router# show ip bgp 172.16.70.96 bestpath-reason
BGP routing table entry for 172.16.0.0/16, version 59086010
Paths: (3 available, best #2, table default)
Multipath: eBGP  Advertised to update-groups:   1  2  3  5  6  7  8  9
  3491 5486, (received & used)
    203.0.113.126 (metric 12989) from 198.51.100.13 (198.51.100.13)
      Origin EGP, metric 0, localpref 300, valid, internal
      Community: 3549:4713 3549:31276
      Originator: 198.51.100.84, Cluster list: 0.0.0.91, 0.0.0.121
      Best Path Evaluation: Lower local preference
  3491 5486, (received & used)
    203.0.113.126 (metric 12989) from 198.51.100.210  (198.51.100.210 )
      Origin EGP, metric 0, localpref 300, valid, internal, best
      Community: 3549:4713 3549:31276
      Originator: 198.51.100.84, Cluster list: 0.0.0.91, 0.0.0.121
      Best Path Evaluation: Overall best path
    203.0.113.126 (metric 12989) from 198.51.100.210  (198.51.100.210 )
      Origin EGP, metric 0, localpref 300, valid, internal
      Community: 3549:4713 3549:31276
      Originator: 198.51.100.84, Cluster list: 0.0.0.91, 0.0.0.121
      Best Path Evaluation: Longer cluster length
```

show ip bgp vpnv4

To display VPN Version 4 (VPNv4) address information from the Border Gateway Protocol (BGP) table, use the **show ip bgp vpnv4** command in user EXEC or privileged EXEC mode.

show ip bgp vpnv4 [*command*]

Syntax Description

command	(Optional) Any BGP command supported by the **show ip bgp vpnv4** command .

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
16.9	This command was introduced.

Usage Guidelines

Use this command to display VPNv4 information from the BGP database. The **show ip bgp vpnv4 all** command displays all available VPNv4 information. The **show ip bgp vpnv4 all summary** command displays BGP neighbor status. The **show ip bgp vpnv4 all labels** command displays label information.

Examples

The following example shows all available VPNv4 information in a BGP routing table:

```
Device# show ip bgp vpnv4 all

BGP table version is 18, local router ID is 10.14.14.14
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP,? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 1:101 (default for vrf vpn1)
*>i10.6.6.6/32       10.0.0.21              11    100      0 ?
*> 10.7.7.7/32       10.150.0.2             11         32768 ?
*>i10.69.0.0/30      10.0.0.21               0    100      0 ?
*> 10.150.0.0/24     0.0.0.0                 0         32768 ?
```

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

Table 9: show ip bgp vpnv4 all Field Descriptions

Field	Description
Network	Displays the network address from the BGP table.
Next Hop	Displays the address of the BGP next hop.
Metric	Displays the BGP metric.
LocPrf	Displays the local preference.
Weight	Displays the BGP weight.
Path	Displays the BGP path per route.

The following example shows how to display a table of labels for NLRI prefixes that have a route distinguisher value of 100:1.

```
Device# show ip bgp vpnv4 rd 100:1 labels

Network            Next Hop       In label/Out label
Route Distinguisher: 100:1 (vrf1)
   10.0.0.0         10.20.0.60      34/nolabel
   10.0.0.0         10.20.0.60      35/nolabel
   10.0.0.0         10.20.0.60      26/nolabel
                    10.20.0.60      26/nolabel
   10.0.0.0         10.15.0.15      nolabel/26
```

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

Table 10: show ip bgp vpnv4 rd labels Field Descriptions

Field	Description
Network	Displays the network address from the BGP table.
Next Hop	Specifies the BGP next hop address.
In label	Displays the label (if any) assigned by this router.

Field	Description
Out label	Displays the label assigned by the BGP next-hop router.

The following example shows VPNv4 routing entries for the VRF named vpn1:

```
Device# show ip bgp vpnv4 vrf vpn1

BGP table version is 18, local router ID is 10.14.14.14
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale, m multipath, b backup-path, x best-external
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 100:1 (default for vrf test1)
*> 10.1.1.1/32      192.168.1.1              0             0 100 i
*bi                 10.4.4.4                 0    100      0 100 i
*> 10.2.2.2/32      192.168.1.1                           0 100 i
*bi                 10.4.4.4                 0    100      0 100 i
*> 172.16.1.0/24    192.168.1.1              0             0 100 i
* i                 10.4.4.4                 0    100      0 100 i
r> 192.168.1.0      192.168.1.1              0             0 100 i
rbi                 10.4.4.4                 0    100      0 100 i
*> 192.168.3.0      192.168.1.1                           0 100 i
*bi                 10.4.4.4                 0    100      0 100 i
```

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

Table 11: show ip bgp vpnv4 vrf Field Descriptions

Field	Description
Network	Displays the network address from the BGP table.
Next Hop	Displays the address of the BGP next hop.
Metric	Displays the BGP metric.
LocPrf	Displays the local preference.
Weight	Displays the BGP weight.
Path	Displays the BGP path per route.

The following example shows attributes for network 192.168.9.0 that include multipaths, best path, and a recursive-via-host flag:

```
Device# show ip bgp vpnv4 vrf vpn1 192.168.9.0 255.255.255.0

BGP routing table entry for 100:1:192.168.9.0/24, version 44
Paths: (2 available, best #2, table test1)
  Additional-path
  Advertised to update-groups:
     2
  100, imported path from 400:1:192.168.9.0/24
    10.8.8.8 (metric 20) from 10.5.5.5 (10.5.5.5)
      Origin IGP, metric 0, localpref 100, valid, internal, backup/repair
      Extended Community: RT:100:1 RT:200:1 RT:300:1 RT:400:1
```

```
    Originator: 10.8.8.8, Cluster list: 10.5.5.5 , recursive-via-host
    mpls labels in/out nolabel/17
100, imported path from 300:1:192.168.9.0/24
  10.7.7.7 (metric 20) from 10.5.5.5 (10.5.5.5)
    Origin IGP, metric 0, localpref 100, valid, internal, best
    Extended Community: RT:100:1 RT:200:1 RT:300:1 RT:400:1
    Originator: 10.7.7.7, Cluster list: 10.5.5.5 , recursive-via-host
    mpls labels in/out nolabel/17
```

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

Table 12: show ip bgp vpnv4 all network-address Field Descriptions

Field	Description
BGP routing table entry for ... version	Internal version number of the table. This number is incremented whenever the table changes.
Paths	Number of autonomous system paths to the specified network. If multiple paths exist, one of the multipaths is designated the best path.
Multipath	Indicates the maximum paths configured (iBGP or eBGP).
Advertised to non peer-group peers	IP address of the BGP peers to which the specified route is advertised.
10.22.7.8 (metric 11) from 10.11.3.4 (10.0.0.8)	Indicates the next hop address and the address of the gateway that sent the update.
Origin	Indicates the origin of the entry. It can be one of the following values: • IGP—Entry originated from Interior Gateway Protocol (IGP) and was advertised with a **network** router configuration command. • incomplete—Entry originated from other than an IGP or Exterior Gateway Protocol (EGP) and was advertised with the **redistribute** router configuration command. • EGP—Entry originated from an EGP.
metric	If shown, the value of the interautonomous system metric.
localpref	Local preference value as set with the **set local-preference route-map** configuration command. The default value is 100.
valid	Indicates that the route is usable and has a valid set of attributes.
internal/external	The field is internal if the path is learned via iBGP. The field is external if the path is learned via eBGP.
multipath	One of multiple paths to the specified network.
best	If multiple paths exist, one of the multipaths is designated the best path and this path is advertised to neighbors.
Extended Community	Route Target value associated with the specified route.

Field	Description
Originator	The router ID of the router from which the route originated when route reflector is used.
Cluster list	The router ID of all the route reflectors that the specified route has passed through.

The following example shows routes that BGP could not install in the VRF table:

```
Device# show ip bgp vpnv4 vrf xyz rib-failure

Network            Next Hop                      RIB-failure   RIB-NH Matches
Route Distinguisher: 2:2 (default for vrf bar)
10.1.1.2/32        10.100.100.100      Higher admin distance              No
10.111.111.112/32  10.9.9.9            Higher admin distance             Yes
```

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

Table 13: show ip bgp vpnv4 vrf rib-failure Field Descriptions

Field	Description
Network	IP address of a network entity.
Next Hop	IP address of the next system that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the router has some non-BGP routes to this network.
RIB-failure	Cause of the Routing Information Base (RIB) failure. Higher admin distance means that a route with a better (lower) administrative distance, such as a static route, already exists in the IP routing table.
RIB-NH Matches	Route status that applies only when Higher admin distance appears in the RIB-failure column and the **bgp suppress-inactive** command is configured for the address family being used. There are three choices: • Yes—Means that the route in the RIB has the same next hop as the BGP route or that the next hop recurses down to the same adjacency as the BGP next hop. • No—Means that the next hop in the RIB recurses down differently from the next hop of the BGP route. • n/a—Means that the **bgp suppress-inactive** command is not configured for the address family being used.

NSF/SSO: MPLS VPN

The following example shows the information displayed on the active and standby Route Processors when they are configured for NSF/SSO: MPLS VPN.

Active Route Processor

```
Device# show ip bgp vpnv4 all labels
```

```
Network          Next Hop   In label/Out label
Route Distinguisher: 100:1 (vpn1)
10.12.12.12/32   0.0.0.0    16/aggregate(vpn1)
10.0.0.0/8       0.0.0.0    17/aggregate(vpn1)
Route Distinguisher: 609:1 (vpn0)
10.13.13.13/32   0.0.0.0    18/aggregate(vpn0)

Router# show ip bgp vpnv4 vrf vpn1 labels

Network          Next Hop   In label/Out label
Route Distinguisher: 100:1 (vpn1)
10.12.12.12/32   0.0.0.0    16/aggregate(vpn1)
10.0.0.0/8       0.0.0.0    17/aggregate(vpn1)
```

Standby Route Processor

```
Device# show ip bgp vpnv4 all labels

Network       Masklen   In label
Route Distinguisher: 100:1
10.12.12.12   /32       16
10.0.0.0      /8        17
Route Distinguisher: 609:1
10.13.13.13   /32       18

Router# show ip bgp vpnv4 vrf vpn1 labels

Network        Masklen   In label
Route Distinguisher: 100:1
10.12.12.12    /32       16
10.0.0.0       /8        17
```

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

Table 14: show ip bgp vpnv4 labels Field Descriptions

Field	Description
Network	The network address from the BGP table.
Next Hop	The BGP next-hop address.
In label	The label (if any) assigned by this router.
Out label	The label assigned by the BGP next-hop router.
Masklen	The mask length of the network address.

The following example displays output, including the explicit-null label, from the **show ip bgp vpnv4 all labels** command on a CSC-PE router:

```
Device# show ip bgp vpnv4 all labels

   Network          Next Hop      In label/Out label
Route Distinguisher: 100:1 (v1)
   10.0.0.0/24       10.0.0.0        19/aggregate(v1)
   10.0.0.1/32       10.0.0.0        20/nolabel
   10.1.1.1/32       10.0.0.0        21/aggregate(v1)
```

```
   10.10.10.10/32    10.0.0.1        25/exp-null

   10.168.100.100/32
                     10.0.0.1        23/exp-null
   10.168.101.101/32
                     10.0.0.1        22/exp-null
```

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

Table 15: show ip bgp vpnv4 all labels Field Descriptions

Field	Description
Network	Displays the network address from the BGP table.
Next Hop	Displays the address of the BGP next hop.
In label	Displays the label (if any) assigned by this router.
Out label	Displays the label assigned by the BGP next-hop router.
Route Distinguisher	Displays an 8-byte value added to an IPv4 prefix to create a VPN IPv4 prefix.

The following example displays separate router IDs for each VRF in the output. The router ID is shown next to the VRF name.

```
Device# show ip bgp vpnv4 all

BGP table version is 5, local router ID is 172.17.1.99
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 1:1 (default for vrf vrf_trans) VRF Router ID 10.99.1.2
*> 192.168.4.0      0.0.0.0                  0         32768 ?
Route Distinguisher: 42:1 (default for vrf vrf_user) VRF Router ID 10.99.1.1
*> 192.168.5.0      0.0.0.0                  0         32768 ?
```

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

Table 16: show ip bgp vpnv4 all (VRF Router ID) Field Descriptions

Field	Description
Route Distinguisher	Displays an 8-byte value added to an IPv4 prefix to create a VPN IPv4 prefix.
vrf	Name of the VRF.
VRF Router ID	Router ID for the VRF.

BGP Event-Based VPN Import

In the following example, the BGP Event-Based VPN Import feature is configured. When the **import path selection** command is configured, but the **strict** keyword is not included, then a safe import path selection policy is in effect. When a path is imported as the best available path (when the best

path or multipaths are not eligible for import), the imported path includes the wording “imported safety path,” as shown in the output.

```
Device# show ip bgp vpnv4 all 172.17.0.0

BGP routing table entry for 45000:1:172.17.0.0/16, version 10
Paths: (1 available, best #1, table vrf-A)
Flag: 0x820
   Not advertised to any peer
   2, imported safety path from 50000:2:172.17.0.0/16
     10.0.101.1 from 10.0.101.1 (10.0.101.1)
       Origin IGP, metric 200, localpref 100, valid, internal, best
       Extended Community: RT:45000:100
```

In the following example, BGP Event-Based VPN Import feature configuration information is shown. When the **import path selection** command is configured with the **all** keyword, any path that matches an RD of the specified VRF will be imported, even though the path does not match the Route Targets (RT) imported by the specified VRF. In this situation, the imported path is marked as “not-in-vrf” as shown in the output. Note that on the net for vrf-A, this path is not the best path because any paths that are not in the VRFs appear less attractive than paths in the VRF.

```
Device# show ip bgp vpnv4 all 172.17.0.0

BBGP routing table entry for 45000:1:172.17.0.0/16, version 11
Paths: (2 available, best #2, table vrf-A)
Flag: 0x820
   Not advertised to any peer
   2
     10.0.101.2 from 10.0.101.2 (10.0.101.2)
       Origin IGP, metric 100, localpref 100, valid, internal, not-in-vrf
       Extended Community: RT:45000:200
       mpls labels in/out nolabel/16
   2
     10.0.101.1 from 10.0.101.1 (10.0.101.1)
       Origin IGP, metric 50, localpref 100, valid, internal, best
       Extended Community: RT:45000:100
mpls labels in/out nolabel/16
```

In the following example, the unknown attributes and discarded attributes associated with the prefix are displayed.

```
Device# show ip bgp vpnv4 all 10.0.0.0/8

BGP routing table entry for 100:200:10.0.0.0/8, version 0
Paths: (1 available, no best path)
  Not advertised to any peer
  Refresh Epoch 1
  Local
    10.0.103.1 from 10.0.103.1 (10.0.103.1)
      Origin IGP, localpref 100, valid, internal
      Extended Community: RT:1:100
      Connector Attribute: count=1
       type 1 len 12 value 22:22:10.0.101.22
      mpls labels in/out nolabel/16
      unknown transitive attribute: flag E0 type 129 length 32
        value 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
0000
      unknown transitive attribute: flag E0 type 140 length 32
```

```
        value 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
0000
      unknown transitive attribute: flag E0 type 120 length 32
        value 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
0000
      discarded unknown attribute: flag C0 type 128 length 32
        value 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
0000
```

BGP—VPN Distinguisher Attribute

The following example is based on the BGP—VPN Distinguisher Attribute feature. The output displays an Extended Community attribute, which is the VPN distinguisher (VD) of 104:1.

```
Device# show ip bgp vpnv4 unicast all 1.4.1.0/24

BGP routing table entry for 104:1:1.4.1.0/24, version 28
Paths: (1 available, best #1, no table)
   Advertised to update-groups:
      1
   Refresh Epoch 1
   1001
     19.0.101.1 from 19.0.101.1 (19.0.101.1)
       Origin IGP, localpref 100, valid, external, best
       Extended Community: VD:104:1
       mpls labels in/out nolabel/16
       rx pathid: 0, tx pathid: 0x0
```

BGP—Support for iBGP Local-AS

The following example includes “allow-policy” in the output, indicating that the BGP—Support for iBGP Local-AS feature was configured for the specified neighbor by configuring the **neighbor allow-policy** command.

```
Device# show ip bgp vpnv4 all neighbors 192.168.3.3 policy

Neighbor: 192.168.3.3, Address-Family: VPNv4 Unicast
Locally configured policies:
 route-map pe33 out
 route-reflector-client
 allow-policy
 send-community both
```

show ip bgp vpnv4 vrf

To display VPN Version 4 (VPNv4) information for a VRF Routing/Forwarding instance from the Border Gateway Protocol (BGP) table, use the **show ip bgp vpnv4 vrf** command in privileged EXEC mode.

show ip bgp vpnv4 vrf *vrf-number*

Syntax Description

vrf-number	Specifies the vrf number to be displayed.

Command Default

None

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines Use this command to display VPN Version 4 (VPNv4) Network information for a VRF Routing/Forwarding instance from the Border Gateway Protocol (BGP) table.

Example

The following example shows how to display the VPNv4 BGP routing table information from VRF.

```
Device# show ip bgp vpnv4 vrf 1
BGP table version is 18, local router ID is 10.14.14.14
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal, r RIB-failure,
 S Stale, m multipath, b backup-path, x best-external
Origin codes: i - IGP, e - EGP, ? - incomplete
Network Next Hop Metric LocPrf Weight Path
Route Distinguisher: 100:1 (default for vrf test1)
*> 10.1.1.1/32 192.168.1.1 0 0 100 i
*bi 10.4.4.4 0 100 0 100 i
*> 10.2.2.2/32 192.168.1.1 0 100 i
*bi 10.4.4.4 0 100 0 100 i
*> 172.16.1.0/24 192.168.1.1 0 0 100 i
* i 10.4.4.4 0 100 0 100 i
r> 192.168.1.0 192.168.1.1 0 0 100 i
rbi 10.4.4.4 0 100 0 100 i
*> 192.168.3.0 192.168.1.1 0 100 i
*bi 10.4.4.4 0 100 0 100 i
```

Table 17: Related Commands

Commands	Description
show ip bgp vpnv4 all	Displays information about all VPN NLRIs.
show ip bgp vpnv4 rd	Displays information for a route distinguisher.

show ip cef vrf

To display the Cisco Express Forwarding forwarding table associated with a Virtual Private Network (VPN) routing or forwarding instance (VRF), use the **show ip cef vrf** command in privileged EXEC mode.

show ip cef vrf *vrf-name ip-prefix* **internal**

Syntax Description

vrf-name	Specifies the name of the VRF from which routes are replicated.
ip-prefix	(Optional) IP prefix of entries to show, in dotted decimal format (A.B.C.D).
internal	Display internal data structures.

Command Default None

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	This command was introduced.

Usage Guidelines Used with only the vrf-name argument, the **show ip cef vrf** command shows a shortened display of the Cisco Express Forwarding table.

Used with the **internal** keyword, the **show ip cef vrf** command shows internal data structures information for all Cisco Express Forwarding table entries.

Examples The following is a sample output from the **show ip cef vrf** command that shows the replicated routes from VRF 1:

```
Device# show ip cef vrf 2 10.10.10.97 internal
10.10.10.97/32, epoch 0, RIB[S], refcnt 6, per-destination sharing
  sources: RIB
  feature space:
    IPRM: 0x00048000
    Broker: linked, distributed at 3rd priority
  subblocks:
    Replicated from VRF 1
  ifnums:
    GigabitEthernet3(9): 10.20.1.2
  path list 7F890C8E2F20, 7 locks, per-destination, flags 0x69 [shble, rif, rcrsv, hwcn]
    path 7F890FB18F08, share 1/1, type recursive, for IPv4
      recursive via 10.20.1.2[IPv4:1], fib 7F890B609578, 1 terminal fib, v4:1:10.20.1.2/32
      path list 7F890C8E3148, 2 locks, per-destination, flags 0x49 [shble, rif, hwcn]
          path 7F890FB19178, share 1/1, type adjacency prefix, for IPv4
            attached to GigabitEthernet3, IP adj out of GigabitEthernet3, addr 10.20.1.2
7F890FAE4CD8
  output chain:
    IP adj out of GigabitEthernet3, addr 10.20.1.2 7F890FAE4CD8
```

show ip msdp vrf count

To display the number of sources and groups originated in MSDP SA messages and the number of SA messages from an MSDP peer in the SA cache. use the **show ip msdp vrf count** command in privileged EXEC mode.

Command Default None

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.11.1a	This command is supported in Cisco Catalyst SD-WAN

Usage Guidelines For usage guidelines, see the Cisco IOS XE show ip msdp count command.

Example

The following example displays the number of sources and groups originated in MSDP SA messages and the number of SA messages from an MSDP peer in the SA cache.

```
Device# show ip msdp vrf 1 count
SA State per Peer Counters, <Peer>: <# SA learned>
    10.168.3.11: 1
    10.168.11.15: 0
    10.168.12.12: 0
    10.168.14.14: 0
    10.168.5.24: 0

SA State per ASN Counters, <asn>: <# sources>/<# groups>
    Total entries: 1
    ?: 1/1
```

show ip msdp vrf peer

To display detailed information about Multicast Source Discovery Protocol (MSDP) peers, use the **show ip msdp vrf peer** command in privileged EXEC mode.

Command Modes

Privileged EXEC (#)

Command History

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.11.1a	This command is supported in Cisco Catalyst SD-WAN

Usage Guidelines

For usage guidelines, see the Cisco IOS XE show ip msdp peer command.

Examples

The following example displays detailed information about Multicast Source Discovery Protocol (MSDP) peers.

```
Device# show ip msdp vrf 1 peer 10.135.250.116
MSDP Peer 10.135.250.116 (?), AS ?
  Connection status:
    State: Up, Resets: 0, Connection source: GigabitEthernet5 (10.168.21.28)
    Uptime(Downtime): 16w4d, Messages sent/received: 169100/169106
    Output messages discarded: 82
    Connection and counters cleared 16w4d    ago
    Peer is member of mesh-group site3
  SA Filtering:
    Input (S,G) filter: sa-filter, route-map: none
    Input RP filter: none, route-map: none
    Output (S,G) filter: none, route-map: none
    Output RP filter: none, route-map: none
  SA-Requests:
    Input filter: none
  Peer ttl threshold: 0
  SAs learned from this peer: 0
  Number of connection transitions to Established state: 1
    Input queue size: 0, Output queue size: 0
```

```
MD5 signature protection on MSDP TCP connection: not enabled
Message counters:
  RPF Failure count: 0
  SA Messages in/out: 10700/10827
  SA Requests in: 0
  SA Responses out: 0
  Data Packets in/out: 0/10
```

show ip msdp vrf sa-cache

To display the (S,G) state learned from Multicast Source Discovery Protocol (MSDP) peers, use the **show ip msdp vrf sa-cache** command in privileged EXEC mode.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.11.1a	This command is supported in Cisco Catalyst SD-WAN

Usage Guidelines

For usage guidelines, see the Cisco IOS XE show ip msdp sa-cache command.

Example

The following example displays the (S,G) state learned from Multicast Source Discovery Protocol (MSDP) peers. This command gives information about MSDP SA messages received from the MSDP peer. In the case of Cisco IOS XE Catalyst SD-WAN devices configured for MSDP interworking, the SA message is advertised as OMP source active.

```
Device# show ip msdp vrf 1 sa-cache
MSDP Source-Active Cache - 1 entries
(10.169.1.1, 12.169.1.1), RP 11.41.41.41, AS ?,6d20h/00:05:55, Peer 12.168.3.11
```

show ip msdp vrf summary

To display Multicast Source Discovery Protocol (MSDP) peer status, use the **show ip msdp vrf summary**command in privileged EXEC mode.

Command Modes

Privileged EXEC (#)

Command History

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.11.1a	This command is supported in Cisco Catalyst SD-WAN

Usage Guidelines

For usage guidelines, see the Cisco IOS XE show ip msdp summary command.

Example

The following example displays Multicast Source Discovery Protocol (MSDP) peer status.

```
Device# show ip msdp vrf 1 summary
MSDP Peer Status Summary
Peer Address     AS    State    Uptime/  Reset SA    Peer Name
                                Downtime Count Count
12.168.3.11      ?     Up       17w6d    0     1     ?
12.168.11.15     ?     Up       17w6d    0     0     ?
12.168.12.12     ?     Up       17w6d    0     0     ?
12.168.14.14     ?     Up       17w6d    0     0     ?
12.168.5.24      ?     Up       17w6d    1     0     ?
```

show ip interface

To display a summary of IP, status and configuration of device interfaces, use the **show ip interface** command in privileged EXEC mode.

show ip interface [**brief**] [*type*] [*number*] [**stats** | **topology** { *WORD* | **all** | **base** } **stats** | **unnumbered** { **detail** }]

Syntax Description

brief	(Optional) Displays brief summary of IP status and configuration.
type	(Optional) Interface Type.
number	(Optional) Interface Number.
stats	(Optional) Shows sum statistics.
topology	(Optional) Topology qualifier for filtering statistics.
WORD	(Optional) Shows the instance topology statistics.
all	(Optional) Shows all topologies statistics.
base	(Optional) Shows base topologies statistics.
stats	(Optional) Shows topology statistics.
unnumbered	(Optional) Displays IP unnumbered status.
detail	(Optional) Displays detailed IP unnumbered status.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

The Cisco IOS software automatically enters a directly connected route in the routing table if the interface is usable (which means that it can send and receive packets). If an interface is not usable, the directly connected routing entry is removed from the routing table. Removing the entry lets the software use dynamic routing protocols to determine backup routes to the network, if any.

If the interface can provide two-way communication, the line protocol is marked up. If the interface hardware is usable, the interface is marked up.

If you specify an optional interface type, information for that specific interface is displayed. If you specify no optional arguments, information about all the interfaces is displayed.

Example

The following example shows how to display interface information on all interfaces.

```
Device# show ip interface

GigabitEthernet0/0/0 is up, line protocol is up
Internet address is 10.10.10.10/24
Broadcast address is 255.255.255.255
Address determined by unknown means
MTU is 1500 bytes
<output truncated>

GigabitEthernet0/0/2 is down, line protocol is down
Internet protocol processing disabled
GigabitEthernet0 is administratively down, line protocol is down
Internet address is 192.168.1.1/24
Broadcast address is 255.255.255.255
Address determined by unknown means
MTU is 1500 bytes
<output truncated>

Dialer1 is up, line protocol is up
Internet protocol processing disabled
Loopback89 is up, line protocol is up
Internet protocol processing disabled
Loopback65528 is up, line protocol is up
Internet address is 192.168.1.1/32
Broadcast address is 255.255.255.255
Address determined by unknown means
MTU is 1514 bytes
<output truncated>
```

The following example shows how to display interface information on Gigabit Ethernet interface 0/0/0.

```
Device# show ip interface GigabitEthernet 0/0/0
GigabitEthernet0/0/0 is up, line protocol is up
Internet address is 10.10.10.10/24
Broadcast address is 255.255.255.255
Address determined by unknown means
MTU is 1500 bytes
Helper address is not set
Directed broadcast forwarding is disabled
Outgoing Common access list is not set
Outgoing access list is not set
Inbound Common access list is not set
Inbound access list is not set
Proxy ARP is disabled (Globally)
Local Proxy ARP is disabled
Security level is default
```

```
Split horizon is enabled
ICMP redirects are never sent
ICMP unreachables are always sent
ICMP mask replies are never sent
IP fast switching is enabled
IP Flow switching is disabled
IP CEF switching is enabled
IP CEF switching turbo vector
IP Null turbo vector
Associated unicast routing topologies:
Topology "base", operation state is UP
IP multicast fast switching is enabled
IP multicast distributed fast switching is disabled
IP route-cache flags are Fast, CEF
Router Discovery is disabled
IP output packet accounting is disabled
IP access violation accounting is disabled
TCP/IP header compression is disabled
RTP/IP header compression is disabled
Probe proxy name replies are disabled
Policy routing is disabled
Network address translation is disabled
BGP Policy Mapping is disabled
Input features: MCI Check
IPv4 WCCP Redirect outbound is disabled
IPv4 WCCP Redirect inbound is disabled
IPv4 WCCP Redirect exclude is disabled
```

The following example shows how to display only stats information on Gigabit Ethernet interface 0/0/0.

```
Device# show ip interface GigabitEthernet 0/0/0 stats

GigabitEthernet0/0/0
5 minutes input rate 0 bits/sec, 0 packet/sec,
5 minutes output rate 0 bits/sec, 0 packet/sec,
0 packets input, 0 bytes,
0 packets output, 0 bytes.
```

The following example shows how to display brief summary of IP status and configuration on Gigabit Ethernet interface 0/0/0.

```
Device# show ip interface brief GigabitEthernet 0/0/0

Interface IP-Address OK? Method Status Protocol
GigabitEthernet0/0/0 10.10.10.10 YES other up up
```

The following example shows how to display the number of IP unnumbered status on Gigabit Ethernet interface 0/0/0.

```
Device# show ip interface GigabitEthernet 0/0/0 unnumbered

Number of unnumbered interfaces with polling: 0
```

The following example shows how to display all topologies stats on Gigabit Ethernet interface 0/0/0.

```
Device# show ip interface GigabitEthernet 0/0/0 topology all stats

GigabitEthernet0/0/0
Topology: base
5 minutes input rate 0 bits/sec, 0 packet/sec,
5 minutes output rate 0 bits/sec, 0 packet/sec,
0 packets input, 0 bytes,
0 packets output, 0 bytes.
```

show ip interface brief

To display a summary of IP, status and configuration of device interfaces, use the **show ip interface brief** command in privileged EXEC mode.

show ip interface brief
show ip interface brief [*type*] [*number*] [**stats** | **topology** { *WORD* | **all** | **base** } **stats**]

Syntax Description

None	Brief summary of IP, status and configuration.
type	(Optional) Interface Type.
number	(Optional) Interface Number.
stats	(Optional) Show sum statistics.
topology	(Optional) Topology qualifier for filtering statistics.
WORD	Shows the instance topology statistics.
all	Shows all topologies statistics.
base	Shows base topologies statistics.
stats	Shows topology statistics.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

Use the **show ip interface brief** command to display a summary of the device interfaces. This command displays the IP address, the interface status, and other information.

The **show ip interface brief** command does not display any information related to unicast RPF.

Example

The following example shows how to display a summary of the usability status information for each interface.

```
Device# show ip interface brief
Interface              IP-Address      OK? Method  Status        Protocol
Vlan1                  unassigned      YES NVRAM   administra
                                                   -tively down  down
GigabitEthernet0/0     unassigned      YES NVRAM   down          down
GigabitEthernet1/0/1   unassigned      YES NVRAM   down          down
GigabitEthernet1/0/2   unassigned      YES unset   down          down
```

```
GigabitEthernet1/0/3 unassigned  YES unset   down          down
<output truncated>
```

Table 18: Related Commands

Commands	Description
show interface description	Shows interface status and description.

show ip nat redundancy

To view information about the IP address associated with the Hot Standby Router Protocol (HSRP) redundancy group name, use the **show ip nat redundancy** command in privileged EXEC mode.

show ip nat redundancy

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	This command was introduced.

Examples

The following is an example output for the **show ip nat redundancy** command:

```
Device# show ip nat redundancy
IP             Redundancy-Name    ID     Use-count
192.168.0.200  hsrp_lan           0      1
```

The output above shows the IP address associated with the HSRP group name.

For more information on static NAT mapping with HSRP, see the *Cisco SD-WAN NAT Configuration Guide*.

Related Commands

Commands	Description
show ip nat translations	Displays active NAT translations.
show standby	Displays HSRP information.

show ip nat route-dia

To show the number of NAT DIA-enabled routes, use the **show ip nat dia-route** command in privileged EXEC mode.

show ip nat dia-route

Syntax Description This command has no arguments or keywords.

Command Default NAT DIA route status information is not displayed.

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.8.1a	This command is supported for Cisco Catalyst SD-WAN.

Examples The following is a sample output from the **show ip nat dia-route** command:

```
Device# show ip nat route-dia
route add [1] addr [0.0.0.0] vrfid [2] prefix len [0]
route add [1] addr [0.0.0.0] vrfid [4] prefix len [0]
```

show ip nat statistics

To display Network Address Translation (NAT) statistics, use the **show ip nat statistics** command in user EXEC or privileged EXEC mode.

show ip nat statistics

Syntax Description This command has no arguments or keywords.

Command Modes User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
16.10	This command was introduced.

Examples The following is sample output from the **show ip nat statistics** command:

```
Device# show ip nat statistics

Total translations: 2 (0 static, 2 dynamic; 0 extended)
Outside interfaces: Serial0
Inside interfaces: Ethernet1
Hits: 135  Misses: 5
Expired translations: 2
Dynamic mappings:
-- Inside Source
access-list 1 pool net-208 refcount 2
 pool net-208: netmask 255.255.255.240
        start 172.16.233.208 end 172.16.233.221
        type generic, total addresses 14, allocated 2 (14%), misses 0
```

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

Table 19: show ip nat statistics Field Descriptions

Field	Description
Total translations	Number of translations active in the system. This number is incremented each time a translation is created and is decremented each time a translation is cleared or times out.
Outside interfaces	List of interfaces marked as outside with the **ip nat outside** command.
Inside interfaces	List of interfaces marked as inside with the **ip nat inside** command.
Hits	Number of times the software does a translations table lookup and finds an entry.
Misses	Number of times the software does a translations table lookup, fails to find an entry, and must try to create one.
Expired translations	Cumulative count of translations that have expired since the router was booted.
Dynamic mappings	Indicates that the information that follows is about dynamic mappings.
Inside Source	Indicates that the information that follows is about an inside source translation.
access-list	Access list number being used for the translation.
pool	Name of the pool (in this case, net-208).
refcount	Number of translations using this pool.
netmask	IP network mask being used in the pool.
start	Starting IP address in the pool range.
end	Ending IP address in the pool range.
type	Type of pool. Possible types are generic or rotary.
total addresses	Number of addresses in the pool available for translation.
allocated	Number of addresses being used.
misses	Number of failed allocations from the pool.

show ip nat translations

To display active Network Address Translation (NAT) translations, use the **show ip nat translations** command in privilege EXEC mode.

show ip nat translations [**inside** *global-ip*] [**outside** *local-ip*] [**icmp**] [**tcp**] [**udp**] [**verbose**] [**vrf** *vrf-name*]

Syntax Description

icmp	(Optional) Displays Internet Control Message Protocol (ICMP) entries.

inside *global-ip*	(Optional) Displays entries for only a specific inside global IP address.
outside *local-ip*	(Optional) Displays entries for only a specific outside local IP address.
tcp	(Optional) Displays TCP protocol entries.
udp	(Optional) Displays User Datagram Protocol (UDP) entries.
verbose	(Optional) Displays additional information for each translation table entry, including how long ago the entry was created and used.
vrf *vrf-name*	(Optional) Displays VPN routing and forwarding (VRF) traffic-related information.

Command Modes

Privilege EXEC (#)

Command History

Release	Modification
16.10	This command was introduced.

Examples

The following is sample output from the **show ip nat translations** command. Without overloading, two inside hosts are exchanging packets with some number of outside hosts.

```
Device# show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
--- 10.69.233.209     192.168.1.95       ---                ---
--- 10.69.233.210     192.168.1.89       ---                --
```

With overloading, a translation for a Domain Name Server (DNS) transaction is still active, and translations for two Telnet sessions (from two different hosts) are also active. Note that two different inside hosts appear on the outside with a single IP address.

```
Device# show ip nat translations
Pro Inside global        Inside local       Outside local      Outside global
udp 10.69.233.209:1220  192.168.1.95:1220  172.16.2.132:53    172.16.2.132:53
tcp 10.69.233.209:11012 192.168.1.89:11012 172.16.1.220:23    172.16.1.220:23
tcp 10.69.233.209:1067  192.168.1.95:1067  172.16.1.161:23    172.16.1.161:23
```

The following is sample output that includes the **verbose** keyword:

```
Device# show ip nat translations verbose
Pro Inside global        Inside local       Outside local      Outside global
udp 172.16.233.209:1220  192.168.1.95:1220  172.16.2.132:53    172.16.2.132:53
        create 00:00:02, use 00:00:00, flags: extended
tcp 172.16.233.209:11012 192.168.1.89:11012 172.16.1.220:23    172.16.1.220:23
        create 00:01:13, use 00:00:50, flags: extended
tcp 172.16.233.209:1067  192.168.1.95:1067  172.16.1.161:23    172.16.1.161:23
        create 00:00:02, use 00:00:00, flags: extended
```

The following is sample output that includes the **vrf** keyword:

```
Device# show ip nat translations vrf
abc
Pro Inside global      Inside local       Outside local      Outside global
--- 10.2.2.1            192.168.121.113    ---                ---
--- 10.2.2.2            192.168.122.49     ---                ---
```

```
--- 10.2.2.11           192.168.11.1       ---                ---
--- 10.2.2.12           192.168.11.3       ---                ---
--- 10.2.2.13           172.16.5.20        ---                ---
Pro Inside global      Inside local       Outside local      Outside global
--- 10.2.2.3            192.168.121.113    ---                ---
--- 10.2.2.4            192.168.22.49      ---                ---
```

The following is sample output that includes the **esp** keyword:

```
Device# show ip nat translations esp

Pro Inside global         Inside local          Outside local         Outside global
esp 192.168.22.40:0      192.168.122.20:0     192.168.22.20:0      192.168.22.20:28726CD9

esp 192.168.22.40:0       192.168.122.20:2E59EEF5 192.168.22.20:0     192.168.22.20:0
```

The following is sample output that includes the **esp** and **verbose** keywords:

```
Device# show ip nat translation esp verbose

Pro Inside global         Inside local          Outside local         Outside global
esp 192.168.22.40:0      192.168.122.20:0     192.168.22.20:0      192.168.22.20:28726CD9

    create 00:00:00, use 00:00:00,
    flags:
extended, 0x100000, use_count:1, entry-id:192, lc_entries:0
esp 192.168.22.40:0       192.168.122.20:2E59EEF5 192.168.22.20:0     192.168.22.20:0
    create 00:00:00, use 00:00:00, left 00:04:59, Map-Id(In):20,
    flags:
extended, use_count:0, entry-id:191, lc_entries:0
```

The following is sample output that includes the **inside**keyword:

```
Device# show ip nat translations inside 10.69.233.209
Pro Inside global        Inside local       Outside local      Outside global
udp 10.69.233.209:1220  192.168.1.95:1220  172.16.2.132:53    172.16.2.132:53
```

The following is sample output when NAT that includes the **inside**keyword:

```
Device# show ip nat translations inside 10.69.233.209
Pro Inside global        Inside local       Outside local      Outside global
udp 10.69.233.209:1220  192.168.1.95:1220  172.16.2.132:53    172.16.2.132:53
```

The following is a sample output that displays information about NAT port parity and conservation:

```
Device# show ip nat translations
Pro  Inside global         Inside local          Outside local         Outside global
udp  200.200.0.100:5066    100.100.0.56:5066     200.200.0.56:5060     200.200.0.56:5060
udp  200.200.0.100:1025    100.100.0.57:10001    200.200.0.57:10001    200.200.0.57:10001
udp  200.200.0.100:10000   100.100.0.56:10000    200.200.0.56:10000    200.200.0.56:10000
udp  200.200.0.100:1024    100.100.0.57:10000    200.200.0.57:10000    200.200.0.57:10000
udp  200.200.0.100:10001   100.100.0.56:10001    200.200.0.56:10001    200.200.0.56:10001
udp  200.200.0.100:9985    100.100.0.57:5066     200.200.0.57:5060     200.200.0.57:5060
Total number of translations: 6
```

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

Table 20: show ip nat translations Field Descriptions

Field	Description
Pro	Protocol of the port identifying the address.
Inside global	The legitimate IP address that represents one or more inside local IP addresses to the outside world.
Inside local	The IP address assigned to a host on the inside network; probably not a legitimate address assigned by the Network Interface Card (NIC) or service provider.
Outside local	IP address of an outside host as it appears to the inside network; probably not a legitimate address assigned by the NIC or service provider.
Outside global	The IP address assigned to a host on the outside network by its owner.
create	How long ago the entry was created (in hours:minutes:seconds).
use	How long ago the entry was last used (in hours:minutes:seconds).
flags	Indication of the type of translation. Possible flags are: • extended--Extended translation • static--Static translation • destination--Rotary translation • outside--Outside translation • timing out--Translation will no longer be used, due to a TCP finish (FIN) or reset (RST) flag.

show ip pim bsr-router

To view information about a bootstrap router (BSR), use the **show ip pim bsr-router** command in privileged EXEC mode.

show ip pim [**vrf** *vrf-name*] **bsr-router**

Syntax Description

vrf *vrf-name*	(Optional) Displays information about a BSR associated with the multicast virtual private network's (MVPN) multicast routing and forwarding instance (MVRF) specified for the *vrf-name* argument.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE show ip pim bsr-router command.

Examples

The following is sample output from the **show ip pim bsr-router** command:

```
Device# show ip pim bsr-router
PIMv2 Bootstrap information
This system is the Bootstrap Router (BSR)
  BSR address: 172.16.143.28
  Uptime: 04:37:59, BSR Priority: 4, Hash mask length: 30
  Next bootstrap message in 00:00:03 seconds
Next Cand_RP_advertisement in 00:00:03 seconds.
  RP: 172.16.143.28(Ethernet0), Group acl: 6
```

show ip pim rp

To view information about the mappings for the PIM group to the active rendezvous points (RPs), use the **show ip pim rp** command in privileged EXEC mode.

show ip pim [**vrf** *vrf-name*] **rp mapping** [*rp-address*]

Syntax Description

vrf *vrf-name*	(Optional) Configures the router to announce its candidacy as a BSR for the multicast virtual private network's (MVPN) multicast routing and forwarding instance (MVRF) specified for the *vrf-name* argument.
rp mapping *rp-address*	(Optional) Displays information about the mappings for the PIM group to the active RPs.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

Use this command to view information about the mappings for the PIM group to the active RPs.

Examples

The following is sample output from the **show ip pim vrf rp mapping** command:

```
Device# show ip pim vrf 1 rp mapping
PIM Group-to-RP Mappings
This system is a candidate RP (v2)
This system is the Bootstrap Router (v2)
```

```
Group(s) 224.0.0.0/4
RP 10.1.10.2 (?), v2
Info source: 10.1.10.2 (?), via bootstrap, priority 0, holdtime 75
Uptime: 15:46:47, expires: 00:00:57
Group(s) 225.0.0.0/8
RP 10.1.10.2 (?), v2
Info source: 10.1.10.2 (?), via bootstrap, priority 0, holdtime 75
Uptime: 15:46:47, expires: 00:00:57
RP 10.1.10.1 (?), v2
Info source: 10.1.10.1 (?), via bootstrap, priority 10, holdtime 75
Uptime: 15:45:45, expires: 00:00:59
Group(s) 226.0.0.0/8
RP 10.1.10.2 (?), v2
Info source: 10.1.10.2 (?), via bootstrap, priority 0, holdtime 75
Uptime: 15:46:55, expires: 00:00:49
RP 10.1.10.1 (?), v2
Info source: 10.1.10.1 (?), via bootstrap, priority 10, holdtime 75
Uptime: 15:46:02, expires: 00:01:09
Group(s) 227.0.0.0/8
RP 10.1.10.2 (?), v2
Info source: 10.1.10.2 (?), via bootstrap, priority 0, holdtime 75
Uptime: 15:47:13, expires: 00:00:59
RP 10.1.10.1 (?), v2
Info source: 10.1.10.1 (?), via bootstrap, priority 10, holdtime 75
Uptime: 15:46:20, expires: 00:00:53
Group(s) 228.0.0.0/8
RP 10.1.10.2 (?), v2
Info source: 10.1.10.2 (?), via bootstrap, priority 0, holdtime 75
Uptime: 15:47:31, expires: 00:01:13
```

show ip protocols

To display the parameters and the current state of the active routing protocol process, use the **show ip protocols** command in privileged EXEC mode.

show ip protocols [**multicast** | **summary** | **topology** *topology-name* | **vrf** *vrf-name* | | [**append** | **begin** | **count** | **exclude** | **format** | **include** | **redirect** | **section** | **tee**]]

Syntax Description

multicast	(Optional) Displays multicast global information.
topology*topology-name*	(Optional) Displays protocols for a topology instance.
summary	(Optional) Displays summary information.
vrf*vrf-name*	(Optional) Displays protocols for a VPN Routing/Forwarding instance.

|	(Optional) Displays information for the specified output modifiers: • append: Append redirected output to URL (URLs supporting append operation only). • begin: Begin with the line that matches. • count: Count number of lines which match regexp. • exclude: Exclude lines that match. • format: Format the output using the specified spec file. • include: Include lines that match. • redirect: Redirect output to URL. • section: Filter a section of output. • tee: Copy output to URL.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE show ip protocols command.

Examples

The following sample output from the **showipprotocols** command shows section of RIP:

```
Device# show ip protocols | sec rip
Routing Protocol is "rip"
  Outgoing update filter list for all interfaces is not set
  Incoming update filter list for all interfaces is not set
  Sending updates every 30 seconds, next due in 19 seconds
  Invalid after 180 seconds, hold down 180, flushed after 240
  Redistributing: rip
  Neighbor(s):
    41.1.1.2
  Default version control: send version 2, receive version 2
    Interface                         Send  Recv  Triggered RIP  Key-chain
    GigabitEthernet1                  2     2          No        none
    Loopback10                        2     2          No        none
  Automatic network summarization is in effect
  Maximum path: 4
  Routing for Networks:
    41.0.0.0
  Routing Information Sources:
    Gateway         Distance      Last Update
    41.1.1.2             120      00:00:15
  Distance: (default is 120)
```

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

Table 21: show ip protocols Field Descriptions

Field	Description
Routing Protocol is...	Name and autonomous system number of the currently running routing protocol.
Outgoing update filter list for all interfaces...	Indicates whether a filter for outgoing routing updates has been specified with the **distribute-listout** command.
Incoming update filter list for all interfaces...	Indicates whether a filter for incoming routing updates has been specified with the **distribute-listin** command.
Redistributing:	Indicates whether route redistribution has been enabled with the **redistribute** command.
Distance	Internal and external administrative distance. Internal distance is the degree of preference given to RIP internal routes. External distance is the degree of preference given to RIP external routes.
Maximum path	Maximum number of parallel routes that the RIP can support.
Maximum hopcount	Maximum hop count (in decimal).
Maximum metric variance	Metric variance used to find feasible paths for a route.
Automatic Summarization	Indicates whether route summarization has been enabled with the **auto-summary** command.
Routing for Networks:	Networks for which the routing process is currently injecting routes.
Routing Information Sources:	Lists all the routing sources that the Cisco IOS software is using to build its routing table. The following is displayed for each source: • IP address • Administrative distance • Time the last update was received from this source

show ip rip database

To display summary address entries in the Routing Information Protocol (RIP) routing database, if relevant routes are being summarized based upon a summary address, use the **show ip rip database** command in privileged EXEC mode.

show ip rip database [*ip-address mask* | **vrf** *vrf-id*]

Syntax Description

ip-address	(Optional) Specifies IP address (network) for which routing information is displayed.

mask	(Optional) Specifies argument for the subnet mask. The subnet mask must also be specified if the IP address argument is entered.
vrf	(Optional) Specifies VPN routing or forwarding instance.
vrf-id	VPN routing or forwarding instance name.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC(#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE show ip rip database command.

Examples

The following is a sample output from the **show ip rip database** command displaying the contents of the RIP private database:

```
Device# show ip rip database vrf 1
10.0.0.1/8 auto-summary
10.1.1.1/32 directly connected, Loopback1
10.2.2.2/8 auto-summary
10.2.2.2/8
[1] via 10.10.10.2, 00:00:29, GigabitEthernet 1/0/1
10.20.20.20/32
[1] via 10.10.10.2, 00:00:03, GigabitEthernet 1/0/1
10.0.0.1/8 auto-summary
10.10.10.0/24 directly connected, GigabitEthernet 1/0/1
```

The following is a sample output from the **show ip rip database** command displaying a summary address entry for route 10.11.0.0/16, with a child route active:

```
Device# show ip rip database
10.11.0.0/16    auto-summary
10.11.0.0/16
[1] via 172.16.1.2, 00:00:00, GigabitEthernet1
```

The table below describes the fields in the display.

Table 22: show ip rip database command Field Descriptions

Field	Description
10.11.0.0/16 auto-summary	Specifies summary address entry.
10.11.0.0/16 [1] via 172.16.1.2, 00:00:00, GigabitEthernet1	RIP is used to discover the destination 10.11.0.0/16. There is a source advertising it. 172.16.1.2 through GigabitEthernet1.

show ip rip neighbors

To display the Routing Information Protocol (RIP) neighbors for which Bidirectional Forwarding Detection (BFD) sessions are created, use the **show ip rip neighbors** command in privileged EXEC mode.

show ip rip neighbors

Syntax Description

This command has no argument or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE show ip rip neighbors command.

Examples

The following is a sample output from the **show ip rip neighbors** command displaying RIP BFD neighbors:

```
Device# show ip rip neighbors
BFD sessions created for the RIP neighbors
Neighbor      Interface         SessionHandle
10.10.10.2    GigabitEthernet1    1
```

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

Table 23: show ip rip neighbors command Field Descriptions

Field	Description
Neighbor	Specifies neighboring router for which BFD sessions are created.
Interface	Specifies the interface type of the neigboring router.
SessionHandle	Specifies the unique session handle number to track the neighbor. The BFD system provides this number.

show ip route

To display contents of the routing table, use the **show ip route** command in user EXEC or privileged EXEC mode.

show ip route [*ip-address* [**repair-paths** | **next-hop-override** [**dhcp**] | *mask* [**longer-prefixes**]] | *protocol* [*process-id*] | **list** [*access-list-number access-list-name*] | **static download** | **update-queue**]

Syntax Description

ip-address	(Optional) IP address for which routing information should be displayed.
repair-paths	(Optional) Displays the repair paths.
next-hop-override	(Optional) Displays the Next Hop Resolution Protocol (NHRP) next-hop overrides that are associated with a particular route and the corresponding default next hops.
dhcp	(Optional) Displays routes added by the Dynamic Host Configuration Protocol (DHCP) server.
mask	(Optional) Subnet mask.
longer-prefixes	(Optional) Displays output for longer prefix entries.
protocol	(Optional) The name of a routing protocol or the keyword **connected**, **mobile**, **static**, or **summary**. If you specify a routing protocol, use one of the following keywords: **bgp**, **eigrp**, **hello**, **isis**, **odr**, **ospf**, **nhrp**, or **rip**.
process-id	(Optional) Number used to identify a process of the specified protocol.
list	(Optional) Filters output by an access list name or number.
access-list-number	(Optional) Access list number.
access-list-name	(Optional) Access list name.
static	(Optional) Displays static routes.
download	(Optional) Displays routes installed using the authentication, authorization, and accounting (AAA) route download function. This keyword is used only when AAA is configured.
update-queue	(Optional) Displays Routing Information Base (RIB) queue updates.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
17.3.1	This command was introduced.

The following is sample output from the **show iproute** command when an IP address is not specified:

```
Device# show ip route

Codes: R - RIP derived, O - OSPF derived,
       C - connected, S - static, B - BGP derived,
       * - candidate default route, IA - OSPF inter area route,
       i - IS-IS derived, ia - IS-IS, U - per-user static route,
       o - on-demand routing, M - mobile, P - periodic downloaded static route,
       D - EIGRP, EX - EIGRP external, E1 - OSPF external type 1 route,
       E2 - OSPF external type 2 route, N1 - OSPF NSSA external type 1 route,
       N2 - OSPF NSSA external type 2 route
Gateway of last resort is 10.119.254.240 to network 10.140.0.0
```

```
O E2 10.110.0.0 [160/5] via 10.119.254.6, 0:01:00, Ethernet2
E    10.67.10.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
O E2 10.68.132.0 [160/5] via 10.119.254.6, 0:00:59, Ethernet2
O E2 10.130.0.0 [160/5] via 10.119.254.6, 0:00:59, Ethernet2
E    10.128.0.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
E    10.129.0.0 [200/129] via 10.119.254.240, 0:02:22, Ethernet2
E    10.65.129.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
E    10.10.0.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
E    10.75.139.0 [200/129] via 10.119.254.240, 0:02:23, Ethernet2
E    10.16.208.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
E    10.84.148.0 [200/129] via 10.119.254.240, 0:02:23, Ethernet2
E    10.31.223.0 [200/128] via 10.119.254.244, 0:02:22, Ethernet2
E    10.44.236.0 [200/129] via 10.119.254.240, 0:02:23, Ethernet2
E    10.141.0.0 [200/129] via 10.119.254.240, 0:02:22, Ethernet2
E    10.140.0.0 [200/129] via 10.119.254.240, 0:02:23, Ethernet2
```

The following sample output from the **show ip routes** command includes routes learned from IS-IS Level 2:

```
Device# show ip route

Codes: R - RIP derived, O - OSPF derived,
       C - connected, S - static, B - BGP derived,
       * - candidate default route, IA - OSPF inter area route,
       i - IS-IS derived, ia - IS-IS, U - per-user static route,
       o - on-demand routing, M - mobile, P - periodic downloaded static route,
       D - EIGRP, EX - EIGRP external, E1 - OSPF external type 1 route,
       E2 - OSPF external type 2 route, N1 - OSPF NSSA external type 1 route,
       N2 - OSPF NSSA external type 2 route
Gateway of last resort is not set
     10.89.0.0 is subnetted (mask is 255.255.255.0), 3 subnets
C       10.89.64.0 255.255.255.0 is possibly down,
          routing via 0.0.0.0, Ethernet0
i L2    10.89.67.0 [115/20] via 10.89.64.240, 0:00:12, Ethernet0
i L2    10.89.66.0 [115/20] via 10.89.64.240, 0:00:12, Ethernet0
```

The following is sample output from the **show ip route** *ip-address mask* **longer-prefixes** command. When this keyword is included, the address-mask pair becomes the prefix, and any address that matches that prefix is displayed. Therefore, multiple addresses are displayed. The logical AND operation is performed on the source address 0.0.0.0 and the mask 0.0.0.0, resulting in 0.0.0.0. Each destination in the routing table is also logically ANDed with the mask and compared with 0.0.0.0. Any destinations that fall into that range are displayed in the output.

```
Device# show ip route 0.0.0.0 0.0.0.0 longer-prefixes

Codes: R - RIP derived, O - OSPF derived,
       C - connected, S - static, B - BGP derived,
       * - candidate default route, IA - OSPF inter area route,
       i - IS-IS derived, ia - IS-IS, U - per-user static route,
       o - on-demand routing, M - mobile, P - periodic downloaded static route,
       D - EIGRP, EX - EIGRP external, E1 - OSPF external type 1 route,
       E2 - OSPF external type 2 route, N1 - OSPF NSSA external type 1 route,
       N2 - OSPF NSSA external type 2 route

Gateway of last resort is not set

S    10.134.0.0 is directly connected, Ethernet0
S    10.10.0.0 is directly connected, Ethernet0
S    10.129.0.0 is directly connected, Ethernet0
S    10.128.0.0 is directly connected, Ethernet0
S    10.49.246.0 is directly connected, Ethernet0
S    10.160.97.0 is directly connected, Ethernet0
```

```
S    10.153.88.0 is directly connected, Ethernet0
S    10.76.141.0 is directly connected, Ethernet0
S    10.75.138.0 is directly connected, Ethernet0
S    10.44.237.0 is directly connected, Ethernet0
S    10.31.222.0 is directly connected, Ethernet0
S    10.16.209.0 is directly connected, Ethernet0
S    10.145.0.0 is directly connected, Ethernet0
S    10.141.0.0 is directly connected, Ethernet0
S    10.138.0.0 is directly connected, Ethernet0
S    10.128.0.0 is directly connected, Ethernet0
     10.19.0.0 255.255.255.0 is subnetted, 1 subnets
C       10.19.64.0 is directly connected, Ethernet0
     10.69.0.0 is variably subnetted, 2 subnets, 2 masks
C       10.69.232.32 255.255.255.240 is directly connected, Ethernet0
S       10.69.0.0 255.255.0.0 is directly connected, Ethernet0
```

The following sample outputs from the **show ip route** command display all downloaded static routes. A “p” indicates that these routes were installed using the AAA route download function.

```
Device# show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
       U - per-user static route, o - ODR, P - periodic downloaded static route
       T - traffic engineered route

Gateway of last resort is 172.16.17.1 to network 10.0.0.0

        172.31.0.0/32 is subnetted, 1 subnets
P       172.31.229.41 is directly connected, Dialer1 0.0.0.0/0 is subnetted, 3 subnets
P       10.1.1.0 [200/0] via 172.31.229.41, Dialer1
P       10.1.3.0 [200/0] via 172.31.229.41, Dialer1
P       10.1.2.0 [200/0] via 172.31.229.41, Dialer1

Device# show ip route static

     172.16.4.0/8 is variably subnetted, 2 subnets, 2 masks
P       172.16.1.1/32 is directly connected, BRI0
P       172.16.4.0/8 [1/0] via 10.1.1.1, BRI0
S    172.31.0.0/16 [1/0] via 172.16.114.65, Ethernet0
S    0.0.0.0/0 is directly connected, BRI0
P    0.0.0.0/0 is directly connected, BRI0
     172.16.0.0/16 is variably subnetted, 5 subnets, 2 masks
S       172.16.114.201/32 is directly connected, BRI0
S       172.16.114.205/32 is directly connected, BRI0
S       172.16.114.174/32 is directly connected, BRI0
S       172.16.114.12/32 is directly connected, BRI0
P    0.0.0.0/8 is directly connected, BRI0
P    0.0.0.0/16 is directly connected, BRI0
P    10.2.2.0/24 is directly connected, BRI0
S*   0.0.0.0/0 [1/0] via 172.16.114.65, Ethernet0
S    172.16.0.0/16 [1/0] via 172.16.114.65, Ethernet0
```

The following sample output from the **show ip route static download** command displays all active and inactive routes installed using the AAA route download function:

```
Device# show ip route static download

Connectivity: A - Active, I - Inactive
```

```
A     10.10.0.0 255.0.0.0 BRI0
A     10.11.0.0 255.0.0.0 BRI0
A     10.12.0.0 255.0.0.0 BRI0
A     10.13.0.0 255.0.0.0 BRI0
I     10.20.0.0 255.0.0.0 172.21.1.1
I     10.22.0.0 255.0.0.0 Serial0
I     10.30.0.0 255.0.0.0 Serial0
I     10.31.0.0 255.0.0.0 Serial1
I     10.32.0.0 255.0.0.0 Serial1
A     10.34.0.0 255.0.0.0 192.168.1.1
A     10.36.1.1 255.255.255.255 BRI0 200 name remote1
I     10.38.1.9 255.255.255.0 192.168.69.1
```

The following sample outputs from the **show ip route nhrp** command display shortcut switching on the tunnel interface:

```
Device# show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP
Gateway of last resort is not set
0.0.0.0/16 is variably subnetted, 3 subnets, 2 masks
C       10.1.1.0/24 is directly connected, Tunnel0
C       172.16.22.0 is directly connected, Ethernet1/0
H       172.16.99.0 [250/1] via 10.1.1.99, 00:11:43, Tunnel0
     10.11.0.0/24 is subnetted, 1 subnets
C       10.11.11.0 is directly connected, Ethernet0/0

Device# show ip route nhrp

H       172.16.99.0 [250/1] via 10.1.1.99, 00:11:43, Tunnel0
```

The following are sample outputs from the **show ip route** command when the **next-hop-override** keyword is used. When this keyword is included, the NHRP next-hop overrides that are associated with a particular route and the corresponding default next hops are displayed.

```
================================================================
1) Initial configuration
================================================================

Device# show ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP
       + - replicated route

Gateway of last resort is not set
      10.2.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        10.2.1.0/24 is directly connected, Loopback1
L        10.2.1.1/32 is directly connected, Loopback1
      0.0.0.0/24 is subnetted, 1 subnets
S        10.10.10.0 is directly connected, Tunnel0
```

```
      10.11.0.0/24 is subnetted, 1 subnets
S        10.11.11.0 is directly connected, Ethernet0/0

Device# show ip route next-hop-override

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP
       + - replicated route

Gateway of last resort is not set
      10.2.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        10.2.1.0/24 is directly connected, Loopback1
L        10.2.1.1/32 is directly connected, Loopback1
      10.0.0.0/24 is subnetted, 1 subnets
S        10.10.10.0 is directly connected, Tunnel0
      10.11.0.0/24 is subnetted, 1 subnets
S        10.11.11.0 is directly connected, Ethernet0/0

Device# show ip cef

Prefix               Next Hop             Interface
.
.
.
10.2.1.255/32         receive              Loopback1
10.10.10.0/24        attached             Tunnel0  <<<<<<<<
10.11.11.0/24        attached             Ethernet0/0
172.16.0.0/12          drop
.
.
.
==============================================================
2) Add a next-hop override
   address = 10.10.10.0
   mask = 255.255.255.0
   gateway = 10.1.1.1
   interface = Tunnel0
==============================================================

Device# show ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP
       + - replicated route

Gateway of last resort is not set
      10.2.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        10.2.1.0/24 is directly connected, Loopback1
L        10.2.1.1/32 is directly connected, Loopback1
      10.0.0.0/24 is subnetted, 1 subnets

S        10.10.10.0 is directly connected, Tunnel0
      10.11.0.0/24 is subnetted, 1 subnets
S        10.11.11.0 is directly connected, Ethernet0/0
```

```
Device# show ip route next-hop-override

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP
       + - replicated route

Gateway of last resort is not set
      10.2.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        10.2.1.0/24 is directly connected, Loopback1
L        10.2.1.1/32 is directly connected, Loopback1
      10.0.0.0/24 is subnetted, 1 subnets

S        10.10.10.0 is directly connected, Tunnel0
                   [NHO][1/0] via 10.1.1.1, Tunnel0
      10.11.0.0/24 is subnetted, 1 subnets
S        10.11.11.0 is directly connected, Ethernet0/0

Device# show ip cef

Prefix               Next Hop             Interface
.
.
.
10.2.1.255/32         receive              Loopback110.10.10.0/24

10.10.10.0/24       10.1.1.1             Tunnel0

10.11.11.0/24       attached            Ethernet0/0
10.12.0.0/16 drop
.
.
.
================================================================
3) Delete a next-hop override
   address = 10.10.10.0
   mask = 255.255.255.0
   gateway = 10.11.1.1
   interface = Tunnel0
================================================================

Device# show ip route

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP
       + - replicated route

Gateway of last resort is not set
      10.2.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        10.2.1.0/24 is directly connected, Loopback1
L        10.2.1.1/32 is directly connected, Loopback1
      10.0.0.0/24 is subnetted, 1 subnets
S        10.10.10.0 is directly connected, Tunnel0
      10.11.0.0/24 is subnetted, 1 subnets
```

```
S        10.11.11.0 is directly connected, Ethernet0/0

Device# show ip route next-hop-override

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP
       + - replicated route

Gateway of last resort is not set
      10.2.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        10.2.1.0/24 is directly connected, Loopback1
L        10.2.1.1/32 is directly connected, Loopback1
      10.0.0.0/24 is subnetted, 1 subnets
S        10.10.10.0 is directly connected, Tunnel0
      10.11.0.0/24 is subnetted, 1 subnets
S        10.11.11.0 is directly connected, Ethernet0/0

Device# show ip cef

Prefix               Next Hop             Interface
.
.
.
10.2.1.255/32         receive              Loopback110.10.10.0/24

10.10.10.0/24        attached             Tunnel0
10.11.11.0/24        attached             Ethernet0/0
10.120.0.0/16 drop
.
.
.
```

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

Table 24: show ip route Field Descriptions

Field	Description
Codes (Protocol)	Indicates the protocol that derived the route. It can be one of the following values: • B—BGP derived • C—Connected • D—Enhanced Interior Gateway Routing Protocol (EIGRP) • EX—EIGRP external • H—NHRP • i—IS-IS derived • ia—IS-IS • L—Local • M—Mobile • o—On-demand routing • O—Open Shortest Path First (OSPF) derived • P—Periodic downloaded static route • R—Routing Information Protocol (RIP) derived • S—Static • U—Per-user static route • +—Replicated route
Codes (Type)	Type of route. It can be one of the following values: • *—Indicates the last path used when a packet was forwarded. This information is specific to nonfast-switched packets. • E1—OSPF external type 1 route • E2—OSPF external type 2 route • IA—OSPF interarea route • L1—IS-IS Level 1 route • L2—IS-IS Level 2 route • N1—OSPF not-so-stubby area (NSSA) external type 1 route • N2—OSPF NSSA external type 2 route
10.110.0.0	Indicates the address of the remote network.

Field	Description
[160/5]	The first number in brackets is the administrative distance of the information source; the second number is the metric for the route.
via 10.119.254.6	Specifies the address of the next device to the remote network.
0:01:00	Specifies the last time the route was updated (in hours:minutes:seconds).
Ethernet2	Specifies the interface through which the specified network can be reached.

The following is sample output from the **show ip route** command when an IP address is specified:

```
Device# show ip route 0.0.0.0

Routing entry for 0.0.0.0/0
    Known via "isis", distance 115, metric 20, type level-1
    Redistributing via isis
    Last update from 10.191.255.251 on Fddi1/0, 00:00:13 ago
    Routing Descriptor Blocks:
    * 10.22.22.2, from 10.191.255.247, via Serial2/3
       Route metric is 20, traffic share count is 1
       10.191.255.251, from 10.191.255.247, via Fddi1/0
       Route metric is 20, traffic share count is 1
```

When an IS-IS router advertises its link-state information, the router includes one of its IP addresses to be used as the originator IP address. When other routers calculate IP routes, they store the originator IP address with each route in the routing table.

The preceding example shows the output from the **show ip route** command for an IP route generated by IS-IS. Each path that is shown under the Routing Descriptor Blocks report displays two IP addresses. The first address (10.22.22.2) is the next-hop address. The second is the originator IP address from the advertising IS-IS router. This address helps you determine the origin of a particular IP route in your network. In the preceding example, the route to 0.0.0.0/0 was originated by a device with IP address 10.191.255.247.

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

Table 25: show ip route with IP Address Field Descriptions

Field	Description
Routing entry for 0.0.0.0/0	Network number and mask.
Known via...	Indicates how the route was derived.
Redistributing via...	Indicates the redistribution protocol.
Last update from 10.191.255.251	Indicates the IP address of the router that is the next hop to the remote network and the interface on which the last update arrived.
Routing Descriptor Blocks	Displays the next-hop IP address followed by the information source.
Route metric	This value is the best metric for this Routing Descriptor Block.
traffic share count	Indicates the number of packets transmitted over various routes.

The following sample output from the **show ip route** command displays the tag applied to the route 10.22.0.0/16. You must specify an IP prefix to see the tag value. The fields in the display are self-explanatory.

```
Device# show ip route 10.22.0.0

Routing entry for 10.22.0.0/16
  Known via "isis", distance 115, metric 12
  Tag 120, type level-1
  Redistributing via isis
  Last update from 172.19.170.12 on Ethernet2, 01:29:13 ago
  Routing Descriptor Blocks:
    * 172.19.170.12, from 10.3.3.3, via Ethernet2
        Route metric is 12, traffic share count is 1
        Route tag 120
```

The following example shows that IP route 10.8.8.0 is directly connected to the Internet and is the next-hop (option 3) default gateway. Routes 10.1.1.1 [1/0], 10.3.2.1 [24/0], and 172.16.2.2 [1/0] are static, and route 0.0.0.0/0 is a default route candidate. The fields in the display are self-explanatory.

```
Device# show ip route

Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route
Gateway of last resort is 10.0.19.14 to network 0.0.0.0
10.0.0.0/24 is subnetted, 1 subnets
C 10.8.8.0 is directly connected, Ethernet1
  10.0.0.0/32 is subnetted, 1 subnets
S 10.1.1.1 [1/0] via 10.8.8.1
  10.0.0.0/32 is subnetted, 1 subnets
S 10.3.2.1 [24/0] via 10.8.8.1
  172.16.0.0/32 is subnetted, 1 subnets
S 172.16.2.2 [1/0] via 10.8.8.1
  10.0.0.0/28 is subnetted, 1 subnets
C 10.0.19.0 is directly connected, Ethernet0
  10.0.0.0/24 is subnetted, 1 subnets
C 10.15.15.0 is directly connected, Loopback0
S* 10.0.0.0/0 [1/0] via 10.0.19.14
```

The following sample output from the **show ip route repair-paths** command shows repair paths marked with the tag [RPR]. The fields in the display are self-explanatory:

```
Device# show ip route repair-paths

Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP
       + - replicated route, % - next hop override

Gateway of last resort is not set
```

```
      10.0.0.0/32 is subnetted, 3 subnets
C        10.1.1.1 is directly connected, Loopback0
B        10.2.2.2 [200/0] via 172.16.1.2, 00:31:07
                  [RPR][200/0] via 192.168.1.2, 00:31:07
B        10.9.9.9 [20/0] via 192.168.1.2, 00:29:45
                  [RPR][20/0] via 192.168.3.2, 00:29:45
      172.16.0.0/16 is variably subnetted, 2 subnets, 2 masks
C        172.16.1.0/24 is directly connected, Ethernet0/0
L        172.16.1.1/32 is directly connected, Ethernet0/0
      192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C        192.168.1.0/24 is directly connected, Serial2/0
L        192.168.1.1/32 is directly connected, Serial2/0
B     192.168.3.0/24 [200/0] via 172.16.1.2, 00:31:07
                     [RPR][200/0] via 192.168.1.2, 00:31:07
B     192.168.9.0/24 [20/0] via 192.168.1.2, 00:29:45
                     [RPR][20/0] via 192.168.3.2, 00:29:45
B     192.168.13.0/24 [20/0] via 192.168.1.2, 00:29:45
                      [RPR][20/0] via 192.168.3.2, 00:29:45

Device# show ip route repair-paths 10.9.9.9

>Routing entry for 10.9.9.9/32
>  Known via "bgp 100", distance 20, metric 0
>  Tag 10, type external
>  Last update from 192.168.1.2 00:44:52 ago
>  Routing Descriptor Blocks:
>  * 192.168.1.2, from 192.168.1.2, 00:44:52 ago, recursive-via-conn
>      Route metric is 0, traffic share count is 1
>      AS Hops 2
>      Route tag 10
>      MPLS label: none
>    [RPR]192.168.3.2, from 172.16.1.2, 00:44:52 ago
>      Route metric is 0, traffic share count is 1
>      AS Hops 2
>      Route tag 10
>      MPLS label: none
```

show ip route rip

To display contents of the RIP routing table, use the **show ip route rip** command in privileged EXEC mode.

show ip route rip | [append *resource-locator* **| begin** *LINE* **| count** *LINE* **| exclude** *LINE* **| format** *file-location* **| include** *LINE* **| redirect** *resource-locator* **| section** *LINE* **| tee** *resource-locator* **]**

Syntax Description

append	Appends redirected output to URL (URLs supporting append operation only).
begin	Begins with the line that matches.
count	Counts number of lines which match regexp.
exclude	Excludes lines that match.
format	Formats the output using the specified spec file.
include	Includes lines that match.

redirect	Redirects output to URL.
section	Filters a section of output.
tee	Copies output to URL.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

Example

The following sample output displays the IP routing table associated with RIP:

```
Device# show ip route rip
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
       & - replicated local route overrides by connected

Gateway of last resort is 10.0.5.13 to network 10.10.10.10

R     10.11.0.0/16 [120/1] via 172.16.1.2, 00:00:02, GigabitEthernet1
```

show ip route vrf

To display the IP routing table associated with a specific VPN routing and forwarding (VRF) instance, use the **show ip route vrf** command in user EXEC or privileged EXEC mode.

show ip route vrf { *vrf-name* | * } [**connected** | *protocol* [*as-number*] | **list** [*list-number*] | **profile** | **static** | **summary** | [*ip-prefix/ip-address*] [*mask* | **longer-prefixes**] | **repair-paths** | **dhcp** | **supernets-only** | **tag** { *tag-value* | *tag-value-dotted-decimal* [*mask*] }]

Syntax Description

vrf-name or *	Name of the VRF. Use the asterisk (*) wildcard to include all the VRFs.
connected	(Optional) Displays all the connected routes in a VRF.

protocol	(Optional) Routing protocol. To specify a routing protocol, use one of these keywords: **bgp**, **egp**, **eigrp**, **hello**, **igrp**, **isis**, **ospf**, or **rip**.
as-number	(Optional) Autonomous system number.
list *number*	(Optional) Specifies the IP access list to be displayed.
profile	(Optional) Displays the IP routing table profile.
static	(Optional) Displays static routes.
summary	(Optional) Displays a summary of routes.
ip-prefix	(Optional) Network for which routing information is displayed.
ip-address	(Optional) Address for which routing information is displayed.
mask	(Optional) Network mask.
longer-prefixes	(Optional) Displays longer prefix entries.
repair-paths	(Optional) Displays repair paths.
dhcp	(Optional) Displays routes added by the DHCP server.
supernets-only	(Optional) Displays only supernet entries.
tag	(Optional) Displays information about route tags in the VRF table.
tag-value	(Optional) Route tag values as a plain decimals.
tag-value-dotted-decimal	(Optional) Route tag values as a dotted decimals.
mask	(Optional) Route tag wildcard mask.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.
Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	This command was modified. Supports inter-service VPNs route leaking and redistribution.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE show ip route vrf command.

Examples

The following is a sample output from the **show ip route vrf** *vrf-name* command displaying routes under VRF 2 table:

```
Device# show ip route vrf 2
Routing Table: 2
```

```
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
       & - replicated local route overrides by connected

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
S   +    10.10.10.97/32 [1/0] via 10.20.1.2 (1)
C        10.20.2.0/24 is directly connected, GigabitEthernet5
L        10.20.2.1/32 is directly connected, GigabitEthernet5
```

The following is a sample output from the **show ip route vrf** *vrf-name* **rip** command displaying RIP routes under a VRF table:

```
Device# show ip route vrf 1 rip
Routing Table: 1
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
H - NHRP, G - NHRP registered, g - NHRP registration summary
o - ODR, P - periodic downloaded static route, l - LISP
a - application route
+ - replicated route, % - next hop override, p - overrides from PfR
& - replicated local route overrides by connected

Gateway of last resort is not set

10.14.0.0/32 is subnetted, 1 subnets
R 10.14.14.14 [120/1] via 10.20.25.18, 00:00:18, GigabitEthernet5
```

The following is a sample output from the **show ip route vrf** command, displaying the IP routing table associated with a VRF named 1:

```
Device# show ip route vrf 1
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       I - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
       U - per-user static route, o - ODR
       T - traffic engineered route

Gateway of last resort is not set

B    10.0.0.0/8 [200/0] via 10.13.13.13, 00:24:19
C    10.0.0.0/8 is directly connected, GigabitEthernet1/3
B    10.0.0.0/8 [20/0] via 10.0.0.1, 02:10:22
B    10.0.0.0/8 [200/0] via 10.13.13.13, 00:24:20
```

This following is a sample output from the **show ip route vrf** *vrf-name* **rip** command using the **bgp** keyword, displaying BGP entries in the IP routing table associated with a VRF named 1:

```
Device# show ip route vrf 1 bgp
B  10.0.0.0/8 [200/0] via 10.13.13.13, 03:44:14
B  10.0.0.0/8 [20/0] via 10.0.0.1, 03:44:12
B  10.0.0.0/8 [200/0] via 10.13.13.13, 03:43:14
```

The following is a sample output from the **show ip route vrf** command, displaying repair paths in the routing table. The fields in the display are self-explanatory:

```
Device# show ip route vrf test1 repair-paths 192.168.3.0
Routing Table: test1
Routing entry for 192.168.3.0/24
  Known via "bgp 10", distance 20, metric 0
  Tag 100, type external
  Last update from 192.168.1.1 00:49:39 ago
  Routing Descriptor Blocks:
  * 192.168.1.1, from 192.168.1.1, 00:49:39 ago, recursive-via-conn
      Route metric is 0, traffic share count is 1
      AS Hops 1
      Route tag 100
      MPLS label: none
    [RPR]10.4.4.4 (default), from 10.5.5.5, 00:49:39 ago, recursive-via-host
      Route metric is 0, traffic share count is 1
      AS Hops 1
      Route tag 100
      MPLS label: 29
MPLS Flags: MPLS Required, No Global
```

Using wildcard for VRF name

This example uses the asterisk (*) wildcard for *vrf-name*, with the **summary** keyword. All the VRFs are included, in this case, **default**, **blue**, and **red**.

```
Device# show ip route vrf * summary
IP routing table name is default (0x0)
IP routing table maximum-paths is 32
Route Source    Networks    Subnets     Replicates  Overhead    Memory (bytes)
application     0           0           0           0           0
connected       0           2           0           192         624
static          1           1           0           192         624
internal        1                                               672
Total           2           3           0           384         1920

IP routing table name is blue (0x2)
IP routing table maximum-paths is 32
Route Source    Networks    Subnets     Replicates  Overhead    Memory (bytes)
application     0           0           0           0           0
connected       0           0           0           0           0
static          0           0           0           0           0
internal        0                                               40
Total           0           0           0           0           40

IP routing table name is red (0x5)
IP routing table maximum-paths is 32
Route Source    Networks    Subnets     Replicates  Overhead    Memory (bytes)
application     0           0           0           0           0
connected       0           0           0           0           0
```

```
static          0           0           0           0           0
internal        0                                               40
Total           0           0           0           0           40
```

show ip sla summary

To display summary statistics for IP Service Level Agreements (SLA) operations, use the **show ip sla summary** command in privileged EXEC mode.

show ip sla summary

destination	(Optional) Displays destination-address-based statistics.
destination-ip-address	IP address of the destination device.
destination-hostname	Hostname of the destination device.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.2(3)T	This command was introduced.
Cisco IOS XE Release 3.7S	This command was integrated into Cisco IOS XE Release 3.7S.
15.1(2)SG	This command was integrated into Cisco IOS Release 15.1(2)SG.
Cisco IOS XE Release 3.4SG	This command was integrated into Cisco IOS XE Release 3.4SG.
15.3(2)S	This command was implemented on the Cisco ASR 901 Series Aggregation Services Routers.
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command is supported for Cisco Catalyst SD-WAN.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE show ip sla summary command.

Examples

The following is a sample output from the **show ip sla summary** command:

```
Device# show ip sla summary
IPSLAs Latest Operation Summary
Codes: * active, ^ inactive, ~ pending
All Stats are in milliseconds. Stats with u are in microseconds

ID     Type    Destination  Stats     Return      Last
                                      Code        Run
---------------------------------------------------------------------------------------------
```

```
*53    http     10.1.1.1     RTT=2      OK  35 seconds ago
*54    http     10.1.1.10    RTT=2      OK  1 minute, 35 seconds ago
```

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

Table 26: show ip sla summary command Field Descriptions

Field	Description
ID	IP SLA operations identifier.
Destination	IP address or hostname of the destination device for the listed operation.
Stats	RTT, in milliseconds.

show ipv6 access-list

To display the contents of all current IPv6 access lists, use the **show ipv6 access-list** command in privileged EXEC mode.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.11.1a	This command is supported in Cisco Catalyst SD-WAN

Usage Guidelines

For usage guidelines, see the Cisco IOS XE show ipv6 access-list command.

Example

The following example displays the contents of all current IPv6 access lists.

```
Device#show ipv6 access-list
IPv6 access list seq_1-seq-rule1-v6-acl_
    permit ipv6 object-group source_prefix object-group dest_prefix sequence 11
```

show ipv6 dhcp binding

To display automatic client bindings from the Dynamic Host Configuration Protocol (DHCP) for IPv6 server binding table, use the **show ipv6 dhcp binding** command in user EXEC or privileged EXEC mode

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For more information about this command, see the Cisco IOS XE show ipv6 dhcp binding command.

The following is sample output from the show ipv6 dhcp binding command displays all automatic client bindings from the DHCP for IPv6 server binding table.

DHCPv6 Address Allocation

```
Device# show ipv6 dhcp binding
Client: FE80::250:56FF:FEBD:8261
  DUID: 00030001001EE6DBF500
  Username : unassigned
  VRF : 10
  IA NA: IA ID 0x00080001, T1 10000, T2 16000
    Address: 5001:DB8:1234:42:500C:B3FA:54A7:F63D
            preferred lifetime 20000, valid lifetime 20000
            expires at Oct 26 2021 01:17 PM (19925 seconds)
```

DHCPv6 Prefix Delegation

```
Device# show ipv6 dhcp binding
Client: FE80::250:56FF:FEBD:8261
  DUID: 00030001001EE6DBF500
  Username : unassigned
  VRF : 10
  Interface : GigabitEthernet0/0/3
  IA PD: IA ID 0x00080001, T1 100, T2 160
    Prefix: 2001:BB8:1602::/48
            preferred lifetime 200, valid lifetime 200
            expires at Oct 26 2021 08:01 AM (173 seconds
```

show ipv6 dhcp database

To display the Dynamic Host Configuration Protocol (DHCP) for IPv6 binding database agent information, use the **show ipv6 dhcp database** command in user EXEC or privileged EXEC mode.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

The following is sample output from the show ipv6 dhcp database command.

The following is sample output from the show ipv6 dhcp pool command to DHCP for IPv6 configuration pool information.

```
Device# show ipv6 dhcp database
Database agent bootflash:
  write delay: 300 seconds, transfer timeout: 300 seconds
  last written at Oct 26 2021 08:01 AM, write timer expires in 250 seconds
  last read at never
  successful read times 0
  failed read times 0
  successful write times 2
  failed write times 0
```

show ipv6 dhcp interface

To display Dynamic Host Configuration Protocol (DHCP) for IPv6 interface information, use the **show ipv6 dhcp interface** command in user EXEC or privileged EXEC mode.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For more information about this command, see the Cisco IOS XE show ipv6 dhcp interface command

The following is sample output from the show ipv6 dhcp interface command to display DHCP for IPv6 interface information.

DHCPv6 Address Allocation

```
Device# show ipv6 dhcp interface GigabitEthernet0/0/2
GigabitEthernet0/0/2 is in client mode
  Prefix State is IDLE
  Address State is OPEN
  Renew for address will be sent in 00:01:09
  List of known servers:
    Reachable via address: FE80::250:56FF:FEBD:DBD1
    DUID: 00030001001EBD43F800
    Preference: 0
    Configuration parameters:
      IA NA: IA ID 0x00080001, T1 100, T2 160
        Address: 2010:AB8:0:1:95D1:CFC:F227:23FB/128
                 preferred lifetime 200, valid lifetime 200
                 expires at Oct 26 2021 07:28 AM (170 seconds)
      DNS server: 2001:DB8:3000:3000::42
      Domain name: example.com
      Information refresh time: 0
      Vendor-specific Information options:
          Enterprise-ID: 100
  Prefix Rapid-Commit: disabled
  Address Rapid-Commit: disabled
```

DHCPv6 Prefix Delegation

```
Device# show ipv6 dhcp interface GigabitEthernet0/0/2
GigabitEthernet0/0/2 is in client mode
  Prefix State is OPEN
  Renew will be sent in 00:01:34
  Address State is IDLE
  List of known servers:
    Reachable via address: FE80::250:56FF:FEBD:DBD1
    DUID: 00030001001EBD43F800
    Preference: 0
    Configuration parameters:
      IA PD: IA ID 0x00080001, T1 100, T2 160
        Prefix: 2001:DB8:1202::/48
                 preferred lifetime 200, valid lifetime 200
                 expires at Oct 26 2021 07:30 AM (194 seconds)
      DNS server: 2001:DB8:3000:3000::42
      Domain name: example.com
      Information refresh time: 0
  Prefix name: prefix_from_server
```

```
  Prefix Rapid-Commit: disabled
  Address Rapid-Commit: disabled
```

DHCPv6 with SLAAC

```
Device# show ipv6 dhcp interface GigabitEthernet0/0/2
GigabitEthernet0/0/2 is in client mode
  Prefix State is IDLE (0)
  Information refresh timer expires in 23:59:49
  Address State is IDLE
  List of known servers:
    Reachable via address: FE80::250:56FF:FEBD:DBD1
    DUID: 00030001001EBD43F800
    Preference: 0
    Configuration parameters:
      DNS server: 2001:DB8:3000:3000::42
      Domain name: example.com
      Information refresh time: 0
      Vendor-specific Information options:
          Enterprise-ID: 100
  Prefix Rapid-Commit: disabled
  Address Rapid-Commit: disabled
```

show ipv6 dhcp pool

To display Dynamic Host Configuration Protocol (DHCP) for IPv6 configuration pool information, use the **show ipv6 dhcp pool** command in user EXEC or privileged EXEC mode.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For more information about this command, see the Cisco IOS XE show ipv6 dhcp pool command.

The following is sample output from the show ipv6 dhcp pool command to DHCP for IPv6 configuration pool information.

DHCPv6 Address Allocation

```
Device# show ipv6 dhcp pool
DHCPv6 pool: relay_server
  VRF 10
  Prefix pool: dhcpv6-pool2
  Address allocation prefix: 5001:DB8:1234:42::/64 valid 20000 preferred 20000 (1 in use,
0 conflicts)
               preferred lifetime 200, valid lifetime 200
  DNS server: 2001:BB8:3000:3000::42
  Domain name: relay.com
  Information refresh: 60
  Vendor-specific Information options:
  Enterprise-ID: 10
    suboption 1 address 2001:DB8:1234:42::10
    suboption 2 ascii 'ip phone'
  Active clients: 1
  Pool is configured to include all configuration options in REPLY
```

DHCPv6 Prefix Delegation

```
Device# show ipv6 dhcp pool
DHCPv6 pool: relay_server
  VRF 10
  Prefix pool: dhcpv6-pool2
  Address allocation prefix: 5001:DB8:1234:42::/64 valid 20000 preferred 20000 (0 in use,
0 conflicts)
               preferred lifetime 200, valid lifetime 200
  DNS server: 2001:BB8:3000:3000::42
  Domain name: relay.com
  Information refresh: 60
  Vendor-specific Information options:
  Enterprise-ID: 10
    suboption 1 address 2001:DB8:1234:42::10
    suboption 2 ascii 'ip phone'
  Active clients: 1
  Pool is configured to include all configuration options in REPLY
```

show ipv6 route vrf

To display IPv6 routing table information that is associated with a VPN routing and forwarding (VRF) instance, use the **show ipv6 route vrf** command in privileged EXEC mode.

show ipv6 route vrf *table name/vrf-id*

Syntax Description

table name/vrf-id	Table name or VRF identifier.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.8.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE show ipv6 route vrf command.

The following is a sample output from the **show ipv6 route vrf** command displaying information about the IPv6 routing table that is associated with VRF 1:

```
Device# show ipv6 route vrf 1
IPv6 Routing Table - 1 - 11 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination
       NDr - Redirect, RL - RPL, O - OSPF Intra, OI - OSPF Inter
       OE1 - OSPF ext 1, OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1
       ON2 - OSPF NSSA ext 2, la - LISP alt, lr - LISP site-registrations
       ld - LISP dyn-eid, lA - LISP away, le - LISP extranet-policy
       lp - LISP publications, ls - LISP destinations-summary, a - Application
       m - OMP
R   1100::/64 [120/2]
     via FE80::20C:29FF:FE2E:13FF, GigabitEthernet2
R   2000::/64 [120/2]
     via FE80::20C:29FF:FE51:762F, GigabitEthernet2
R   2001:10::/64 [120/2]
     via FE80::20C:29FF:FE82:D659, GigabitEthernet2
```

```
R   2500::/64 [252/11], tag 44270
     via FE80::20C:29FF:FEE1:5237, GigabitEthernet2
C   2750::/64 [0/0]
     via GigabitEthernet2, directly connected
L   2750::1/128 [0/0]
     via GigabitEthernet2, receive
R   2777::/64 [252/11], tag 44270
     via FE80::20C:29FF:FEE1:5237, GigabitEthernet2
m   2900::/64 [251/0]
     via 192.168.1.5%default
R   3000::/64 [120/2]
     via FE80::20C:29FF:FE2E:13FF, GigabitEthernet2
R   3400::/64 [252/11], tag 44270
     via FE80::20C:29FF:FE51:762F, GigabitEthernet2
L   FF00::/8 [0/0]
     via Null0, receive
```

show key chain

To display authentication key information, use the **showkeychain** command in EXEC mode.

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	This command was introduced.

Usage Guidelines

For more information about this command, see the Cisco IOS XE show key chain

Examples

The following is sample output from the **showkeychain** command:

```
Device# show key chain
Key-chain trees:
    key 1 -- text "chestnut"
        accept lifetime (always valid) - (always valid) [valid now]
        send lifetime (always valid) - (always valid) [valid now]
    key 2 -- text "birch"
        accept lifetime (00:00:00 Dec 5 2020) - (23:59:59 Dec 5 2020)
        send lifetime (06:00:00 Dec 5 2020) - (18:00:00 Dec 5 2020)
```

show lacp

To display Link Aggregation Control Protocol (LACP) channel-group information, use the **show lacp** command in privileged EXEC mode.

show lacp [*channel-group-number* | { **counters** | **internal** | **neighbor** | **sys-id** }]

Syntax Description

channel-group-number	(Optional) Channel group number. The range is 1 to 128.
counters	Displays traffic information.
internal	Displays internal information.

neighbor	Displays neighbor information.
sys-id	Displays the system identifier that is being used by LACP. The system identifier consists of the LACP system priority and the device MAC address.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	This command was introduced.

Usage Guidelines

You can enter any **show lacp** command to display the active channel-group information. To display specific channel information, enter the **show lacp** command with a channel-group number.

If you do not specify a channel group, information for all channel groups appears.

You can enter the channel-group-number to specify a channel group for all keywords except **sys-id**

Examples

The following is a sample output from the **show lacp counters** privileged EXEC command.

```
Device# show lacp counters
LACPDUs Marker Marker Response LACPDUs
Port Sent Recv Sent Recv Sent Recv Pkts Err
---------------------------------------------------------------------
Channel group: 10
Te0/1/0 51 0 0 0 0 0 0
Te0/1/1 60 52 0 0 0 0 0
```

Examples

The following is a sample output from the **show lacp internal** privileged EXEC command.

```
Device# show lacp internal
Flags: S - Device is requesting Slow LACPDUs
F - Device is requesting Fast LACPDUs
A - Device is in Active mode P - Device is in Passive mode

Channel group 10
LACP port Admin Oper Port Port
Port Flags State Priority Key Key Number State
Te0/1/0 SA susp 32768 0xA 0xA 0x41 0x7D
Te0/1/1 SA bndl 32768 0xA 0xA 0x42 0x3D
```

Examples

The following is a sample output from the **show lacp neighbor** privileged EXEC command.

```
Device# show lacp neighbor
Flags: S - Device is requesting Slow LACPDUs
F - Device is requesting Fast LACPDUs
A - Device is in Active mode P - Device is in Passive mode
```

```
Channel group 10 neighbors

LACP port Admin Oper Port Port
Port Flags Priority Dev ID Age key Key Number State
Te0/1/0 SP 0 0000.0000.0000 420125s 0x0 0x0 0x0 0x0
Te0/1/1 SP 32768 3c13.cc93.4100 26s 0x0 0x1 0x4 0x3C
```

Examples

The following is a sample output from the **show lacp sys-id** privileged EXEC command.

```
Device# show lacp sys-id
32765,0002.4b29.3a00
```

show logging cacert

To view the list of all installed certificates on the device along their date of expiry, use the **show logging cacert** command in privileged EXEC mode.

show logging cacert

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.13.1a	This command is supported for Cisco Catalyst SD-WAN.

Examples

The following is a sample output from the **show logging cacert** command that is used to display the list of all installed certificates on the device along their date of expiry. The fields shown in the display are self-explanatory.

```
Device# show logging cacert
INDEX  NAME      VALIDITY
-----------------------------------------
0      cert.pem  Fri Jun 21 20:35:10 2024
```

show logging profile sdwan internal filter

To view messages logged by binary trace for Cisco-SD-WAN-specific processes and process modules, use the **show logging profile sdwan internal filter** command in the privileged EXEC mode. The messages are displayed in chronological order.

show logging profile sdwan internal filter [*filter-string*]

Syntax Description

filter-string	Displays the filter for a specific SD-WAN instance. Range:1 to 65531

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.15.1a	This command was introduced.

Usage Guidelines

Use **show platform hardware qfp active feature bfd datapath sdwan summary** to get the local descriptor value for a session.

Examples

The following sample displays the show output from a logging profile for a device 20008:

```
Device# show logging profile sdwan internal filter string 20008

Logging display requested on 2024/06/18 09:12:56 (UTC) for Hostname: [cedge3], Model:
[C8000V], Version: [17.15.01], SN: [91KQWKQZRMD], MD_SN: [SSI130300YK]

Displaying logs from the last 0 days, 0 hours, 10 minutes, 0 seconds
executing cmd on chassis local ...
Unified Decoder Library Init .. DONE
Found 1 UTF Streams

2024/06/18 09:12:53.690092174 {ftmd_R0-0}{255}: [ftmd-bfd] [24539]: (debug): [LOGID:3] RA
enabled for LD value:20008
2024/06/18 09:12:53.691445109 {ftmd_R0-0}{255}: [ftmd-bfd] [24539]: (debug): [LOGID:11] BFD
 msg for ld(20008) with state (1) update reason (2)
2024/06/18 09:12:53.691505178 {ftmd_R0-0}{255}: [ftmd-bfd] [24539]: (debug): [LOGID:192]
tunnel_public_tloc_msg : ld 20008 tun_rec_index 8 tloc_index 32779 public tloc 0.0.0.0/0
2024/06/18 09:12:53.691549078 {ftmd_R0-0}{255}: [ftmd-bfd] [24539]: (debug): [LOGID:195]
tunnel_public_tloc_msg :  ld 20008 tloc_index 32779 already knows public tloc 0.0.0.0/0
2024/06/18 09:12:53.691550747 {ftmd_R0-0}{255}: [ftmd-ttm] [24539]: (debug): [LOGID:30] BFD
 session gone down
2024/06/18 09:12:53.691562033 {ftmd_R0-0}{255}: [ftmd-bfd] [24539]: (debug): [LOGID:175]
BFD-session TNL 172.16.13.254:12346->192.168.4.37:12346, : Increment the WAN interface
counters by 1
2024/06/18 09:12:53.691584809 {ftmd_R0-0}{255}: [ftmd-umts] [24539]: (debug): [LOGID:64]
free ctxt for probe PERIODIC lc biz-internet period 1800 src 172.16.13.254 dst 192.168.4.37
2024/06/18 09:12:53.691606267 {ftmd_R0-0}{255}: [ftmd-bfd] [24539]: (debug): [LOGID:39]
Sending Link BFD status message to TTM, status DOWN tun_idx 8,
172.16.255.13/biz-internet:172.16.255.17/mpls/IPSEC
2024/06/18 09:12:53.691614231 {ftmd_R0-0}{255}: [vipcommon-msgq] [24539]: (debug): Queued
Message of size 51 to target TTMD
2024/06/18 09:12:53.691698393 {ftmd_R0-0}{255}: [vipcommon-msgq] [24539]: (debug): Sent
Message of size 51 to target TTMD
2024/06/18 09:12:53.692575643 {ftmd_R0-0}{255}: [libjournal] [24539]: (debug): Write-Line
of msg:ttm to  Succeed
2024/06/18 09:12:53.692584386 {ftmd_R0-0}{255}: [ftmd-ttm] [24539]: (debug): [LOGID:77]
Received TLOC add from Caller:[tloc_replay_specific_tloc] , tloc Index: 32779 (tloc ID:
tloc_origin=REMOTE, tloc_id: 172.16.255.17 : mpls : ipsec) Origin REMOTE. Capability 0x3f.
 TLOC attribute: 0X1008012E0FE43A6
2024/06/18 09:12:53.692591033 {ftmd_R0-0}{255}: [ftmd-ttm] [24539]: (debug): [LOGID:38]
System 172.16.255.17, site 17, local 0, on_demand old 1, new 1
```

```
2024/06/18 09:12:53.692600925 {ftmd_R0-0}{255}: [ftmd-ttm] [24539]: (debug): [LOGID:100]
tloc_add  (REMOTE_TLOC)
2024/06/18 09:12:53.692606364 {ftmd_R0-0}{255}: [ftmd-ttm] [24539]: (debug): [LOGID:110]
tloc_index 32771 BFD Address Family is IPV4
2024/06/18 09:12:53.692608238 {ftmd_R0-0}{255}: [ftmd-ttm] [24539]: (debug): [LOGID:53] Not
 MRF Migration in Process, local tloc color: 2, remote tloc color 2, local tloc region id:
 0, remote tloc region id: 65534, remote site id: 17
2024/06/18 09:12:53.692610564 {ftmd_R0-0}{255}: [ftmd-ttm] [24539]: (debug): [LOGID:59]
Local site on_demand: True, Remote site 17, on_demand: False, Active
2024/06/18 09:12:53.692617126 {ftmd_R0-0}{255}: [ftmd-bfd] [24539]: (debug): [LOGID:42]
ftm-binos_bfd_sess_add : ENTER
2024/06/18 09:12:53.692622639 {ftmd_R0-0}{255}: [ftmd-bfd] [24539]: (debug): [LOGID:41] FTM
 create BFD internal pak - dst pvt: 192.168.4.37:12346
2024/06/18 09:12:53.692623822 {ftmd_R0-0}{255}: [ftmd-bfd] [24539]: (debug): [LOGID:46]
ftm-binos_bfd_sess_add : init symnat with  ZEROs
2024/06/18 09:12:53.692626824 {ftmd_R0-0}{255}: [ftmd-bfd] [24539]: (debug): [LOGID:47] BFD
 TLV attributes: Encap: 1, My_pub_ip:192.168.4.33, My_pub_port:12346, Remote_ip: 192.168.4.37,
 Remote_port: 12346, Max tunnel MTU: 0, capabilities: 0, Ipsec Overhead: 38
2024/06/18 09:12:53.692628621 {ftmd_R0-0}{255}: [ftmd-bfd] [24539]: (debug): [LOGID:48] Got
 session record color:2, local_color:2
2024/06/18 09:12:53.692630040 {ftmd_R0-0}{255}: [ftmd-bfd] [24539]: (debug): [LOGID:50] BFD
 Add Message FTM->FMAN-RP parameters Hello interval: 1000, Local Discriminator: 20007, Local
 color: 2, if_number: 7, session_type:IPV4, detect multiplier:7 max_tunnel_mtu:1442 BFD
State: UP, adj_id: 0xf810006f, capabilities: 352, ipsec_overhead: 38, poll interval: 600000,
 sdwan_bfd_flags: 0x1 my_pub_ip/port:192.168.4.33/12346 my_symnat_pub_ip/port:0.0.0.0/0
remote_ip/port:192.168.4.37/12346
2024/06/18 09:12:53.692654059 {ftmd_R0-0}{255}: [libjournal] [24539]: (debug): Write-Line
of msg:fman-rp to  Succeed
2024/06/18 09:12:53.694167194 {ftmd_R0-0}{255}: [ftmd-binos] [24539]: (debug): [LOGID:4]
send BINOS protobuf message(size=181)
2024/06/18 09:12:53.694169543 {ftmd_R0-0}{255}: [ftmd-bfd] [24539]: (debug): [LOGID:51]
ftm-binos_bfd_sess_add : EXIT
2024/06/18 09:12:53.694173216 {ftmd_R0-0}{255}: [ftmd-ttm] [24539]: (debug): [LOGID:118]
BFD session created for TLOC:32779:32771 is_up=UP is_suspended=No,  p_session:0x7627d2b9d960
2024/06/18 09:12:53.694177030 {ftmd_R0-0}{255}: [ftmd-ttm] [24539]: (debug): [LOGID:120]
attr_flag 31 downstream min 0,default 0 max 0, period 0 up 0
2024/06/18 09:12:53.694179927 {ftmd_R0-0}{255}: [ftmd-ttm] [24539]: (debug): [LOGID:110]
tloc_index 32770 BFD Address Family is IPV4
```

show macsec hw detail

To display detailed hardware-related information about MACsec on a Cisco IOS XE Catalyst SD-WAN device, use the **show macsec hw detail** command in privileged EXEC mode.

show macsec hw detail

Syntax Description

This command has no keywords or arguments.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.12.1a	This command is supported for Cisco Catalyst SD-WAN.

Examples

This is sample output of the **show macsec hw detail** command.

```
Device# show macsec hw detail
MACsec Capable Interface         RxSA Inuse
-------------------------------------------
 TenGigabitEthernet0/0/5       :        1


Other Debug Statistics
Interface TenGigabitEthernet0/0/5 HMAC:
RxOctets              0  RxUcastPkts           0  RxMcastPkts           0
RxBcastPkts           0  RxDiscards            0  RxErrors              0
TxOctets              0  TxUcastPkts           0  TxMcastPkts           0
TxBcastPkts           0  TxErrors              0
LMAC:
RxOctets           5595  RxUcastPkts          22  RxMcastPkts           9
RxBcastPkts           0  RxDiscards            0  RxErrors              0
TxOctets           1710  TxUcastPkts          15  TxMcastPkts           0
TxBcastPkts           0  TxErrors              0
```

show macsec mka-request-notify

To view information about MACsec (Media Access Control Security) enabled interfaces, including the counts of control plane transmit and delete secure channels, transmit security associations, receive secure channels, and delete security associations, as well as the MKA (MACsec Key Agreement) notification count on the interface **TenGigabitEthernet0/0/5**, use the **show macsec mka-request-notify** command in privileged EXEC mode.

show macsec mka-request-notify

Syntax Description

This command has no keywords or arguments.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.12.1a	This command is supported for Cisco Catalyst SD-WAN.

Examples

This is sample output of the **show macsec mka-request-notify** command.

```
Device# show macsec mka-request-notify
MACsec Enabled Interface         CR_TX_SC  DEL_TX_SC  INST_TX_SA  CR_RX_SC  DEL_RX_SC
INST_RX_SA  DEL_RX_SA  MKA_NOTIFY
-------------------------------------------------------------------------------------------
 TenGigabitEthernet0/0/5       :       18        17        18        18         0
18          11         0
```

show macsec summary

To display a summary of MACsec information on the device, including MACsec capable interfaces, installed secure channels, and MACsec enabled interfaces with their associated receive secure channels and VLAN, use the **show macsec summary** command in privileged EXEC mode.

show macsec summary

Syntax Description This command has no keywords or arguments.

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.12.1a	This command is supported for Cisco Catalyst SD-WAN.

Examples This is sample output of the **show macsec summary** command.

```
Device# show macsec summary
MACsec Capable Interface                Extension              Installed Rx SC
-------------------------------------------------------------------------------
 TenGigabitEthernet0/0/0                 One tag-in-clear
 TenGigabitEthernet0/0/1                 One tag-in-clear
 TenGigabitEthernet0/0/2                 One tag-in-clear
 TenGigabitEthernet0/0/3                 One tag-in-clear
 TenGigabitEthernet0/0/4                 One tag-in-clear
 TenGigabitEthernet0/0/5                 One tag-in-clear                1
 TenGigabitEthernet0/0/6                 One tag-in-clear
 TenGigabitEthernet0/0/7                 One tag-in-clear
 TenGigabitEthernet0/1/0                 One tag-in-clear
 TenGigabitEthernet0/1/1                 One tag-in-clear
 TenGigabitEthernet0/1/2                 One tag-in-clear
 TenGigabitEthernet0/1/3                 One tag-in-clear
 FortyGigabitEthernet0/2/0               One tag-in-clear
 FortyGigabitEthernet0/2/4               One tag-in-clear
 FortyGigabitEthernet0/2/8               One tag-in-clear
 GigabitEthernet0                        One tag-in-clear
 SDWAN System Intf IDB                   One tag-in-clear
 SDWAN vmanage_system IDB                One tag-in-clear
 LIIN0                                   One tag-in-clear
 LI-Null0                                One tag-in-clear
 Loopback65528                           One tag-in-clear
 Loopback65529                           One tag-in-clear
 SR0                                     One tag-in-clear
 Tunnel1                                 One tag-in-clear
 VoIP-Null0                              One tag-in-clear

 MACsec Enabled Interface         Receive SC   VLAN
-----------------------------------------------------
 TenGigabitEthernet0/0/5       :        1         0
```

show macsec status interface

To display the MACsec configuration and status of an interface, use the **show macsec status interface** command in privileged EXEC mode.

show macsec status interface

Syntax Description This command has no keywords or arguments.

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.12.1a	This command is supported for Cisco Catalyst SD-WAN.

Examples

This is sample output of the **show macsec status interface** command.

```
Device# show macsec status interface TenGigabitEthernet 0/0/5
Capabilities:
  Ciphers Supported:        GCM-AES-128 GCM-AES-256 GCM-AES-XPN-128 GCM-AES-XPN-256
  Cipher:                   GCM-AES-128
  Confidentiality Offset:   0
  Replay Window:            64
  Delay Protect Enable:     FALSE
  Access Control:           must-secure
  Include-SCI:              TRUE

 Transmit SC:
  SCI:                      E8D322D32085000D
  Transmitting:             TRUE
 Transmit SA:
  Next PN:                  10002
  Delay Protect AN/nextPN:  NA/0

 Receive SC:
  SCI:                      A03D6E5D037F0045
  Receiving:                TRUE
 Receive SA:
  Next PN:                  10077
  AN:                       1
  Delay Protect AN/LPN:     0/0
```

show mka default-policy

To display information about the MACsec Key Agreement (MKA) Protocol default policy, use the **show mka default-policy** command in privileged EXEC mode.

show mka default-policy [{ **sessions detail** } | **session detail**]

Syntax Description

sessions	(Optional) Displays a summary of active MKA sessions that have the default policy applied.
Detail	(Optional) Displays detailed configuration information for the default policy and the interface names to which the default policy is applied, or displays detailed status information about all active MKA sessions that have the default policy applied.

Syntax Description

This command has no keywords or arguments.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.12.1a	This command is supported for Cisco Catalyst SD-WAN.

Examples

This is sample output of the **show mka default-policy detail** command:

```
Device# show mka default-policy detail
MKA Policy Configuration ("*DEFAULT POLICY*")
=========================
MKA Policy Name...........*DEFAULT POLICY*
Key Server Priority.......0
Confidentiality Offset....0
Delay Protect.............FALSE
SAK-Rekey On-Peer-Loss....0
SAK-Rekey Interval........0
Send Secure Announcement..DISABLED
Include ICV Indicator.....TRUE
SCI Based SSCI............FALSE
Use Updated Ethernet Hdr..NO
Cipher Suite(s)......... GCM-AES-128
                         GCM-AES-256

Applied Interfaces...
```

Examples

The following is a sample output from the **show mka default-policy sessions** command.

```
Device# show mka default-policy sessions
Summary of All Active MKA Sessions with MKA Policy "*DEFAULT POLICY*"...

=============================================================================================================
Interface       Local-TxSCI          Policy-Name       Inherited          Key-Server

Port-ID         Peer-RxSCI           MACsec-Peers      Status             CKN

=============================================================================================================
Te0/0/5         e8d3.22d3.2085/000d  *DEFAULT POLICY*  NO                 NO

13              a03d.6e5d.037f/0045  1                 Secured            10
```

The following is a sample output from the **show mka default-policy sessions detail** command.

```
Device# show mka default-policy sessions detail

MKA Detailed Status for MKA Session
===================================
Status: SECURED - Secured MKA Session with MACsec

Local Tx-SCI.............. e8d3.22d3.2085/000d
Interface MAC Address.... e8d3.22d3.2085
MKA Port Identifier...... 13
Interface Name........... TenGigabitEthernet0/0/5
Audit Session ID.........
CAK Name (CKN)........... 10
Member Identifier (MI)... DE832E171DCC70441E997F96
Message Number (MN)...... 80
EAP Role................. NA
Key Server............... NO
MKA Cipher Suite......... AES-256-CMAC

Latest SAK Status........ Rx & Tx
Latest SAK AN............ 1
Latest SAK KI (KN)....... 811368FD2F9F9CC82C1894C800000012 (18)
Old SAK Status........... No Rx, No Tx
Old SAK AN............... 0
Old SAK KI (KN).......... RETIRED (0)
```

```
SAK Transmit Wait Time... 0s (Not waiting for any peers to respond)
SAK Retire Time.......... 0s (No Old SAK to retire)
SAK Rekey Time........... 0s (SAK Rekey interval not applicable)

MKA Policy Name.......... *DEFAULT POLICY*
Key Server Priority...... 0
Delay Protection......... NO
Delay Protection Timer.......... 0s (Not enabled)

Confidentiality Offset... 0
Algorithm Agility........ 80C201
SAK Rekey On Live Peer Loss........ NO
Send Secure Announcement.. DISABLED
SCI Based SSCI Computation.... NO
SAK Cipher Suite......... 0080C20001000001 (GCM-AES-128)
MACsec Capability........ 3 (MACsec Integrity, Confidentiality, & Offset)
MACsec Desired........... YES

# of MACsec Capable Live Peers............ 1
# of MACsec Capable Live Peers Responded.. 0

Live Peers List:
  MI                        MN          Rx-SCI (Peer)        KS        RxSA          SSCI
                                                             Priority  Installed
  ----------------------------------------------------------------------------------------
  811368FD2F9F9CC82C1894C8  379101      a03d.6e5d.037f/0045  0         YES            0

Potential Peers List:
  MI                        MN          Rx-SCI (Peer)        KS        RxSA          SSCI
                                                             Priority  Installed
  ----------------------------------------------------------------------------------------

Dormant Peers List:
  MI                        MN          Rx-SCI (Peer)        KS        RxSA          SSCI
                                                             Priority  Installed
  ----------------------------------------------------------------------------------------


MKA Detailed Status for MKA Session
===================================
Status: INITIALIZING - Searching for Peer (Waiting to receive first Peer MKPDU)

Local Tx-SCI............. e8d3.22d3.2085/000d
Interface MAC Address.... e8d3.22d3.2085
MKA Port Identifier...... 13
Interface Name........... TenGigabitEthernet0/0/5
Audit Session ID.........
CAK Name (CKN)........... 11
Member Identifier (MI)... 6758F1CA5F050202DC742B03
Message Number (MN)...... 79
EAP Role................. NA
Key Server............... YES
MKA Cipher Suite......... AES-256-CMAC

Latest SAK Status........ Rx & Tx
Latest SAK AN............ 1
Latest SAK KI (KN)....... 811368FD2F9F9CC82C1894C800000012 (18)
Old SAK Status........... No Rx, No Tx
Old SAK AN............... 0
Old SAK KI (KN).......... RETIRED (0)

SAK Transmit Wait Time... 0s (Not waiting for any peers to respond)
SAK Retire Time.......... 0s (No Old SAK to retire)
```

```
SAK Rekey Time.......... 0s (SAK Rekey interval not applicable)

MKA Policy Name.......... *DEFAULT POLICY*
Key Server Priority...... 0
Delay Protection......... NO
Delay Protection Timer.......... 0s (Not enabled)

Confidentiality Offset... 0
Algorithm Agility........ 80C201
SAK Rekey On Live Peer Loss........ NO
Send Secure Announcement.. DISABLED
SCI Based SSCI Computation.... NO
SAK Cipher Suite......... 0080C20001000001 (GCM-AES-128)
MACsec Capability........ 3 (MACsec Integrity, Confidentiality, & Offset)
MACsec Desired........... YES

# of MACsec Capable Live Peers............ 0
# of MACsec Capable Live Peers Responded.. 0

Live Peers List:
  MI                        MN          Rx-SCI (Peer)        KS        RxSA          SSCI
                                                             Priority  Installed
  ----------------------------------------------------------------------------------------

Potential Peers List:
  MI                        MN          Rx-SCI (Peer)        KS        RxSA          SSCI
                                                             Priority  Installed
  ----------------------------------------------------------------------------------------

Dormant Peers List:
  MI                        MN          Rx-SCI (Peer)        KS        RxSA          SSCI
                                                             Priority  Installed
  ----------------------------------------------------------------------------------------
```

show mka keychains

To display the list of MACsec keychains configured on a Cisco IOS XE Catalyst SD-WAN device, use the **show mka keychains** command in privileged EXEC mode.

show mka keychains

Syntax Description

This command has no keywords or arguments.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.12.1a	This command is supported for Cisco Catalyst SD-WAN.

Examples

This is sample output of the **show mka keychains** command.

```
Device# show mka keychains

MKA PSK Keychain(s) Summary...

Keychain        Latest CKN                                                  Interface(s)
```

```
Name             Latest CAK                                                                    Applied

=============================================================================================================
mka-keychain128  10                                                                           Te0/0/5

                 <HIDDEN>
```

show mka policy

To display the MACsec policies configured on a Cisco IOS XE Catalyst SD-WAN device, use the **show mka default-policy** command in privileged EXEC mode.

show mka default-policy

Syntax Description This command has no keywords or arguments.

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.12.1a	This command is supported for Cisco Catalyst SD-WAN.

Examples This is sample output of the **show mka default-policy** command:

```
Device# show mka policy MKA-128
MKA Policy Summary...

Codes : CO - Confidentiality Offset, ICVIND - Include ICV-Indicator,
        SAKR OLPL - SAK-Rekey On-Live-Peer-Loss,
        DP - Delay Protect, KS Prio - Key Server Priority

Policy            KS   DP    CO SAKR  ICVIND Cipher          Interfaces
Name              Prio          OLPL         Suite(s)        Applied
============================================================================
MKA-128           0    FALSE 0  FALSE TRUE   GCM-AES-128     Te0/0/5
```

show mka sessions

To display the active MACsec sessions on a Cisco IOS XE Catalyst SD-WAN device, use the **show mka sessions** command in privileged EXEC mode.

show mka sessions

Syntax Description This command has no keywords or arguments.

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.12.1a	This command is supported for Cisco Catalyst SD-WAN.

Examples

This is sample output of the **show mka sessions** command.

```
Device# show mka sessions
Total MKA Sessions....... 1
      Secured Sessions... 1
      Pending Sessions... 0

=============================================================================================================
Interface       Local-TxSCI          Policy-Name       Inherited          Key-Server

Port-ID         Peer-RxSCI           MACsec-Peers      Status             CKN

=============================================================================================================
Te0/0/5         e8d3.22d3.2085/000d  MKA-128           NO                 NO

13              a03d.6e5d.037f/0045  1                 Secured            10
```

The following is a sample output from the **show mka sessions detail** command.

```
Device# show mka sessions detail
MKA Detailed Status for MKA Session
===================================
Status: SECURED - Secured MKA Session with MACsec

Local Tx-SCI.............. e8d3.22d3.2085/000d
Interface MAC Address.... e8d3.22d3.2085
MKA Port Identifier...... 13
Interface Name........... TenGigabitEthernet0/0/5
Audit Session ID.........
CAK Name (CKN)........... 10
Member Identifier (MI)... DE832E171DCC70441E997F96
Message Number (MN)...... 134
EAP Role................. NA
Key Server............... NO
MKA Cipher Suite......... AES-256-CMAC

Latest SAK Status........ Rx & Tx
Latest SAK AN............ 1
Latest SAK KI (KN)....... 811368FD2F9F9CC82C1894C800000012 (18)
Old SAK Status........... No Rx, No Tx
Old SAK AN............... 0
Old SAK KI (KN).......... RETIRED (0)

SAK Transmit Wait Time... 0s (Not waiting for any peers to respond)
SAK Retire Time.......... 0s (No Old SAK to retire)
SAK Rekey Time........... 0s (SAK Rekey interval not applicable)

MKA Policy Name.......... MKA-128
Key Server Priority...... 0
Delay Protection......... NO
Delay Protection Timer.......... 0s (Not enabled)

Confidentiality Offset... 0
Algorithm Agility........ 80C201
SAK Rekey On Live Peer Loss........ NO
Send Secure Announcement.. DISABLED
SCI Based SSCI Computation.... NO
SAK Cipher Suite......... 0080C20001000001 (GCM-AES-128)
MACsec Capability........ 3 (MACsec Integrity, Confidentiality, & Offset)
MACsec Desired........... YES

# of MACsec Capable Live Peers............ 1
# of MACsec Capable Live Peers Responded.. 0
```

```
Live Peers List:
  MI                        MN          Rx-SCI (Peer)        KS        RxSA          SSCI
                                                             Priority  Installed
  ------------------------------------------------------------------------------------------
  811368FD2F9F9CC82C1894C8  379154      a03d.6e5d.037f/0045  0         YES            0

Potential Peers List:
  MI                        MN          Rx-SCI (Peer)        KS        RxSA          SSCI
                                                             Priority  Installed
  ------------------------------------------------------------------------------------------

Dormant Peers List:
  MI                        MN          Rx-SCI (Peer)        KS        RxSA          SSCI
                                                             Priority  Installed
  ------------------------------------------------------------------------------------------


MKA Detailed Status for MKA Session
===================================
Status: INITIALIZING - Searching for Peer (Waiting to receive first Peer MKPDU)

Local Tx-SCI.............. e8d3.22d3.2085/000d
Interface MAC Address.... e8d3.22d3.2085
MKA Port Identifier...... 13
Interface Name........... TenGigabitEthernet0/0/5
Audit Session ID.........
CAK Name (CKN)........... 11
Member Identifier (MI)... 6758F1CA5F050202DC742B03
Message Number (MN)...... 133
EAP Role................. NA
Key Server............... YES
MKA Cipher Suite......... AES-256-CMAC

Latest SAK Status........ Rx & Tx
Latest SAK AN............ 1
Latest SAK KI (KN)....... 811368FD2F9F9CC82C1894C800000012 (18)
Old SAK Status........... No Rx, No Tx
Old SAK AN............... 0
Old SAK KI (KN).......... RETIRED (0)

SAK Transmit Wait Time... 0s (Not waiting for any peers to respond)
SAK Retire Time.......... 0s (No Old SAK to retire)
SAK Rekey Time........... 0s (SAK Rekey interval not applicable)

MKA Policy Name.......... MKA-128
Key Server Priority...... 0
Delay Protection......... NO
Delay Protection Timer.......... 0s (Not enabled)

Confidentiality Offset... 0
Algorithm Agility........ 80C201
SAK Rekey On Live Peer Loss........ NO
Send Secure Announcement.. DISABLED
SCI Based SSCI Computation.... NO
SAK Cipher Suite......... 0080C20001000001 (GCM-AES-128)
MACsec Capability........ 3 (MACsec Integrity, Confidentiality, & Offset)
MACsec Desired........... YES

# of MACsec Capable Live Peers............ 0
# of MACsec Capable Live Peers Responded.. 0

Live Peers List:
  MI                        MN          Rx-SCI (Peer)        KS        RxSA          SSCI
                                                             Priority  Installed
```

```
  ------------------------------------------------------------------------------------

Potential Peers List:
  MI                      MN          Rx-SCI (Peer)        KS        RxSA          SSCI
                                                           Priority  Installed
  ------------------------------------------------------------------------------------

Dormant Peers List:
  MI                      MN          Rx-SCI (Peer)        KS        RxSA          SSCI
                                                           Priority  Installed
  ------------------------------------------------------------------------------------
```

show mka statistics

To display MACsec statistics on a Cisco IOS XE Catalyst SD-WAN device, use the **show mka statistics** command in privileged EXEC mode.

show mka statistics

Syntax Description

This command has no keywords or arguments.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.12.1a	This command is supported for Cisco Catalyst SD-WAN.

Examples

This is sample output of the **show mka statistics** command.

```
Device# show mka statistics interface TenGigabitEthernet 0/0/5
MKA Statistics for Session
==========================
Reauthentication Attempts.. 0

CA Statistics
   Pairwise CAKs Derived... 0
   Pairwise CAK Rekeys..... 0
   Group CAKs Generated.... 0
   Group CAKs Received..... 0

SA Statistics
   SAKs Generated.............. 0
   SAKs Rekeyed................ 0
   SAKs Received............... 1
   SAK Responses Received...... 0
   SAK Rekeyed as KN Mismatch.. 0

MKPDU Statistics
   MKPDUs Validated & Rx... 229
      "Distributed SAK".. 1
      "Distributed CAK".. 0
   MKPDUs Transmitted...... 231
      "Distributed SAK".. 0
      "Distributed CAK".. 0
```

show mka summary

To display MACsec statistics on a Cisco IOS XE Catalyst SD-WAN device, use the **show mka summary** command in privileged EXEC mode.

show mka summary

Syntax Description

This command has no keywords or arguments.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.12.1a	This command is supported for Cisco Catalyst SD-WAN.

Examples

This is sample output of the **show mka summary** command.

```
Device# show mka summary
Total MKA Sessions....... 1
      Secured Sessions... 1
      Pending Sessions... 0

=============================================================================================
Interface       Local-TxSCI          Policy-Name       Inherited          Key-Server

Port-ID         Peer-RxSCI           MACsec-Peers      Status             CKN

=============================================================================================
Te0/0/5         e8d3.22d3.2085/000d  MKA-128           NO                 NO

13              a03d.6e5d.037f/0045  1                 Secured            10



MKA Global Statistics
=====================
MKA Session Totals
   Secured..................... 18
   Fallback Secured........... 0
   Reauthentication Attempts.. 0

   Deleted (Secured).......... 17
   Keepalive Timeouts......... 0

CA Statistics
   Pairwise CAKs Derived...... 0
   Pairwise CAK Rekeys........ 0
   Group CAKs Generated....... 0
   Group CAKs Received........ 0

SA Statistics
   SAKs Generated.............. 0
   SAKs Rekeyed................ 0
   SAKs Received............... 18
   SAK Responses Received...... 0
   SAK Rekeyed as KN Mismatch.. 0
```

```
MKPDU Statistics
   MKPDUs Validated & Rx...... 374465
      "Distributed SAK"..... 18
      "Distributed CAK"..... 0
   MKPDUs Transmitted......... 384191
      "Distributed SAK"..... 0
      "Distributed CAK"..... 0

MKA Error Counter Totals
========================
Session Failures
   Bring-up Failures................ 0
   Reauthentication Failures........ 0
   Duplicate Auth-Mgr Handle........ 0

SAK Failures
   SAK Generation................... 0
   Hash Key Generation.............. 0
   SAK Encryption/Wrap.............. 0
   SAK Decryption/Unwrap............ 0
   SAK Cipher Mismatch.............. 0

CA Failures
   Group CAK Generation............. 0
   Group CAK Encryption/Wrap........ 0
   Group CAK Decryption/Unwrap...... 0
   Pairwise CAK Derivation.......... 0
   CKN Derivation................... 0
   ICK Derivation................... 0
   KEK Derivation................... 0
   Invalid Peer MACsec Capability... 0

MACsec Failures
   Rx SC Creation................... 0
   Tx SC Creation................... 0
   Rx SA Installation............... 0
   Tx SA Installation............... 0

MKPDU Failures
   MKPDU Tx............................... 0
   MKPDU Rx ICV Verification.............. 0
   MKPDU Rx Fallback ICV Verification..... 0
   MKPDU Rx Validation.................... 0
   MKPDU Rx Bad Peer MN................... 0
   MKPDU Rx Non-recent Peerlist MN........ 0
SAK USE Failures
   SAK USE Latest KN Mismatch............. 0
   SAK USE Latest AN not in USE........... 0
```

show nat66 dia route

To show the NAT66 DIA route status information and to determine the number of NAT66 DIA-enabled routes, use the **show nat66 dia route** command in privileged EXEC mode.

show nat66 dia route

Syntax Description

This command has no arguments or keywords.

Command Default No NAT66 DIA route status information is displayed.

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Examples The following is a sample output from the **show nat66 dia route** command:

```
Device# show nat66 route-dia
Total interface NAT66 DIA enabled count [1]
route add [1] addr [2001:DB8:A14:19::] vrfid [2] prefix len [64]
route add [1] addr [2001:DB8:3D0:1::] vrfid [2] prefix len [64]
```

show nat64 map-e

To view information about the Network Address Translation (NAT64) Mapping of Address and Port Using Encapsulation (MAP-E) domain and associated parameters, use the **show nat64 map-e** command in privileged EXEC mode.

show nat64 map-e

Syntax Description This command has no arguments or keywords.

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	This command was introduced.

Examples The following is an example output for the **show nat64 map-e** command:

```
Device# show nat64 map-e
MAP-E Domain 9126
   Mode MAP
   Border-relay-address
      Ip-v6-address 2001:DB8::9
   Basic-mapping-rule
      Ip-v6-prefix 2001:DB8:A110::/48
      Ip-v4-prefix 10.1.1.0/24
      Port-parameters
         Share-ratio 16   Contiguous-ports 64   Start-port 1024
         Share-ratio-bits 4   Contiguous-ports-bits 6   Port-offset-bits 6
      Port-set-id 1
```

The output above shows the MAP-E domain and the associated parameters.

For more information on MAP-E with NAT64, see the *Cisco SD-WAN NAT Configuration Guide*.

Related Commands

Commands	Description
nt64 provisioning	Configure the MAP-E domain and parameters for NAT64.

show nat66 nd

To display the NAT66 discovery neighbors table, use the **show nat66 nd** command in privileged EXEC mode.

show nat66 nd

Syntax Description This command has no arguments or keywords.

Command Default No NAT66 discovery neighbors table is displayed.

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Examples The following is a sample output from the **show nat66 nd** command:

```
Device# show nat66 nd
NAT66 Neighbor Discovery

ND prefix DB:
  2001:DB8:A1:F::/80
  2001:DB8:A1:F:0:1::/80
  2001:DB8:A1:F:1::/64
  2001:DB8:A1:F:2::/64
  2001:DB8:A1:F:3::/64

ipv6 ND entries:
  2001:DB8:A1:F::F
  2001:DB8:A1:F::11
```

show nat66 prefix

To show the status of the NAT66 prefix configuration and to display the NAT66 configured prefixes, use the **show nat66 prefix** command in privileged EXEC mode.

show nat66 prefix

Syntax Description This command has no arguments or keywords.

Command Default No IPv6 configured prefixes are displayed.

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Examples The following is a sample output from the **show nat66 prefix** command, and shows the NAT66 prefixes that were configured:

```
Device# show nat66 prefix
Prefixes configured: 1
NAT66 Prefixes
Id: 1 Inside 2001:DB8:AB01::/64 Outside 2001:DB8:AB02::/64
```

show nat66 statistics

To verify the NAT66 interface and global configuration, use the **show nat66 statistics** command in privileged EXEC mode.

show nat66 statistics

Syntax Description This command has no arguments or keywords.

Command Default No NAT66 interface and global configuration statistics are displayed.

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command is supported for Cisco Catalyst SD-WAN.

Examples The following is a sample output from the **show nat66 statistics** command and shows the packet headers that were translated.

```
Device# show nat66 statistics
NAT66 Statistics

Global Stats:
   Packets translated (In -> Out)
      : 7
   Packets translated (Out -> In)
      : 7
```

show object-group

To display object group configuration, use the **show object-group** command in privileged EXEC mode.

show object-group name *object-group-name*

Syntax Description

name *object-group-name*	(Optional) Displays information for a specific object group.

Command Default

Information for all the object groups is displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

Use the **show object-group** command to display configurations for all object groups or just for a specific object group.

Examples

The following is example output from the **show object-group** command:

```
Device# show object-group name Zone1_to_Zone1-seq-Rule_1-geo-dstn-og_
GEO object group Zone1_to_Zone1-seq-Rule_1-geo-dstn-og_
country FRA
```

show policy-firewall session platform detail

To display display detailed information about firewall sessions on a Cisco IOS XE Catalyst SD-WAN device, particularly when high availability is involved, use the **show policy-firewall session platform detail** command in privileged EXEC mode.

show policy-firewall session platform detail

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.15.1a	This command is supported for Cisco Catalyst SD-WAN.

Usage Guidelines

Use the **show policy-firewall session platform detail** to display detailed information about firewall sessions on the platform, particularly when high availability is involved. This command is used to gather comprehensive data about active firewall sessions, including session states, counters, and other important metrics.

Examples

The following is sample output from the **show policy-firewall session platform detail** command.

```
Device# show policy-firewall session platform detail
[s=session i=imprecise channel c=control channel d=data channel u=utd inspect A/D=appfw
action allow/deny]
Session ID:0x100000B7 192.168.11.10 34157 10.0.12.131 80 proto 6 (1:1:1:1) (3:0x3000050:http)
 [sc]
pscb : 0x156da640, key1_flags: 0x00000000
bucket : 34590, prev 0x0, next 0x0 fw_flags: 0x01800000 0x20c06a21,
Flattened-AVC HA-AVC
Root Protocol-TCP Initiator Alert Proto-State:Timewait Session-db HA-create Max-session
icmp_error count 0 ureachable arrived: no
```

```
scb state: active, nxt_timeout: 100, refcnt: 1 NBAR verdict count 0
ha nak cnt: 0, rg: 1
hostdb: 0x0, L7: 0x0, stats: 0x160ebfc0, child: 0x0
isn: 1826966309 last ack: 987459709 next seq: 1826966394 wnd_size: 2169783926
wnd_scale: 29200
isn: 987459708 last ack: 987459708 next ack: 987459708 wnd_size: 2169783926
wnd_scale: 65535
tcp flags: 0x00000000 : : proto: 0018: l7 ooo drop 0x010 l7_prot 0x12 - http
root scb: 0x0 act_blk: 0x160e3f00
ingress/egress intf: GigabitEthernet3.101 (65530), GigabitEthernet1 (65530)
current time 284036397554511 create tstamp: 283915721110241 last access: 284035994128283
now 284036397556361 csec left
nat_out_local_addr:port: 10.0.12.131:80
nat_in_global_addr:port: ********************
ip6: addr1 :: addr2 ::
key ip4: addr1 10.0.12.131:80 addr2 192.168.11.10:34157
syncookie fixup: 0x0, halfopen linkage: 0x0 0x0
cxsc_cft_fid: 0x00000000
tw timer: 0x00000000 0x00000000 0x00000000 0x14f53101
domain_ab1 0x0 l4 per filter stats 0x0 avc class id 0x3 http SGT: 0 DGT: 0
NAT handles 0x11194110 0x00000000
FlowDB in2out 0x00000000 alloc_epoch 0 out2in 0x00000000 alloc_epoch 0 ppe tid 0
icmp_err_time 0 utd_context_id 0, classification epoch scb: 0x1 actblk :0x1 avc class stats
 0x0
VPN id src 1, dst 0
zone pair ZP_ZONE_1_untrusted_ZON_47132514 class
ZONE_1_TO_UNTRUSTED-seq-SEQUENCE-829881385-cm_
```

show performance monitor cache

To view performance monitor cache details, use the **show performance monitor cache** command in privileged EXEC mode.

show performance monitor cache [**detail** | **format** { **csv** | **table** | **record** }]

show performance monitor cache [**monitor** *monitor-name*]

Syntax Description

detail	(Optional) Displays detailed cache information.
format	Displays cache information in one of the formats specified: • CSV • record • table
monitor *monitor-name*	Displays cache information for the specified monitor name.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	This command can be used to view performance monitor cache details in controller mode.

Example

The following is sample output from the **show performance monitor cache** command:

```
Device# show performance monitor cache

Monitor: CISCO-media_ipv4


 Data Collection Monitor:


  Cache type:                              Synchronized (Platform cache)

  Cache size:                                     4000

  Current entries:                                   0


  Flows added:                                       0

  Flows aged:                                        0

  Synchronized timeout (secs):                      60



 Monitor: 175_SDWAN-art_ipv4


 Data Collection Monitor:


  Cache type:                              Synchronized (Platform cache)

  Cache size:                                    11250

  Current entries:                                   0


  Flows added:                                       0

  Flows aged:                                        0

  Synchronized timeout (secs):                      60
```

show performance monitor context

To view information about performance monitor configuration for a specified context, use the **show performance monitor context** command in privileged EXEC mode.

show performance monitor context *context* [**configuration** | **exporter** | **interface** | **summary** | **traffic-monitor**]

Syntax Description

context	Name of the performance monitor context. If a context name is not specified, all contexts are displayed.
configuration	(Optional) Displays all configuration of the specified context. This command can be used to convert the auto configuration to the traditional configuration.
exporter	(Optional) Displays the operational information about the exporters attached to the specified context.
interface	(Optional) Displays information about the performance monitor interface.
summary	(Optional) Displays information about the enabled traffic monitors and the interfaces to which they are attached.
traffic-monitor	(Optional) Displays information about the traffic-monitors configured for the performance monitor.

Command Default

When none of the optional keywords and arguments is specified, information is displayed for all contexts.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	This command can be used in Cisco SD-WAN controller mode.

Usage Guidelines

Use the **show performance monitor context** command to view all configuration for the specified context.

Example

The following are sample outputs from the **show performance monitor context** command:

```
Device# show performance monitor context CISCO-MONITOR summary

================================================================================

|                              CISCO-MONITOR                                   |

================================================================================

Description: User defined


Based on profile: sdwan-performance


Coarse-grain NBAR based profile


Configured traffic monitors
```

```
============================

 application-response-time:

 media: class-and match_audio


Attached to Interfaces

=====================

 Tunnel1
```

The following sample output shows exporter details for the performance monitor context named CISCO-MONITOR.

```
Device# show performance monitor context CISCO-MONITOR exporter

================================================================================

|                  Exporters information of context CISCO-MONITOR                |

================================================================================


Flow Exporter CISCO-MONITOR:

  Description:              performance monitor context CISCO-MONITOR exporter

  Export protocol:          IPFIX (Version 10)

  Transport Configuration:

    Destination type:       IP

    Destination IP address: 10.75.212.84

    Source IP address:      10.74.28.19

    Source Interface:       GigabitEthernet0/0/0

    Transport Protocol:     UDP

    Destination Port:       2055

    Source Port:            63494

    DSCP:                   0x0

    TTL:                    255

    Output Features:        Used

  Options Configuration:

    interface-table (timeout 600 seconds) (active)

    sampler-table (timeout 600 seconds) (active)

    application-table (timeout 600 seconds) (active)
```

```
    sub-application-table (timeout 600 seconds) (active)
    application-attributes (timeout 600 seconds) (active)
    tunnel-tloc-table (timeout 600 seconds) (active)
Flow Exporter CISCO-MONITOR:
  Packet send statistics (last cleared 04:13:19 ago):
    Successfully sent:         10270                  (13709142 bytes)

  Client send statistics:
    Client: Option options interface-table
      Records added:           312
        - sent:                312
      Bytes added:             31824
        - sent:                31824

    Client: Option options sampler-table
      Records added:           28
        - sent:                28
      Bytes added:             1344
        - sent:                1344

    Client: Option options application-name
      Records added:           38766
        - sent:                38766
      Bytes added:             3217578
        - sent:                3217578

    Client: Option sub-application-table
      Records added:           858
        - sent:                858
      Bytes added:             144144
        - sent:                144144

    Client: Option options application-attributes
```

```
  Records added:           38038
    - sent:                38038
  Bytes added:             9813804
    - sent:                9813804

Client: Option options tunnel-tloc-table
  Records added:           26
    - sent:                26
  Bytes added:             1352
    - sent:                1352

Client: MMA EXPORTER GROUP MMA-EXP-1
  Records added:           0
  Bytes added:             0



Client: Flow Monitor CISCO-MONITOR-art_ipv4
  Records added:           0
  Bytes added:             0

Client: Flow Monitor CISCO-MONITOR-media_ipv4
  Records added:           0
  Bytes added:             0
```

show platform hardware qfp active classification class-group-manager class-group client cce name

To view an optimized policy for a firewall, use the **show platform hardware qfp active classification class-group-manager class-group client cce name** command in user EXEC or privileged EXEC mode.

show platform hardware qfp active classification class-group-manager class-group client cce name

Command Default None

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

The following is sample output from the **show platform hardware qfp active classification class-group-manager class-group client cce name** command.

```
Device# show platform hardware qfp active classification class-group-manager class-group
client cce name FW_POLICY1-opt
class-group [cce-cg:12272256] FW_POLICY1-opt (classes: 2)
 clients: fw
 fields: ipv4_og_src:4 any:1 dst_geo_id:4  (100000:0:0:200:100000:00000000)
  (2097151) class: logical-expression [12272256.2734225] FW_POLICY1-seq-1-cm_ (filters: 1)
          lexp: LOG-EXP: [1]
    (1) filter: generic [12272256.2734225.1] (rules: 4)
      (1) rule: generic  [12272256.2734225.1.1] (permit)
         match ipv4_og_src 1
         match dst_geo_id 0xc24 / 0xffff
      (2) rule: generic  [12272256.2734225.1.2] (permit)
         match ipv4_og_src 1
         match dst_geo_id 0x1164 / 0xffff
      (3) rule: generic  [12272256.2734225.1.3] (permit)
         match ipv4_og_src 1
         match dst_geo_id 0xe2a / 0xffff
      (4) rule: generic  [12272256.2734225.1.4] (permit)
         match ipv4_og_src 1
         match dst_geo_id 0x1a9a / 0xffff
  (4294967295) class: logical-expression [12272256.1593] class-default (filters: 1)
          lexp: LOG-EXP: [1]
    (1) filter: generic [12272256.1593.1] (rules: 1)
      (1) rule: generic  [12272256.1593.1.1] (permit)
         match any
```

show platform hardware qfp active classification class-group-manager class-group client sdwan

To view the policy name or group-id in class-group-manager and to get the detail info, use the **show platform hardware qfp active classification class-group-manager class-group client sdwan** command in privileged EXEC mode.

show platform hardware qfp active classification class-group-manager class-group client sdwan { **all** | **name** *class-group-name* | *class-group-id* }

Syntax Description

all	All class group.
name *class-group-name*	Name of the class group.

class-group-id	Class group id. Range: 0 to 4294967295

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	This command was introduced.

Usage Guidelines

This command displays information that helps you to troubleshoot related issues about policy name or group-id in class-group-manager.

Examples

The following is a sample output from the **show platform hardware qfp active classification class-group-manager class-group client sdwan** command:

```
Device# show platform hardware qfp active classification class-group-manager class-group
client sdwan all
QFP classification class client all group
  class-group [SDWAN:21] DATA_POLICY-vpn_1
  class-group [SDWAN:22] AAR_POLICY-vpn_1

Device# show platform hardware qfp active classification class-group-manager class-group
client sdwan 21
class-group [sdwan-cg:21] DATA_POLICY-vpn_1 (classes: 8)
 clients:
 fields: l4_dst:2 ipv4_og_src:8 ipv4_og_dst:24 ipv6_og_src:1 ipv6_og_dst:2 any:1
ip_protocol_range:2 dns_request:4 dns_response:4
og_usr_app_id:6  (300100:600:0:100200:1300:00000000)
  (11) class: logical-expression [21.11] DATA_POLICY-vpn_1-seq-11 (filters: 7)
          lexp: LOG-EXP: ,
    (1) filter: generic [10.11.1] (rules: 1)
      (1) rule: generic  [10.11.1.1] (permit)
         match l4_dst range 5060 5060

Device# show platform hardware qfp active classification class-group-manager class-group
client sdwan name AAR_POLICY-vpn_1
class-group [sdwan-cg:22] AAR_POLICY-vpn_1 (classes: 6)
 clients:
 fields: ip_tos:1 l4_dst:1 ipv4_og_src:6 ipv4_og_dst:12 ipv6_og_src:1 ipv6_og_dst:2 any:1
ip_protocol_range:1 dns_request:3 dns_response:3
og_usr_app_id:4  (300110:600:0:100200:1300:00000000)
  (1) class: logical-expression [22.1] AAR_POLICY-vpn_1-seq-1 (filters: 10)
          lexp: LOG-EXP: ,
    (1) filter: generic [10.1.1] (rules: 2)
      (1) rule: generic  [10.1.1.1] (permit)
         match ipv4_og_src 57419
      (2) rule: generic  [10.1.1.2] (permit)
         match ipv4_og_src 57420
    (2) filter: generic [10.1.2] (rules: 6)
      (1) rule: generic  [10.1.2.1] (permit)
         match ipv4_og_dst 57421
      (2) rule: generic  [10.1.2.2] (permit)
```

show platform hardware qfp active classification class-group-manager object-group

To get the name or id of the tag membership in class-group-manager, use the **show platform hardware qfp active classification class-group-manager object-group** command in privileged EXEC mode.

show platform hardware qfp active classification class-group-manager object-group { **all** | **name** *object-group-name* | **type** { **IPv4** | **IPv6** | **ref_ace_v4** } }

Syntax Description

all	All object group.
name *object-group-name*	Name of the Object-Group.
type	Type of the Object-Group.
ref_ace_v4	Reflect ACE V4.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	This command was introduced.

Usage Guidelines

This command displays information that can help you to troubleshoot issues about the tag membership in class-group-manager.

Examples

The following is a sample output from the **show platform hardware qfp active classification class-group-manager object-group** command, use to verify the object-group IDs.

```
Device# show platform hardware qfp active classification class-group-manager object-group
all
QFP classification object-group all
  multicast_pfx_t:57417  Type: IPV4  No. of Entries: 1
  pfx1_t:57418  Type: IPV4  No. of Entries: 1
  pfx21_t:57419  Type: IPV4  No. of Entries: 1
  pfx22_t:57420  Type: IPV4  No. of Entries: 2
  pfx31_t:57421  Type: IPV4  No. of Entries: 5
  pfx32_t:57422  Type: IPV4  No. of Entries: 1
  pfx33_t:57423  Type: IPV4  No. of Entries: 1
  pfx34_t:57424  Type: IPV4  No. of Entries: 1
  pfx35_t:57425  Type: IPV4  No. of Entries: 1
  pfx36_t:57426  Type: IPV4  No. of Entries: 1
  subnet_0_t:57427  Type: IPV4  No. of Entries: 1
  v6_pfx1_t_v6:57428  Type: IPV6  No. of Entries: 1
  v6_pfx21_t_v6:57429  Type: IPV6  No. of Entries: 2
  v6_pfx22_t_v6:57430  Type: IPV6  No. of Entries: 3
  apps_facebook_type_app_id_t:57431  Type: USR-APPID  No. of Entries: 2
  apps_ms_type_app_id_t:57432  Type: USR-APPID  No. of Entries: 6
  apps_webex_type_app_id_t:57433  Type: USR-APPID  No. of Entries: 6
  apps_zoom_type_app_id_t:57434  Type: USR-APPID  No. of Entries: 1
```

show platform hardware qfp active classification feature message all

To display recent Classification Feature Manager (CFM) syslog messages on a Cisco Quantum Flow Processor (QFP), use the **show platform hardware qfp active classification feature message** command in privileged EXEC mode.

show platform hardware qfp active classification feature message { **all** | **clear** }

Syntax Description

all	Displays all the CFM syslog message buffer.
clear	Clears the syslog circular buffer.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.8.1a	This command was introduced.

Usage Guidelines

Use this command to debug CFM related issues in a QFP by analyzing the feature manager messages.

This command displays the CFM syslog message buffer. A message buffer can save up to 300 messages in a fixed-size buffer. The messages are displayed in the last in, first out (LIFO) order.

Example

The following example displays the recent CFM syslog messages.

```
Device# show platform hardware qfp active active classification feature message all
Sep 24 08:35:52.670: : CPP_FM_CLIENT_WARNING: ATTACH request failed for acl client id[acl:32]
 name[lab-lenient1] label[0]. Error code: 0x1c(No space left on device)


Sep 24 08:35:50.763: : CPP_FM_SW_TCAM_WARNING: CACE EXMEM allocation fail: acl client
id[acl-cg:32] name[lab-lenient1] attempted to allocate114971756 bytes


Sep 24 04:58:13.425: : CPP_FM_CLIENT_WARNING: ATTACH request failed for qos client
id[cce:8265536] name[inputPolicy] label[0]. Error code: 0x71(No route to host)


Sep 24 04:58:13.424: : CPP_FM_TCAM_CE_WARNING: Failed to select tcam key: could not find
matching key format for qos client id[cce:8265536] name[inputPolicy] field
bit-map[18050:0:300000:200:0:00000000]
```

show platform hardware qfp active classification feature-manager exmem-usage

To display the External Memory Manager (EXMEM) usage on a Cisco Quantum Flow Processor (QFP), use the **show platform hardware qfp active classification feature-manager exmem-usage** command in privileged EXEC mode.

show platform hardware qfp active classification feature-manager exmem-usage sorted

Syntax Description

sorted	Displays the memory usage sorted at the policy level. The policy with the highest EXMEM usage appears first.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.8.1a	This command was introduced.

Usage Guidelines

Use this command to display the EXMEM usage at the client level and at the policy level.

Example

The following example shows how to display the EXMEM memory usage for various clients. The display order is according to the client ID.

```
Device# show platform hardware qfp active active classification feature-manager exmem-usage

EXMEM Usage Information

Total exmem used by CACE: 39668

Client       Id   Total VMR     Total Usage   Total%   Alloc     Free
-------------------------------------------------------------------------
acl           0      11           2456          6         88       84
qos           2     205          31512         79          7        5
fw            4       8            892          2          2        1
obj-group    39      82           4808         12          5        2
```

The following example shows how to display the memory usage sorted at the policy level. The policy with the highest EXMEM usage appears first.

```
Device# show platform hardware qfp active active classification feature-manager exmem-usage
 sorted

EXMEM Usage Information

Total VMR entries used by CACE: 306
```

```
Total exmem used by CACE: 39668

CG-Id               Name                Client          VMR        Usage       Label
-------------------------------------------------------------------------------------
cce:8265536         inputPolicy          QOS            198        30680       107
obj-group:7            ---               OBJ-GROUP       80         3928       103
cce:13747824         fw-policy           FW               8          892        26
cce:482000           odm                 QOS              7          832       102
acl:29               og_acl              ACL              4          764       105
acl:30               og_acl_1            ACL              4          764       104
acl:5                acl111              ACL              2          488        83
acl:6                acl112              ACL              1          440        84
obj-group:5            ---               OBJ-GROUP        1          440        80
obj-group:3            ---               OBJ-GROUP        1          440        77
```

show platform hardware qfp active classification feature-manager statistics

To display Classification Feature Manager (CFM) error statistics, use the **show platform hardware qfp active classification feature-manager statistics** command in privileged EXEC mode.

This command **show platform hardware qfp active classification feature-manager statistics** has been added to admin-tech. For more information on **admin-tech** command, see request admin-tech

show platform hardware qfp active classification feature-manager statistics

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco vManage CLI templates.

Usage Guidelines

Use this command for troubleshooting a client in a QFP by analysing the feature manager requests statistics.

Example

The following example shows how to display the CFM error statistics.

```
Device# show platform hardware qfp active active classification feature-manager statistics
Client          Id  Attach      Err     ReplaceCG   Err     Edit        Err     Release
Err     Detach      Err     RelToTCAM   Err
     Drop

obj-group      39  2           0       0           0       0           0       0
0       0           0       0           0
     0
sdwan-approu   46  1           0       0           0       1           0       1
0       0           0       0           0
```

```
     0
sdwan-dp      47  1            0       0           0       1           0       1
0       0           0       0           0
     0
```

show platform hardware qfp active feature acl control

To display whether Security Group Access Control List (SGACL) logging is enabled or disabled, use the **show platform hardware qfp active feature acl control** command in privileged EXEC mode.

show platform hardware qfp active feature acl control

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.15.1a	This command is supported for Cisco Catalyst SD-WAN.

Usage Guidelines

Use the **show platform hardware qfp active feature acl control** to display whether SGACL logging is enabled or disabled.

Examples

The following is sample output from the **show platform hardware qfp active feature acl control** command. In this example, SGACL logging is enabled.

```
Device# show platform hardware qfp active feature acl control
Stats Poll Period: 0
Stats Entry Size: 16
Ha Init: 1
Fm Ready: 0
IPv4 Logging Threshold: 2147483647
IPv4 Logging Interval: 0
IPv6 Logging Threshold: 350000
IPv6 Logging Interval: 0
Maximum Aces Per Acl: 256000
Stats Update size: 180
Maximum Entries: 0
Maximum Entries per Classifier: 0
Result Bit Size: 0
Result Start Bit Pos: 0
Maximum Profiles: 0
Maximum Blocks per Profile: 0
Device Select: 0
Maximum Tree Depth: 0
Dimention: 0
Number Cuts: 0
HSL Support: TRUE // sgacl hsl logging is enabled
HSL Force Disable: FALSE
```

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

Field	Description
Stats Poll Period	The interval (in seconds) at which statistics are polled. A value of 0 indicates that polling is disabled.
Stats Entry Size	The size of each statistics entry in bytes.
Ha Init	Indicates whether High Availability (HA) initialization has been completed. A value of 1 means it is initialized.
Fm Ready	Indicates whether the Forwarding Manager (FM) is ready. A value of 0 means it is not ready.
IPv4 Logging Threshold	The threshold for logging IPv4 packets.
IPv4 Logging Interval	The interval (in seconds) for logging IPv4 packets. A value of 0 indicates that interval-based logging is disabled.
IPv6 Logging Threshold	The threshold for logging IPv6 packets.
IPv6 Logging Interval	The interval (in seconds) for logging IPv6 packets. A value of 0 indicates that interval-based logging is disabled.
Maximum Aces Per Acl	The maximum number of Access Control Entries (ACEs) allowed per ACL.
Stats Update size	The size of the statistics update in bytes.
Maximum Entries	The maximum number of entries allowed. A value of 0 may indicate that there is no set limit or that the feature is disabled.
Maximum Entries per Classifier	The maximum number of entries allowed per classifier. A value of 0 may indicate that there is no set limit or that the feature is disabled.
Result Bit Size	The size of the result bit field. A value of 0 may indicate that this feature is not in use.
Result Start Bit Pos	The starting bit position for the result field. A value of 0 may indicate that this feature is not in use.
Maximum Profiles	The maximum number of profiles allowed. A value of 0 may indicate that there is no set limit or that the feature is disabled.
Maximum Blocks per Profile	The maximum number of blocks allowed per profile. A value of 0 may indicate that there is no set limit or that the feature is disabled.
Device Select	The device selection parameter. A value of 0 may indicate a default or unspecified device.
Maximum Tree Depth	The maximum depth of the tree structure used for ACL processing. A value of 0 may indicate that this feature is not in use.
Dimension	Refers to the dimensionality of the ACL processing structure. A value of 0 may indicate that this feature is not in use.

Field	Description
Number Cuts	The number of cuts or divisions used in the ACL processing structure. A value of 0 may indicate that this feature is not in use.
HSL Support	Indicates whether HSL is supported on the device. A value of TRUE means HSL is supported and enabled.
HSL Force Disable	Indicates whether HSL is forcibly disabled. A value of FALSE means HSL is not forcibly disabled and can be used.

show platform hardware qfp active feature acl dp hsl configuration

To display the configuration for Security Group Access Control List (SGACL) HSL, use the **show platform hardware qfp active feature acl dp hsl configuration** command in privileged EXEC mode.

show platform hardware qfp active feature acl dp hsl configuration

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.15.1a	This command was introduced.

Usage Guidelines

Use the **show platform hardware qfp active feature acl dp hsl configuration** to display the configuration for SGACL HSL as set up on the device.

Examples

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

```
Device# show platform hardware qfp active feature acl dp hsl configuration
ACL DP HSL Config:
HSL Supported: TRUE
HSL SGACL Enabled: TRUE
SGACL HSL Setup:
Handle Session/Instance: 127/63
Version: 9
Dest Type: 3
HSL Enable: TRUE
HSL BackPressure Enable: FALSE
Base Memory Addr: <0xpXXXX>
Memory Size (bytes): 147560
Max Records: 1024
Record Threshold: 256
Memory Threshold (bytes): 32768
Record Timeout (ms): 512
Export Timeout (ms): 4
MTU Size (bytes): 1450
```

```
Template Refresh Timer: 0
Template Refresh Packets: 0
Source Id: 0x404”
Max Record Size (bytes): 104
```

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

Field	Description
HSL Supported	Indicates that HSL is supported on the device.
HSL SGACL Enabled	Indicates that HSL for SGACL logging is enabled on the device.
Handle Session/Instance	Represents the session and instance handle numbers used for HSL configuration.
Version	Indicates the version of the HSL configuration being used.
Dest Type	Specifies the destination type for the HSL logs. This could refer to the type of logging destination, such as a syslog server or a specific logging format.
HSL Enable	Indicates that HSL is enabled for SGACL logging.
HSL BackPressure Enable	Indicates whether backpressure is enabled for HSL. Backpressure is a flow control mechanism to prevent buffer overflow. A value of FALSE means it is not enabled.
Base Memory Addr	The base memory address used for HSL logging. This is a placeholder for the actual memory address.
Memory Size (bytes)	The total memory size allocated for HSL logging, in bytes.
Max Records	The maximum number of log records that can be stored in the HSL memory.
Record Threshold	The threshold number of records that triggers certain actions, such as exporting logs.
Memory Threshold (bytes)	The memory usage threshold, in bytes, that triggers certain actions, such as exporting logs.
Record Timeout (ms)	The timeout period, in milliseconds, for log records before they are exported.
Export Timeout (ms)	The timeout period, in milliseconds, for exporting log records.
MTU Size (bytes)	The Maximum Transmission Unit (MTU) size, in bytes, for HSL log packets. This defines the largest size of a packet that can be transmitted.
Template Refresh Timer	The interval, in seconds, for refreshing the HSL template. A value of 0 indicates that template refresh is disabled.
Template Refresh Packets	The number of packets after which the HSL template is refreshed. A value of 0 indicates that template refresh based on packet count is disabled.
Source Id	The source identifier used for HSL logging. This is a hexadecimal value that uniquely identifies the source of the logs.
Max Record Size (bytes)	The maximum size, in bytes, of a single log record.

show platform hardware qfp active feature acl dp hsl statistics

To display the logging statistics for Security Group Access Control List (SGACL) HSL from the device, use the **show platform hardware qfp active feature acl dp hsl statistics** command in privileged EXEC mode.

show platform hardware qfp active feature acl dp hsl statistics

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.15.1a	This command was introduced.

Usage Guidelines

Use the **show platform hardware qfp active feature acl dp hsl statistics** to display the logging statistics for SGACL HSL from the device.

Examples

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

```
Device# show platform hardware qfp active feature acl dp hsl statistics
ACL DP HSL Statistics:
HSL Supported: TRUE
HSL SGACL Enabled: TRUE
SGACL Export Statistics
-----------------------
Records sent (to HSL): 2
Records dropped (before HSL): 0
Record alloc failures: 0
Records dropped flag: Off
Records sent (by HSL): 0
Records dropped (by HSL): 0
HSL packets dropped flag: Off
HSL buffer flow-on (count): 0
SGACL HSL Statistics
--------------------
Records exported: 2
Packets exported: 2
Bytes exported: 168
Dropped records: 0
Dropped packets (inc. Punt drops): 0
Dropped bytes: 0
```

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

Field	Description
HSL Supported: TRUE	Indicates that High Speed Logging (HSL) is supported on the device.
HSL SGACL Enabled: TRUE	Indicates that HSL for SGACL logging is enabled on the device.
Records sent (to HSL)	The number of SGACL log records that have been sent to the HSL system for processing.

Field	Description
Records dropped (before HSL)	The number of SGACL log records that were dropped before reaching the HSL system.
Record alloc failures	The number of times the system failed to allocate memory for SGACL log records.
Records dropped flag	Indicates whether the flag for dropping records is active. "Off" means no records are currently being dropped due to this flag.
Records sent (by HSL)	The number of SGACL log records that have been successfully sent by the HSL system.
Records dropped (by HSL)	The number of SGACL log records that were dropped by the HSL system.
HSL packets dropped flag	Indicates whether the flag for dropping HSL packets is active. **Off**means no HSL packets are currently being dropped due to this flag.
HSL buffer flow-on (count)	The number of times the HSL buffer has been in a flow-on state, which typically indicates high buffer usage or potential overflow conditions.
Records exported	The total number of SGACL log records that have been exported by the HSL system.
Packets exported	The total number of packets associated with the exported SGACL log records.
Bytes exported	The total number of bytes associated with the exported SGACL log records.
Dropped records	The total number of SGACL log records that have been dropped during the export process.
Dropped packets (inc. Punt drops)	The total number of packets that have been dropped during the export process, including those dropped due to punt conditions (packets that are forwarded to the control plane for processing).
Dropped bytes	The total number of bytes that have been dropped during the export process.

show platform hardware qfp active feature bfd datapath

To display information about the BFD datapath summary in a data plane, use the **show platform hardware qfp active feature bfd datapath** command in privileged EXEC (#).

show platform hardware qfp active feature bfd datapath [**sdwan-summary**] [**sdwan ld** *sdwan-ld*]

Syntax Description

sdwan-summary	Displays the summary for a specific Cisco SD-WAN device.

sdwan ld *sdwan-ld*	Displays the status for a specific SDWAN instance. Specify Cisco SD-WAN local discriminator value. Range:1 to 65531

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.15.1a	This command was introduced.

Usage Guidelines

Use the command **show platform hardware qfp active feature bfd datapath sdwan-summary** to find out the local discriminator value for a particular BFD session. Then, you can run **show platform hardware qfp active feature bfd datapath sdwan ld** *sdwan ld* to display information about BFD datapath in the data plane for that session.

Examples

The following sample output displays the summary of BFD sessions in a data plane:

```
Device# show platform hardware qfp active feature bfd datapath sdwan summary
Total number of session: 12
LD       SrcIP      DstIP          TX         RX     Encap    State  AppProbe    AdjId
20001  192.168.4.0  172.16.17.1   183527   182839   IPSEC    Up     YES      GigabitEthernet1
 (0xf810000f)
20002  172.16.1.0   172.16.17.1   183535   182850   IPSEC    Up     YES      GigabitEthernet3
 (0xf810001f)
20003  192.168.4.1  192.168.4.0   182429   182003   IPSEC    Up     YES      GigabitEthernet1
 (0xf810002f)
20004  172.16.4.0   192.168.5.0   183129   181973   IPSEC    Up     YES      GigabitEthernet3
 (0xf810003f)
20005  192.168.4.1  192.168.4.0   175600   174575   IPSEC    Up     YES      GigabitEthernet1
 (0xf810004f)
20006  172.16.0.0   192.168.5.0   175596   174569   IPSEC    Up     YES      GigabitEthernet3
 (0xf810005f)
20007  192.168.4.0  192.168.3.3   183550   182864   IPSEC    Up     YES      GigabitEthernet1
 (0xf810006f)
20008  172.16.1.1   192.168.3.3   183568   182880   IPSEC    Up     YES      GigabitEthernet3
 (0xf810007f)
20009  192.168.4.0  192.168.1.1   182718   182410   IPSEC    Up     YES      GigabitEthernet1
 (0xf810008f)
20010  172.16.17.1  192.168.1.1   183381   182440   IPSEC    Up     YES      GigabitEthernet3
 (0xf810009f)
20011  192.168.5.0  172.16.1.0    175548   174523   IPSEC    Up     YES      GigabitEthernet1
 (0xf81000af)
20012  172.16.1.2   172.16.1.1    175572   174547   IPSEC    Up     YES      GigabitEthernet3
 (0xf81000bf)
```

The following sample output displays the BFD datapath information in data plane:

```
Device# show platform hardware qfp active feature bfd datapath sdwan ld 20008
LD                    : 20008
My Private IP         : 172.16.1.1
Remote Private IP     : 192.168.4.0
Tx Stats              : 183600
Rx Stats              : 182912
```

```
Encap Type            : IPSEC
State                 : Up
AppProbe              : YES
IPSec Out SA ID       : 0x24000024
Tunnel Rec ID         : 8
IfName                : GigabitEthernet3 (0xf810007f)
Uidb                  : 65528
Config Tx Timer       : 1000000
Conig Detect Timer    : 7000000
Actual Tx Timer       : 1000000
Actual Detect Timer   : 7000000
My Pub IP             : 172.16.1.0
My Pub Port           : 12346
My Symmetric NAT IP   : 0.0.0.0
My Symmetric NAT Port : 0
Remote public IP      : 192.168.4.0
Remote public Port    : 12346
MTU(config), Actual   : 1442, 1442
Farend PMTU           : 1442
My Capabilities       : 0x160
Remote Capabilities   : 0x160
SDWAN BFD flags       : ||||||| (0x0)
local_color           : 4
Ipsec Overhead        : 38
PFR stats for SLA default (addr:0xf14c02a0)
Number of pkts  : 524
Loss Count      : 0
Latency(1/16ms) : 416
Jitter(1/16ms)  : 832
Following are SDWAN stats
Echo Tx         : 182005
req          : 91415
reply        : 90590
Echo Rx         : 181317
req          : 90590
reply        : 90727
PMTU Tx         : 1595
PMTU RX         : 1595
AppProbeIDValid  NextProbeID StatAddr #Packets  Loss Latency(1/16ms) Jitter(1/16ms)
1         N         0        f14c02c0    0       0       0             0
2         N         0        f14c02e0    0       0       0             0
3         N         0        f14c0300    0       0       0             0
4         N         0        f14c0320    0       0       0             0
5         N         0        f14c0340    0       0       0             0
6         N         0        f14c0360    0       0       0             0
```

show platform hardware qfp active feature bfd datapath

To display information about BFD datapath in the data plane, use the **show platform hardware qfp active feature bfd datapath sdwan ld** command in privileged EXEC (#).

show platform hardware qfp active feature bfd datapath [**sdwan ld** *sdwan-ld*]

Syntax Description

sdwan ld *sdwan-ld*	Displays the status for a specific SDWAN instance. Specify Cisco SD-WAN ld value. Range:1 to 65531

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.15.1a	This command was introduced.

Usage Guidelines

Use the command **show platform hardware qfp active feature bfd datapath sdwan-summary** to find out the local discriminator (LD) value for a particular BFD session. Then, you can run **show platform hardware qfp active feature bfd datapath sdwan ld** *sdwan ld* to display information about BFD datapath in the data plane for that session. For more information, see command **show platform hardware qfp active feature bfd datapath sdwan-summary**.

Examples

The following sample output displays the BFD datapath information in data plane:

```
Device# show platform hardware qfp active feature bfd datapath sdwan ld 20008
LD                    : 20008
My Private IP         : 172.16.1.1
Remote Private IP     : 192.168.4.0
Tx Stats              : 183600
Rx Stats              : 182912
Encap Type            : IPSEC
State                 : Up
AppProbe              : YES
IPSec Out SA ID       : 0x24000024
Tunnel Rec ID         : 8
IfName                : GigabitEthernet3 (0xf810007f)
Uidb                  : 65528
Config Tx Timer       : 1000000
Conig Detect Timer    : 7000000
Actual Tx Timer       : 1000000
Actual Detect Timer   : 7000000
My Pub IP             : 172.16.1.0
My Pub Port           : 12346
My Symmetric NAT IP   : 0.0.0.0
My Symmetric NAT Port : 0
Remote public IP      : 192.168.4.0
Remote public Port    : 12346
MTU(config), Actual   : 1442, 1442
Farend PMTU           : 1442
My Capabilities       : 0x160
Remote Capabilities   : 0x160
SDWAN BFD flags       : ||||||| (0x0)
local_color           : 4
Ipsec Overhead        : 38
PFR stats for SLA default (addr:0xf14c02a0)
Number of pkts  : 524
```

```
Loss Count      : 0
Latency(1/16ms) : 416
Jitter(1/16ms)  : 832
Following are SDWAN stats
Echo Tx         : 182005
req          : 91415
reply        : 90590
Echo Rx         : 181317
req          : 90590
reply        : 90727
PMTU Tx         : 1595
PMTU RX         : 1595
AppProbeIDValid  NextProbeID StatAddr #Packets  Loss Latency(1/16ms) Jitter(1/16ms)
1         N         0        f14c02c0    0       0       0             0
2         N         0        f14c02e0    0       0       0             0
3         N         0        f14c0300    0       0       0             0
4         N         0        f14c0320    0       0       0             0
5         N         0        f14c0340    0       0       0             0
6         N         0        f14c0360    0       0       0             0
```

show platform hardware qfp active feature firewall drop

To view the drop counters and drop reasons for a firewall, use the **show platform hardware qfp active feature firewall drop** command in user EXEC or privileged EXEC mode.

show platform hardware qfp active feature firewall drop

Command Default

None

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

The following sample output displays the drop reasons.

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

-----------------------------------------------------------------------------
Drop Reason                                                           Packets
-----------------------------------------------------------------------------
ICMP ERR Pkt:exceed burst lmt                                              42
ICMP Unreach pkt exceeds lmt                                              305
UDP - Half-open session limit exceed                                        2
```

show platform hardware qfp active feature geo client

To display the hardware information used for a Cisco Quantum Flow Processor (QFP) to troubleshoot the geo client database, use the **show platform hardware qfp active feature geo client** command in privileged EXEC mode.

show platform hardware qfp active feature geo client { **country** { **all** | **code** *country-code* } | **info** | **stats** }

Syntax Description

country	Displays geo client country information.
all	Displays all the geo client country and continent codes.
code *country-code*	Displays the three-letter country code.
info	Displays information about the control plane policing (CoPP) geo client.
stats	Displays if the geodatabase is enabled or disabled, including updates and errors for troubleshooting.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

The reference counter keeps track of how many IP address table entries belong to the specified country.

Examples

The following are example outputs from the **show platform hardware qfp active feature geo client** command:

```
Device# show platform hardware qfp active feature geo client country all
Country code  ISO-3 code  Country name     Continent code   Continent name   Ref count
-------------------------------------------------------------------------------------
0             ?           unknown          0                **               0
4             afg         afghanistan      4                as               524
8             alb         albania          5                eu               295
```

```
Device# show platform hardware qfp active feature geo client info

Geo DB enabled

DB in use
    File name: /usr/binos/conf/geo_ipv4_db
    Number of entries installed: 415278
    Version: 2134.ajkdbnakjsdn
    Datapath PPE Address: 0x00000000ef2b7010
    Size (bytes): 6644448
    Exmem Handle: 0x0083800109080003
```

```
Country table
    Datapath PPE Address: 0x00000000ef0cf000
    Size (bytes): 16000
    Exmem Handle: 0x0081980009080003
```

The **1** for **Enable received** indicates that the geodatabase has been enabled on the device.

```
Device# show platform hardware qfp active feature geo client stats
CPP client Geo DB stats
-----------------------
  Enable received           : 1
  Modify received           : 0
  Disable received          : 0
  Enable failed             : 0
  Modify failed             : 0
  Disable failed            : 0
  IPv4 table write failed   : 0
  Persona write failed      : 0
  Country table write failed : 0
```

show platform hardware qfp active feature geo datapath

To display information about the hardware used on a Cisco Quantum Flow Processor (QFP) for troubleshooting geo datapath issues, use the **show platform hardware qfp active feature geo datapath** command in privileged EXEC mode.

show platform hardware qfp active feature geo datapath { **country** { **alpha** *alpha-country-code* | **numeric** *numeric-country-code* } | **ip_table** *ip-address* | **memory** | **stats** }

Syntax Description

country	Displays geo client country information.
alpha *alpha-country-code*	Displays the alphabetic country code.
numeric *numeric-country-code*	Displays the numeric country code. Valid values are 1 to 1000.
ip_table *ip-address*	Displays the content of the IP address database.
memory	Displays memory information in the available tables.
stats	Tracks the IP address table lookup results.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

The datapath uses the geodatabase to map IP addresses to geo codes. Geo codes are used for TCAM (ternary content-addressable memory) lookup and classification of data packets.

Examples

The following are example outputs for the **show platform hardware qfp active feature geo datapath** command:

```
Device# show platform hardware qf active feature geo datapath country alpha fra
Country alpha code: fra
Country numeric code: 250
GEO country info:
Country alpha code: fra
Continent alpha code: eu
Continent numeric code: 5
Country ref count: 0
Country hit count: 1
```

```
Device# show platform hardware qfp active feature geo datapath memory
Table-Name   Address      Size
----------------------------------------
Country DB   0xe83a8890   1000
IPV4 DB      0xe9a794a0   415278
```

```
Device# show platform hardware qfp active feature geo datapath stats
GEO Stats:
        lookup hit: 14611371
        lookup miss: 0
        error ip table: 0
        error country table: 0
        country table hit: 14611371
        country table miss: 0
```

show platform hardware qfp active feature nat datapath hsl

To display information about Network Address Translation (NAT) datapath High-Speed Logging (HSL), use the **show platform hardware qfp active feature nat datapath hsl** command in privileged EXEC mode.

show platform hardware qfp active feature nat datapath hsl

Syntax Description

This command has no arguments or keywords.

Command Default

Information about NAT datapath HSL is not displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	This command was introduced.
Cisco IOS XE Release 17.6.4 and later 17.6.x releases	

Usage Guidelines

The **show platform hardware qfp active feature nat datapath hsl** command provides information about NAT HSL-specific configurations and enables you to do the following:

- Allows you to troubleshoot NAT issues
- Allows you to verify the feature configurations

Examples

The following is a sample output from the **show platform hardware qfp active feature nat datapath hsl** command that is used to verify the configuration:

```
Device# show platform hardware qfp active feature nat datapath hsl
HSL cfg dip 10.10.0.1 dport 1020 sip 10.21.0.16 sport 53738 vrf 0
nat hsl handle 0x3d007d template id 261 pool_exh template id 263
LOG_TRANS_ADD 132148
LOG_TRANS_DEL 132120
LOG_POOL_EXH 0
```

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

Table 27: show platform hardware Field Descriptions

Field	Description
dip	Destination IP address
dport	Destination port address
sip	Source IP address
sport	Source port address
vrf	VRF ID
LOG_TRANS_ADD	NAT translation added log
LOG_TRANS_DEL	NAT translation deleted log
LOG_POOL_EXH	Pool exhaustion log. NAT also sends an HSL message when a NAT pool runs out of addresses (also called pool exhaustion).

show platform hardware qfp active feature nat datapath map

To display information about NAT mapping tables, use the **show platform hardware qfp active feature nat datapath map** command in privileged EXEC mode.

show platform hardware qfp active feature nat datapath map

Syntax Description

This command has no arguments or keywords.

Command Default

Information about NAT mapping tables is not displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.8.1a	This command is supported for Cisco Catalyst SD-WAN.

Examples

The following is a sample output from the **show platform hardware qfp active feature nat datapath map** command:

```
Device# show platform hardware qfp active feature nat datapath map
I/f Map Table

if_handle 65529 next 0x0 hash_index 220
laddr 0.0.0.0 lport 0 map 0xdec942c0 refcnt 0
gaddr 200.60.10.1 gport 0 proto 0 vrfid 0x0
src_type 1 flags 0x80100 cpmapid 3
I/f Map Table End
edm maps 0
mapping id 1 pool_id 0 if_handle 0xfff9 match_type 0 source_type 1 domain 0 proto 0 Local
IP 0.0.0.0, Local Port 0 Global IP 200.60.10.1
Global Port 0 Flags 0x80100 refcount 0 cp_mapping_id 3 next 0x0 hashidx 50 vrfid 0 vrf_tableid
 0x0 rg 0 pap_enabled 0 egress_ifh 0x14
```

show platform hardware qfp active feature nat datapath sess-dump

To display a session's summary from the NAT database, use the **show platform hardware qfp active feature nat datapath sess-dump** command in privileged EXEC mode.

show platform hardware qfp active feature nat datapath sess-dump

Syntax Description

This command has no arguments or keywords.

Command Default

Session summary information for the NAT database is not displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.8.1a	This command is supported for Cisco Catalyst SD-WAN.

Examples

The following is a sample output from the **show platform hardware qfp active feature nat datapath sess-dump** command:

```
Device# show platform hardware qfp active feature nat datapath sess-dump
id 0xdd70c1d0 io 10.20.24.150 oo 10.20.25.150 io 5201 oo 5201 it 200.60.10.1 ot 10.20.25.150
 it 5201 ot 5201 pro 6 vrf 4 tableid
4 bck 65195 in_if 0 out_if 20 ext_flags 0x1 in_pkts 183466
in_bytes 264182128 out_pkts 91731 out_bytes 2987880flowdb in2out fh 0x0 flowdb out2in fh
0x0
id 0xdd70c090 io 10.20.24.150 oo 10.20.25.150 io 25965 oo 25965 it 200.60.10.1 ot 10.20.25.150
 it 25965 ot 25965
pro 1 vrf 4 tableid 4 bck 81393 in_if 0 out_if 20 ext_flags 0x1 in_pkts 27 in_bytes 38610
out_pkts 27
out_bytes 38610flowdb in2out fh 0x0 flowdb out2in fh 0x0
```

show platform hardware qfp active feature nat datapath stats

To display information about NAT datapath statistics, use the **show platform hardware qfp active feature nat datapath stats** command in privileged EXEC mode.

show platform hardware qfp active feature nat datapath stats

Syntax Description This command has no arguments or keywords.

Command Default Information about NAT datapath statistics is not displayed.

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.8.1a	This command is supported for Cisco Catalyst SD-WAN.

Examples The following is a sample output from the **show platform hardware qfp active feature nat datapath stats** command:

```
Device# show platform hardware qfp active feature nat datapath stats
non_extended 0 entry_timeouts 0 statics 0 static net 0 hits 0 flowdb_hits 0 misses 0
nat_rx_pkts 346062 nat_tx_pkts 666522 nat_unmarked_pkts 0
nat_stick_rx_pkts 0 nat_stick_i2o_pkts 0 nat_stick_o2i_pkts 0
nat_res_port_in2out 0 nat_res_port_out2in 0
non_natted_in2out 0 nat_bypass 0 non_natted_out2in 0
ipv4_nat_stick_forus_hits_pkts 0 ipv4_nat_stick_hit_sb 0
ipv4_nat_stick_ha_ar_pkts 0 ipv4_nat_stick_ha_tcp_fin 0 ipv4_nat_stick_failed_ha_pkts 0
ipv4_nat_alg_bind_pkts 0
Proxy stats:
 ipc_retry_fail 0 cfg_rcvd 12 cfg_rsp 17

Number of sess 0 udp 0 tcp 0 icmp 0
```

show platform hardware qfp active feature nat datapath summary

To display configured and operational data specific to NAT, use the **show platform hardware qfp active feature nat datapath summary** command in privileged EXEC mode.

show platform hardware qfp active feature nat datapath summary

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	This command was introduced.

Usage Guidelines

The **show platform hardware qfp active feature nat datapath summary** command summarizes the following information:

- NAT-specific configurations and statistics
- Allows you to troubleshoot NAT issues
- Provides an overview of features configured

Example

The following is a sample output from the **show platform hardware qfp active feature nat datapath summary** command.

```
Device# show platform hardware qfp active feature nat datapath summary

Nat setting mode: sdwan-default
Number of pools configured: 1
Timeouts: 0(tcp), 0(udp), 0(icmp), 60(dns),
60(syn), 60(finrst), 86400(pptp), 3600(rmap-entry)
pool watermark: not configured
Nat active mapping inside:0 outside:0 static:2 static network:0
Nat datapath debug: enabled
Nat synchronization: enabled
Nat bpa: not configured; pap: not configured
Nat gatekeeper: on
Nat limit configured: no
Vpns configured with match-in-vrf: yes
Nat packet drop: none
Total active translations: 4 (2 static, 2 dynamic, 2 extended)
Platform specific maximum translations: 131072 configured: none
```

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

Table 28: show platform hardware qfp active feature nat datapath summary Field Descriptions

Fields	Description
NAT setting mode	Configures NAT mode to default or cgn or sdwan-default.
Number of pools configured	Configures number of pools for NAT.
Timeouts	Specifies the timeout value that applies to DNS connections (default is 60 secs), ICMP flows (default is 60 secs), TCP port (default is 86400 secs), UDP port (default is 300 secs), synchronous (SYN) timeout value (default is 60 secs), finish and reset timeout value (default is 60 secs), Point-to-Point Tunneling Protocol (PPTP) timeout (default is 86400 secs), Route map entry timeout value (default is 3600 secs).
pool watermark	Generates alerts before addresses in an address pool and are exhausted based on watermark settings.
NAT active mapping	Specifies the statistics of different (inside, outside, static, static network) NAT rules configured.

Fields	Description
NAT debug	Enables debug logging in NAT.
NAT synchronization	Enables NAT synchronization between redundant devices.
NAT bpa	The bulk logging and port block allocation feature allocates a block of port for translation; supported for cgn mode only.
NAT gatekeepers	Optimizes non-natted flows from using excessive CPU usage.
NAT limit configured	The rate limiting NAT translation feature provides you more control over how NAT addresses are used.
VPNs configured with match-in-vrf	Enables inside and outside traffic in the same VRF.
NAT packet drop	Determines if NAT has dropped any packet. Displays true or none.
Total active translations	Displays total number of active IPv4 NAT translations.
Platform specific maximum translations	Configures maximum number of supported IP NAT translations that are specific to the platform.

show platform hardware qfp active feature nat66 datapath prefix

To verify the passed interface stateless NAT66 prefix configuration, use the **show platform hardware qfp active feature nat66 datapath prefix** command in privileged EXEC mode.

show platform hardware qfp active feature nat66 datapath prefix

Syntax Description

This command has no arguments or keywords.

Command Default

No NAT66-configured prefixes are displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command is supported for Cisco Catalyst SD-WAN.

Examples

The following is a sample output from the **show platform hardware qfp active feature nat66 datapath prefix** command:

```
Device# show platform hardware qfp active feature nat66 datapath prefix
prefix hasht 0x89628400 max 2048 chunk 0x8c392bb0 hash_salt 719885386
```

```
NAT66 hash[1] id(1) len(64) vrf(0) in: 2001:db8:ab01:0000:0000:0000:0000:0000 out:
2001:db8:ab02:0000:0000:0000:0000:0000 in2out: 7 out2in: 7
```

show platform hardware qfp active feature nat66 datapath statistics

To verify the global NAT66 statistics, use the **show platform hardware qfp active feature nat66 datapath statistics** command in privileged EXEC mode.

show platform hardware qfp active feature nat66 datapath statistics

Syntax Description

This command has no arguments or keywords.

Command Default

No NAT66 global statistics are displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command is supported for Cisco Catalyst SD-WAN.

Examples

The following is a sample output from the **show platform hardware qfp active feature nat66 datapath statistics** command:

```
Device# show platform hardware qfp active feature nat66 datapath statistics
in2out xlated pkts 7
out2in xlated pkts 7
NAT66_DROP_SC_INVALID_PKT 0
NAT66_DROP_SC_BAD_DGLEN 0
NAT66_DROP_SC_PLU_FAIL 22786
NAT66_DROP_SC_PROCESS_V6_ERR 0
NAT66_DROP_SC_INVALID_EMBEDDED 0
NAT66_DROP_SC_SRC_RT 0
NAT66_DROP_SC_NOT_ENABLED 0
NAT66_DROP_SC_NO_GPM 0
NAT66_DROP_SC_LOOP 0
in2out_pkts 22768 out2in_pkts 22793
in2out_pkts_untrans 22761 out2in_pkts_untrans 22786
in2out_lookup_pass 7 out2in_lookup_pass 7
in2out_lookup_fail 0 out2in_lookup_fail 22786
mem_alloc_fail 0 prefix_fail 0
total prefix count 1
```

show platform hardware qfp active feature sdwan client phy-wan-bind-list

To display the list of interfaces bound to the Physical WAN interface, use the **show platform hardware qfp active feature sdwan client phy-wan-bind-list** command in user EXEC mode.

show platform hardware qfp active feature sdwan client phy-wan-bind-list

Command Default None

Command Modes User EXEC (>)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	This command was introduced.

Examples The following sample output displays the list of interfaces bound to the Physical WAN interface.

```
Device# show platform hardware qfp active feature sdwan client phy-wan-bind-list
physical interface(if_hdl)------------bind interfaces(if_hdl)

GigabitEthernet0/0/0(7)               GigabitEthernet0/0/0(7)
```

show platform hardware qfp active feature utd config

To verify the UTD data plane configuration, use the **show platform hardware qfp active feature utd config** command in privileged EXEC mode.

show platform hardware qfp active feature utd config

Command Default None

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Usage Guidelines Use this command to display UTD datapath configuration and status.

Example

The following example shows the UTD datapath configuration and status.

```
Device# show platform hardware qfp active feature utd config
Global configuration
  NAT64: disabled
  Drop pkts: disabled
  Multi-tenancy: disabled
  Data plane initialized: yes
  TLS Decryption Policy: disabled
```

```
Divert controller mode: enabled
SN threads: 12
CFT inst_id 0 feat id 4 fo id 4 chunk id 17
Max flows: 55000
```

Note There is a maximum number of flows supported by UTD, and you can use the **show platform hardware qfp active feature utd config** command to identify the maximum number of concurrent sessions supported on a Cisco IOS XE Catalyst SD-WAN device. Max flows are defined for each Cisco IOS XE Catalyst SD-WAN device, and it differs by devices and release versions. This example displays a Max Flow value defined for 55000 sessions.

show platform hardware qfp active interface if-name

To display packet drop statistics for each interface in the Quantum Flow Processor (QFP), use the **show platform hardware qfp active interface if-name** command in privileged EXEC mode.

show platform hardware qfp active interface if-name *type number* **statistics** [**clear_drop** | **detail** | **drop_summary** [**subinterface**]]

Syntax Description

type	Interface Type.
number	Interface Number.
statistics	Tx/Rx and Drop statistics.
clear_drop	(Optional) Clears drop stats after reading.
detail	(Optional) Shows drop cause IDs.
drop_summary	(Optional) Drops stats summary report.
subinterface	(Optional) Shows subinterface and their drop stats.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

Use this command for troubleshooting an interface in a QFP by analyzing the statistics of packet drops.

Example

The following example shows how to display the statistics of packet drops on the Gigabit Ethernet interface 0/0/0.

```
Device# show platform hardware qfp active interface if-name gigabitEthernet 0/0/0 statistics
------------------------------------------------------------------
Receive Stats Packets Octets
------------------------------------------------------------------
Ipv4 2 322
Ipv6 0 0
Tag 0 0
McastIpv4 0 0
McastIpv6 0 0
Other 3 204
------------------------------------------------------------------
Transmit Stats Packets Octets
------------------------------------------------------------------
Ipv4 2 178
Ipv6 0 0
Tag 0 0
McastIpv4 0 0
McastIpv6 0 0
Other 0 0
------------------------------------------------------------------
Input Drop Stats Packets Octets
------------------------------------------------------------------
Ipv4uRpfStrictFailed 5 590
Ipv6uRpfStrictFailed 5 590
------------------------------------------------------------------
Output Drop Stats Packets Octets
------------------------------------------------------------------
The Egress drop stats were all zero
------------------------------------------------------------------
Drop Stats Summary:
note: 1) these drop stats are only updated when PAL
reads the interface stats.
2) the interface stats include the subinterface
Interface Rx Pkts Tx Pkts
------------------------------------------------------------------------------
GigabitEthernet0/0/0 25 0
```

show platform hardware qfp active statistics drop

To display the drop statistics for all interfaces, use the **show platform hardware qfp active statistics drop** command in user EXEC mode.

show platform hardware qfp active statistics drop

Command Default None

Command Modes User EXEC (>)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	This command was introduced.

Examples

The following sample output displays the drop statistics for all interfaces.

```
Device# show platform hardware qfp active statistics drop
Last clearing of QFP drops statistics : never


-----------------------------------------------------------------------
Global Drop Stats                          Packets                Octets
-----------------------------------------------------------------------
Disabled                                         4                   266
Ipv4EgressIntfEnforce                           15                 10968
Ipv6NoRoute                                      6                   336
Nat64v6tov4                                      6                   480
SVIInputInvalidMac                             244                 15886
SdwanImplicitAclDrop                           160                 27163
UnconfiguredIpv4Fia                         942525              58524580
UnconfiguredIpv6Fia                          77521               9587636
```

show platform hardware qfp active feature firewall datapath rg

To display detailed information about the firewall datapath within a redundancy group on a Cisco IOS XE Catalyst SD-WAN device, use the **show platform hardware qfp active feature firewall datapath rg** command in privileged EXEC mode.

show platform hardware qfp active feature firewall datapath rg

Syntax Description

group	Display details of the firewall datapath for a redundancy group.
all	Displays all statistics providing detailed insights into the current state and performance metrics of both the active and standby components of an high availability system.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.15.1a	This command is supported for Cisco Catalyst SD-WAN.

Usage Guidelines

Use the **show platform hardware qfp active feature firewall datapath rg** to display detailed information about the firewall datapath within a redundancy group.

Examples

The following is a sample output from the **show platform hardware qfp active feature firewall datapath rg** command with the redundancy group set to 1.

```
Device# show platform hardware qfp active feature firewall datapath rg 1

rg 1, rg_state 0x00030035 (Active, Transport Up, Flow On, AR Transport UP, Allow New Sessions,
 Update Peer)
11 (RG Active) ha_handle 0x00020102 rg_flags 0x0 session id 0x5

==== HA general stat ====
Initial bulksync retry count 0
Allocated retry entries 0
Current retry queue depth 0
Maximum queued retries 0
Max retries queued ever 0
Stats were all zero

==== HA active stat ====
Total received messages 1
Session create requests 5
Session delete requests 5
Bulksync requests received 1
Bulksync complete 1
Session sync attempt: create 5
Session sync attempt: delete 5

==== HA standby stat ====
Stats were all zero
```

Examples

The following is a sample output from the **show platform hardware qfp active feature firewall datapath rg** command with the redundancy group set to all.

```
Device# show platform hardware qfp active feature firewall datapath rg all

rg 1, rg_state 0x00030035 (Active, Transport Up, Flow On, AR Transport UP, Allow New Sessions,
 Update Peer)
11 (RG Active) ha_handle 0x00020102 rg_flags 0x0 session id 0x5

==== HA general stat ====
Initial bulksync retry count 0
Allocated retry entries 0
Current retry queue depth 0
Maximum queued retries 0
Max retries queued ever 0
Total retry allocations 0
Retry allocation failures 0
Total retry entries queued 0
Flow on 0
Flow off 0
Retry timeout 0

==== HA active stat ====
```

```
Total received messages 1
Missing RII 0
Session create requests 5
Session delete requests 5
Session update requests 0
Bulksync requests received 1
Bulksync complete 1
L7 buffers allocated 0
L7 buf alloc failure 0
Failed to send L7 data 0
L7 data sent 0
Invalid opcode recvd 0
Message too short 0
Bad version number 0
Bad magic number 0
Create NAKs received 0
No HA buffer 0
No buffer false positive 0
Session sync attempt: create 5
Session sync attempt: update 0
Session sync attempt: delete 5
Session sync attempt: l7 data 0
vrf mapping failures 0
Invalid protocol 0
PAM classificaiton failure 0
Classificaiton failure 0
Could not find parent flow 0
Asymmetric routing injection 0
Data transport down 0
Bad bulk sync feature id 0
Bad bulk sync message length 0
Bulk sync error: init not complete 0
Bulk sync - active now standby 0
Bulk sync - Standby not read 0
Transport Down 0
Attempt to initiate bulk sync on active 0
Invalid no response bulk sync timer on active 0
Bulk sync request retry re-queued 0
Bulk sync request retry re-queue failed 0
Bulk sync done re-queued 0
Bulk sync done re-queue failed 0

==== HA standby stat ====
Total received messages 0
Session create requests 0
Session delete requests 0
Session update requests 0
Create NAK sent 0
Inspection policy not found 0
Could not create session 0
Could not create subordinate session 0
New sessions not allowed 0
Could not locate ingress uidb RII 0
Could not locate egress uidb RII 0
RG not configured 0
Could not locate uidb sub-block 0
Invalid zone - no inspection 0
Invalid zone - drop 0
Invalid zone pair 0
Classification failed 0
Classification results missing stats 0
Subflow RG mismatch 0
RG mismatch on create/flow exists 0
Could not find session 0
```

```
Session RG mismatch 0
Session delete miss 0
Session delete RG mismatch 0
Layer 7 data 0
Rcvd bad opcode 0
Msg too short 0
Unsupported msg version 0
Bulk sync requested 0
Bulk sync requested timeout 0
Bulk sync requested failed 0
Bulk Sync msg sent 0
Bulk sync complete 0
Peer not identified 0
Could not allocate msg buffer 0
Could not find VRF 0
Asymmetric routing redirect 0
Asymmetric routing redirect failed - no uidb_sb 0
Asymmetric routing redirect failed - no AR 0
Transport Down 0
Bulk sync failed : no response 0
Existing session removed/replaced 0
Invalid message magic number 0
```

show platform hardware qfp active feature firewall drop all

To display all drop counts, use the **show platform hardware qfp active feature firewall drop all** command in privileged EXEC mode.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.11.1a	This command is supported in Cisco Catalyst SD-WAN

Example

The following example displays all drop counts,.

```
Device#show platform hardware qfp active feature firewall drop all
-----------------------------------------------------------------------------
Drop Reason                                                          Packets
-----------------------------------------------------------------------------
Invalid L4 header                                                          0
Invalid ACK flag                                                           0
Invalid ACK number                                                         0
Invalid TCP initiator                                                      0
SYN with data                                                              0
Invalid window scale option                                                0
Invalid Segment in SYNSENT                                                 0
Invalid Segment in SYNRCVD                                                 0
TCP out of window                                                          0
TCP window overflow                                                        0
TCP extra payload after FIN                                                0
Invalid TCP flags                                                          0
Invalid sequence number                                                    0
Retrans with invalid flags                                                 0
```

```
TCP out-of-order segment                                                 0
SYN flood drop                                                           0
INT ERR:synflood h-tdl alloc fail                                        0
Synflood blackout drop                                                   0
TCP - Half-open session limit exceed                                     0
Too many packet per flow                                                 0
ICMP ERR PKT per flow exceeds                                            0
Unexpect TCP pyld in handshake                                           0
INT ERR:Undefined direction                                              0
SYN inside current window                                                0
RST inside current window                                                0
Stray Segment                                                            0
RST sent to responder                                                    0
ICMP INT ERR:Missing NAT info                                            0
ICMP INT ERR:Fail to get ErrPkt                                          0
ICMP INT ERR:Fail to get Statbk                                          0
ICMP INT ERR:direction undefined                                         0
ICMP PKT rcvd in SCB close st                                            0
Missed IP hdr in ICMP packet                                             0
ICMP ERR PKT:no IP or ICMP                                               0
ICMP ERR Pkt:exceed burst lmt                                            0
ICMP Unreach pkt exceeds lmt                                             0
ICMP Error Pkt invalid sequence                                          0
ICMP Error Pkt invalid ACK                                               0
ICMP Error Pkt too short                                                 0
Exceed session limit                                                     0
Packet rcvd in SCB close state                                           0
Pkt rcvd after CX req teardown                                           0
CXSC not running                                                         0
Zone-pair without policy                                                 0
Same zone without Policy                                                 0
ICMP ERR:Policy not present                                              0
Classification Failed                                                    0
Policy drop:non tcp/udp/icmp                                             0
PAM lookup action drop                                                   0
ICMP Error Packet TCAM missed                                            0
Security policy misconfigure                                             0
INT ERR:Get stat blk failed                                              0
IPv6 dest addr lookup failed                                             0
SYN cookie max dst reached                                               0
INT ERR:syncook d-tbl alloc failed                                       0
SYN cookie being triggered                                               0
Fragment drop                                                            0
Policy drop:classify result                                             11
ICMP policy drop:classify result                                         0
L7 segmented packet not allow                                            0
L7 fragmented packet not allow                                           0
L7 unknown proto type                                                    0
L7 inspection returns drop                                               0
Promote fail due to no zone pair                                         0
Promote fail due to no policy                                            0
Firewall Create Session fail                                             0
Firewall No new session allow                                            0
Not a session initiator                                                  0
Firewall invalid zone                                                   18
Firewall AR standby                                                      0
Firewall no forwarding allow                                             0
Firewall back pressure                                                   0
Firewall LISP hdr restore fail                                           0
Firewall LISP inner pkt insane                                           0
Firewall LISP inner ipv4 insane                                          0
Firewall LISP inner ipv6 insane                                          0
Firewall zone check failed                                               0
Could not register flow with FBD                                         0
```

```
Invalid drop event                                                      0
Invalid drop event                                                      0
Invalid drop event                                                      0
Invalid ICMP sequence number                                            0
UDP - Half-open session limit exceed                                    0
ICMP - Half-open session limit exceed                                   0
AVC Policy drop:classify result                                         0
Could not aquire session lock                                           0
No Zone-pair found                                                      0
```

show platform hardware qfp active feature bridge-domain datapath sdwan-flood-list

To display information about flood list of a bridge domain in the data plane, use the **show platform hardware qfp active feature bridge-domain datapath sdwan-flood-list** command in privileged EXEC (#).

show platform hardware qfp active feature bridge-domain datapath [*bridge-domain-id*] [**sdwan-flood-list**]

Syntax Description

bridge-domain-id	Displays the L2VPN status for a specific L2VPN SDWAN instance. Specify vc-id the value. Range:1 to 65531
sdwan-flood-list	Displays Virtual Circuit (VC) ID that is used to identify a particular bridge domain. Specify vc-id the value. Range:1 to 65531

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.14.1a	This command was introduced.

Examples

The following sample output displays the Cisco SD-WAN flood list for a bridge-domain in data plane:

```
Device# show platform hardware qfp active feature bridge-domain datapath 13 sdwan-flood-list
l2vpn:13 sdwan-olist:0xe0d36d80

Flood List for Bridge Domain 13:
 BDI13
 SDWAN oce_base:0xe1961a40 intf:SFI13.13.4210709 flags:
 SDWAN oce_base:0xe1961680 intf:SFI13.13.4210709 flags:
```

show platform packet-trace

To view detailed packet tracer statistics for a specified trace ID or summary statistics for all the filtered packets, for up to 1024 records, use the **show platform packet-trace** command in privileged EXEC mode.

show platform packet-trace [**details** *trace-id*] [**summary**]

Syntax Description

details *trace-id*	(Optional) Displays packet trace details for the specified trace ID.
summary	(Optional) Displays packet trace statistics for the specified packets.
trace-id	(Optional) Displays packet statistics for the specified trace-id. Range: 0 to 1023.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.8.1a	This command was introduced.

Example

The following example displays the packet trace summary.

```
Device# show platform packet-trace summary

Pkt   Input                Output               State  Reason
0     INJ.12               Gi2                  FWD
1     Gi2                  internal0/0/rp:0     PUNT   5   (CLNS IS-IS Control)
2     INJ.1                Gi2                  FWD
3     INJ.1                Gi2                  FWD
4     Gi2                  internal0/0/rp:0     PUNT   5   (CLNS IS-IS Control)
5     Gi2                  internal0/0/rp:0     PUNT   5   (CLNS IS-IS Control)
6     INJ.1                Gi2                  FWD
7     INJ.1                Gi2                  FWD
8     Gi2                  internal0/0/rp:0     PUNT   5   (CLNS IS-IS Control)
9     Gi2                  internal0/0/rp:0     PUNT   5   (CLNS IS-IS Control)
10    Gi2                  internal0/0/rp:0     PUNT   5   (CLNS IS-IS Control)
11    INJ.1                Gi2                  FWD
12    Gi2                  internal0/0/rp:0     PUNT   5   (CLNS IS-IS Control)
13    INJ.1                Gi2                  FWD
14    INJ.1                Gi2                  FWD
```

The following is the sample output for the show packet trace details command, which is displayed for the specified trace ID 0.

```
Device# show platform packet-trace packet 0

Packet: 0           CBUG ID: 4321
Summary
  Input     : GigabitEthernet2
  Output    : GigabitEthernet3
  State     : FWD
  Timestamp
    Start   : 1124044721695603 ns (09/20/2022 01:47:28.531049 UTC)
    Stop    : 1124044722142898 ns (09/20/2022 01:47:28.531497 UTC)
Path Trace
  Feature: IPV4(Input)
    Input       : GigabitEthernet2
    Output      : <unknown>
    Source      : 10.10.10.10
    Destination : 20.20.20.20
    Protocol    : 1 (ICMP)
  Feature: DEBUG_COND_INPUT_PKT
    Entry       : Input - 0x814670b0
    Input       : GigabitEthernet2
    Output      : <unknown>
    Lapsed time : 600 ns
  Feature: IPV4_INPUT_DST_LOOKUP_ISSUE
    Entry       : Input - 0x81494d2c
    Input       : GigabitEthernet2
    Output      : <unknown>
    Lapsed time : 1709 ns
  Feature: IPV4_INPUT_ARL_SANITY
    Entry       : Input - 0x814690e0
    Input       : GigabitEthernet2
    Output      : <unknown>
    Lapsed time : 1274 ns
  Feature: IPV4_INPUT_DST_LOOKUP_CONSUME
    Entry       : Input - 0x81494d28
    Input       : GigabitEthernet2
    Output      : <unknown>
    Lapsed time : 269 ns
  Feature: IPV4_INPUT_FOR_US_MARTIAN
    Entry       : Input - 0x81494d34
    Input       : GigabitEthernet2
    Output      : <unknown>
    Lapsed time : 384 ns
  Feature: DEBUG_COND_APPLICATION_IN
    Entry       : Input - 0x814670a0
    Input       : GigabitEthernet2
    Output      : <unknown>
    Lapsed time : 107 ns
  Feature: DEBUG_COND_APPLICATION_IN_CLR_TXT
    Entry       : Input - 0x8146709c
    Input       : GigabitEthernet2
    Output      : <unknown>
    Lapsed time : 36 ns
  Feature: IPV4_INPUT_LOOKUP_PROCESS
    Entry       : Input - 0x81494d40
    Input       : GigabitEthernet2
    Output      : GigabitEthernet3
    Lapsed time : 38331 ns
  Feature: IPV4_INPUT_IPOPTIONS_PROCESS
    Entry       : Input - 0x81495258
    Input       : GigabitEthernet2
    Output      : GigabitEthernet3
    Lapsed time : 259 ns
  Feature: IPV4_INPUT_GOTO_OUTPUT_FEATURE
    Entry       : Input - 0x8146ab58
```

```
    Input       : GigabitEthernet2
    Output      : GigabitEthernet3
    Lapsed time : 9485 ns
  Feature: IPV4_VFR_REFRAG
    Entry       : Output - 0x81495c6c
    Input       : GigabitEthernet2
    Output      : GigabitEthernet3
    Lapsed time : 520 ns
  Feature: IPV6_VFR_REFRAG
    Entry       : Output - 0x81496600
    Input       : GigabitEthernet2
    Output      : GigabitEthernet3
    Lapsed time : 296 ns
  Feature: MPLS(Output)
    Input       : GigabitEthernet2
    Output      : GigabitEthernet3
    Label Stack Entry[1]: 0x03e850fe
      StackEnd:NO, TTL:254, EXP:0, Label:16005, is SDWAN:NO
    Label Stack Entry[2]: 0x000121fe
      StackEnd:YES, TTL:254, EXP:0, Label:18, is SDWAN:NO
  Feature: MPLS_OUTPUT_ADD_LABEL
    Entry       : Output - 0x8145e130
    Input       : GigabitEthernet2
    Output      : GigabitEthernet3
    Lapsed time : 29790 ns
  Feature: MPLS_OUTPUT_L2_REWRITE
    Entry       : Output - 0x812f4724
    Input       : GigabitEthernet2
    Output      : GigabitEthernet3
    Lapsed time : 23041 ns
  Feature: MPLS_OUTPUT_FRAG
    Entry       : Output - 0x8149ae5c
    Input       : GigabitEthernet2
    Output      : GigabitEthernet3
    Lapsed time : 785 ns
  Feature: MPLS_OUTPUT_DROP_POLICY
    Entry       : Output - 0x8149ebdc
    Input       : GigabitEthernet2
    Output      : GigabitEthernet3
    Lapsed time : 14697 ns
  Feature: MARMOT_SPA_D_TRANSMIT_PKT
    Entry       : Output - 0x814ac56c
    Input       : GigabitEthernet2
    Output      : GigabitEthernet3
    Lapsed time : 45662 ns
Packet Copy In
  00505683 d54f0050 56830863 08004500 00641018 0000ff01 6f450a0a 0a0a1414
  14140800 3839001c 00000000 00005b3a eabaabcd abcdabcd abcdabcd abcdabcd
Packet Copy Out
  00505683 d4900050 5683429a 884703e8 50fe0001 21fe4500 00641018 0000fe01
  70450a0a 0a0a1414 14140800 3839001c 00000000 00005b3a eabaabcd abcdabcd
```

show platform packet-trace fia-statistics

To view Feature Invocation Array (FIA) statistics about a feature, use the **show platform packet-trace fia-statistics** command in the privileged EXEC mode.

show platform packet-trace fia-statistics

Command Default None

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.11.1a	This command was introduced.

Example

The following example displays FIA statistics on Cisco IOS XE Catalyst SD-WAN devices.

```
Device# show platform packet-trace fia-statistics

Feature                                          Count  Min(ns)   Max(ns)   Avg(ns)
-------------------------------------------------------------------------------------
INTERNAL_TRANSMIT_PKT_EXT                           66     4720     28400     13333
MARMOT_SPA_D_TRANSMIT_PKT_EXT                       16     4560     16920     11955
L2_SVI_OUTPUT_BRIDGE_EXT                             1     3640      3640      3640
INTERNAL_INPUT_GOTO_OUTPUT_FEATURE_EXT              16     1680      3880      2755
IPV4_INPUT_LOOKUP_PROCESS_EXT                        1     2720      2720      2720
IPV4_OUTPUT_L2_REWRITE_EXT                           1     2240      2240      2240
IPV4_OUTPUT_DROP_POLICY_EXT                          4     1040      2880      2050
IPV4_INTERNAL_DST_LOOKUP_CONSUME_EXT                 1     1960      1960      1960
SSLVPN_INJECT_TX_MSG_EXT                            15      600      2440      1746
IPV4_INTERNAL_FOR_US_EXT                             1     1560      1560      1560
LAYER2_OUTPUT_QOS_EXT                               63      280      2480      1537
LAYER2_OUTPUT_DROP_POLICY_EXT                       78      120      3120      1525
LAYER2_INPUT_LOOKUP_PROCESS_EXT                     15      280      2240      1312
UPDATE_ICMP_PKT_EXT                                  1     1280      1280      1280
DEBUG_COND_MAC_EGRESS_EXT                            3      840      1160       973
IPV4_INTERNAL_INPUT_SRC_LOOKUP_CONSUME_EXT           1      960       960       960
IPV4_PREF_TX_IF_SELECT_EXT                           1      800       800       800
DEBUG_COND_OUTPUT_PKT_EXT                           66       80      1640       707
IPV4_INTERNAL_ARL_SANITY_EXT                         3      240       960       666
IPV4_INTERNAL_INPUT_SRC_LOOKUP_ISSUE_EXT             1      640       640       640
IPV4_VFR_REFRAG_EXT                                  5      320       920       640
EVC_EFP_VLAN_TAG_ATTACH_EXT                         15       80      1040       629
L2_SVI_OUTPUT_GOTO_OUTPUT_FEATURE_EXT                1      520       520       520
LAYER2_VLAN_INJECT_EXT                              15      120       760       504
L2_ES_OUTPUT_PRE_TX_EXT                             16        0      1000       502
DEBUG_COND_APPLICATION_IN_EXT                        1      480       480       480
DEBUG_COND_APPLICATION_OUT_CLR_TXT_EXT               3       80       720       426
DEBUG_COND_INPUT_PKT_EXT                            16       80       880       417
IPV4_OUTPUT_FRAG_EXT                                 1      360       360       360
DEBUG_COND_APPLICATION_IN_CLR_TXT_EXT                1      320       320       320
DEBUG_COND_APPLICATION_OUT_EXT                       3      240       280       266
LFTS_INJECT_PKT_EXT                                 16       40       480       250
LAYER2_BRIDGE_INJECT_EXT                            15       40       560       234
```

show platform software common-classification f0 tag

To display the tag information from forwarding manager on forwarding plane (FMAN-FP), use the **show platform software common-classification f0 tag** command in privileged EXEC mode.

show platform software common-classification f0 tag { *all* | *tag-id* { **app-list** | **prefix-list** | **sets** | **summary** } }

Syntax Description

f0	Embedded-Service-Processor slot 0.
all	All tags.
id	Tag ID. Range: 1 to 4294967295.
summary	Displays the summary information for one particular tag-instance. Based on this show output, user can further display prefix-list or app-list or sets for this tag-instance.
prefix-list	Prefix list type members.
app-list	App ID list type members.
sets	Tag rule sets.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	This command was introduced.

Usage Guidelines

The **show platform software common-classification fo tag** command is used for troubleshooting purposes.

Examples

The following is a sample output from the **show platform software common-classification fo tag** command displaying the tag information from a forwarding manager on a forwarding plane (FMAN-FP):

```
Device# show platform software common-classification F0 tag all
Total Number of TAGs: 9
tag id       tag name              tag type     num clients  num sets     num member types
  total members
-------------------------------------------------------------------------------------------------
900          special_TAG7          Per Type OR  0            2            1
  2
10000        DP_V4_TAG1            Per Type OR  1            1            1
  1
11000        DP_V4_TAG2            Per Type OR  1            2            1
  2
12000        DP_V4_TAG3            Per Type OR  1            6            1
  6
20000        DP_V6_TAG4            Per Type OR  1            1            1
  1
21000        DP_V6_TAG5            Per Type OR  1            2            1
  2
50000        APP_webex_TAG8        Per Type OR  1            1            1
  1
60000        APP_facebook_TAG9     Per Type OR  1            1            1
  1
70000        APP_office_TAG10      Per Type OR  1            2            1
  2

Device# show platform software common-classification f0 tag 1 summary
TAG ID: 1
TAG TYPE: Per Type OR
```

```
TAG Name: net1
Is Dummy: F

client data:
  client id     client name
  ---------------------------------
  166           SDWAN

member data:
  Prefix List           6
  App List              3
```

```
Device# show platform software common-classification f0 tag 1 prefixList
 member details:
  member detail type    member id     member data
  ------------------------------------------------
  IPv4 Prefix List      65537         100
  IPv6 Prefix List      65538         101
  IPv4 Prefix List      65540         103
  IPv6 Prefix List      65541         104
  IPv6 Prefix List      65544         107
  IPv4 Prefix List      65546         109
```

```
Device# show platform software common-classification f0 tag 1 appList
 member details:
  member detail type    member id     member data
  ------------------------------------------------
  App List              65539         102
  App List              65542         105
  App List              65545         108
```

```
Device# show platform software common-classification f0 tag 1 set
Total Number of SETs: 18
  Set ID        member detail type    member id     member data
  ------------------------------------------------------------
  1             IPv4 Prefix List      65537         100
  1             App List              65539         102
  2             IPv4 Prefix List      65537         100
  2             App List              65542         105
  3             IPv4 Prefix List      65537         100
  3             App List              65545         108
  4             IPv6 Prefix List      65538         101
  4             App List              65539         102
  5             IPv6 Prefix List      65538         101
```

show platform software cpu alloc

To view the CPU cores allocated on a device, use the **show platform software cpu alloc** command in privileged EXEC mode.

show platform software cpu alloc

Command Modes

privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	This command was introduced.

Example

Following is the sample output from the **show platform software cpu alloc** command and shows the core allocation on a Cisco Catalyst 8000V instance with six cores:

```
Device# show platform software cpu alloc

CPU alloc information:


  Control plane cpu alloc: 0


  Data plane cpu alloc: 4-5


  Service plane cpu alloc: 1-3


  Template used: CLI-service_plane_heavy
```

This example shows the core allocation on a Cisco Catalyst 8000V instance with eight cores:

```
Device# show platform software cpu alloc

CPU alloc information:


  Control plane cpu alloc: 0


  Data plane cpu alloc: 6-7


  Service plane cpu alloc: 1-5


  Template used: CLI-service_plane_heavy
```

This example shows the core allocation on a Cisco Catalyst 8000V instance with 12 cores:

```
Device# show platform software cpu alloc

CPU alloc information:


  Control plane cpu alloc: 0


  Data plane cpu alloc: 9-11


  Service plane cpu alloc: 1-8
```

```
  Template used: CLI-service_plane_heavy
```

This example shows the core allocation on a Cisco Catalyst 8000V instance with 16 cores:

```
Device# show platform software cpu alloc

CPU alloc information:


  Control plane cpu alloc: 0


  Data plane cpu alloc: 12-15


  Service plane cpu alloc: 1-11


  Template used: CLI-service_plane_heavy
```

show platform software ipsec fp active flow

To display information about active instances of IPsec flows, 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. Range: 0 - 4294967295

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.15.1a	This command is supported in Cisco Catalyst SD-WAN. Starting from Cisco IOS XE Catalyst SD-WAN Release 17.15.1a, the output of this command was modified with an increased flow ID range. Range: 0 - 4294967295

Usage Guidelines

For usage guidelines, see the Cisco IOS XE show platform software ipsec fp active flow command.

The following is sample output from the **show platform software ipsec fp active flow** command for flow ID 2146:

```
Device# show platform software ipsec fp active flow identifier 2146
========== Flow id: 2146
              mode: transport
         direction: outbound
          protocol: esp
               SPI: 0x000102
     local IP addr: 213.103.103.0
    remote IP addr: 170.132.2.2
  crypto device id: 0
     crypto map id: 1043
            SPD id: 3
        QFP SPD id: 3
   ACE line number: 1
     QFP SA handle: 3024
   QFP SA PPE addr: 0x83af0210
IOS XE interface id: 56
     interface name: Tunnel2
       use path MTU: 1480
  Crypto SA ctx id: 0x000000006d01f7aa
            cipher: AES-256 GCM (AAD with AH-NO-ID)
              auth: null
 initial seq.number: 0
      timeout, mins: 0
              flags: exp time;exp traffic;NAT-T;NAT orig address;
Time limits

    soft limit(sec): 0
    hard limit(sec): 809108523
Traffic limits

     soft limit(kB): 0
     hard limit(kB): 17448352331316854784
no expiry sent

     total soft expiry notification: 0
     total hard expiry notification: 0
     total rekey request received: 0
     total rekey request updated : 0
     total rekey request skipped : 0
-- NAT-T

     local UDP port: 12346
    remote UDP port: 12346
    original IP addr: 170.132.2.2
     inline_tagging: DISABLED
 ext_ar_window_size: 0
Classifier: range

   src IP addr low: 213.103.103.0
  src IP addr high: 213.103.103.0
   dst IP addr low: 170.132.2.2
  dst IP addr high: 170.132.2.2
      src port low: 12346
     src port high: 12346
      dst port low: 12346
     dst port high: 12346
      protocol low: 0
     protocol high: 255
------------- Statistics

            octets(delta): 0
```

```
      total octets(delta): 10664523917613334528
           packets(delta): 106058
   dropped packets(delta): 0
      replay drops(delta): 0
      auth packets(delta): 0
        auth fails(delta): 0
 encrypted packets(delta): 106058
     encrypt fails(delta): 0
---------- End statistics

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

         cpp aom id: 28463
         cgm aom id: 28462
          n2 aom id: 28459
          if aom id: 0
```

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

Table 29: 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.

Field	Description
initial seq.number	Initial sequence number.
timeout, mins	Timeout, in minutes.
flags	Flags set for the packet flow.
Peer Flow handle	Peer flow identifier.
Time limits soft limit	Minimum permissible time limit.
Time limits hard limit	Maximum permissible time limit.
Traffic limits soft limit	Minimum permissible traffic limit.
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.

Field	Description
dst port high	Highest range of the destination port.
protocol low	Starting range of the protocol.
protocol high	Highest range of the protocol.
octets	Number of octets in the packet.
total octets	Total number of octets.
packets	Number of packets.
dropped packets	Number of packets dropped.
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.

show platform software memory

To display memory information for a specified process, use the **show platform software memory** command in privileged EXEC mode or diagnostic mode.

show platform software memory [**database**] *process slot* **alloc** *parameter* [**brief**]

Syntax Description

database	(Optional) Displays database memory information for the specified process.

process	A message process. Valid values: • cfgmgr: Configuration manager process • cxpd: Cloud Express process used for Microsoft Office 365 • dbgd: Speed test process • fpmd: Forwarding Policy manager process • ftm: Forwarding table manager process • ompd: Overlay management protocol daemon process • ttmd: Tunnel manager process • vdaemon: vDeamon process
slot	Hardware slot from which process messages must be logged. Valid values: • rp active: Active RP • r0: Slot 0
statistics	Message statistics. Valid values: • callsite: CallSite display • type component: Component-based memory statistics • type data: Data type based memory statistics • backtrace: Backtrace display
brief	(Optional) Displays abbreviated output.

Command Default

This command has no default behavior.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Support was added for Cisco Catalyst SD-WAN processes.

Usage Guidelines

You can use the **debug platform software memory ftm rp active alloc** command in privileged EXEC mode to start, stop, or clear callsite or backtrace tracking.

Example

The following example shows how to display software platform memory for active RPs at CallSites:

```
Device# show platform software memory ftm rp active alloc callsite
callsite: 1079865346, thread_id: 7921
allocs: 10, frees: 1, alloc_bytes: 1239, free_bytes: 40, call_diff: 9, byte_diff: 1199
callsite: 276369408, thread_id: 7921
```

```
allocs: 1, frees: 0, alloc_bytes: 16960, free_bytes: 0, call_diff: 1, byte_diff: 16960
callsite: 279023616, thread_id: 7921
allocs: 1, frees: 0, alloc_bytes: 57360, free_bytes: 0, call_diff: 1, byte_diff: 57360
callsite: 1079865349, thread_id: 7921
allocs: 3, frees: 2, alloc_bytes: 4560, free_bytes: 3040, call_diff: 1, byte_diff: 1520
callsite: 1347823618, thread_id: 7921
allocs: 1, frees: 0, alloc_bytes: 1536, free_bytes: 0, call_diff: 1, byte_diff: 1536
callsite: 1347823619, thread_id: 7921
allocs: 1, frees: 0, alloc_bytes: 40, free_bytes: 0, call_diff: 1, byte_diff: 40
callsite: 1347823620, thread_id: 7921
allocs: 1, frees: 0, alloc_bytes: 8208, free_bytes: 0, call_diff: 1, byte_diff: 8208
callsite: 279746563, thread_id: 7921
allocs: 1, frees: 0, alloc_bytes: 336, free_bytes: 0, call_diff: 1, byte_diff: 336
callsite: 279746564, thread_id: 7921
allocs: 1, frees: 0, alloc_bytes: 57384, free_bytes: 0, call_diff: 1, byte_diff: 57384
callsite: 2156775457, thread_id: 7921
allocs: 1, frees: 0, alloc_bytes: 1688, free_bytes: 0, call_diff: 1, byte_diff: 1688
callsite: 1348148375, thread_id: 7921
allocs: 1, frees: 0, alloc_bytes: 40, free_bytes: 0, call_diff: 1, byte_diff: 40
callsite: 3492619269, thread_id: 7921
allocs: 1, frees: 0, alloc_bytes: 32, free_bytes: 0, call_diff: 1, byte_diff: 32
callsite: 1348148376, thread_id: 7921
allocs: 1, frees: 0, alloc_bytes: 35, free_bytes: 0, call_diff: 1, byte_diff: 35
callsite: 1348148377, thread_id: 7921
allocs: 1, frees: 0, alloc_bytes: 40, free_bytes: 0, call_diff: 1, byte_diff: 40
callsite: 3492619268, thread_id: 7921
allocs: 1, frees: 0, alloc_bytes: 88, free_bytes: 0, call_diff: 1, byte_diff: 88
```

The following example shows how to display component-based memory statistics for active RPs:

```
Device# show platform software memory ftm rp active alloc type component
Module: vista
   Allocated: 541300, Requested: 540292, Overhead: 1008
   Allocations: 18, Null Allocations: 0, Frees: 0
 Module: bmalloc
   Allocated: 167591, Requested: 160647, Overhead: 6944
   Allocations: 940, Null Allocations: 0, Frees: 816
 Module: systime
   Allocated: 72, Requested: 16, Overhead: 56
   Allocations: 1, Null Allocations: 0, Frees: 0
 Module: tdllib_c
   Allocated: 1584, Requested: 1304, Overhead: 280
   Allocations: 6, Null Allocations: 0, Frees: 1
 Module: chasfs
   Allocated: 13046, Requested: 12542, Overhead: 504
   Allocations: 19, Null Allocations: 0, Frees: 10
 Module: pcohort
   Allocated: 654, Requested: 206, Overhead: 448
   Allocations: 13, Null Allocations: 0, Frees: 5
 Module: vs_lock
   Allocated: 840, Requested: 672, Overhead: 168
   Allocations: 3, Null Allocations: 0, Frees: 0
 Module: flashlib
   Allocated: 7920, Requested: 7864, Overhead: 56
   Allocations: 1, Null Allocations: 0, Frees: 0
 Module: default
   Allocated: 4450977, Requested: 4243329, Overhead: 207648
   Allocations: 32752, Null Allocations: 0, Frees: 29044
 Module: lib
   Allocated: 0, Requested: 0, Overhead: 0
   Allocations: 6, Null Allocations: 0, Frees: 6
```

show platform software nat66 fp active

To verify the NAT66 forwarding processor information, use the **show platform software nat66 fp active prefix-translation** command in privileged EXEC mode.

show platform software nat66 fp active { configuration | interface | prefix-translation | statistics }

Syntax Description

configuration	Displays configuration information for the forwarding processor.
interface	Displays interface information.
prefix-translation	Displays prefix-translation information.
statistics	Displays statistics from the forwarding processor.

Command Default No NAT66 forwarding processor information is displayed.

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Examples The following is a sample output from the **show platform software nat66 fp active** command:

```
Device# show platform software nat66 fp active interface
NAT66 Interface:
IF Handle 7:
  Enabled TRUE , Inside FALSE
IF Handle 10:
  Enabled TRUE , Inside FALSE
```

show platform software nat66 rp active

To verify the NAT66 route processor (RP) information, use the **show platform software nat66 rp active** command in privileged EXEC mode.

show platform software nat66 rp active { interface | prefix-translation }

Syntax Description

interface	Displays interface information.
prefix-translation	Displays prefix-translation information.

Command Default No NAT66 route processor information is displayed.

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Examples

The following is a sample output from the **show platform software nat66 rp active** command:

```
Device# show platform software nat66 rp active interface


NAT66 Interface:
IF Handle 7:
  Enabled TRUE , Inside FALSE
IF Handle 10:
Enabled TRUE , Inside FALSE
```

show platform software sdwan ftmd bridge-domain

To display the current configuration and status of all bridge domains on the Cisco Catalyst SD-WAN Forwarding and Timing Module Daemon (FTMD), use the **show platform software sdwan ftmd bridge-domain** command in privileged EXEC mode.

show platform software sdwan ftmd bridge-domain [*bridge-domain-id*]

Syntax Description

bridge-domain-id	Lists the bridge-domain information in FTM for a specific bridge domain.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.14.1a	This command was introduced.

Usage Guidelines

Use these commands only on Cisco IOS XE Catalyst SD-WAN devices.

The following is a sample output that shows all bridge domains:

```
Device# show platform software sdwan ftmd bridge-domain
L2vpn Bridge-domain 12 Table:
  sdwan efp dpidx: 4210708(0x404014)
  Label: 1004 lbl-nhop-id: 196611 (binosId=0xf830003f)
  Bum Label: 1005 bum-lbl-nhop-id: 196612 (binosId=0xf830004f)
  Remote Site Table(1 entries in total):
    remote-site-id: 501 sla-nhop-id: 29 (binosId=0xf80001df)
L2vpn Bridge-domain 13 Table:
  sdwan efp dpidx: 4210709(0x404015)
  Label: 1006 lbl-nhop-id: 196613 (binosId=0xf830005f)
  Bum Label: 1007 bum-lbl-nhop-id: 196614 (binosId=0xf830006f)
```

```
  Remote Site Table(2 entries in total):
    remote-site-id: 501 sla-nhop-id: 30 (binosId=0xf80001ef)
remote-site-id: 503 sla-nhop-id: 33 (binosId=0xf800021f)
```

The following is a sample output that shows a specific bridge-domain:

```
Device# show platform software sdwan ftmd bridge-domain 13
L2vpn Bridge-domain 13 Table:
  sdwan efp dpidx: 4210709(0x404015)
  Label: 1006 lbl-nhop-id: 196613 (binosId=0xf830005f)
  Bum Label: 1007 bum-lbl-nhop-id: 196614 (binosId=0xf830006f)
  Remote Site Table(2 entries in total):
    remote-site-id: 501 sla-nhop-id: 30 (binosId=0xf80001ef)
    remote-site-id: 503 sla-nhop-id: 33 (binosId=0xf800021f)
```

show platform software sdwan multicast active-sources vrf

To view the entries for a specific Cisco IOS XE SD-WAN multicast active sources on VRF node, use the **show platform software sdwan multicast active-sources vrf** command in privileged EXEC mode.

show platform software sdwan multicast active-sources vrf *vrf-id*

Syntax Description

vrf *vrf-id*	Displays hardware entry information that is based on the specified virtual routing and forwarding (VRF) ID. Valid values are from 1 to 65530.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.15.1a	This command was introduced.

Usage Guidelines

Use this command to view hardware information based on the specified VRF value, and to verify that system IP addresses are configured with spt-only mode.

Examples

The following is sample output from the **show platform software sdwan multicast active-sources vrf** command:

```
Device# show platform software sdwan multicast active-sources vrf 1

Multicast SDWAN Overlay Received Source-Active Routes:
  (10.0.0.0, 255.0.0.0) src-orig: 192.168.0.0, next-hop: 192.168.255.254
      src-orig-count: 1, rp-addr: 10.0.0.1
```

show platform software sdwan multicast remote-nodes vrf

To view the entries for a specific Cisco IOS XE SD-WAN multicast remote node, use the **show platform software sdwan multicast remote-nodes vrf** command in privileged EXEC mode.

show platform software sdwan multicast remote-nodes vrf *vrf-id*

Syntax Description

vrf *vrf-id*	Displays hardware entry information that is based on the specified virtual routing and forwarding (VRF) ID. Valid values are from 1 to 65530.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

Use this command to view hardware information based on the specified VRF value, and to verify that system IP addresses are configured with spt-only mode.

Examples

The following is sample output from the **show platform software sdwan multicast remote-nodes vrf** command:

```
Device# show platform software sdwan multicast remote-nodes vrf 1

Multicast SDWAN Overlay Remote Nodes (* - Replicator):
                                          Received                Sent
                SPT-Only                (X,G)      (S,G)      (X,G)      (S,G)
System IP       Mode         Label   Join/Prune Join/Prune Join/Prune Join/Prune
172.16.255.11   Yes          1003        0/0        0/0        0/0        0/0
172.16.255.14   Yes          1003        0/0        0/0        1/0      10/10
172.16.255.16   Yes          1003        0/0        0/0        0/0        0/0
172.16.255.21   Yes          1003        0/0        0/0        0/0        0/0
```

show platform software sdwan qos

To display Quality of Service (QoS) information, such as QoS configuration, policies, and statistics, use the **show platform software sdwan qos** command in privileged EXEC mode.

show platform software sdwan qos
adapt { **history** { **Dialer** *interface-number* | **GigabitEthernet** *gigabitethernet-interface-number* | **Tunnel** *tunnel-interface-number* | **all** } | **stats** } | **policy** | **target** | **template** | **summary**

Syntax Description

adapt	Show adaptive QoS information. • **history**: Show adaptive QoS history information. • **Dialer** *interface-number*: Dialer interface number Range: 0 through 255 • **GigabitEthernet** *gigabitethernet-interface-number*: GigabitEthernet interface number Range: 1 through 32 • **Tunnel** *tunnel-interface-number*: Tunnel interface number Range: 1 through 2147483647 • **all**: All adaptive QoS history information, including dialer, GigabitEthernet, and tunnel information. • **stats**: Show adaptive QoS statistics information.
policy	Show session QoS policy-map information.
target	Show session QoS target information.
template	Show session QoS template information.
summary	Show a summary of session QoS database information.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.13.1a	Added the **summary** and **sessions** keywords.

Example

Confirm the count of sessions, policies, WAN interfaces, and adaptive QoS sessions.

```
Device# show platform software sdwan qos summary
============ Session QoS Summary Database ============
maximum sdwan qos session support : 2000
number of qos wan interfaces : 2
number of sdwan session qos installed : 2000
number of adaptive qos session installed : 0
number of sdwan policy-map instances : 400
```

Verifies the count of reuse policies. Count of reuse policies refers to the number of policies that are being reused across the network.

```
Device# show platform software sdwan qos policy
============ Session QoS Policy Database ============
policy bandwidth remaining-ratio template sessions
SDWANPolicy4210705 101600000 10 qos_policy_4class 5
```

```
SDWANPolicy4210707 101800000 10 qos_policy_4class 5
SDWANPolicy4210709 307802000 30 qos_policy_4class 5
SDWANPolicy4210711 308002000 30 qos_policy_4class 5
SDWANPolicy4210713 308202000 30 qos_policy_4class 5
SDWANPolicy4210715 308402000 30 qos_policy_4class 5
SDWANPolicy4210717 308602000 30 qos_policy_4class 5
SDWANPolicy4210719 308802000 30 qos_policy_4class 5
SDWANPolicy4210721 309802000 30 qos_policy_4class 5
```

Provides the number of sessions allowed per WAN interface.

```
Device# show platform software sdwan qos template
============ Session QoS Template Database ============
interface name interface id QoS template name sessions
GigabitEthernet1 7 qos_policy_4class 1000
GigabitEthernet4 10 qos_policy_4class 1000
```

Provides information about all the session details.

```
Device# show platform software sdwan qos target
============ Session QoS Target Database ============
src-addr               dst-addr            sport   dport   proto remote-tloc    dummy-intf
           tunnel         policy               bandwidth
10.0.0.8               192.0.2.254            12346   12346   IPSEC 10.0.0.6
SDWANSession4212705   Tunnel1        SDWANPolicy4212007    203401
10.0.0.8               192.0.2.254            12346   12346   IPSEC 10.0.0.6
SDWANSession4212707   Tunnel1        SDWANPolicy4211995    208801
10.0.0.8               192.0.2.254            12346   12346   IPSEC 10.0.0.6
SDWANSession4212709   Tunnel1        SDWANPolicy4211937    206001
10.0.0.8               192.0.2.254            12346   12346   IPSEC 10.0.0.6
SDWANSession4212711   Tunnel1        SDWANPolicy4211939    206201
10.0.0.8               192.0.2.254            12346   12346   IPSEC 10.0.0.6
SDWANSession4212713   Tunnel1        SDWANPolicy4211941    206401
10.0.0.8               192.0.2.254            12346   12346   IPSEC 10.0.0.6
SDWANSession4212715   Tunnel1        SDWANPolicy4211961    204001
10.0.0.8               192.0.2.254            12346   12346   IPSEC 10.0.0.6
SDWANSession4212717   Tunnel1        SDWANPolicy4211973    204201
```

show policy-firewall config

To validate the configured zone based firewall, use the **show policy-firewall config** command in user EXEC or privileged EXEC mode command in user EXEC or privileged EXEC mode.

show policy-firewall config

Command Default

None

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

The following sample outputs displays the configured firewall policy.

```
Device# show policy-firewall config
Zone-pair              : ZP_SRC_INTF1_DIA_INTF_TEST
Source Zone            : SRC_INTF1
  Member Interfaces:
    GigabitEthernet3.101
Destination Zone       : DIA_INTF
  Member Interfaces:
    GigabitEthernet1
    GigabitEthernet2
    GigabitEthernet4
Service-policy inspect : TEST-opt
  Class-map : TEST-seq-1-cm_ (match-all)
   Match access-group name TEST-seq-Rule_1-acl_
  Action : inspect
   Parameter-map : Default
  Class-map : TEST-seq-11-cm_ (match-all)
   Match access-group name TEST-seq-Rule_2-acl_
  Action : inspect
   Parameter-map : Default
  Class-map : class-default (match-any)
   Match any
  Action : drop log
   Parameter-map : Default
```

show policy-map interface Port-channel

To monitor and troubleshoot Quality of Service (QoS) issues on a port-channel interface, use the **show policy-map interface Port-channel** command in privileged EXEC mode.

show policy-map interface Port-channel

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.13.1a	This command is supported for Cisco Catalyst SD-WAN.

Examples

The following is a sample output from the **show policy-map interface Port-channel** command that is used to monitor and troubleshoot Quality of Service (QoS) issues on a port channel interface:

```
Device# show policy-map interface Port-channel 1
Port-channel1

  Service-policy output: shape_Port-channel1

    Class-map: class-default (match-any)
      121 packets, 20797 bytes
      5 minute offered rate 2000 bps, drop rate 0000 bps
      Match: any
      Queueing
      queue limit 416 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 121/20797
      shape (average) cir 100000000, bc 400000, be 400000
      target shape rate 100000000
```

```
Service-policy : qos_template

  queue stats for all priority classes:
    Queueing
    priority level 1
    queue limit 512 packets
    (queue depth/total drops/no-buffer drops) 0/0/0
    (pkts output/bytes output) 121/20797

  Class-map: Critical (match-any)
    121 packets, 20797 bytes
    5 minute offered rate 2000 bps, drop rate 0000 bps
    Match: qos-group 0
    police:
        rate 15 %
        rate 15000000 bps, burst 468750 bytes
      conformed 121 packets, 20797 bytes; actions:
        transmit
      exceeded 0 packets, 0 bytes; actions:
        drop
      conformed 2000 bps, exceeded 0000 bps
    Priority: Strict, b/w exceed drops: 0

    Priority Level: 1

  Class-map: Business (match-any)
    0 packets, 0 bytes
    5 minute offered rate 0000 bps, drop rate 0000 bps
    Match: qos-group 1
    Queueing
    queue limit 416 packets
    (queue depth/total drops/no-buffer drops) 0/0/0
    (pkts output/bytes output) 0/0
    bandwidth remaining 55%

  Class-map: Best-Effort (match-any)
    0 packets, 0 bytes
    5 minute offered rate 0000 bps, drop rate 0000 bps
    Match: qos-group 2
    Queueing
    queue limit 416 packets
    (queue depth/total drops/no-buffer drops) 0/0/0
    (pkts output/bytes output) 0/0
    bandwidth remaining 10%

  Class-map: Bulk (match-any)
    0 packets, 0 bytes
    5 minute offered rate 0000 bps, drop rate 0000 bps
    Match: qos-group 3
    Queueing
    queue limit 416 packets
    (queue depth/total drops/no-buffer drops) 0/0/0
    (pkts output/bytes output) 0/0
    bandwidth remaining 20%

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

    queue limit 416 packets
    (queue depth/total drops/no-buffer drops) 0/0/0
    (pkts output/bytes output) 0/0
```

show processes cpu platform

To view utilization of the individual control, data, and service planes, use the **show processes cpu platform** command in privileged EXEC mode.

show processes cpu platform [**history** | **location** | **monitor** | **profile** { **CP** | **DP** | **SP** } | **sorted** [**5sec** | **1min** | **5min**]]

Syntax Description

history	Show CPU usage history of the system.
location	Field-replacable unit (FRU) location. An is a component or module within a network device, such as a router or switch, that can be replaced without needing to send the entire device back to the manufacturer. The FRU location refers to where these units are located within the device.
monitor	Monitor running Cisco IOS XE processes.
profile {**CP** | **DP** | **SP**}	Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 17.13.1a Show CPU ulitization per profile. • **CP**: Show CPU usage of control plane. • **DP**: Show CPU usage of data plane. • **SP**: Show CPU usage of service plane.
sorted [**5sec** | **1min** | **5min**]	Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 17.13.1a Show sorted output based on percentage of usage for Cisco IOS XE processes. Optionally, you can specify the interval: • **5sec**: (Default) Sort based on a 5-second interval. • **1min**: Sort based on a 1-minute interval. • **5min**: Sort based on a 5-minute interval.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.13.1a	Added the **profile** and **sorted** options.

Usage Guidelines

Some Cisco IOS XE Catalyst SD-WAN devices generate CPU utilization alarms indicating high usage, despite the system functioning in a healthy state. This show command separates the CPU usage and provides a more accurate report of the actual CPU usage on all three planes, the control plane, the data plane, and the service plane.

Note The edge devices with greater than 8 GB of memory on Cisco IOS XE Catalyst SD-WAN Release 17.8.1a and later releases provides additional DRAM resources of 512 MB for the QFP in the system.

Example

The following sample outputs of the **show processes cpu platform** command display the CPU utilizations for the control plane, the data plane, and the service plane.

```
Device# show processes cpu platform profile CP
CPU utilization for five seconds: 1%, one minute: 1%, five minutes: 1%
Core 0: CPU utilization for five seconds: 2%, one minute: 1%, five minutes: 1%
Core 1: CPU utilization for five seconds: 2%, one minute: 1%, five minutes: 1%
Core 12: CPU utilization for five seconds: 1%, one minute: 1%, five minutes: 1%
Core 13: CPU utilization for five seconds: 2%, one minute: 1%, five minutes: 1%
Control plane process utilization for five seconds: 5%, one minute: 7%, five minutes: 7%
Pid PPid 5Sec 1Min 5Min Status Size Name
------------------------------------------------------------------------------------
9089 8683 0% 0% 0% S 2764 pman
9096 9089 0% 0% 0% S 26332 psd
9367 8683 0% 0% 0% S 2776 pman
9376 9367 1% 1% 1% S 857688 linux_iosd-imag
9595 8683 0% 0% 0% S 2760 pman
...

Device# show processes cpu platform profile DP
CPU utilization for five seconds: 7%, one minute: 9%, five minutes: 9%
Core 2: CPU utilization for five seconds: 3%, one minute: 2%, five minutes: 3%
Core 3: CPU utilization for five seconds: 1%, one minute: 1%, five minutes: 1%
Core 4: CPU utilization for five seconds: 1%, one minute: 1%, five minutes: 1%
Core 5: CPU utilization for five seconds: 3%, one minute: 5%, five minutes: 5%
Core 6: CPU utilization for five seconds: 2%, one minute: 2%, five minutes: 2%
Core 7: CPU utilization for five seconds: 1%, one minute: 1%, five minutes: 1%
Core 8: CPU utilization for five seconds: 27%, one minute: 35%, five minutes: 36%
Core 9: CPU utilization for five seconds: 31%, one minute: 48%, five minutes: 50%
Core 10: CPU utilization for five seconds: 21%, one minute: 21%, five minutes: 21%
Core 11: CPU utilization for five seconds: 21%, one minute: 22%, five minutes: 22%
Core 14: CPU utilization for five seconds: 1%, one minute: 1%, five minutes: 1%
Core 15: CPU utilization for five seconds: 1%, one minute: 1%, five minutes: 1%
Core 16: CPU utilization for five seconds: 1%, one minute: 1%, five minutes: 1%
Core 17: CPU utilization for five seconds: 1%, one minute: 1%, five minutes: 1%
Core 18: CPU utilization for five seconds: 1%, one minute: 1%, five minutes: 1%
Core 19: CPU utilization for five seconds: 1%, one minute: 1%, five minutes: 1%
Data plane process utilization for five seconds: 171%, one minute: 171%, five minutes: 171%
Pid PPid 5Sec 1Min 5Min Status Size Name
------------------------------------------------------------------------------------
15833 15219 0% 0% 0% S 2764 pman
15840 15833 172% 171% 171% S 900668 ucode_pkt_PPE0

Device# show processes cpu platform profile SP
CPU utilization for five seconds: 1%, one minute: 1%, five minutes: 1%
Core 0: CPU utilization for five seconds: 1%, one minute: 1%, five minutes: 1%
```

show policy-map type inspect

To view active firewall sessions, use the **show policy-map type inspect** command in privileged EXEC mode.

show policy-map type inspect

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

The following sample outputs displays the view active firewall sessions.

```
Device# show policy-map type inspect
  Policy Map type inspect optimized FW_POLICY1-opt
    Class FW_POLICY1-seq-1-cm_
      Inspect
    Class class-default

  Policy Map type inspect pm1
    Class cm1
      Inspect
    Class class-default
```

show redundancy application control-interface group

To display detailed information about the control interfaces used for application redundancy groups on a Cisco IOS XE Catalyst SD-WAN device, 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	Displays the redundancy group information.

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.15.1a	This command is supported for Cisco Catalyst SD-WAN.

Usage Guidelines Use **show redundancy application control-interface group** to display detailed information about the control interface for application redundancy groups on a Cisco IOS XE Catalyst SD-WAN device. The control interface is the network interface used to manage and monitor redundancy operations. This command provides insights into the control interfaces used for redundancy, including their status, configuration details, and any relevant statistics.

Examples The following is sample output from the **show redundancy application control-interface group** command.

```
Device# show redundancy application control-interface group 1

The control interface for rg[1] is Port-channel1
Interface is Control interface associated with the following protocols: 1
```

```
BFD Enabled
Interface Neighbors:
Peer: 10.1.55.14 Active RGs: 2 Standby RGs: 1 BFD handle: 0

The control interface for rg[2] is Port-channel1
Interface is Control interface associated with the following protocols: 1
BFD Enabled
Interface Neighbors:
Peer: 10.1.55.14 Active RGs: 2 Standby RGs: 1 BFD handle: 0
```

show redundancy application data-interface group

To display detailed information about the data interfaces for a specific application redundancy group on a Cisco IOS XE Catalyst SD-WAN device, use the **show redundancy application data-interface group** command in privileged EXEC mode.

show redundancy application data-interface group

Syntax Description

group-id	Displays the redundancy group information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.15.1a	This command is supported for Cisco Catalyst SD-WAN.

Examples

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

```
Device# show redundancy application data-interface group

The data interface for rg[1] is Port-channel1
The data interface for rg[2] is Port-channel1
```

show redundancy application group

To display information about the redundancy groups configured on a Cisco IOS XE Catalyst SD-WAN device, use the **show redundancy application group** command in privileged EXEC mode.

show redundancy application group

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.15.1a	This command is supported for Cisco Catalyst SD-WAN.

Usage Guidelines

Use the **show redundancy application group** command to view detailed information about the redundancy groups configured on a Cisco IOS XE Catalyst SD-WAN device, showing their RG IDs, RG names, and current states (active or standby). This information helps to monitor and manage high availability and failover configurations effectively.

Examples

The following is sample output from the **show redundancy application group** command. The fields in the display are self-explanatory.

```
Device# show redundancy application group

Group ID    Group Name                     State
--------    ----------                     -----
1           Redundancy-1                  ACTIVE
2           Redundancy-2                  STANDBY
```

The following is a sample output from the **show redundancy application group** command with group id. This command provides information about the specified redundancy application group on a Cisco IOS XE Catalyst SD-WAN device. It includes the administrative and operational states, roles of the current and peer devices, communication status, path optimization, and redundancy framework states.

```
Device# show redundancy application group 1

Group ID:1
Group Name:

Administrative State: No Shutdown
Aggregate operational state : Up
My Role: ACTIVE
Peer Role: STANDBY
Peer Presence: Yes
Peer Comm: Yes
Peer Progression Started: Yes
Path Optimization: Enabled
TLOC Pref Change: 0

RF Domain: btob-one
         RF state: ACTIVE
         Peer RF state: STANDBY HOT
```

The following is a sample output from the **show redundancy application group all** command. This command provides displays the status and details of all application redundancy groups configured on a Cisco IOS XE Catalyst SD-WAN device. This command provides information about the redundancy groups, including their current state (active or standby), the roles of the devices within each group, and other relevant details necessary for managing and troubleshooting high availability setups.

```
Device# show redundancy application group all

Faults states Group 1 info:
        Runtime priority: [100]
                RG Faults RG State: Up.
                        Total # of switchovers due to faults:           0
                        Total # of down/up state changes due to faults: 2

RG Protocol RG 1
------------------
        Role: Active
        Init Role: Active
        Negotiation Flags 0x1
        Tunnel: UP, DIA: DOWN
```

```
        Negotiation: Enabled
        Priority: 100
        Protocol state: Active
        Ctrl Intf(s) state: Up
        Active Peer: Local
        Standby Peer: address 10.1.55.14, priority 100, intf Po1
        Log counters:
                role change to active: 11
                role change to standby: 7
                disable events: rg down state 3, rg shut 0
                ctrl intf events: up 5, down 2, admin_down 1
                reload events: local request 1, peer request 0

RG Media Context for RG 1
--------------------------
        Ctx State: Active
        Protocol ID: 1
        Media type: Default
        Control Interface: Port-channel1
        Current Hello timer: 3000
        Configured Hello timer: 3000, Hold timer: 10000
        Peer Hello timer: 3000, Peer Hold timer: 10000
        Stats:
                Pkts 9982, Bytes 618884, HA Seq 0, Seq Number 9982, Pkt Loss 0
                Authentication not configured
                Authentication Failure: 0
                Reload Peer: TX 0, RX 0
                Resign: TX 3, RX 4
        Standby Peer: Present. Hold Timer: 10000
                Pkts 7365, Bytes 250410, HA Seq 0, Seq Number 9984, Pkt Loss 0


Group ID:1
Group Name:

Administrative State: No Shutdown
Aggregate operational state : Up
My Role: ACTIVE
Peer Role: STANDBY
Peer Presence: Yes
Peer Comm: Yes
Peer Progression Started: Yes
Path Optimization: Enabled
TLOC Pref Change: 0

RF Domain: btob-one
         RF state: ACTIVE
         Peer RF state: STANDBY HOT

Faults states Group 2 info:
        Runtime priority: [100]
                RG Faults RG State: Up.
                        Total # of switchovers due to faults:           0
                        Total # of down/up state changes due to faults: 0

RG Protocol RG 2
-----------------
        Role: Standby
        Init Role: Standby
        Negotiation Flags 0x1
        Tunnel: UP, DIA: DOWN
        Negotiation: Enabled
        Priority: 100
        Protocol state: Standby-hot
```

```
        Ctrl Intf(s) state: Up
        Active Peer: address 10.1.55.14, priority 100, intf Po1
        Standby Peer: Local
        Log counters:
                role change to active: 3
                role change to standby: 3
                disable events: rg down state 0, rg shut 0
                ctrl intf events: up 1, down 0, admin_down 0
                reload events: local request 0, peer request 0

RG Media Context for RG 2
--------------------------
        Ctx State: Standby
        Protocol ID: 1
        Media type: Default
        Control Interface: Port-channel1
        Current Hello timer: 3000
        Configured Hello timer: 3000, Hold timer: 10000
        Peer Hello timer: 3000, Peer Hold timer: 10000
        Stats:
                Pkts 7377, Bytes 457374, HA Seq 0, Seq Number 7377, Pkt Loss 0
                Authentication not configured
                Authentication Failure: 0
                Reload Peer: TX 0, RX 0
                Resign: TX 3, RX 2
        Active Peer: Present. Hold Timer: 10000
                Pkts 7157, Bytes 243338, HA Seq 0, Seq Number 7374, Pkt Loss 0


Group ID:2
Group Name:

Administrative State: No Shutdown
Aggregate operational state : Up
My Role: STANDBY
Peer Role: ACTIVE
Peer Presence: Yes
Peer Comm: Yes
Peer Progression Started: Yes
Path Optimization: Enabled
TLOC Pref Change: 0

RF Domain: btob-two
         RF state: STANDBY HOT
         Peer RF state: ACTIVE
```

show redundancy application group protocol

To display information about the redundancy protocol for application redundancy groups configured on a Cisco IOS XE Catalyst SD-WAN device, use the **show redundancy application group protocol** command in privileged EXEC mode.

show redundancy application group protocol

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.15.1a	This command is supported for Cisco Catalyst SD-WAN.

Usage Guidelines

Use the **show redundancy application group protocol** to display detailed information about the redundancy protocol for application redundancy groups configured on a Cisco IOS XE Catalyst SD-WAN device. This command provides insights into the protocol-specific settings and status, which can include the current state of the redundancy protocol, the synchronization status, and other protocol-related details necessary for managing and troubleshooting high availability configurations.

Examples

The following is sample output from the **show redundancy application group protocol** command.

```
Device# show redundancy application group protocol

RG Protocol RG 1
------------------
        Role: Active
        Init Role: Active
        Negotiation Flags 0x1
        Tunnel: UP, DIA: DOWN
        Negotiation: Enabled
        Priority: 100
        Protocol state: Active
        Ctrl Intf(s) state: Up
        Active Peer: Local
        Standby Peer: address 10.1.55.14, priority 100, intf Po1
        Log counters:
                role change to active: 11
                role change to standby: 7
                disable events: rg down state 3, rg shut 0
                ctrl intf events: up 5, down 2, admin_down 1
                reload events: local request 1, peer request 0

RG Media Context for RG 1
--------------------------
        Ctx State: Active
        Protocol ID: 1
        Media type: Default
        Control Interface: Port-channel1
        Current Hello timer: 3000
        Configured Hello timer: 3000, Hold timer: 10000
        Peer Hello timer: 3000, Peer Hold timer: 10000
        Stats:
                Pkts 10001, Bytes 620062, HA Seq 0, Seq Number 10001, Pkt Loss 0
                Authentication not configured
                Authentication Failure: 0
                Reload Peer: TX 0, RX 0
                Resign: TX 3, RX 4
        Standby Peer: Present. Hold Timer: 10000
                Pkts 7385, Bytes 251090, HA Seq 0, Seq Number 10004, Pkt Loss 0



RG Protocol RG 2
------------------
        Role: Standby
        Init Role: Standby
        Negotiation Flags 0x1
        Tunnel: UP, DIA: DOWN
        Negotiation: Enabled
```

```
        Priority: 100
        Protocol state: Standby-hot
        Ctrl Intf(s) state: Up
        Active Peer: address 10.1.55.14, priority 100, intf Po1
        Standby Peer: Local
        Log counters:
                role change to active: 3
                role change to standby: 3
                disable events: rg down state 0, rg shut 0
                ctrl intf events: up 1, down 0, admin_down 0
                reload events: local request 0, peer request 0

RG Media Context for RG 2
--------------------------
        Ctx State: Standby
        Protocol ID: 1
        Media type: Default
        Control Interface: Port-channel1
        Current Hello timer: 3000
        Configured Hello timer: 3000, Hold timer: 10000
        Peer Hello timer: 3000, Peer Hold timer: 10000
        Stats:
                Pkts 7396, Bytes 458552, HA Seq 0, Seq Number 7396, Pkt Loss 0
                Authentication not configured
                Authentication Failure: 0
                Reload Peer: TX 0, RX 0
                Resign: TX 3, RX 2
        Active Peer: Present. Hold Timer: 10000
                Pkts 7177, Bytes 244018, HA Seq 0, Seq Number 7394, Pkt Loss 0
```

show redundancy rii

To display detailed information about the Redundancy Interface Identifiers (RII) on a Cisco IOS XE Catalyst SD-WAN device, use the **show redundancy rii** command in privileged EXEC mode.

show redundancy rii

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.15.1a	This command is supported for Cisco Catalyst SD-WAN.

Usage Guidelines

Use the **show redundancy rii** to display specific RII values assigned to interfaces, indicating how these interfaces are mapped and associated with RIIs.

Examples

The following is sample output from the **show redundancy rii** command.

```
Device# show redundancy rii
No. of RIIs in database: 10
 Interface                        RII Id     decrement
  GigabitEthernet3.104          :   2049          0
  GigabitEthernet3.103          :   2050          0
  GigabitEthernet3.102          :   2051          0
  GigabitEthernet7              :   2053          0
  GigabitEthernet3.105          :   2054          0
```

```
  Tunnel2                       :   513           0
  Tunnel1                       :   514           0
  GigabitEthernet3.101          :   2052          0
  GigabitEthernet2              :   1             0
  GigabitEthernet1              :   2             0
```

show sdwan alarms detail

To view detailed information about each alarm separated by a new line, use the **show sdwan alarms detail** command in privileged EXEC mode. This command provides better readability into the alarms.

show sdwan alarms detail

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.12.x	This command was introduced.

Examples

The following is a sample output of the **show sdwan alarms detail** command:

```
vm5#show sdwan alarms detail

alarms 2023-06-01:00:38:46.868569
 event-name     geo-fence-alert-status
 severity-level minor
 host-name      Router
 kv-pair        [ system-ip=:: alert-type=device-tracking-stop alert-msg=Device Tracking
stopped in Geofencing Mode latitude=N/A longitude=N/A geo-color=None ]
-----------------------------------------------------

alarms 2023-06-01:00:38:47.730907
 event-name     system-reboot-complete
 severity-level major
 host-name      Router
 kv-pair        [ ]
-----------------------------------------------------

alarms 2023-06-01:00:39:00.633682
 event-name     pki-certificate-event
 severity-level critical
 host-name      Router
 kv-pair        [ trust-point=Trustpool event-type=pki-certificate-install
valid-from=2008-11-18T21:50:24+00:00 expires-at=2033-11-18T21:59:46+00:00 is-ca-cert=true
subject-name=cn=Cisco Root CA M1,o=Cisco issuer-name=cn=Cisco Root CA M1,o=Cisco
serial-number=2ED20E7347D333834B4FDD0DD7B6967E ]
-----------------------------------------------------
```

show sdwan alarms summary

To view alarm details such as the timestamp, event name, and severity in a tabular format, use the **show sdwan alarms summary** command in privileged EXEC mode. This command provides better readability into the alarms.

show sdwan alarms summary

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.12.x	This command was introduced.

Examples

The following is a sample output of the **show sdwan alarms summary** command:

```
vm5#show sdwan alarms summary

time-stamp                    event-name                                    severity-l

-------------------------------------------------------------------------------------
2023-06-01:00:38:46.868569      geo-fence-alert-status                        minor

2023-06-01:00:38:47.730907      system-reboot-complete                        major

2023-06-01:00:39:00.633682     pki-certificate-event                        critical

2023-06-01:00:39:00.644209     pki-certificate-event                        critical

2023-06-01:00:39:00.649363     pki-certificate-event                        critical

2023-06-01:00:39:00.652777     pki-certificate-event                        critical

2023-06-01:00:39:00.658387     pki-certificate-event                        critical

2023-06-01:00:39:00.661119     pki-certificate-event                        critical

2023-06-01:00:39:00.665882     pki-certificate-event                        critical

2023-06-01:00:39:00.669655     pki-certificate-event                        critical

2023-06-01:00:39:00.674912     pki-certificate-event                        critical

2023-06-01:00:39:00.683510     pki-certificate-event                        critical

2023-06-01:00:39:00.689850     pki-certificate-event                        critical

2023-06-01:00:39:00.692883     pki-certificate-event                        critical

2023-06-01:00:39:00.699143     pki-certificate-event                        critical

2023-06-01:00:39:00.702386     pki-certificate-event                        critical

2023-06-01:00:39:00.703653     pki-certificate-event                        critical
```

```
2023-06-01:00:39:00.704488      pki-certificate-event                    critical

2023-06-01:00:39:01.949479      pki-certificate-event                    critical

2023-06-01:00:40:38.992382      interface-state-change                     major

2023-06-01:00:40:39.040929      fib-updates                                minor

2023-06-01:00:40:39.041866      fib-updates                                minor
```

show sdwan appqoe

To view infrastructure statistics, NAT statistics, resource manager resources and statistics, TCP optimization status, and service chain status, use the **show sdwan appqoe** command in privileged EXEC mode.

show sdwan appqoe { **infra-statistics** | **nat-statistics** | **rm-statistics** | **ad-statistics** | **aoim-statistics** | **rm-resources** | **tcpopt status** | **service-chain status** | **libuinet-statistics** [**sppi** | **verbose**] }

Syntax Description

infra-statistics	Displays infra statistics
nat-statistics	Displays NAT statistics
rm-statistics	Displays resource manager status
ad-statistics	Displays the status for auto discovery of peer devices
aoim-statistics	Displays the statistics for one time exchange of information between peer devices
rm-resources	Displays resource manager resources
tcpopt status	Displays information about TCP optimization
service-chain status	Displays service chain status
libuinet-statistics sppi verbose	Displays libuinet statistics

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	Command introduced.

```
Device# show sdwan appqoe tcpopt status
=============================================================
                  TCP-OPT Status
=============================================================

Status
------
TCP OPT Operational State      : RUNNING
TCP Proxy Operational State    : RUNNING
```

```
Device#show sdwan appqoe nat-statistics
============================================================
              NAT Statistics
============================================================
 Insert Success      : 48975831
 Delete Success      : 48975823
 Duplicate Entries   : 19
 Allocation Failures : 0
 Port Alloc Success  : 0
 Port Alloc Failures : 0
 Port Free Success   : 0
 Port Free Failures  : 0
```

```
Device# show sdwan appqoe service-chain status
Service                  State
-------                  -----
SNORT Connection         UP
```

```
Device#  sdwan appqoe libuinet-statistics
============================================================
              Libuinet Statistics
============================================================
SPPI Statistics:
 Available Packets          : 1214696704
 Errored Available Packets  : 111235402
 Rx Packets                 : 1214696704
 Failed Rx Packets          : 0
 Tx Packets                 : 1124139791
 Tx Full Wait               : 0
 Failed Tx Packets          : 0
 PD Alloc Success           : 1226942851
 PD Alloc Failed            : 0
 PB Current Count           : 32768
 Pipe Disconnect            : 0

Vpath Statistics:
 Packets In                 : 1214696704
 Control Packets            : 250438
 Data Packets               : 1214446263
 Packets Dropped            : 351131
 Non-Vpath Packets          : 3
 Decaps                     : 1214446263
 Encaps                     : 1123889349
 Packets Out                : 1111643206
 Syn Packets                : 12248341
 Syn Drop Max PPS Reached   : 0
 IP Input Packets           : 1214095132
 IP Input Bytes             : 856784254349
 IP Output Packets          : 1111643202
 IP Output Bytes            : 917402419856
 Flow Info Allocs           : 12248341
 Flow Info Allocs Failed    : 0
 Flow Info Allocs Freed     : 12248339
 Rx Version Prob Packets    : 1
 Rx Control Packets         : 250437
 Rx Control Healthprobe Pkts: 250437
 ICMP incoming packet count: 0
 ICMP processing success: 0
 ICMP processing failures: 0
 Non-Syn nat lkup failed Pkts: 348691
 Nat lkup success for Syn Pkts: 248
 Vpath drops due to min threshhold: 0
 Flow delete notify TLV Pkts: 12246147
 Failed to allocate flow delete notify TLV Pkts: 0
 Failed to send flow delete notify TLV Pkts: 0
```

```
 Failed to create new connection: 2192

Device# show sdwan appqoe rm-resources
============================================================
              RM Resources
============================================================
RM Global Resources :
 Max Services Memory (KB)    : 1537040
 Available System Memory(KB) : 3074080
 Used Services Memory (KB)   : 228
 Used Services Memory (%)    : 0
 System Memory Status        : GREEN
 Num sessions Status         : GREEN
 Overall HTX health Status   : GREEN

Registered Service Resources :
TCP Resources:
 Max Sessions                : 40000
 Used Sessions               : 42
 Memory Per Session          : 128
SSL Resources:
 Max Sessions                : 40000
 Used Sessions               : 2
 Memory Per Session          : 50
Device# show sdwan appqoe ad-statistics

============================================================

              Auto-Discovery Statistics

============================================================

 Auto-Discovery Option Length Mismatch       : 0

 Auto-Discovery Option Version Mismatch      : 0

 Tcp Option Length Mismatch                  : 6

 AD Role set to NONE                         : 0

 [Edge] AD Negotiation Start                 : 96771

 [Edge] AD Negotiation Done                  : 93711

 [Edge] Rcvd SYN-ACK w/o AD options          : 0

 [Edge] AOIM sync Needed                     : 99

 [Core] AD Negotiation Start                 : 10375

 [Core] AD Negotiation Done                  : 10329

 [Core] Rcvd ACK w/o AD options              : 0

 [Core] AOIM sync Needed                     : 0
Device# show sdwan appqoe aoim-statistics

============================================================

              AOIM Statistics

============================================================
```

```
 Total Number Of Peer Syncs      : 1

 Current Number Of Peer Syncs in Progress      : 0

 Number Of Peer Re-Syncs Needed      : 1

 Total Passthrough Connections Due to Peer Version Mismatch   : 0

 AOIM DB Size (Bytes): 4194304


 LOCAL AO Statistics

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

 Number Of AOs      : 2

 AO             Version   Registered

 SSL             1.2        Y

 DRE             0.23       Y


 PEER Statistics

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

 Number Of Peers      : 1

 Peer ID: 203.203.203.11

 Peer Num AOs      : 2

 AO             Version   InCompatible

 SSL             1.2        N

 DRE             0.23       N
```

show sdwan appqoe dreopt

To view various DRE optimization statistics, use the **show sdwan appqoe dreopt** command in privileged EXEC mode.

show sdwan appqoe dreopt { **auto-bypass** | **crypt** | **status** [**detail**] }

Syntax Description

auto-bypass	Displays the auto-bypass details of DRE optimization.
crypt	Displays cache encryption status.
status	Displays DRE optimization status.
detail	(Optional) Displays a more detailed status of DRE optimization.

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	This command was introduced.
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	This command was modified to include details of DRE profiles. This feature was introduced in Cisco IOS XE Catalyst SD-WAN Release 17.6.1a.

The following example shows the status of DRE optimization. To view the status in more detail, use the **show sdwan appqoe dreopt status detail** command.

```
Device# show sdwan appqoe dreopt status

DRE ID                                          : 52:54:dd:d0:e2:8d-0176814f0f66-93e0830d

DRE uptime                                      : 18:27:43

Health status                                   : GREEN

Health status change reason                     : None

Last health status change time                  : 18:25:29

Last health status notification sent time        : 1 second

DRE cache status                                : Active

Disk cache usage                                : 91%

Disk latency                                    : 16 ms

Active alarms:

  None


Configuration:

  Profile type                                  : Default

  Maximum connections                           : 750

  Maximum fanout                                : 35

  Disk size                                     : 400 GB

  Memory size                                   : 4096 MB

  CPU cores                                     : 1

  Disk encryption                               : ON
```

The following example shows how to view the auto-bypass status of DRE optimization.

```
Device# show sdwan appqoe dreopt auto-bypass

      Server IP   Port       State    DRE LAN BYTES    DRE WAN BYTES    DRE COMP   Last
Update   Entry Age
```

```
-----------------------------------------------------------------------------------------------------

      10.0.0.1    9088       Monitor      48887002724      49401300299   0.000000
13:41:51   03:08:53
```

The following example shows how to view the cache encryption status for DRE.

```
Device# show sdwan appqoe dreopt crypt

Status: Success

Atempts: 1

1611503718:312238        DECRYPT REQ SENT

1611503718:318198        CRYPT SUCCESS

ENCRYPTION:

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

BLK NAME        :  No of Oper  | Success | Failure

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

SIGNATURE BLOCK |     210404     210404          0

SEGMENT BLOCK   |     789411     789411          0

SECTION BLOCKS  |      49363      49363          0

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

DECRYPTION:

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

BLK NAME        :  No of Oper  | Success | Failure

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

SIGNATURE BLOCK |     188616     188616          0

SEGMENT BLOCK   |          1          1          0

SECTION BLOCKS  |     366342     366342          0

-------------------------------------------------
```

Following is the sample output from the **show sdwan appqoe dreopt status** command. This example shows the details of the DRE profile applied.

```
Device# show sdwan appqoe dreopt status
DRE ID                                          : 52:54:dd:e5:58:5a-01791db8c691-c5b3336c
DRE uptime                                      : 20:58:23
Health status                                   : GREEN
Health status change reason                     : None
Last health status change time                  : 19:40:37
Last health status notification sent time       : 1 second
DRE cache status                                : Active
Disk cache usage                                : 0%
Disk latency                                    : 0 ms
Active alarms:
  None
Configuration:
```

```
Profile type                              : S
Maximum connections                       : 750
Maximum fanout                            : 35
Disk size                                 : 60 GB
Memory size                               : 2048 MB
CPU cores                                 : 1
Disk encryption
```

show sdwan appqoe dreopt statistics

To view DRE optimization statistics, use the **show sdwan appqoe dreopt statistics** command in privileged EXEC mode.

show sdwan appqoe dreopt statistics [**detail** | **peer** [**detail** | **peer** *peer-ip* | **peer-no** *peer-id*]]

Syntax Description

detail	(Optional) Displays detailed DRE optimization statistics.
peer *peer-ip*	(Optional) Displays DREOPT peer details.
peer-no *peer-id*	(Optional) Displays DRE optimization details for peer-no.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	Command introduced.

The following information show how to view DRE optimization statistics.

```
Device# show sdwan appqoe dreopt statistics

Total connections                 : 3714

Max concurrent connections        : 552

Current active connections        : 0

Total connection resets           : 1081

Total original bytes              : 360 GB

Total optimized bytes             : 164 GB

Overall reduction ratio           : 54%

Disk size used                    : 91%

Cache details:

  Cache status                      : Active

  Cache Size                        : 407098 MB

  Cache used                        : 91%
```

```
  Oldest data in cache               : 03:02:07:55

  Replaced(last hour): size          : 0 MB
```

The following example shows DRE optimization statistics for a peer device.

```
Device# show sdwan appqoe dreopt statistics peer 209.165.201.1

  Peer No.  System IP          Hostname    Active connections    Cummulative connections

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

         0  209.165.201.1       dreopt              0                       3714
```

show sdwan appqoe error recent

To view details of recent AppQoE errors, use the **show sdwan appqoe error recent** command in privileged EXEC mode.

show sdwan appqoe error recent

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	This command was introduced.

Example

The following is sample output from the **show sdwan appqoe error recent**

```
Device# show sdwan appqoe error recent

Appqoe Statistics Recent

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

Label                        Current value        Value(30 sec bfr)      Value(60 sec bfr)

RM TCP used sessions                20702                20026                21005

RM SSL used sessions                19376                18528                18824

RM health status change to yellow   47                   47                   47

RM health status change to green    47                   47                   47

RM TCP session allocated            28412162             28406875             28402421

RM TCP session freed                28391460             28386849             28381416

RM SSL session allocated            28412144             28406857             28402403

RM SSL session freed                28392768             28388329             28383579
```

TCP number of connections	27597418	27592148	27588196
TCP number of flows created	28412162	28406875	28402421
TCP number of flows deleted	28389923	28385898	28381006
TCP number of current connections	19687	19026	20504
TCP failed connections	813651	813649	813646
TCP syncache added	28411831	28406269	28402046
vPath drop due to pps	578	578	578
vPath new connection failed	11757	11757	11757
BBR Active connections	38108	35305	38252
BBR sendmap allcation failed	0	0	0
SPPI available packets	3898784336	3896241285	3893452077
SPPI failed received packets	0	0	0
SPPI failed transmitted packets	0	0	0
SPPI pipe disconnected	0	0	0
HPUT SYS TIMER callout deleted	0	0	0
HPUT HPTS TIMER callout deleted	0	0	0
HPUT SYS TIMER timer deleted	111372027	111351614	111325475
HPUT HPTS TIMER timer deleted	11873674	11873666	11873651
HPUT SYS TIMER node is empty	0	0	0
HPUT HPTS TIMER node is empty	459711	459708	459699
Untrusted Certificate	0	0	0
Unable to get Proxy certificate	954	954	954
Expired Certificate	0	0	0
OCSP Cert Verification Failure	0	0	0
Endpoint Alert	0	0	0
FIN/RST Received during handshake	172444	172444	172444
Session Alloc Failures	0	0	0
C2S WCAPI DENY packet	0	0	0
S2C WCAPI DENY packet	0	0	0

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

Table 30: show sdwan appqoe error recent Field Descriptions

Field	Description
RM TCP used sessions	The number of resource manager sessions used by TCP proxy
RM SSL used sessions	The number of resource manager sessions used by SSL proxy
RM health status change to yellow	The number of times the status of the resource manager changed to yellow
RM health status change to green	The number of times the status of the resource manager changed to green
RM TCP session allocated	The number of resource manager sessions allocated by TCP proxy
RM TCP session freed	The number of resource manager sessions freed by TCP proxy
RM SSL session allocated	The number of resource manager sessions allocated by SSL proxy
RM SSL session freed	The number of resource manager sessions freed by SSL proxy
TCP number of connections	The total number of TCP connections
TCP number of flows created	The total number of TCP flows created
TCP number of flows deleted	The total number of TCP flows deleted
TCP number of current connections	The total number of current TCP connections
TCP syncache added	The total number of SYN cache entries
vPath drop due to pps	The total number of transport channel SYN entries dropped because the packet-per-second limit is reached
vPath new connection failed	The total number of new transport channel connections that failed
BBR Active Connections	The total number of active connections for Bottleneck Bandwidth and Round-trip (BBR) propagation
BBR sendmap allocation failed	The total numbers of BBR total send map allocation failures
SPPI available packets	Total packets available for Service Plane Packet Interface (SPPI)
SPPI pipe disconnected	SPPI pipe is disconnected

Field	Description
SPPI failed received packets	SPPI failed to receive packets
SPPI failed transmit packets	SPPI failed to transmit packets
HPUT SYS TIMER callout deleted	System timer callout was deleted
HPUT HPTS TIMER callout deleted	The high-precision timers (HPTS) callout was deleted
HPUT SYS TIMER timer deleted	The system timer was deleted
HPUT HPTS TIMER timer deleted	The HPTS timer was deleted
HPUT SYS TIMER node is empty	The system timer node is empty
HPUT HPTS TIMER node is empty	The HPTS timer node is empty
Untrusted Certificate	Total number of SSL sessions dropped because of untrusted certificates
Unable to get Proxy certificate	The total number of sessions dropped because the SSL proxy certificate couldn't be retrieved
Expired Certificate	The total number of SSL sessions dropped due to expired certificates
OCSP Cert Verification Failure	The number of failures because the OSCP certificate verification failed
Endpoint Alert	The number of SSL proxy sessions dropped because of endpoint alerts
FIN/RST Received during handshake	SSL was dropped because TCP connection was closed
Session Alloc Failures	SSL proxy could not allocate sessions
C2S WCAPI DENY packet	The SSL client to server packet was denied
S2C WCAPI DENY packet	The SSL server to client packet was denied

show sdwan appqoe flow closed all

To display the summary of AppQoE expired flows on a device, use the **show sdwan appqoe flow closed all** command in privileged EXEC mode.

show sdwan appqoe flow closed all

Command Default None

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	This command was introduced.

Examples

The following sample output displays the summary of AppQoE expired flows.

```
Device# show sdwan appqoe flow closed all
Current Historical Optimized Flows: 16

Optimized Flows
---------------
T:TCP, S:SSL, U:UTD, D:DRE, H:HTTP
RR: DRE Reduction Ratio

Flow ID      VPN  Source IP:Port        Destination IP:Port   Service  RR%
22977217840  1    30.1.50.2:34940       30.1.51.2:80          T        -
13598953631  1    30.1.50.2:34936       30.1.51.2:80          T        -
17348519476  1    30.1.50.2:34938       30.1.51.2:80          T        -
11495519740  1    30.1.50.2:34934       30.1.51.2:80          T        -
29497270355  1    30.1.50.2:34942       30.1.51.2:80          T        -
32442796471  1    30.1.50.2:34944       30.1.51.2:80          T        -
34529471700  1    30.1.50.2:34946       30.1.51.2:80          T        -
39369775743  1    30.1.50.2:34948       30.1.51.2:80          T        -
46676987507  1    30.1.50.2:34950       30.1.51.2:80          T        -
8568888344   1    30.1.50.2:34932       30.1.51.2:80          T        -
63035789628  1    30.1.50.2:34958       30.1.51.2:80          T        -
48746883856  1    30.1.50.2:34952       30.1.51.2:80          T        -
51709149940  1    30.1.50.2:34954       30.1.51.2:80          T        -
58212427671  1    30.1.50.2:34956       30.1.51.2:80          T        -
66801636855  1    30.1.50.2:34960       30.1.51.2:80          T        -
68888309908  1    30.1.50.2:34962       30.1.51.2:80          T        -
```

Related Commands

Command	Description
show sdwan appqoe flow closed flow-id *flow-id*	Displays AppQoE expired flow details for a single specific flow.
show sdwan appqoe flow flow-id *flow-id*	Displays the details of a single specific flow.
show sdwan appqoe flow vpn-id *vpn-id* **server-port** *server-port*	Displays the flows for a specific VPN on a device.

show sdwan appqoe flow closed flow-id

To display AppQoE expired flow details for a signle specific flow on a device, use the **show sdwan appqoe flow closed flow-id** command in privileged EXEC mode.

show sdwan appqoe flow closed flow-id *flow-id*

Supported Parameters

flow-id	Specify a flow id.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	This command was introduced.

Examples

The following sample output displays the AppQoE expired flow details for a signle specific flow.

```
Device# show sdwan appqoe flow closed flow-id 66801636855
Flow ID: 66801636855

VPN: 1  APP: 0 [Client 30.1.50.2:34960 - Server 30.1.51.2:80]

TCP stats
---------
Client Bytes Received   : 139
Client Bytes Sent       : 10486028
Server Bytes Received   : 10486028
Server Bytes Sent       : 139

Client Bytes sent to SSL: 0
Server Bytes sent to SSL: 0

C2S HTX to DRE Bytes    : 0
C2S HTX to DRE Pkts     : 0
S2C HTX to DRE Bytes    : 0
S2C HTX to DRE Pkts     : 0
C2S DRE to HTX Bytes    : 0
C2S DRE to HTX Pkts     : 0
S2C DRE to HTX Bytes    : 0
S2C DRE to HTX Pkts     : 0

C2S HTX to HTTP Bytes   : 0
C2S HTX to HTTP Pkts    : 0
S2C HTX to HTTP Bytes   : 0
S2C HTX to HTTP Pkts    : 0
C2S HTTP to HTX Bytes   : 0
C2S HTTP to HTX Pkts    : 0
S2C HTTP to HTX Bytes   : 0
S2C HTTP to HTX Pkts    : 0

C2S SVC Bytes to SSL    : 0
S2C SVC Bytes to SSL    : 0
C2S SSL to TCP Tx Pkts  : 0
C2S SSL to TCP Tx Bytes : 0
S2C SSL to TCP Tx Pkts  : 0
S2C SSL to TCP Tx Bytes : 0

C2S TCP Tx Pkts Success : 1
C2S TCP Tx Pkts Failed  : 0
```

```
S2C TCP Tx Pkts Success : 7515
S2C TCP Tx Pkts Failed  : 0

TCP Client IP TOS       : 0x28
TCP Server IP TOS       : 0x28
TCP Client Rx Pause     : 0x1
TCP Server Rx Pause     : 0x1
TCP Client Tx Pause     : 0x0
TCP Server Tx Pause     : 0x0
Client Flow Pause State : 0x0
Server Flow Pause State : 0x0
Client Flow Control     : 0x0
Server Flow Control     : 0x0
Snort close sent : 0x0
Snort init close handled: 0x0
TCP Flow Bytes Consumed[C2S][Og] : 0
TCP Flow Bytes Consumed[C2S][Tm] : 0
TCP Flow Bytes Consumed[S2C][Og] : 0
TCP Flow Bytes Consumed[S2C][Tm] : 0
TCP Client Close Done   : 0x1
TCP Server Close Done   : 0x1
TCP Client FIN Rcvd     : 0x1
TCP Server FIN Rcvd     : 0x1
TCP Client RST Rcvd     : 0x0
TCP Server RST Rcvd     : 0x0
TCP Client FIN Sent     : 0x1
TCP Server FIN Sent     : 0x1
Flow Cleanup State      : 0x7
TCP Flow Events
   1. time:2252.112679   ::   Event:TCPPROXY_EVT_FLOW_CREATED
   2. time:2252.112697   ::   Event:TCPPROXY_EVT_AD_RX_SYN_WITHOUT_OPTIONS
   3. time:2252.112725   ::   Event:TCPPROXY_EVT_SYNCACHE_ADDED
   4. time:2252.112736   ::   Event:TCPPROXY_EVT_AD_TX_EDGE_SYNACK_NO_OPTIONS
   5. time:2252.113091   ::   Event:TCPPROXY_EVT_AD_RX_EDGE_ACK
   6. time:2252.113180   ::   Event:TCPPROXY_EVT_ACCEPT_DONE
   7. time:2252.113286   ::   Event:TCPPROXY_EVT_AD_TX_EDGE_SYN
   8. time:2252.113292   ::   Event:TCPPROXY_EVT_CONNECT_START
   9. time:2253.113338   ::   Event:TCPPROXY_EVT_AD_TX_EDGE_SYN
  10. time:2254.122111   ::   Event:TCPPROXY_EVT_AD_RX_EDGE_SYNACK_WITH_OPTIONS
  11. time:2254.122209   ::   Event:TCPPROXY_EVT_CONNECT_DONE
  12. time:2254.122230   ::   Event:TCPPROXY_EVT_DATA_ENABLED_SUCCESS
  13. time:2254.122281   ::   Event:TCPPROXY_EVT_AD_TX_EDGE_ACK
  14. time:2254.122299   ::   Event:TCPPROXY_EVT_AD_TX_EDGE_ACK
  15. time:2757.323156   ::   Event:TCPPROXY_EVT_FIN_RCVD_CLIENT_FD_C2S
  16. time:2757.323164   ::   Event:TCPPROXY_EVT_FIN_SENT_SERVER_FD_C2S
  17. time:2757.330780   ::   Event:TCPPROXY_EVT_FIN_RCVD_SERVER_FD_S2C
  18. time:2757.330781   ::   Event:TCPPROXY_EVT_SERVER_TCP_CLOSED
  19. time:2757.330781   ::   Event:TCPPROXY_EVT_ENABLE_RX_SOCK_ON_STACK_CLOSED_SERVER
  20. time:2757.330790   ::   Event:TCPPROXY_EVT_FIN_SENT_CLIENT_FD_S2C
  21. time:2757.330807   ::   Event:TCPPROXY_EVT_CLOSE_CLIENT_FD_S2C
  22. time:2757.330807   ::   Event:TCPPROXY_EVT_CLOSE_SERVER_FD_C2S
  23. time:2757.330807   ::   Event:TCPPROXY_EVT_PROXY_CLOSE
  24. time:2757.330962   ::   Event:TCPPROXY_EVT_CLIENT_TCP_CLOSED
  25. time:2757.330963   ::   Event:TCPPROXY_EVT_ALL_TCP_CLOSED_CLEANUP
  26. time:2763.084297   ::   Event:TCPPROXY_EVT_CLEANUP_COMPLETE


TCP BBR Client Statistics:
 BBR States Transition
     STARTUP To DRAIN State     : 0
     STARTUP To PROBEBW State   : 1
     STARTUP To PROBERTT State  : 0
     DRAIN To PROBEBW State     : 0
     PROBEBW To PROBERTT State  : 21
```

```
    PROBERTT To STARTUP State  : 0
    PROBERTT To PROBEBW State  : 21
    IDLEEXIT To PROBEBW State  : 0
 HPTS Timer Started
    Wrong Timer                : 0
    Persistent Timeout         : 0
    Keepalive Timeout          : 0
    Connection Initialization  : 0
    BBR do segment unlock1     : 1
    BBR do segment unlock2     : 0
    PACE Segment               : 20828
    BBR output wtime error msg size: 0
    BBR output wtime default   : 0
    BBR do wtime error nonufs  : 6
 HPTS Timer Stopped
    Wrong Timer                : 0
    Cancel Timer               : 6008
    Persistent Mode Exit       : 0
    BBR Do Segment Unlock      : 0
    Packets needs to be paced  : 7388
    Exempt early               : 0
    Delay exceed               : 91
    Connection Closed          : 0
 Pacing Delay (in us)
    Equals 0           : 0
    1 to 5             : 7341
    6 to 10            : 15
    11 to 20           : 63
    21 to 50           : 15
    50 to 100          : 4
    101 to 500         : 0
    501 to 1000        : 36
    Greater than 1000  : 13361
 RTT (in ms)
    Less than 1       : 2009
    Equals 1          : 2
    1 To 50           : 4297
    51 To 100         : 0
    101 To 150        : 0
    151 To 200        : 0
    Greater than 200  : 0
 Bandwidth
    Less Than 1KBps     : 2
    1KBps To 250KBps    : 5618
    251KBps To 500KBps  : 1
    500KBps To 1MBps    : 0
    1MBps To 2MBps      : 2
    2MBps To 5MBps      : 257
    5MBps To 10MBps     : 194
    Greater Than 10MBps : 234
 BBR Output Bytes              : 10486028
 TCP Segments Lost             : 0
 TCP Segment Sent              : 7820
 Retransmitted Segments        : 0
 Conn. drop due to no progress : 0
 TCP Segment Sent through HPTS : 7355
 Max Send Buffer Reached       : 20830
 Max Send Congestion Window    : 353998
 Current TCP Send Window       : 821632

HPTS Statistics:
 Timer Expired Early         : 0
 Delay in Timer Expiry       : 7441
 Callout Scheduled           : 0
```

```
 Lasttick is gt current tick : 0
 Maxticks Overflow           : 0
 Timer WakeUp Immediately    : 0
 Inp Added back to same slot : 0
 Distance To Travel Overflow : 0
 Available On Wheel Overflow : 0
 Available On Wheel lt Pacer : 0
 HPTS Is Hopelessly Behind   : 0
 HPTS Is Stuck In Loop       : 0
 HPTS Is Back On Sleep       : 0
 HPTS Wheel Wrapped          : 0
 HPTS Wheel Time Exceeded    : 0
 Forced close from FIN_WAIT_2  : 0

TCP BBR Server Statistics:
 BBR States Transition
     STARTUP To DRAIN State     : 0
     STARTUP To PROBEBW State   : 0
     STARTUP To PROBERTT State  : 0
     DRAIN To PROBEBW State     : 0
     PROBEBW To PROBERTT State  : 0
     PROBERTT To STARTUP State  : 0
     PROBERTT To PROBEBW State  : 0
     IDLEEXIT To PROBEBW State  : 0
 HPTS Timer Started
     Wrong Timer                 : 0
     Persistent Timeout          : 0
     Keepalive Timeout           : 0
     Connection Initialization   : 0
     BBR do segment unlock1      : 3755
     BBR do segment unlock2      : 0
     PACE Segment                : 3
     BBR output wtime error msg size: 0
     BBR output wtime default    : 0
     BBR do wtime error nonufs   : 4203
 HPTS Timer Stopped
     Wrong Timer                : 0
     Cancel Timer               : 3757
     Persistent Mode Exit       : 0
     BBR Do Segment Unlock      : 0
     Packets needs to be paced  : 4039
     Exempt early               : 0
     Delay exceed               : 0
     Connection Closed          : 0
 Pacing Delay (in us)
     Equals 0           : 0
     1 to 5             : 0
     6 to 10            : 0
     11 to 20           : 0
     21 to 50           : 0
     50 to 100          : 1
     101 to 500         : 0
     501 to 1000        : 0
     Greater than 1000  : 7958
 RTT (in ms)
     Less than 1       : 0
     Equals 1          : 0
     1 To 50           : 1
     51 To 100         : 0
     101 To 150        : 0
     151 To 200        : 0
     Greater than 200  : 448
 Bandwidth
     Less Than 1KBps     : 449
```

```
    1KBps To 250KBps    : 0
    251KBps To 500KBps  : 0
    500KBps To 1MBps    : 0
    1MBps To 2MBps      : 0
    2MBps To 5MBps      : 0
    5MBps To 10MBps     : 0
    Greater Than 10MBps : 0
 BBR Output Bytes               : 139
 TCP Segments Lost              : 0
 TCP Segment Sent               : 4204
 Retransmitted Segments         : 0
 Conn. drop due to no progress  : 0
 TCP Segment Sent through HPTS  : 163
 Max Send Buffer Reached        : 4204
 Max Send Congestion Window     : 1073725440
 Current TCP Send Window        : 0

HPTS Statistics:
 Timer Expired Early          : 0
 Delay in Timer Expiry        : 1
 Callout Scheduled            : 0
 Lasttick is gt current tick  : 0
 Maxticks Overflow            : 0
 Timer WakeUp Immediately     : 0
 Inp Added back to same slot  : 0
 Distance To Travel Overflow  : 0
 Available On Wheel Overflow  : 0
 Available On Wheel lt Pacer  : 0
 HPTS Is Hopelessly Behind    : 0
 HPTS Is Stuck In Loop        : 0
 HPTS Is Back On Sleep        : 0
 HPTS Wheel Wrapped           : 0
 HPTS Wheel Time Exceeded     : 0
 Forced close from FIN_WAIT_2  : 0
```

Related Commands

Command	Description
show sdwan appqoe flow closed all	Displays the summary of AppQoE expired flows on a device.
show sdwan appqoe flow flow-id *flow-id*	Displays the details of a single specific flow.
show sdwan appqoe flow vpn-id *vpn-id* **server-port** *server-port*	Displays the flows for a specific VPN on a device.

show sdwan appqoe flow flow-id

To display the details for a single specific flow, use the **show sdwan appqoe flow flow-id** command in privileged EXEC mode.

show sdwan appqoe flow flow-id *flow-id*

Supported Parameters

flow-id	Specify a flow id.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	This command was introduced.

Examples

The following sample output displays the details for a single specific flow.

```
Device# show sdwan appqoe flow flow-id 68888309908
Flow ID: 68888309908

VPN: 1  APP: 0 [Client 30.1.50.2:34962 - Server 30.1.51.2:80]

TCP stats
---------
Client Bytes Received   : 139
Client Bytes Sent       : 2625440
Server Bytes Received   : 2625440
Server Bytes Sent       : 139

Client Bytes sent to SSL: 0
Server Bytes sent to SSL: 0

C2S HTX to DRE Bytes    : 0
C2S HTX to DRE Pkts     : 0
S2C HTX to DRE Bytes    : 0
S2C HTX to DRE Pkts     : 0
C2S DRE to HTX Bytes    : 0
C2S DRE to HTX Pkts     : 0
S2C DRE to HTX Bytes    : 0
S2C DRE to HTX Pkts     : 0

C2S HTX to HTTP Bytes   : 0
C2S HTX to HTTP Pkts    : 0
S2C HTX to HTTP Bytes   : 0
S2C HTX to HTTP Pkts    : 0
C2S HTTP to HTX Bytes   : 0
C2S HTTP to HTX Pkts    : 0
S2C HTTP to HTX Bytes   : 0
S2C HTTP to HTX Pkts    : 0

C2S SVC Bytes to SSL    : 0
S2C SVC Bytes to SSL    : 0
C2S SSL to TCP Tx Pkts  : 0
C2S SSL to TCP Tx Bytes : 0
S2C SSL to TCP Tx Pkts  : 0
S2C SSL to TCP Tx Bytes : 0

C2S TCP Tx Pkts Success : 1
C2S TCP Tx Pkts Failed  : 0
```

```
S2C TCP Tx Pkts Success : 1912
S2C TCP Tx Pkts Failed  : 0
TCP Client IP TOS       : 0x28
TCP Server IP TOS       : 0x28
TCP Client Rx Pause     : 0x0
TCP Server Rx Pause     : 0x0
TCP Client Tx Enabled   : 0x0
TCP Server Tx Enabled   : 0x0
Client Flow Pause State : 0x0
Server Flow Pause State : 0x0
Client Flow Control     : 0x0
Server Flow Control     : 0x0
Snort close sent : 0x0
Snort init close handled: 0x0
TCP Flow Bytes Consumed[C2S][Og] : 0
TCP Flow Bytes Consumed[C2S][Tm] : 0
TCP Flow Bytes Consumed[S2C][Og] : 0
TCP Flow Bytes Consumed[S2C][Tm] : 0
TCP Client Close Done   : 0x0
TCP Server Close Done   : 0x0
TCP Client FIN Rcvd     : 0x0
TCP Server FIN Rcvd     : 0x0
TCP Client RST Rcvd     : 0x0
TCP Server RST Rcvd     : 0x0
TCP Client FIN Sent     : 0x0
TCP Server FIN Sent     : 0x0
Flow Cleanup State      : 0x0
AD State            : AD_STATE_TX_ACK
AD Nego Role        : AD_ROLE_EDGE
AD peer ID          : 0xc0a80d01
AD configured Policy: 0x8
AD derived Policy   : 0x8
AD peer Policy      : 0x0
AD applied Policy   : 0x0
AOIM sync Needed    : No
Client Resume Enq Count : 0
Client Resume Enq Ign   : 0
Client Resume Process   : 0
Client Resume Process Ign : 0
Server Resume Enq Count : 0
Server Resume Enq Ign   : 0
Server Resume Process   : 0
Server Resume Process Ign : 0
DRE C2S Paused Count        : 0
DRE C2S Resumed Sent Count  : 0
DRE C2S Resume Recv Count   : 0
DRE S2C Paused Count        : 0
DRE S2C Resume Sent Count   : 0
DRE S2C Resume Recv Count   : 0
HTTP C2S Paused Count        : 0
HTTP C2S Resumed Sent Count  : 0
HTTP C2S Resume Recv Count   : 0
HTTP S2C Paused Count        : 0
HTTP S2C Resume Sent Count   : 0
HTTP S2C Resume Recv Count   : 0
SSL RD Pause/fail C2S Orig  : 0/0
SSL RD Resume Notify C2S Og : 0
SSL RD Resume C2S Orig      : 0
SSL RD Pause/fail C2S Term  : 0/0
SSL RD Resume Notify C2S Tm : 0
SSL RD Resume C2S Term      : 0
SSL RD Pause/fail S2C Orig  : 0/0
SSL RD Resume Notify S2C Og : 0
SSL RD Resume S2C Orig      : 0
```

```
SSL RD Pause/fail S2C Term  : 0/0
SSL RD Resume Notify S2C Tm : 0
SSL RD Resume S2C Term      : 0
SSL Proxy Client Bytes [C2S]: 0
SSL Proxy Client Bytes [S2C]: 0
SSL Proxy Server Bytes [C2S]: 0
SSL Proxy Server Bytes [S2C]: 0
Rx Client Queue Length      : 0
Rx Server Queue Length      : 0
SVC-to-Client Queue Length  : 0
SVC-to-Server Queue Length  : 0
TCP Flow Events
   1. time:2781.598055   ::   Event:TCPPROXY_EVT_FLOW_CREATED
   2. time:2781.598077   ::   Event:TCPPROXY_EVT_AD_RX_SYN_WITHOUT_OPTIONS
   3. time:2781.598128   ::   Event:TCPPROXY_EVT_SYNCACHE_ADDED
   4. time:2781.598145   ::   Event:TCPPROXY_EVT_AD_TX_EDGE_SYNACK_NO_OPTIONS
   5. time:2781.598473   ::   Event:TCPPROXY_EVT_AD_RX_EDGE_ACK
   6. time:2781.598621   ::   Event:TCPPROXY_EVT_ACCEPT_DONE
   7. time:2781.598739   ::   Event:TCPPROXY_EVT_AD_TX_EDGE_SYN
   8. time:2781.598747   ::   Event:TCPPROXY_EVT_CONNECT_START
   9. time:2781.599958   ::   Event:TCPPROXY_EVT_AD_RX_EDGE_SYNACK_WITH_OPTIONS
  10. time:2781.599984   ::   Event:TCPPROXY_EVT_AD_TX_EDGE_ACK
  11. time:2781.599985   ::   Event:TCPPROXY_EVT_CONNECT_DONE
  12. time:2781.600006   ::   Event:TCPPROXY_EVT_DATA_ENABLED_SUCCESS
  13. time:2781.600061   ::   Event:TCPPROXY_EVT_AD_TX_EDGE_ACK


TCP BBR Client Statistics:
 BBR States Transition
     STARTUP To DRAIN State     : 0
     STARTUP To PROBEBW State   : 1
     STARTUP To PROBERTT State  : 0
     DRAIN To PROBEBW State     : 0
     PROBEBW To PROBERTT State  : 1
     PROBERTT To STARTUP State  : 0
     PROBERTT To PROBEBW State  : 1
     IDLEEXIT To PROBEBW State  : 0
 HPTS Timer Started
     Wrong Timer                : 0
     Persistent Timeout         : 0
     Keepalive Timeout          : 0
     Connection Initialization  : 0
     BBR do segment unlock1     : 1
     BBR do segment unlock2     : 0
     PACE Segment               : 4752
     BBR output wtime error msg size: 0
     BBR output wtime default   : 0
     BBR do wtime error nonufs  : 7
 HPTS Timer Stopped
     Wrong Timer                : 0
     Cancel Timer               : 984
     Persistent Mode Exit       : 0
     BBR Do Segment Unlock      : 0
     Packets needs to be paced  : 1881
     Exempt early               : 0
     Delay exceed               : 17
     Connection Closed          : 0
 Pacing Delay (in us)
     Equals 0           : 0
     1 to 5             : 1885
     6 to 10            : 5
     11 to 20           : 1
     21 to 50           : 2
     50 to 100          : 1
```

```
    101 to 500         : 0
    501 to 1000        : 7
    Greater than 1000  : 2859
 RTT (in ms)
    Less than 1       : 1051
    Equals 1          : 1
    1 To 50           : 0
    51 To 100         : 0
    101 To 150        : 0
    151 To 200        : 0
    Greater than 200  : 0
 Bandwidth
    Less Than 1KBps     : 1
    1KBps To 250KBps    : 889
    251KBps To 500KBps  : 0
    500KBps To 1MBps    : 0
    1MBps To 2MBps      : 0
    2MBps To 5MBps      : 39
    5MBps To 10MBps     : 64
    Greater Than 10MBps : 59
 BBR Output Bytes               : 2628130
 TCP Segments Lost              : 0
 TCP Segment Sent               : 1958
 Retransmitted Segments         : 0
 Conn. drop due to no progress : 0
 TCP Segment Sent through HPTS : 1877
 Max Send Buffer Reached        : 4752
 Max Send Congestion Window     : 196370
 Current TCP Send Window        : 321024

HPTS Statistics:
 Timer Expired Early          : 0
 Delay in Timer Expiry        : 1894
 Callout Scheduled            : 0
 Lasttick is gt current tick : 0
 Maxticks Overflow            : 0
 Timer WakeUp Immediately     : 0
 Inp Added back to same slot : 0
 Distance To Travel Overflow : 0
 Available On Wheel Overflow : 0
 Available On Wheel lt Pacer : 0
 HPTS Is Hopelessly Behind    : 0
 HPTS Is Stuck In Loop        : 0
 HPTS Is Back On Sleep        : 0
 HPTS Wheel Wrapped           : 0
 HPTS Wheel Time Exceeded     : 0
 Forced close from FIN_WAIT_2  : 0

TCP BBR Server Statistics:
 BBR States Transition
    STARTUP To DRAIN State     : 0
    STARTUP To PROBEBW State   : 0
    STARTUP To PROBERTT State  : 0
    DRAIN To PROBEBW State     : 0
    PROBEBW To PROBERTT State  : 0
    PROBERTT To STARTUP State  : 0
    PROBERTT To PROBEBW State  : 0
    IDLEEXIT To PROBEBW State  : 0
 HPTS Timer Started
    Wrong Timer                 : 0
    Persistent Timeout          : 0
    Keepalive Timeout           : 0
    Connection Initialization   : 0
    BBR do segment unlock1      : 976
```

```
    BBR do segment unlock2      : 0
    PACE Segment                : 3
    BBR output wtime error msg size: 0
    BBR output wtime default    : 0
    BBR do wtime error nonufs   : 979
 HPTS Timer Stopped
    Wrong Timer                 : 0
    Cancel Timer                : 978
    Persistent Mode Exit        : 0
    BBR Do Segment Unlock       : 0
    Packets needs to be paced   : 978
    Exempt early                : 0
    Delay exceed                : 0
    Connection Closed           : 0
 Pacing Delay (in us)
    Equals 0           : 0
    1 to 5             : 1
    6 to 10            : 0
    11 to 20           : 0
    21 to 50           : 0
    50 to 100          : 0
    101 to 500         : 0
    501 to 1000        : 0
    Greater than 1000  : 1958
 RTT (in ms)
    Less than 1       : 0
    Equals 1          : 0
    1 To 50           : 2
    51 To 100         : 0
    101 To 150        : 0
    151 To 200        : 0
    Greater than 200  : 0
 Bandwidth
    Less Than 1KBps     : 1
    1KBps To 250KBps    : 1
    251KBps To 500KBps  : 0
    500KBps To 1MBps    : 0
    1MBps To 2MBps      : 0
    2MBps To 5MBps      : 0
    5MBps To 10MBps     : 0
    Greater Than 10MBps : 0
 BBR Output Bytes               : 139
 TCP Segments Lost              : 0
 TCP Segment Sent               : 980
 Retransmitted Segments         : 0
 Conn. drop due to no progress : 0
 TCP Segment Sent through HPTS : 1
 Max Send Buffer Reached        : 982
 Max Send Congestion Window     : 1073725440
 Current TCP Send Window        : 0

HPTS Statistics:
 Timer Expired Early          : 0
 Delay in Timer Expiry        : 1
 Callout Scheduled            : 0
 Lasttick is gt current tick : 0
 Maxticks Overflow            : 0
 Timer WakeUp Immediately     : 0
 Inp Added back to same slot : 0
 Distance To Travel Overflow : 0
 Available On Wheel Overflow : 0
 Available On Wheel lt Pacer : 0
 HPTS Is Hopelessly Behind    : 0
 HPTS Is Stuck In Loop        : 0
```

```
HPTS Is Back On Sleep       : 0
HPTS Wheel Wrapped          : 0
HPTS Wheel Time Exceeded    : 0
Forced close from FIN_WAIT_2  : 0
```

Related Commands

Command	Description
show sdwan appqoe flow closed all	Displays the summary of AppQoE expired flows on a device.
show sdwan appqoe flow closed flow-id *flow-id*	display AppQoE expired flow details for a signle specific flow on a device.
show sdwan appqoe flow vpn-id *vpn-id* **server-port** *server-port*	Displays the flows for a specific VPN on a device.

show sdwan appqoe flow vpn-id

To display flows for a specific VPN on a device, use the **show sdwan appqoe flow vpn-id** command in privileged EXEC mode.

show sdwan appqoe flow vpn-id *vpn-id* **server-port** *server-port*

Supported Parameters

vpn-id	Specify a vpn id.
server-port	Specify a server port number.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	This command was introduced.

Examples

The following sample output displays flows for a specific VPN.

```
Device# show sdwan appqoe flow closed vpn-id 1 server-port 443
Current Historical Optimized Flows: 101

Optimized Flows
---------------
T:TCP, S:SSL, U:UTD, D:DRE, H:HTTP
RR: DRE Reduction Ratio
```

```
Flow ID          VPN Source IP:Port Destination IP:Port Service RR%
53486969779402663 1  11.0.0.5:50621 23.0.0.7:443        TDS 99
53488479953969085 1  11.0.0.5:52664 23.0.0.72:443       T-
53484184343020025 1  11.0.0.7:45862 23.0.0.14:443       TDS 99
53486924218325306 1  11.0.0.7:50518 23.0.0.70:443       TDS 99
```

Related Commands

Command	Description
show sdwan appqoe flow closed flow-id *flow-id*	Displays AppQoE expired flow details on a device.
show sdwan appqoe flow flow-id *flow-id*	Displays AppQoE Active flow details on a device.
show sdwan appqoe flow closed all	Displays the summary of AppQoE expired flows on a device.

show sdwan appqoe status

To view the status of various AppQoE modules, use the **show sdwan appqoe status** command in privileged EXEC mode.

show sdwan appqoe status

This command has no keywords or arguments.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	This command was introduced.

Example

The following is sample output from the **show sdwan appqoe status** command.

```
Device# show sdwan appqoe status

APPQOE Status : GREEN

Service Status:

  SSLPROXY : GREEN

  TCPPROXY : GREEN

  SERVICE CHAIN : GREEN

  RESOURCE MANAGER : GREEN
```

show sdwan app-fwd cflowd collector

To display information about the configured cflowd collectors on Cisco IOS XE Catalyst SD-WAN devices, use the **show sdwan app-fwd cflowd collector** command in privileged exec mode.

show sdwan app-fwd cflowd collector

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Privileged exec (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

Cflowd monitors traffic flowing through Cisco IOS XE Catalyst SD-WAN devices in the overlay network and exports flow information to a collector, where it can be processed by an IPFIX analyzer. A flow-visibility policy must be enabled to see output from this command. This command can be used to display information about the configured cflowd collectors.

Example

The following example shows how to display the information about the configured cflowd collectors.

```
Device# show sdwan app-fwd cflowd collector
flow-monitors flow-export-statistics sdwan_flow_exporter_0
export-client
name "options drop-cause-table"
group Option
protocol-stats bytes-added 17220
protocol-stats bytes-sent 17220
protocol-stats bytes-dropped 0
protocol-stats records-added 492
protocol-stats records-sent 492
protocol-stats records-dropped 0
export-client
name sdwan_flow_monitor
group "Flow Monitor"
protocol-stats bytes-added 0
protocol-stats bytes-sent 0
protocol-stats bytes-dropped 0
protocol-stats records-added 0
protocol-stats records-sent 0
protocol-stats records-dropped 0
export-client
name "options application-attributes"
group Option
protocol-stats bytes-added 377196
protocol-stats bytes-sent 377196
protocol-stats bytes-dropped 0
protocol-stats records-added 1462
protocol-stats records-sent 1462
```

```
protocol-stats records-dropped 0
export-client
name "options application-name"
group Option
protocol-stats bytes-added 123670
protocol-stats bytes-sent 123670
protocol-stats bytes-dropped 0
protocol-stats records-added 1490
protocol-stats records-sent 1490
protocol-stats records-dropped 0
```

Table 31: Related Commands

Commands	Description
show sdwan app-fwd cflowd flow-count	Displays cflowd flow count.
show sdwan app-fwd cflowd flows	Displays cflowd flows.
show sdwan app-fwd cflowd statistics	Displays cflowd statistics information.
show sdwan app-fwd cflowd template	Displays cflowd template information.

show sdwan app-fwd cflowd flows

To display cflowd flow information on Cisco IOS XE Catalyst SD-WAN devices, use the **show sdwan app-fwd cflowd flows** command in privileged EXEC mode.

show sdwan app-fwd cflowd flows [**format table** | **vpn** *vpn-id* [**format table**]]

Syntax Description

format table	(Optional) Displays the flows in table format.
vpn *vpn-id*	(Optional) Displays the flows in a specific VPN. The vpn-id range is from 1 to 65530.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

Use **show sdwan app-fwd cflowd** command to monitor traffic flowing through Cisco IOS XE Catalyst SD-WAN devices in the overlay network and to export flow information to a collector, where it can be processed by an IPFIX analyzer. Flow-visibility policy must be enabled to see output in this command. This command can be used to display cflowd flow information.

Examples

The following example shows how to display cflowd flow information:

```
Device# show sdwan app-fwd cflowd flows
Generating output, this might take time, please wait ...
app-fwd cflowd flows vpn 32 src-ip 10.3.13.2 dest-ip 10.3.13.10 src-port 41708 dest-port
22 dscp 48 ip-proto 6
 tcp-cntrl-bits       24
 icmp-opcode          0
 total-pkts           45
 total-bytes          2736
 start-time           "Mon Nov 30 17:01:08 2020"
 egress-intf-name     GigabitEthernet0/0/1
 ingress-intf-name    internal0/0/rp:0
 application          unknown
 family               network-service
 drop-cause           "No Drop"
 drop-octets          0
 drop-packets         0
 sla-not-met          0
 color-not-met        0
 queue-id             2
 tos                  255
 dscp-output          63
 sampler-id           3
 fec-d-pkts           0
 fec-r-pkts           0
 pkt-dup-d-pkts-orig  0
 pkt-dup-d-pkts-dup   0
 pkt-dup-r-pkts       0
 pkt-cxp-d-pkts       0
 traffic-category     0
 ssl-read-bytes       0
 ssl-written-bytes    0
 ssl-en-read-bytes    0
 ssl-en-written-bytes 0
 ssl-de-read-bytes    0
 ssl-de-written-bytes 0
 ssl-service-type     0
 ssl-traffic-type     0
 ssl-policy-action    0
```

Table 32: Related Commands

Command	Description
show sdwan app-fwd cflowd collector	Displays cflowd collector information.
show sdwan app-fwd cflowd flow-count	Displays cflowd flow count.
show sdwan app-fwd cflowd statistics	Displays cflowd statistics information.
show sdwan app-fwd cflowd template	Displays cflowd template information.

show sdwan app-fwd cflowd flow-count

To display the number of current cflowd traffic flows on Cisco IOS XE Catalyst SD-WAN devices, use the **show sdwan app-fwd cflowd flow-count** command in privileged EXEC mode.

show sdwan app-fwd cflowd flow-count

Syntax Description This command has no keywords or arguments.

Command Default None

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines Cflowd monitors traffic flowing through Cisco IOS XE Catalyst SD-WAN devices in the overlay network and exports flow information to a collector, where it can be processed by an IPFIX analyzer. Flow-visibility policy must be enabled to see output from this command. This command can be used to display the number of current cflowd traffic flows.

Examples

The following example shows how to display the number of current cflowd traffic flows.

```
Device# show sdwan app-fwd cflowd flow-count
VPN  COUNT
------------
*    0
```

Table 33: Related Commands

Command	Description
show sdwan app-fwd cflowd collector	Displays cflowd collector information.
show sdwan app-fwd cflowd flows	Displays cflowd flows.
show sdwan app-fwd cflowd statistics	Displays cflowd statistics information.
show sdwan app-fwd cflowd template	Displays cflowd template information.

show sdwan app-fwd cflowd statistics

To display cflowd packet statistics on Cisco IOS XE Catalyst SD-WAN devices, use the **show sdwan app-fwd cflowd statistics** command in privileged EXEC mode.

show sdwan app-fwd cflowd statistics [**ftm**]

Syntax Description

ftm	(Optional) Displays cflowd Forwarding Table Manager (FTM) statistics information.

Command Default None

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command is qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

Use **show sdwan app-fwd cflowd** command to monitor traffic flowing through Cisco IOS XE Catalyst SD-WAN devices in the overlay network and to export flow information to a collector, where it can be processed by an IPFIX analyzer. Flow-visibility policy must be enabled to see output from this command. This command can be used to display cflowd packet statistics.

Examples

The following example shows how to display cflowd packet statistics.

```
Device# show sdwan app-fwd cflowd statistics
      data_packets              :      30996
      template_packets          :      36
      total-packets             :      9
      flow-refresh              :      0
      flow-ageout               :      0
      flow-end-detected         :      0
      flow-end-forced           :      0
      flow-rate-limit-drop      :      0
```

Table 34: Related Commands

Command	Description
show sdwan app-fwd cflowd collector	Displays cflowd collector information.
show sdwan app-fwd cflowd flow-count	Displays cflowd flow count.
show sdwan app-fwd cflowd flows	Displays cflowd flows.
show sdwan app-fwd cflowd template	Displays cflowd template information.

show sdwan app-fwd cflowd template

To display the cflowd template information that the Cisco IOS XE Catalyst SD-WAN device transmits periodically to the cflowd collector, use the **show sdwan app-fwd cflowd flows** command in privileged EXEC mode.

show sdwan app-fwd cflowd template

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command is qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

Use **show sdwan app-fwd cflowd** to monitor traffic flowing through Cisco IOS XE Catalyst SD-WAN devices in the overlay network and to export flow information to a collector, where it can be processed by an IPFIX analyzer. A cflowd template defines the location of cflowd collectors, how often sets of sampled flows are sent to the collectors, and how often the template is sent to the collectors.

This command can be used to display the cflowd template information that the Cisco IOS XE Catalyst SD-WAN device transmits periodically to the cflowd collector.

Examples

The following example shows how to display the cflowd template information that the Cisco IOS XE Catalyst SD-WAN device transmits periodically to the cflowd collector.

```
Device# show sdwan app-fwd cflowd template
app cflowd template name ""
app cflowd template flow-active-timeout 600
app cflowd template flow-inactive-timeout 60
app cflowd template template-refresh 0
```

Table 35: Related Commands

Command	Description
show sdwan app-fwd cflowd collector	Displays cflowd collector information.
show sdwan app-fwd cflowd flow-count	Displays cflowd flow count.
show sdwan app-fwd cflowd flows	Displays cflowd flows.
show sdwan app-fwd cflowd statistics	Displays cflowd statistics information.

show sdwan app-fwd dpi flows

show sdwan app-fwd dpi flows—Display flow information for the application-aware applications running on the Cisco IOS XE Catalyst SD-WAN device.

show sdwan app-fwd dpi flows [**vpn** *vpn-id*] [**detail**]

Syntax Description

None	List all the flows which go through the Cisco IOS XE Catalyst SD-WAN device

detail	Detailed Information Display detailed information about DPI traffic flows, including total packet and octet counts, and which tunnel (TLOC) the flow was received and transmitted on. **Note** This command displays all the flow information except for Border Gateway Protocols, Internet Control Message Protocol for IPv4, Internet Control Message Protocol for IPv6, Open Shortest Path First, Multicast Transfer Protocol, and Protocol-Independent Multicast in a policy as they are not supported. These application bypass DPI and matching DPI on the applications do not affect a policy.
vpn *vpn-id*	Specific VPN List all application flows running in the subnets in the specific VPN.

Command History

Release	Modification
Cisco IOS XE Release 17.2.1v	Command introduced.

Examples

show sdwan app-fwd dpi flows

```
Device# show sdwan app-fwd dpi flows

app-fwd cflowd flows vpn 7 src-ip 10.7.20.8 dest-ip 10.7.50.10 src-port 0 dest-port 2048
dscp 0 ip-proto 1
 tcp-cntrl-bits           24
 icmp-opcode              2048
 total-pkts               23392
 total-bytes              2339200
 start-time               "Mon Dec 26 09:48:28 2022"
 egress-intf-name         Null
 ingress-intf-name        GigabitEthernet0/0/0
 application              ping
 family                   network-service
 drop-cause               "No Drop"
 drop-octets              0
 drop-packets             0
 sla-not-met              0
 color-not-met            0
 queue-id                 2
 tos                      0
 dscp-output              0
 sampler-id               0
 fec-d-pkts               0
 fec-r-pkts               0
 pkt-dup-d-pkts-orig      0
 pkt-dup-d-pkts-dup       0
 pkt-dup-r-pkts           0
 pkt-cxp-d-pkts           0
 traffic-category         0
 service-area             0
 ssl-read-bytes           0
```

```
 ssl-written-bytes        0
 ssl-en-read-bytes        0
 ssl-en-written-bytes     0
 ssl-de-read-bytes        0
 ssl-de-written-bytes     0
 ssl-service-type         0
 ssl-traffic-type         0
 ssl-policy-action        0
 appqoe-action            0
 appqoe-sn-ip             0.0.0.0
 appqoe-pass-reason       0
 appqoe-dre-input-bytes   0
 appqoe-dre-input-packets 0
 appqoe-flags             0
```

```
Device# show sdwan app-fwd dpi flows table
Generating output, this might take time, please wait ...


                                                                                 PKT
   PKT    PKT   PKT                                        SSL              SSL
                                                    APPQOE  APPQOE
                                                          TCP

                                 SLA  COLOR                                  FEC   FEC   DUP
D  DUP D  DUP   CXP                      SSL    SSL       EN      SSL EN   DE      SSL DE
SSL      SSL      SSL                      APPQOE  DRE      DRE
                             SRC    DEST          IP      CNTRL  ICMP    TOTAL  TOTAL

       DROP      DROP     DROP      NOT  NOT    QUEUE       DSCP    SAMPLER  D      R      PKTS
   PKTS   R      D      TRAFFIC   SERVICE  READ   WRITTEN  READ   WRITTEN  READ   WRITTEN
SERVICE  TRAFFIC  POLICY  APPQOE  APPQOE   PASS     INPUT   INPUT    APPQOE
VPN  SRC IP      DEST IP     PORT   PORT   DSCP  PROTO  BITS   OPCODE  PKTS   BYTES    START
 TIME                 EGRESS INTF NAME      INGRESS INTF NAME     APPLICATION  FAMILY
     CAUSE    OCTETS  PACKETS  MET  MET    ID     TOS  OUTPUT  ID       PKTS  PKTS  ORIG
 DUP    PKTS  PKTS  CATEGORY  AREA     BYTES  BYTES    BYTES  BYTES    BYTES  BYTES    TYPE
     TYPE     ACTION  ACTION  SN IP    REASON  BYTES   PACKETS  FLAGS
-----------------------------------------------------------------------------------------------
7    10.7.20.8   10.7.50.10  0      2048   0     1      24     2048    27886  2788600  Mon
 Dec 26 09:48:28 2022  Null                 GigabitEthernet0/0/0  ping
network-service  No Drop  0       0        0    0      2      0    0       0        0
0     0      0      0     0     0        0        0      0        0      0        0
0        0        0       0       0       0.0.0.0  0       0       0        0
7    10.7.50.10  10.7.20.8   11983  22     48     6      24     0       5625   225072   Mon
 Dec 26 09:48:28 2022  GigabitEthernet0/0/0  internal0/0/rp:0      ssh          terminal
      No Drop  0       0        0    0      2      0    0       0        0     0     0
   0      0     0     0        0        0      0        0      0        0      0        0
        0        0       0       0.0.0.0  0       0       0        0
7    10.7.20.8   10.7.50.10  47897  22     48     6      24     0       10403  416264   Mon
 Dec 26 09:48:28 2022  internal0/0/rp:0      GigabitEthernet0/0/0  ssh          terminal
      No Drop  0       0        0    0      2      0    0       0        0     0     0
   0      0     0     0        0        0      0        0      0        0      0        0
        0        0       0       0.0.0.0  0       0       0        0
7    10.7.50.10  10.7.20.8   22     47897  48     6      24     0       19441  1477468  Mon
 Dec 26 09:48:28 2022  GigabitEthernet0/0/0  internal0/0/rp:0      ssh          terminal
      No Drop  0       0        0    0      2      0    0       0        0     0     0
   0      0     0     0        0        0      0        0      0        0      0        0
        0        0       0       0.0.0.0  0       0       0        0
7    10.7.20.8   10.7.50.10  22     11983  48     6      24     0       10532  800432   Mon
 Dec 26 09:48:28 2022  internal0/0/rp:0      GigabitEthernet0/0/0  ssh          terminal
      No Drop  0       0        0    0      2      0    0       0        0     0     0
   0      0     0     0        0        0      0        0      0        0      0        0
        0        0       0       0.0.0.0  0       0       0        0
                                  SOURCE  DEST
```

```
Device# show sdwan app-fwd dpi flows
app-fwd cflowd flows vpn 7 src-ip 10.7.50.10 dest-ip 10.7.20.8 src-port 11983 dest-port 22
 dscp 48 ip-proto 6
 tcp-cntrl-bits           24
 icmp-opcode              0
 total-pkts               3192
 total-bytes              127716
 start-time               "Mon Dec 26 09:48:28 2022"
 egress-intf-name         GigabitEthernet0/0/0
 ingress-intf-name        internal0/0/rp:0
 application              ssh
 family                   terminal
 drop-cause               "No Drop"
 drop-octets              0
 drop-packets             0
 sla-not-met              0
 color-not-met            0
 queue-id                 2
 tos                      0
 dscp-output              0
 sampler-id               0
 fec-d-pkts               0
 fec-r-pkts               0
 pkt-dup-d-pkts-orig      0
 pkt-dup-d-pkts-dup       0
 pkt-dup-r-pkts           0
 pkt-cxp-d-pkts           0
 traffic-category         0
 service-area             0
 ssl-read-bytes           0
 ssl-written-bytes        0
 ssl-en-read-bytes        0
 ssl-en-written-bytes     0
 ssl-de-read-bytes        0
 ssl-de-written-bytes     0

 ssl-service-type         0
 ssl-traffic-type         0
 ssl-policy-action        0
 appqoe-action            0
 appqoe-sn-ip             0.0.0.0
 appqoe-pass-reason       0
 appqoe-dre-input-bytes   0
 appqoe-dre-input-packets 0
 appqoe-flags             0
```

show sdwan app-fwd dpi summary

To display the DPI summary on Cisco IOS XE Catalyst SD-WAN devices, use the **show sdwan app-fwd dpi summary** command in privileged EXEC mode.

show sdwan app-fwd dpi summary

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command is qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines Deep Packet Inspection (DPI) offers control over how data packets from specific applications or application families are forwarded across the network, allowing you to assign the traffic to be carried by specific tunnels. App-visibility policy must be enabled to see output from this command.

Use **show sdwan app-fwd dpi summary** command to display the DPI summary on Cisco IOS XE Catalyst SD-WAN devices.

Examples

The following example shows how to display the DPI summary on Cisco IOS XE Catalyst SD-WAN devices.

```
Device# show sdwan app-fwd dpi summary
                                                          ACTIVE  INACTIVE
                                                          FLOWS   FLOWS
                    CACHE  CURRENT  HIGH      FLOWS FLOWS TIMED   TIMED
NAME                SIZE   ENTRIES  WATERMARK ADDED AGED  OUT     OUT
-------------------------------------------------------------------------------
sdwan_flow_monitor  80000  0        0          0      0      0       0
```

Table 36: Related Commands

Command	Description
show sdwan app-fwd dpi flows	Displays DPI flows.

show sdwan app-route sla-class

To display application-aware routing SLA classes on Cisco IOS XE Catalyst SD-WAN devices, use the **show sdwan app-route sla-class** command in privileged EXEC mode.

show sdwan app-route sla-class
show sdwan app-route sla-class
jitter *jitter-configured-value* | **latency** *latency-configured-value* | **loss** *loss-percentage* | **name** *sla-class-name*

Syntax Description

None	Displays information for all index, name, packet jitter, packet latency, and packet loss values.
jitter *jitter-configured-value*	(Optional) Displays information for all index, name, packet jitter, packet latency, and packet loss values for the specified jitter value in milliseconds. <0 - 4294967295>

latency *latency-configured-value*	(Optional) Displays information for all index, name, packet jitter, packet latency, and packet loss values for the specified latency value in milliseconds. <0 - 4294967295>
loss *loss-percentage*	(Optional) Displays information for all index, name, packet jitter, packet latency, and packet loss values for the specified loss value in percentage. <0 - 100>
name *sla-class-name*	(Optional) Displays information for all index, name, packet jitter, packet latency, and packet loss values for the specified SLA class name.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

The action taken in application-aware routing is applied based on an SLA (a service-level agreement). An SLA class is defined by the maximum jitter, maximum latency, maximum packet loss, or a combination of these values, for the data plane tunnels of the device.

Use this command to display information for application-aware routing SLA classes configured on Cisco IOS XE Catalyst SD-WAN devices.

Example

The following example shows how to display index, name, packet loss, packet latency, and packet jitter information for all application-aware routing SLA classes configured on Cisco IOS XE Catalyst SD-WAN devices.

```
Device# show sdwan app-route sla-class
INDEX NAME LOSS LATENCY JITTER
------------------------------------------------------
0 __all_tunnels__ 0 0 0
1 test_sla_class 100 50 0
2 test_sla_class2 10 5 50
```

The following example shows how to display index, name, packet loss, packet latency, and packet jitter information for all application-aware routing SLA classes with latency value of 50 configured on Cisco IOS XE Catalyst SD-WAN devices.

```
Device# show sdwan app-route sla-class latency 50
INDEX NAME LOSS LATENCY JITTER
------------------------------------------------------
1 test_sla_class 100 50 0
```

The following example shows how to display index and packet jitter information for all application-aware routing SLA classes configured on Cisco IOS XE Catalyst SD-WAN devices.

```
Device# show sdwan app-route sla-class jitter
INDEX JITTER
-----------------
```

```
0 0
1 0
2 50
```

show sdwan app-route stats

To display statistics about data plane traffic jitter, loss, and latency and other interface characteristics for all operational data plane tunnels on Cisco IOS XE Catalyst SD-WAN devices, use the **show sdwan app-route stats** command in privileged EXEC mode.

show sdwan app-route stats
{ [**local-color** *color*] | [**remote-color** *color*] | [**remote-system-ip** *ip-address*] }

Syntax Description

local-color *color*	(Optional) Displays statistics about data plane traffic jitter, loss, and latency and other interface characteristics for the specified local color.
remote-color *color*	(Optional) Displays statistics about data plane traffic jitter, loss, and latency and other interface characteristics for the specified remote color.
remote-system-ip *ip-address*	(Optional) Displays statistics about data plane traffic jitter, loss, and latency and other interface characteristics for the specified remote system IP.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

The Bidirectional Forwarding Detection (BFD) protocol runs over all data plane tunnels between Cisco IOS XE SD-WAN devices, monitoring the liveness, and network and path characteristics of the tunnels. Application-aware routing uses the information gathered by BFD to determine the transmission performance of the tunnels. Performance is reported in terms of packet latency and packet loss on the tunnel.

BFD sends Hello packets periodically to test the liveness of a data plane tunnel and to check for faults on the tunnel. These Hello packets provide a measurement of packet loss and packet latency on the tunnel. The Cisco IOS XE SD-WAN device records the packet loss and latency statistics over a sliding window of time. BFD keeps track of the six most recent sliding windows of statistics, placing each set of statistics in a separate bucket.

If you configure an application-aware routing policy for the device, it is these statistics that the router uses to determine whether a data plane tunnel's performance matches the requirements of the policy's SLA.

This command can be used to display statistics about data plane traffic jitter, loss, and latency and other interface characteristics for all operational data plane tunnels on Cisco IOS XE SD-WAN devices.

Example

The following example shows how to display statistics about data plane traffic jitter, loss, and latency and other interface characteristics for all operational data plane tunnels on Cisco IOS XE SD-WAN devices.

```
Device# show sdwan app-route status
app-route statistics 100.64.0.30 100.64.0.2 ipsec 12426 12366
remote-system-ip 10.1.0.1
local-color mpls
remote-color mpls
mean-loss 0
mean-latency 2
mean-jitter 0
sla-class-index 0
IPV6 TX IPV6 RX
TOTAL AVERAGE AVERAGE TX DATA RX DATA DATA DATA
INDEX PACKETS LOSS LATENCY JITTER PKTS PKTS PKTS PKTS
------------------------------------------------------------------------------
0 6 0 2 0 0 0 0 0
1 6 0 2 1 0 0 0 0
2 5 0 2 0 0 0 0 0
3 6 0 2 0 0 0 0 0
4 5 0 2 0 0 0 0 0
5 6 0 2 0 0 0 0 0
app-route statistics 100.64.2.2 100.64.2.26 ipsec 12366 12366
remote-system-ip 10.1.0.1
local-color biz-internet
remote-color biz-internet
mean-loss 0
mean-latency 11
mean-jitter 9
sla-class-index 0
IPV6 TX IPV6 RX
TOTAL AVERAGE AVERAGE TX DATA RX DATA DATA DATA
INDEX PACKETS LOSS LATENCY JITTER PKTS PKTS PKTS PKTS
------------------------------------------------------------------------------
0 6 0 10 7 10 10 0 0
1 5 0 9 3 0 0 0 0
2 6 0 12 12 11 11 0 0
3 5 0 10 3 0 0 0 0
4 6 0 9 9 10 10 0 0
5 6 0 12 16 0 0 0 0
app-route statistics 100.64.0.30 100.64.0.6 ipsec 12426 12366
remote-system-ip 10.1.0.2
local-color mpls
remote-color mpls
mean-loss 0
mean-latency 2
mean-jitter 0
sla-class-index 0
IPV6 TX IPV6 RX
TOTAL AVERAGE AVERAGE TX DATA RX DATA DATA DATA
INDEX PACKETS LOSS LATENCY JITTER PKTS PKTS PKTS PKTS
------------------------------------------------------------------------------
0 5 0 1 0 0 0 0 0
1 6 0 1 0 0 0 0 0
2 5 0 2 0 0 0 0 0
3 6 0 1 0 0 0 0 0
4 6 0 2 0 0 0 0 0
5 5 0 2 0 0 0 0 0
app-route statistics 100.64.2.2 100.64.2.30 ipsec 12366 12366
```

```
remote-system-ip 10.1.0.2
local-color biz-internet
remote-color biz-internet
mean-loss 0
mean-latency 13
mean-jitter 7
sla-class-index 0
IPV6 TX IPV6 RX
TOTAL AVERAGE AVERAGE TX DATA RX DATA DATA DATA
INDEX PACKETS LOSS LATENCY JITTER PKTS PKTS PKTS PKTS
------------------------------------------------------------------------------
0 6 0 16 8 10 12 0 0
1 5 0 12 6 0 0 0 0
2 6 0 10 11 11 12 0 0
3 6 0 14 9 0 0 0 0
4 5 0 14 4 11 11 0 0
5 6 0 14 6 0 0 0 0
```

The following example shows how to display statistics about data plane traffic jitter, loss, and latency and other interface characteristics for the specified local color mpls on Cisco IOS XE SD-WAN devices.

```
Device# show sdwan app-route stats local-color mpls
app-route statistics 100.64.0.30 100.64.0.2 ipsec 12426 12366
remote-system-ip 10.1.0.1
local-color mpls
remote-color mpls
mean-loss 0
mean-latency 2
mean-jitter 0
sla-class-index 0
IPV6 TX IPV6 RX
TOTAL AVERAGE AVERAGE TX DATA RX DATA DATA DATA
INDEX PACKETS LOSS LATENCY JITTER PKTS PKTS PKTS PKTS
------------------------------------------------------------------------------
0 6 0 2 0 0 0 0 0
1 6 0 2 1 0 0 0 0
2 5 0 2 0 0 0 0 0
3 6 0 2 0 0 0 0 0
4 5 0 2 0 0 0 0 0
5 6 0 2 0 0 0 0 0
app-route statistics 100.64.0.30 100.64.0.6 ipsec 12426 12366
remote-system-ip 10.1.0.2
local-color mpls
remote-color mpls
mean-loss 0
mean-latency 2
mean-jitter 0
sla-class-index 0
IPV6 TX IPV6 RX
TOTAL AVERAGE AVERAGE TX DATA RX DATA DATA DATA
INDEX PACKETS LOSS LATENCY JITTER PKTS PKTS PKTS PKTS
------------------------------------------------------------------------------
0 5 0 1 0 0 0 0 0
1 6 0 1 0 0 0 0 0
2 5 0 2 0 0 0 0 0
3 6 0 1 0 0 0 0 0
4 6 0 2 0 0 0 0 0
5 5 0 2 0 0 0 0 0
```

The following example shows how to display statistics about data plane traffic jitter, loss, and latency and other interface characteristics for the specified remote system IP 10.1.0.1 on Cisco IOS XE SD-WAN devices.

```
Device# show sdwan app-route stats remote-system-ip 10.1.0.1

app-route statistics 100.64.0.30 100.64.0.2 ipsec 12426 12366
remote-system-ip 10.1.0.1
local-color mpls
remote-color mpls
mean-loss 0
mean-latency 2
mean-jitter 0
sla-class-index 0
IPV6 TX IPV6 RX
TOTAL AVERAGE AVERAGE TX DATA RX DATA DATA DATA
INDEX PACKETS LOSS LATENCY JITTER PKTS PKTS PKTS PKTS
------------------------------------------------------------------------------
0 6 0 2 0 0 0 0 0
1 6 0 2 1 0 0 0 0
2 5 0 2 0 0 0 0 0
3 6 0 2 0 0 0 0 0
4 5 0 2 0 0 0 0 0
5 6 0 2 0 0 0 0 0
app-route statistics 100.64.2.2 100.64.2.26 ipsec 12366 12366
remote-system-ip 10.1.0.1
local-color biz-internet
remote-color biz-internet
mean-loss 0
mean-latency 11
mean-jitter 9
sla-class-index 0
IPV6 TX IPV6 RX
TOTAL AVERAGE AVERAGE TX DATA RX DATA DATA DATA
INDEX PACKETS LOSS LATENCY JITTER PKTS PKTS PKTS PKTS
------------------------------------------------------------------------------
0 6 0 10 7 10 10 0 0
1 5 0 9 3 0 0 0 0
2 6 0 12 12 11 11 0 0
3 5 0 10 3 0 0 0 0
4 6 0 9 9 10 10 0 0
5 6 0 12 16 0 0 0 0
```

Related Commands

Command	Description
show sdwan app-route sla-class	Displays application-aware routing SLA classes.

show sdwan bfd history

To display Cisco Catalyst SD-WAN BFD history on Cisco IOS XE Catalyst SD-WAN devices, use the **show sdwan bfd history** command in privileged EXEC mode.

show sdwan bfd history

Syntax Description This command has no keywords or arguments.

Command Default None

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE SD-WAN Release 17.2.1v	This command is supported for Cisco Catalyst SD-WAN.
Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	The command output shows BFD automatic suspension information.

Usage Guidelines

BFD provides rapid failure detection times between forwarding engines, while maintaining low overhead. If a BFD session is down, it implies that no traffic can flow between those TLOCs. If you identify any traffic disruption between a pair of TLOCs or notice that the session flap count has increased, use the **show sdwan bfd history** command to check the history of your BFD sessions.

Use this command to display Cisco Catalyst SD-WAN BFD history on Cisco IOS XE Catalyst SD-WAN devices.

Example

The following example shows how to display Cisco Catalyst SD-WAN BFD history on Cisco IOS XE Catalyst SD-WAN devices.

Note Beginning with Cisco IOS XE Catalyst SD-WAN Release 17.10.1a, a suspended flag, `Sus`, is added for identifying BFD sessions that are suspended for preventing flapping of BFD sessions.

Related Commands

Command	Description
request platform software sdwan auto-suspend reset	Brings all BFD sessions out of suspension.
show sdwan bfd sessions	Displays Cisco Catalyst SD-WAN BFD sessions.
show sdwan bfd summary	Displays a Cisco Catalyst SD-WAN BFD summary.
show sdwan bfd tloc-summary-list	Displays a Cisco Catalyst SD-WAN BFD TLOC summary list.

show sdwan bfd sessions

To display information about the Cisco SD-WAN BFD sessions on Cisco IOS XE Catalyst SD-WAN devices, use the **show sdwan bfd sessions** command in privileged EXEC mode.

show sdwan bfd sessions [**table** | **alt** | **region-access** | **region-core** | **suspend** { **all** | **local-color** *local-color-value* }]

Syntax Description

table	(Optional) Display output in table format.

alt	(Optional) Display additional information for BFD sessions, such as BFD local discriminator (LD) and if a BFD session is flagged as suspended.
region-access	(Optional) Multi-Region Fabric access region.
region-core	(Optional) Multi-Region Fabric core region.
suspend	(Optional) Display BFD sessions in suspension.
all	(Optional) Display all BFD sessions in suspension.
local-color *local-color-value*	(Optional) Display BFD sessions with a local color.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	This command is supported for Cisco Catalyst SD-WAN.
Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	This command was modified. Added the **suspend** and **alt** keywords. The command output shows BFD automatic suspension information.

Usage Guidelines

BFD provides rapid failure detection times between forwarding engines, while maintaining low overhead. If a BFD session is down, it implies that no traffic can flow between those TLOCs. If you identify any traffic disruption between a pair of TLOCs or notice that the session flap count has increased, use the **show sdwan bfd sessions** command to check the status of your Cisco SD-WAN BFD sessions.

Use this command to display information about the Cisco SD-WAN BFD sessions running on Cisco IOS XE Catalyst SD-WAN devices.

Examples

The following sample output from the **show sdwan bfd sessions** command displays information about the Cisco SD-WAN BFD sessions running on Cisco IOS XE Catalyst SD-WAN devices.

```
Device# show sdwan bfd sessions
                       SOURCE TLOC    REMOTE TLOC               DST PUBLIC   DST PUBLIC        DETECT      TX
SYSTEM IP  SITE ID STATE  COLOR          COLOR         SOURCE IP   IP           PORT       ENCAP  MULTIPLIER  INTERVAL(msec) UPTIME      TRANSITIONS
-----------------------------------------------------------------------------------------------------------------------------------------------------

10.1.0.1   100     up     biz-internet   biz-internet  10.64.2.2  10.64.2.26  12366       ipsec    7           1000           0:00:03:14  0
10.1.0.2   100     up     biz-internet   biz-internet  10.64.2.2  10.64.2.30  12366       ipsec    7           1000           0:00:03:13  0
10.4.0.1   400     up     biz-internet   biz-internet  10.64.2.2  10.64.2.6   18464       ipsec    7           1000           0:00:03:14  0
```

The following sample output from the **show sdwan bfd sessions suspend** command displays the total suspend count and the resuspend count.

```
Device# show sdwan bfd sessions suspend

                       SOURCE TLOC   REMOTE TLOC               DST PUBLIC       DST PUBLIC        RE-SUSPEND  SUSPEND       TOTAL     SUSPEND
SYSTEM IP        STATE    COLOR         COLOR         SOURCE IP     IP             PORT       ENCAP  COUNT       TIME LEFT     COUNT     DURATION
-----------------------------------------------------------------------------------------------------------------------------------------------
172.16.255.14    up       lte           lte           10.1.15.15    10.1.14.14     12426      ipsec  0           0:00:19:52    18        0:00:00:07
```

The following sample output from the **show sdwan bfd sessions alt** command indicates if a BFD session has been suspended:

```
Device# show sdwan bfd sessions alt

*Sus = Suspend
*NA  = Flag Not Set
                                    SOURCE TLOC     REMOTE TLOC                 DST PUBLIC      DST PUBLIC
SYSTEM IP         SITE ID   STATE   COLOR           COLOR           SOURCE IP   IP              PORT        ENCAP  BFD-LD   FLAGS   UPTIME
-------------------------------------------------------------------------------------------------------------------------------------------
172.16.255.14     400       up        3g              lte           10.0.20.15  10.1.14.14      12426       ipsec  20004    NA      0:19:30:40
172.16.255.14     400       up        lte             lte           10.1.15.15  10.1.14.14      12426       ipsec  20003    Sus     0:00:02:46
172.16.255.16     600       up        3g              lte           10.0.20.15  10.0.106.1      12366       ipsec  20002    NA      0:19:30:40
172.16.255.16     600       up        lte             lte           10.1.15.15  10.0.106.1      12366       ipsec  20001    NA      0:19:20:14
```

The following sample output from the **show sdwan bfd sessions table** command displays the traffic with ports in the control range:

```
Device# show sdwan bfd sessions table
                                    SRC     DST                     SITE                                                DETECT      TX
SRC IP       DST IP       PROTO     PORT    PORT    SYSTEM IP       ID    LOCAL COLOR     COLOR           STATE         MULTIPLIER  INTERVAL  UPTIME      TRANSITIONS
-----------------------------------------------------------------------------------------------------------------------------------------------------------
10.1.15.15   10.0.5.11    ipsec     12366   12367   172.16.255.11   100   lte             lte             up            7           1000      0:01:37:43  3
10.1.19.15   10.0.5.11    ipsec     12406   12367   172.16.255.11   100   biz-internet    lte             up            7           1000      0:00:00:51  0
10.1.15.15   10.1.14.14   ipsec     12366   12366   172.16.255.14   400   lte             lte             up            7           1000      0:01:37:43  3
10.1.19.15   10.1.14.14   ipsec     12406   12366   172.16.255.14   400   biz-internet    lte             up            7           1000      0:00:00:51  0
10.1.15.15   10.1.16.16   ipsec     12366   12386   172.16.255.16   600   lte             biz-internet    up            7           1000      0:00:31:41  0
10.1.19.15   10.1.16.16   ipsec     12406   12386   172.16.255.16   600   biz-internet    biz-internet    down          7           1000      NA          0
10.1.15.15   10.0.5.21    ipsec     12366   12377   172.16.255.21   100   lte             lte             up            7           1000      0:01:37:43  3
10.1.19.15   10.0.5.21    ipsec     12406   12377   172.16.255.21   100   biz-internet    lte             up            7           1000      0:00:00:51  0
```

Related Commands

Command	Description
request platform software sdwan auto-suspend reset	Brings all BFD sessions out of suspension.
show sdwan bfd history	Displays Cisco SD-WAN BFD history.
show sdwan bfd summary	Displays a Cisco SD-WAN BFD summary.
show sdwan bfd tloc-summary-list	Displays a Cisco SD-WAN BFD TLOC summary list.

show sdwan bfd sessions region-access

To display a list of bidirectional forwarding detection (BFD) sessions in the Hierarchical SD-WAN access region (any region other than the core region), use the **show sdwan bfd sessions region-access** command in privileged EXEC mode.

sdwan sdwan bfd sessions region-access

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Examples

```
Device# show sdwan bfd sessions region-access
                                  REGION              SOURCE TLOC     REMOTE TLOC                                    DST PUBLIC                      DST
PUBLIC          DETECT      TX
SYSTEM IP         SITE ID   ID     STATE        COLOR           COLOR          SOURCE IP                              IP                              PORT
        ENCAP   MULTIPLIER  INTERVAL(msec) UPTIME          TRANSITIONS
-------------------------------------------------------------------------------------------------------------------------------------------------------
172.21.54.10      2100      2      up           lte             lte            172.16.21.11                           172.16.1.1                      12366
        ipsec   7           1000           12:04:30:17     6
172.21.55.10      2200      2      up           lte             lte            172.16.21.11                           172.16.2.1                      12366
        ipsec   7           1000           12:04:29:47     8
172.21.14.10      22200     2      up           lte             lte            172.16.21.11                           172.16.22.11                    12366
        ipsec   7           1000           12:04:35:03     7
172.21.54.10      2100      2      up           lte             3g             172.16.21.11                           172.17.1.1                      12366
        ipsec   7           1000           12:04:30:01     7
172.21.55.10      2200      2      up           lte             3g             172.16.21.11                           172.17.2.1                      12366
        ipsec   7           1000           12:04:30:05     7
172.21.14.10      22200     2      up           lte             3g             172.16.21.11                           172.17.22.11                    12366
        ipsec   7           1000           12:04:29:27     9
172.21.54.10      2100      2      up           3g              lte            172.17.21.11                           172.16.1.1                      12366
        ipsec   7           1000           12:04:29:27     8
172.21.55.10      2200      2      up           3g              lte            172.17.21.11                           172.16.2.1                      12366
        ipsec   7           1000           12:04:29:26     8
172.21.14.10      22200     2      up           3g              lte            172.17.21.11                           172.16.22.11                    12366
        ipsec   7           1000           12:04:29:26     8
172.21.54.10      2100      2      up           3g              3g             172.17.21.11                           172.17.1.1                      12366
        ipsec   7           1000           12:04:29:27     8
172.21.55.10      2200      2      up           3g              3g             172.17.21.11                           172.17.2.1                      12366
        ipsec   7           1000           12:04:29:26     9
172.21.14.10      22200     2      up           3g              3g             172.17.21.11                           172.17.22.11                    12366
        ipsec   7           1000           12:04:29:26     0
```

show sdwan bfd sessions region-core

To display a list of bidirectional forwarding detection (BFD) sessions in the Hierarchical SD-WAN core region, use the **show sdwan bfd sessions region-core** command in privileged EXEC mode.

sdwan sdwan bfd sessions region-core

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Examples

```
Device# show sdwan bfd sessions region-core
                                  REGION              SOURCE TLOC     REMOTE TLOC                                    DST PUBLIC                      DST
 PUBLIC          DETECT      TX
SYSTEM IP         SITE ID   ID     STATE        COLOR           COLOR          SOURCE IP                              IP                              PORT
        ENCAP   MULTIPLIER  INTERVAL(msec) UPTIME          TRANSITIONS
-------------------------------------------------------------------------------------------------------------------------------------------------------
172.20.11.10      11100     0      up           green           green          172.18.21.11                           172.23.11.11                    12366
        ipsec   7           1000           12:04:29:40     7
172.20.12.10      11100     0      up           green           green          172.18.21.11                           172.23.12.11                    12366
        ipsec   7           1000           12:04:29:40     6
172.21.14.10      22200     0      up           green           green          172.18.21.11                           172.18.22.11                    12366
        ipsec   7           1000           12:04:29:38     10
172.19.15.10      33100     0      up           green           green          172.18.21.11                           172.19.31.11                    12366
        ipsec   7           1000           12:04:29:37     5
```

show sdwan bfd summary

To display Cisco SD-WAN BFD summary information on Cisco IOS XE SD-WAN devices, use the **show sdwan bfd summary** command in privileged EXEC mode.

show sdwan bfd summary [{ **bfd-sessions-total** | **bfd-sessions-up** | **bfd-sessions-max** | **bfd-sessions-flap** | **poll-interval** }]

Syntax Description

bfd-sessions-total	(Optional) Displays only the current number of BFD sessions running.
bfd-sessions-up	(Optional) Displays only the current number of BFD sessions that are in the Up state.
bfd-sessions-max	(Optional) Displays only the total number of BFD sessions that have been created since the device booted up.
bfd-sessions-flap	(Optional) Displays only the number of BFD sessions that have transitioned from the Up state.
poll-interval	(Optional) Displays only the poll interval of all tunnels in milliseconds.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE SD-WAN Release 17.2.1v	This command is supported for Cisco Catalyst SD-WAN.
Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	The command output shows BFD automatic suspension information.

Usage Guidelines

BFD provides rapid failure detection times between forwarding engines, while maintaining low overhead. If a BFD session is down, it implies that no traffic can flow between those TLOCs. If you identify any traffic disruption between a pair of TLOCs or notice that the session flap count has increased, use the **show sdwan bfd summary** command to check the status of your BFD sessions.

Use this command to display Cisco SD-WAN BFD summary information on Cisco IOS XE SD-WAN devices.

Example

The following example shows how to display a Cisco SD-WAN BFD session summary on Cisco IOS XE SD-WAN devices.

```
Device# show sdwan bfd summary
sessions-total 2
sessions-up 2
sessions-max 2
sessions-flap 8
poll-interval 600000
```

The following example shows how to display only the current number of Cisco SD-WAN BFD sessions that are in the up state on Cisco IOS XE SD-WAN devices.

```
Device# show sdwan bfd summary bfd-sessions-up
bfd summary bfd-sessions-up 2
```

The following example shows how to display a Cisco SD-WAN BFD session summary, including which Cisco SD-WAN BFD sessions have been suspended.

```
Device# show sdwan bfd summary
sessions-total           4
```

```
sessions-up              4
sessions-max             4
sessions-flap            4
poll-interval            60000
sessions-up-suspended    1
sessions-down-suspended  0
```

Related Commands

Command	Description
request platform software sdwan auto-suspend reset	Brings all BFD sessions out of suspension.
show sdwan bfd history	Displays Cisco SD-WAN BFD history.
show sdwan bfd sessions	Displays Cisco SD-WAN BFD sessions.
show sdwan bfd tloc-summary-list	Displays a Cisco SD-WAN BFD TLOC summary list.

show sdwan bfd tloc-summary-list

To display Cisco SD-WAN BFD session summary information per TLOC on Cisco IOS XE SD-WAN devices, use the **show sdwan bfd tloc-summary-list** command in privileged EXEC mode.

show sdwan bfd tloc-summary-list [*interface-name*]

Syntax Description

interface-name	(Optional) Displays BFD session summary information on the specified interface.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE SD-WAN Release 17.2.1v	This command is supported for Cisco Catalyst SD-WAN.
Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	The command output shows BFD automatic suspension information.

Usage Guidelines

BFD provides rapid failure detection times between forwarding engines, while maintaining low overhead. If a BFD session is down, it implies that no traffic can flow between those TLOCs. If you identify any traffic disruption between a pair of TLOCs or notice that the session flap count has increased, use the **showsdwanbfdtloc-summary-list** command to check the status of your BFD sessions per TLOC.

You can use this command to display Cisco SD-WAN BFD session summary information per TLOC on Cisco IOS XE SD-WAN devices.

Example

The following example shows how to display Cisco SD-WAN BFD session summary information for all TLOCs on Cisco IOS XE SD-WAN devices.

```
Device# show sdwan bfd tloc-summary-list

SESSIONS SESSIONS SESSIONS
IF NAME ENCAP TOTAL UP FLAP
------------------------------------------------------------
GigabitEthernet0/0/0 ipsec 2 2 8
GigabitEthernet0/0/1 ipsec 2 2 10
```

The following example shows how to display Cisco SD-WAN BFD session summary information on the specified interface GigabitEthernet0/0/0 on Cisco IOS XE SD-WAN devices.

```
Device# show sdwan bfd tloc-summary-list GigabitEthernet0/0/0

SESSIONS SESSIONS SESSIONS
IF NAME ENCAP TOTAL UP FLAP
------------------------------------------------------------
GigabitEthernet0/0/0 ipsec 2 2 8
```

The following example shows how to display Cisco SD-WAN BFD session summary information that includes information for BFD sessions that are up, sessions that are suspended, and sessions that are down and suspended.

```
Device# show sdwan bfd tloc-summary-list
                                                        SESSIONS    SESSIONS
                          SESSIONS  SESSIONS  SESSIONS  UP          DOWN
IF NAME            ENCAP  TOTAL     UP        FLAP      SUSPENDED   SUSPENDED

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

GigabitEthernet1   ipsec     2       2         4          1          0
GigabitEthernet4   ipsec     2       2         0          0          0
```

Related Commands

Command	Description
request platform software sdwan auto-suspend reset	Brings all BFD sessions out of suspension.
show sdwan bfd history	Displays Cisco SD-WAN BFD history.
show sdwan bfd sessions	Displays Cisco SD-WAN BFD sessions.
show sdwan bfd summary	Displays Cisco SD-WAN BFD summary.

show sdwan certificate

To display information about the sdwan certificates on Cisco IOS XE Catalyst SD-WAN devices, use the **show sdwan certificate** command in privileged EXEC mode.

show sdwan certificate { **installed** | **reverse-proxy** | **root-ca-cert** | **serial** | **signing-request** | **validity** }

Syntax Description

installed	Displays sdwan certificate installed.
root-ca-cert	Displays sdwan certificate root-ca-cert.

reverse-proxy	Displays the signed certificate installed on a Cisco IOS XEE SD-WAN device for authentication with a reverse proxy device.
serial	Displays sdwan certificate serial.
signing-request	Displays sdwan certificate signing-request.
validity	Displays sdwan certificate validity.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Support introduced for the keyword **reverse-proxy**.

Usage Guidelines

In the SD-WAN solution, we focus on building secure data plane connections, which involves onboarding physical or virtual WAN edge devices and establishing secure control connections across all the SD-WAN components in the network environment.

Secure onboarding of the SD-WAN edge physical or virtual device requires the device to be identified, trusted and allowed in the same overlay network.

Identity of the WAN edge device is uniquely identified by the chassis ID and certificate serial number. Depending on the WAN edge router, certificates are provided in different ways:

- Hardware-based Cisco IOS XE Catalyst SD-WAN device certificate is stored in the on-board SUDI chip installed during manufacturing.
- Virtual platform (Cisco CSR 1000v) which do not have root certificates preinstalled on the device. For these devices, a One-Time Token (OTK) is provided by Cisco SD-WAN Manager to authenticate the device with the SD-WAN controllers.

Trust of the WAN edge devices is done using the root chain certificates that are pre-loaded in manufacturing, loaded manually, distributed automatically by Cisco SD-WAN Manager, or installed during the Cisco Plug-and-Play automated deployment provisioning process.

The Cisco Catalyst SD-WAN solution uses a model, where the WAN edge devices that are allowed to join the SD-WAN overlay network need to be known by all the SD-WAN controllers beforehand. This is done by adding the WAN edge devices in the Plug-and-Play connect portal (PnP).

Use **show sdwan certificate** command to display information about the Cisco SD-WAN certificates on Cisco IOS XE Catalyst SD-WAN devices to be used for Plug-and-Play, bootstrap or manual onboarding.

Example

The following example shows how to display the decoded certificate signing request installed on Cisco IOS XE Catalyst SD-WAN devices.

```
Device# show sdwan certificate installed
Board-id certificate
--------------------
Certificate:
Data:
Version: 3 (0x2)
Serial Number: 69965125 (0x43bd3a8)
Signature Algorithm: sha256WithRSAEncryption
Issuer: O=Cisco, CN=ACT2 SUDI CA
Validity
Not Before: Aug 5 14:19:01 2019 GMT
Not After : May 14 20:25:41 2029 GMT
Subject: serialNumber=PID:ISR4331/K9 SN:SAMPLESN123, O=Cisco, OU=ACT-2 Lite SUDI,
CN=ISR4331/K9
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public-Key: (2048 bit)
Modulus:
00:cb:cd:16:b1:1f:76:f2:ca:21:4d:9f:32:e5:ef:
79:f4:00:c3:98:15:18:17:20:2d:f3:c4:86:2a:3a:
16:64:4a:e8:f9:93:57:31:87:ae:b5:6d:0a:d7:c2:
93:6c:f6:b2:db:41:7e:0a:16:7f:13:dc:e6:30:35:
f8:1e:e3:e7:20:00:10:2e:71:08:f6:c1:91:8a:1b:
80:d3:a8:cf:df:97:f1:7c:3f:df:2e:1f:d7:27:dd:
02:da:af:98:06:7e:83:3a:83:7a:1e:1f:9f:99:ea:
5f:1a:7c:02:0c:21:10:60:76:db:fe:d9:92:5b:cd:
1b:7e:a6:78:9c:04:10:9f:71:cb:52:90:59:09:9f:
1b:93:48:28:ce:38:e6:d7:db:dd:88:7a:c9:1c:f3:
eb:0b:ab:8c:a2:2a:01:be:27:3e:b1:1c:fe:bc:90:
fb:71:c4:58:c3:41:b0:22:2b:49:93:96:53:58:bf:
16:64:4a:e8:f9:93:57:31:87:ae:b5:6d:0a:d7:c2:
1c:fa:17:d9:4f:53:98:d9:63:ab:c9:54:b0:ef:b9:
8e:1f:d8:70:fd:ef:14:d2:35:96:5b:02:3d:16:23:
03:86:ed:be:6b:34:01:0a:25:66:b5:98:73:b0:3f:
5f:1a:7c:02:0c:21:10:60:76:db:fe:d9:92:5b:cd:
03:86
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Key Usage: critical
Digital Signature, Non Repudiation, Key Encipherment
X509v3 Basic Constraints: critical
CA:FALSE
X509v3 Subject Alternative Name:
othername:<unsupported>
Signature Algorithm: sha256WithRSAEncryption
7b:6c:21:4f:1b:25:73:46:d8:27:79:4c:37:70:a9:b3:57:d7:
24:55:73:11:cc:cb:17:3b:d3:e4:5d:a9:88:8f:92:c8:d8:a4:
41:09:b9:52:a0:45:e4:8f:d2:03:d9:26:8d:cc:59:69:14:e9:
77:e7:ab:30:bf:a5:e8:41:bd:3a:16:9e:91:4f:4b:d3:12:9f:
6d:0a:11:c8:46:d8:81:1b:63:6f:89:22:b6:87:8e:6b:6b:0d:
73:d1:8c:60:77:4e:a3:69:8d:a3:1f:c8:7a:15:ad:d2:68:39:
37:13:25:34:74:4c:b6:05:17:7a:09:6e:83:ed:43:dd:6b:0a:
21:9a:0b:4c:13:63:01:1f:92:ad:19:26:14:fe:0e:2d:86:32:
a6:b0:3f:8f:8e:c4:f9:67:df:03:e9:cb:a3:db:02:bb:44:8c:
24:55:73:11:cc:cb:17:3b:d3:e4:5d:a9:88:8f:92:c8:d8:a4:
ff:39:8a:9b:b4:eb:4d:e8:37:b1:6e:e8:f2:27:ea:85:c1:b3:
6d:0a:11:c8:46:d8:81:1b:63:6f:89:22:b6:87:8e:6b:6b:0d:
27:02:46:b1:cd:91:b9:cc:6e:85:97:a4:67:c7:d1:e0:55:0e:
65:70:ed:79:17:86:9a:70:70:70:8b:a9:e3:81:0b:e5:42:b8:
21:9a:0b:4c
Installed device certificates
-----------------------------
```

The following example shows how to display the root certificate installed on Cisco IOS XE Catalyst SD-WAN devices.

```
Device# show sdwan certificate root-ca-cert
Certificate:
Data:
Version: 3 (0x2)
Serial Number:
b9:a5:54:a0:5b:ac:6b:88
Signature Algorithm: sha256WithRSAEncryption
Issuer: C = US, ST = Texas, L = Dallas, O = Test_Name, OU = Test_Name
Validity
Not Before: Aug 31 21:15:48 2020 GMT
Not After : Dec 9 21:15:48 2020 GMT
Subject: C = US, ST = Texas, L = Dallas, O = Test_Name, OU = Test_Name
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
RSA Public-Key: (2048 bit)
Modulus:
ac:4e:7b:e5:e9:b4:cd:84:95:4d:38:63:c4:a8:52:
e4:35:6e:ec:8b:55:54:a2:91:51:c1:41:e5:48:5f:
20:f6:48:08:2f:d7:bc:1e:c7:a4:dd:27:27:36:25:
5c:26:01:c9:1e:8f:fe:18:0d:94:23:46:a0:24:2f:
ac:24:d9:4b:81:99:ba:ed:71:45:1a:ea:17:03:e7:
ac:4e:7b:e5:e9:b4:cd:84:95:4d:38:63:c4:a8:52:
18:3c:6f:ec:1e:fe:37:31:4d:a7:58:7c:07:ac:06:
88:3e:47:ea:7e:27:d6:21:31:10:dc:5d:30:db:14:
20:f6:48:08:2f:d7:bc:1e:c7:a4:dd:27:27:36:25:
ac:4e:7b:e5:e9:b4:cd:84:95:4d:38:63:c4:a8:52:
97:80:ef:37:e2:96:4f:93:9e:2f:bb:22:7a:cc:bb:
6f:2c:f8:52:b2:f2:07:3c:a9:cc:c6:b2:72:00:c8:
e3:a4:ad:36:fe:70:16:8a:28:48:5c:90:00:d6:8b:
20:f6:48:08:2f:d7:bc:1e:c7:a4:dd:27:27:36:25:
72:1a:56:0b:f2:84:8f:09:fd:0b:42:7e:19:fd:43:
ac:4e:7b:e5:e9:b4:cd:84:95:4d:38:63:c4:a8:52:
70:a0:dc:2e:43:8f:f1:f3:b7:d6:a7:89:d4:41:5d:
f6:73
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Subject Key Identifier:
54:45:B0:9E:ED:59:3E:D5:9F:03:38:F2:3A:44:C0:E3:6A:CB:86:4C
X509v3 Authority Key Identifier:
keyid:54:45:B0:9E:ED:59:3E:D5:9F:03:38:F2:3A:44:C0:E3:6A:CB:86:4C
X509v3 Basic Constraints:
CA:TRUE
Signature Algorithm: sha256WithRSAEncryption
28:85:ea:02:06:1d:65:1f:ab:47:ac:c9:e3:6c:45:4a:0b:dd:
a3:6c:ae:f5:7e:4d:0c:ba:15:7e:e9:b1:d0:81:61:fd:93:72:
8a:0d:21:dc:53:c0:18:4d:8a:dc:3f:bf:76:91:1d:15:4f:72:
28:85:ea:02:06:1d:65:1f:ab:47:ac:c9:e3:6c:45:4a:0b:dd:
ea:f4:e8:de:83:c3:5d:b0:a6:e3:8b:e8:52:db:03:da:26:f3:
9f:67:fe:57:a6:03:b0:5d:47:a6:2b:2b:27:90:57:c6:ca:da:
23:0f:7a:00:78:5d:92:e1:91:c5:f7:ce:f7:e7:09:6f:5b:f9:
28:85:ea:02:06:1d:65:1f:ab:47:ac:c9:e3:6c:45:4a:0b:dd:
9f:67:fe:57:a6:03:b0:5d:47:a6:2b:2b:27:90:57:c6:ca:da:
fd:df:ed:26:f4:1b:39:ab:cf:af:f9:b1:bd:64:7e:72:e4:42:
20:1b:52:96:69:63:46:af:32:7a:45:fe:96:e8:55:14:e1:79:
74:a8:2a:ca:5c:34:ea:cc:2c:35:3a:84:da:df:dd:85:3d:db:
9f:67:fe:57:a6:03:b0:5d:47:a6:2b:2b:27:90:57:c6:ca:da:
28:85:ea:02:06:1d:65:1f:ab:47:ac:c9:e3:6c:45:4a:0b:dd:
98:b3:4f:bc
```

The following example shows how to display the chassis number, board ID serial number, and serial number on Cisco IOS XE Catalyst SD-WAN devices.

```
Device# show sdwan certificate serial
Chassis number: ISR4331/K9-SAMPLESN123 Board ID serial number: 053BE1B7 Subject S/N:
SAMPLESN123
```

The following example shows how to display how long a certificate is valid for on Cisco IOS XE Catalyst SD-WAN devices.

```
Device# show sdwan certificate validity
The certificate is valid from Aug 5 14:19:01 2019 GMT (Current date is Mon Nov 30 22:01:08
 GMT 2020) & valid until May 14 20:25:41 2029 GMT
```

The following is a sample output from the execution of the **show sdwan certificate reverse-proxy** command on a Cisco IOS XE SD-WAN device.

```
Device#show sdwan certificate reverse-proxy

Reverse proxy certificate

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



Certificate:

    Data:

        Version: 1 (0x0)

        Serial Number: 1 (0x1)

        Signature Algorithm: sha256WithRSAEncryption

        Issuer: C = US, CN = 6c63e80a-8175-47de-a455-53a127ee70bd, O = Viptela

        Validity

            Not Before: Jun  2 19:31:08 2021 GMT

            Not After : May 27 19:31:08 2051 GMT

        Subject: C = US, ST = California, CN = C8K-9AE4A5A8-4EB0-E6C1-1761-6E54E4985F78, O
 = ViptelaClient
        Subject Public Key Info:

            Public Key Algorithm: rsaEncryption

                RSA Public-Key: (2048 bit)

                Modulus:

                    00:e2:45:49:53:3a:56:d4:b8:70:59:90:01:fb:b1:

                    44:e3:73:17:97:a3:e9:b7:55:44:d4:2d:dd:13:4a:

                    a8:ef:78:14:9d:bd:b5:69:de:c9:31:29:bd:8e:57:

                    09:f2:02:f8:3d:1d:1e:cb:a3:2e:94:c7:2e:61:ea:

                    e9:94:3b:28:8d:f7:06:12:56:f3:24:56:8c:4a:e7:

                    01:b1:2b:1b:cd:85:4f:8d:34:78:78:a1:26:17:2b:

                    a5:1b:2a:b6:dd:50:51:f8:2b:13:93:cd:a6:fd:f8:

                    71:95:c4:db:fc:a7:83:05:23:68:61:15:05:cc:aa:
```

```
                    60:af:09:ef:3e:ce:70:4d:dd:50:84:3c:9a:57:ce:

                    cb:15:84:3e:cd:b2:b6:30:ab:86:68:17:94:fa:9c:

                    1a:ab:28:96:68:8c:ef:c8:f7:00:8a:7a:01:ca:58:

                    84:b0:87:af:9a:f6:13:0f:aa:42:db:8b:cc:6e:ba:

                    c8:c1:48:d2:f4:d8:08:b1:b5:15:ca:36:80:98:47:

                    32:3a:df:54:35:fe:75:32:23:9f:b5:ed:65:41:99:

                    50:b9:0f:7a:a2:10:59:12:d8:3e:45:78:cb:dc:2a:

                    95:f2:72:02:1a:a6:75:06:87:52:4d:01:17:f2:62:

                    8c:40:ad:29:e4:75:17:04:65:a9:b9:6a:dd:30:95:

                    34:9b

                Exponent: 65537 (0x10001)

    Signature Algorithm: sha256WithRSAEncryption

         99:40:af:23:bb:cf:7d:59:e9:a5:83:78:37:02:76:83:79:02:

         b3:5c:56:e8:c3:aa:fc:78:ef:07:23:f8:14:19:9c:a4:5d:88:

         07:4d:6e:b8:0d:b5:af:fa:5c:f9:55:d0:60:94:d9:24:99:5e:
         33:06:83:03:c3:73:c1:38:48:45:ba:6a:35:e6:e1:51:0e:92:

         c3:a2:4a:a2:e1:2b:da:cd:0c:c3:17:ef:35:52:e1:6a:23:20:

         af:99:95:a2:cb:99:a7:94:03:f3:78:99:bc:76:a3:0f:de:04:

         7d:35:e1:dc:4d:47:79:f4:c8:4c:19:df:80:4c:4f:15:ab:f1:

         61:a2:78:7a:2b:6e:98:f6:7b:8f:d6:55:44:16:79:e3:cd:51:

         0e:27:fc:e6:4c:ff:bb:8f:2d:b0:ee:ed:98:63:e9:c9:cf:5f:

         d7:b1:dd:7b:19:32:22:94:77:d5:bc:51:85:65:f3:e0:93:c7:

         3c:79:fc:34:c7:9f:40:dc:b1:fc:6c:e5:3d:af:2d:77:b7:c3:

         88:b3:89:7c:a6:1f:56:35:3b:35:66:0c:c8:05:b5:28:0b:98:

         19:c7:b0:8e:dc:b7:3f:9d:c1:bb:69:f0:7d:20:95:b5:d1:f0:

         06:35:b7:c4:64:ba:c4:95:31:4a:97:03:0f:04:54:6d:cb:50:

         2f:31:02:59


Device#
```

show sdwan cloudexpress applications

To display the best path that Cloud onRamp for SaaS has selected for each configured SaaS application, on Cisco IOS XE Catalyst SD-WAN devices, use the **show sdwan cloudexpress applications** command in privileged EXEC mode.

show sdwan cloudexpress applications

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 17.2	This command was introduced.
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	The command output may include the Webex application, which is supported from this release.
Cisco IOS XE Catalyst SD-WAN Release 17.8.1a	The command output may include custom applications, which are supported from this release. The output header includes information about the application ID, application type, and the sub-application ID.

Usage Guidelines

The command output includes sections for each configured SaaS application.

Examples

The following is a sample output from the **show sdwan cloudexpress applications** command, as it appears in Cisco IOS XE Catalyst SD-WAN Release 17.8.1a, showing a standard SaaS application (amazon_aws).

```
Device# show sdwan cloudexpress applications
cloudexpress applications vpn 1 app 3 type app-group subapp 0
 application amazon_aws
 exit-type   local
 interface   GigabitEthernet5
 latency     2
 loss        1
```

Table 37: Command Output Header Field Descriptions, Beginning with Cisco IOS XE Catalyst SD-WAN Release 17.8.1a

Output	Description
vpn	Each VPN for which Cloud onRamp for SaaS is enabled appears in the output.
app	Application ID corresponding to the application.
type	Possible values are: app-group, custom-app-group, region
subapp	Sub-application ID corresponding to the application. An application can have one or more sub-application ID's.

The following is a sample output from the **show sdwan cloudexpress applications** command, as it appears in Cisco IOS XE Catalyst SD-WAN Release 17.8.1a, showing the Webex app, which is of type region.

```
Device# show sdwan cloudexpress applications
cloudexpress applications vpn 1 app 15 type region subapp 8
 application webex-us-west-1
 exit-type   local
 interface   GigabitEthernet5
 latency     139
 loss        0
```

The following is a sample output from the **show sdwan cloudexpress applications** command, as it appears in Cisco IOS XE Catalyst SD-WAN Release 17.8.1a, showing a user-defined SaaS application list called example-apps.

```
Device# show sdwan cloudexpress applications
cloudexpress applications vpn 2 app 26 type custom-app-group subapp 0
 application example-apps
 exit-type   local
 interface   GigabitEthernet5
 latency     66
 loss        0
```

The following is a sample output from the **show sdwan cloudexpress applications** command, as it appears beginning with Cisco IOS XE Catalyst SD-WAN Release 17.7.1a.

```
Device# show sdwan cloudexpress applications
cloudexpress applications vpn 1 app-group 3
 application amazon_aws
 exit-type   local
 interface   GigabitEthernet5.101
 latency     3
 loss        0
cloudexpress applications vpn 1 region 8
 application webex-us-west-1
 exit-type   none
 latency     0
 loss        0
```

The following is a sample output from the **show sdwan cloudexpress applications** command, as it appears before Cisco IOS XE Catalyst SD-WAN Release 17.7.1a.

```
Device# show sdwan cloudexpress applications
cloudexpress applications vpn 1 office365
exit-type local
interface GigabitEthernet1
latency   1
loss      40
cloudexpress applications vpn 1 amazon_aws
exit-type         gateway
gateway-system-ip 10.0.0.1
latency           1
loss              0
local-color       lte
remote-color      lte
cloudexpress applications vpn 1 dropbox
exit-type         gateway
gateway-system-ip 10.0.0.1
```

```
latency           19
loss              0
local-color       lte
remote-color      lte
```

show sdwan cloudexpress gateway-exits

show sdwan cloudexpress gateway-exits—Display loss and latency on each gateway exit for applications configured with Cloud OnRamp for SaaS (formerly called CloudExpress service).

show sdwan cloudexpress gateway-exits

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	This command was introduced.
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	The command output may include the Webex application, which is supported from this release.
Cisco IOS XE Catalyst SD-WAN Release 17.8.1a	The command output may include custom applications, which are supported from this release. The output header includes information about the application ID, application type, and the sub-application ID.

Usage Guidelines

The command output includes sections for each configured SaaS application.

Examples

The following is a sample output from the **show sdwan cloudexpress gateway-exits** command, as it appears in Cisco IOS XE Catalyst SD-WAN Release 17.8.1a, showing a standard SaaS application (amazon_aws).

```
Device# show sdwan cloudexpress gateway-exits
cloudexpress gateway-exits vpn 1 app 3 type app-group subapp 0 192.168.1.15
 application  amazon_aws
 latency      1
 loss         1
 local-color  lte
 remote-color lte
```

Table 38: Command Output Header Field Descriptions, Beginning with Cisco IOS XE Catalyst SD-WAN Release 17.8.1a

Output	Description
vpn	Each VPN for which Cloud onRamp for SaaS is enabled appears in the output.

Output	Description
app	Application ID corresponding to the application.
type	Possible values are: app-group, custom-app-group, region
subapp	Sub-application ID corresponding to the application. An application can have one or more sub-application ID's.

The following is a sample output from the **show sdwan cloudexpress gateway-exits** command, as it appears in Cisco IOS XE Catalyst SD-WAN Release 17.8.1a, showing the Webex app, which is of type region.

```
Device# show sdwan cloudexpress gateway-exits
cloudexpress gateway-exits vpn 1 app 15 type region subapp 1 192.168.1.15
 application  webex-us-west-1
 latency      139
 loss         0
 local-color  lte
 remote-color lte
```

The following is a sample output from the **show sdwan cloudexpress gateway-exits** command, as it appears in Cisco IOS XE Catalyst SD-WAN Release 17.8.1a, showing a user-defined SaaS application list called example-apps.

```
Device# show sdwan cloudexpress gateway-exits
cloudexpress gateway-exits vpn 1 app 26 type custom-app-group subapp 0 192.168.1.15
 application  example-apps
 latency      66
 loss         0
 local-color  lte
 remote-color lte
```

The following example shows the command output, as it appears in releases earlier than Cisco IOS XE Catalyst SD-WAN Release 17.7.1a.

```
Device# show sdwan cloudexpress gateway-exits
cloudexpress gateway-exits vpn 1 office365 172.16.255.15
latency 2
loss 0
local-color lte
remote-color lte
cloudexpress gateway-exits vpn 1 office365 172.16.255.16
latency 2
loss 0
local-color lte
remote-color lte
cloudexpress gateway-exits vpn 1 amazon_aws 172.16.255.15
latency 1
loss 0
local-color lte
remote-color lte
cloudexpress gateway-exits vpn 1 amazon_aws 172.16.255.16
latency 1
loss 0
```

```
local-color lte
remote-color lte
```

show sdwan cloudexpress load-balance applications

To view the interface, exit type, and statistics for the best path that Cloud onRamp for SaaS has selected for each configured SaaS application, on Cisco IOS XE Catalyst SD-WAN devices, use the **show sdwan cloudexpress load-balance applications** command in privileged EXEC mode.

show sdwan cloudexpress load-balance applications

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	This command was introduced.
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	The command output may include the Webex application, which is supported from this release.
Cisco IOS XE Catalyst SD-WAN Release 17.8.1a	The command output may include custom applications, which are supported from this release. The output header includes information about the application ID, application type, and the sub-application ID.

Examples

The following is a sample output from the **show sdwan cloudexpress load-balance applications** command, as it appears in Cisco IOS XE Catalyst SD-WAN Release 17.8.1a.

```
Device# show sdwan cloudexpress load-balance applications
cloudexpress load-balance applications-lb vpn 1 app 3 type app-group subapp 0 GigabitEthernet5
application amazon_aws
exit-type local
latency 2
loss 4
cloudexpress load-balance applications-lb vpn 1 app 3 type app-group subapp 0 GigabitEthernet6
application amazon_aws
exit-type local
latency 1
loss 2
```

Table 39: Command Output Header Field Descriptions, Beginning with Cisco IOS XE Catalyst SD-WAN Release 17.8.1a

Output	Description
vpn	Each VPN for which Cloud onRamp for SaaS is enabled appears in the output.
app	Application ID corresponding to the application.
type	Possible values are: app-group, custom-app-group, region

Output	Description
subapp	Sub-application ID corresponding to the application. An application can have one or more sub-application ID's.

The following is a sample output from the **show sdwan cloudexpress load-balance applications** command, as it appears before Cisco IOS XE Catalyst SD-WAN Release 17.7.1a.

```
Device# show sdwan cloudexpress load-balance applications
cloudexpress load-balance applications-lb vpn 10 office365 GigabitEthernet1
exit-type local
latency 1
loss 5
cloudexpress load-balance applications-lb vpn 10 office365 GigabitEthernet2
exit-type local
latency 1
loss 7
```

Table 40: Command Output Header Field Descriptions, Beginning with Cisco IOS XE Catalyst SD-WAN Release 17.8.1a

Output	Description
vpn	Each VPN for which Cloud onRamp for SaaS is enabled appears in the output.

```
Device# show sdwan cloudexpress load-balance applications
cloudexpress load-balance applications-lb vpn 10 office365 GigabitEthernet1
exit-type local
latency 1
loss 5
cloudexpress load-balance applications-lb vpn 10 office365 GigabitEthernet2
exit-type local
latency 1
loss 7
```

show sdwan cloudexpress local-exits

show sdwan cloudexpress local-exits—Display application loss and latency on each Direct Internet Access (DIA) interface enabled for Cloud OnRamp for SaaS (formerly called CloudExpress service).

show sdwan cloudexpress local-exits

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	This command was introduced.

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	The command output may include the Webex application, which is supported from this release.
Cisco IOS XE Catalyst SD-WAN Release 17.8.1a	The command output may include custom applications, which are supported from this release. The output header includes information about the application ID, application type, and the sub-application ID.

Usage Guidelines

The command output includes sections for each configured SaaS application.

Examples

The following is a sample output from the **show sdwan cloudexpress local-exits** command, as it appears in Cisco IOS XE Catalyst SD-WAN Release 17.8.1a, showing a standard SaaS application (amazon_aws).

```
Device# show sdwan cloudexpress local-exits
cloudexpress local-exits vpn 1 app 3 type app-group subapp 0 GigabitEthernet5
 application amazon_aws
 latency     1
 loss        2
```

Table 41: Command Output Header Field Descriptions, Beginning with Cisco IOS XE Catalyst SD-WAN Release 17.8.1a

Output	Description
vpn	Each VPN for which Cloud onRamp for SaaS is enabled appears in the output.
app	Application ID corresponding to the application.
type	Possible values are: app-group, custom-app-group, region
subapp	Sub-application ID corresponding to the application. An application can have one or more sub-application ID's.

The following is a sample output from the **show sdwan cloudexpress local-exits** command, as it appears in Cisco IOS XE Catalyst SD-WAN Release 17.8.1a, showing the Webex app, which is of type region.

```
Device# show sdwan cloudexpress local-exits
cloudexpress local-exits vpn 1 app 15 type region subapp 1 GigabitEthernet5
 application webex-us-west-1
 latency     139
 loss        0
```

The following is a sample output from the **show sdwan cloudexpress local-exits** command, as it appears in Cisco IOS XE Catalyst SD-WAN Release 17.8.1a, showing a user-defined SaaS application list called example-apps.

```
Device# show sdwan cloudexpress local-exits
cloudexpress local-exits vpn 1 app 26 type custom-app-group subapp 0 GigabitEthernet5
 application example-apps
```

```
 latency     66
 loss        0
```

show sdwan cloudexpress local-exits

The following is a sample output from the **show sdwan cloudexpress local-exits** command, as it appears in releases earlier than Cisco IOS XE Catalyst SD-WAN Release 17.7.1a.

```
Device# show sdwan cloudexpress local-exits

VPN APPLICATION INTERFACE LATENCY LOSS
------------------------------------------------------------------------
1 office365 Tunnel100015 10 0
1 office365 Tunnel100016 3 0
1 amazon_aws Tunnel100015 10 0
1 amazon_aws Tunnel100016 3 0
```

show sdwan control

To display information about the control connections and control plane connections on Cisco IOS XE SD-WAN devices, use the **show sdwan control** command in privileged EXEC mode.

show sdwan control
{ **affinity** { **config** | **status** } | **connection-history** | **connection-info** | **connections** | **local-properties** | **statistics** | **summary** | **valid-vmanage-id** | **valid-vsmarts** }

Syntax Description

affinity config	Displays the configuration information about the control connections to one or more Cisco Catalyst SD-WAN Controllers.
affinity status	Displays the status of the control connections to one or more Cisco Catalyst SD-WAN Controllers.
connection-history	Displays the status of the control connections to one or more Cisco Catalyst SD-WAN Controllers.
connection-info	Displays information about the control plane connections.
connections	Displays information about active control plane connections.
local-properties	Displays the basic configuration parameters and local properties related to the control plane.
statistics	Displays statistics about the packets that a device has transmitted and received in the process of establishing and maintaining secure DTLS connections to devices in the overlay network.
summary	Displays a count of devices that the local device is aware.
valid-vmanage-id	Displays the chassis number of the Cisco SD-WAN Manager instances.
valid-vsmarts	Displays the serial numbers of the valid Cisco Catalyst SD-WAN Controllers in the overlay network.

Command Default None

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	Added the Hierarchical SD-WAN region assignment to the the **REG IDs** column when you use the **local-properties** keyword.
Cisco IOS XE Catalyst SD-WAN Release 17.8.1a	For Hierarchical SD-WAN architectures, the **REGION IDs** column shows the secondary region also.

Usage Guidelines In the Cisco SD-WAN overlay network, all Cisco XE SD-WAN devices and Cisco WAN Edge devices establish control connections to all Cisco Catalyst SD-WAN Controllers, to ensure that the routers are always able to properly route data traffic across the network.

One way to manage network scale is to configure affinity between Cisco Catalyst SD-WAN Controllers and WAN Edge routers. To do this, you place each Cisco Catalyst SD-WAN Controller into a controller group, and then you configure which group or groups a WAN Edge router can establish control connections with.

The controller groups are what establishes the affinity between Cisco Catalyst SD-WAN Controllers and WAN Edge routers.

The Cisco SD-WAN control plane operates in conjunction with redundant components to ensure that the overlay network remains resilient if one of the components fails.

This command can be used to display information about the control connections and control plane connections on Cisco IOS XE SD-WAN devices.

Example

The following example shows how to display the configuration information about the control connections to one or more Cisco Catalyst SD-WAN Controllers on Cisco IOS XE SD-WAN devices.

```
Device# show sdwan control affinity config

EFFECTIVE CONTROLLER LIST FORMAT - G(C),... - Where G is the Controller Group ID
C is the Required vSmart Count
CURRENT CONTROLLER LIST FORMAT - G(c)s,... - Where G is the Controller Group ID
c is the current vSmart count
s Status Y when matches, N when does not match
EFFECTIVE
REQUIRED LAST-RESORT
INDEX INTERFACE VS COUNT EFFECTIVE CONTROLLER LIST CURRENT CONTROLLER LIST EQUILIBRIUM
INTERFACE
-----------------------------------------------------------------------------------------------------
0 GigabitEthernet0/0/0 2 0(2) 0(2)Y Yes No
1 GigabitEthernet0/0/1 2 0(2) 0(2)Y Yes No
```

The following example shows how to display information about control plane connection attempts initiated by the local device on Cisco IOS XE SD-WAN devices.

```
Device# show sdwan control connection-history

Legend for Errors
```

```
ACSRREJ - Challenge rejected by peer. NOVMCFG - No cfg in vmanage for device.
BDSGVERFL - Board ID Signature Verify Failure. NOZTPEN - No/Bad chassis-number entry in
ZTP.
BIDNTPR - Board ID not Initialized. OPERDOWN - Interface went oper down.
BIDNTVRFD - Peer Board ID Cert not verified. ORPTMO - Server's peer timed out.
BIDSIG - Board ID signing failure. RMGSPR - Remove Global saved peer.
CERTEXPRD - Certificate Expired RXTRDWN - Received Teardown.
CRTREJSER - Challenge response rejected by peer. RDSIGFBD - Read Signature from Board ID
failed.
CRTVERFL - Fail to verify Peer Certificate. SERNTPRES - Serial Number not present.
CTORGNMMIS - Certificate Org name mismatch. SSLNFAIL - Failure to create new SSL context.
DCONFAIL - DTLS connection failure. STNMODETD - Teardown extra vBond in STUN server mode.
DEVALC - Device memory Alloc failures. SYSIPCHNG - System-IP changed.
DHSTMO - DTLS HandShake Timeout. SYSPRCH - System property changed
DISCVBD - Disconnect vBond after register reply. TMRALC - Timer Object Memory Failure.
DISTLOC - TLOC Disabled. TUNALC - Tunnel Object Memory Failure.
DUPCLHELO - Recd a Dup Client Hello, Reset Gl Peer. TXCHTOBD - Failed to send challenge to
 BoardID.
DUPSER - Duplicate Serial Number. UNMSGBDRG - Unknown Message type or Bad Register msg.
DUPSYSIPDEL- Duplicate System IP. UNAUTHEL - Recd Hello from Unauthenticated peer.
HAFAIL - SSL Handshake failure. VBDEST - vDaemon process terminated.
IP_TOS - Socket Options failure. VECRTREV - vEdge Certification revoked.
LISFD - Listener Socket FD Error. VSCRTREV - vSmart Certificate revoked.
MGRTBLCKD - Migration blocked. Wait for local TMO. VB_TMO - Peer vBond Timed out.
MEMALCFL - Memory Allocation Failure. VM_TMO - Peer vManage Timed out.
NOACTVB - No Active vBond found to connect. VP_TMO - Peer vEdge Timed out.
NOERR - No Error. VS_TMO - Peer vSmart Timed out.
NOSLPRCRT - Unable to get peer's certificate. XTVMTRDN - Teardown extra vManage.
NEWVBNOVMNG- New vBond with no vMng connections. XTVSTRDN - Teardown extra vSmart.
NTPRVMINT - Not preferred interface to vManage. STENTRY - Delete same tloc stale entry.
HWCERTREN - Hardware vEdge Enterprise Cert Renewed HWCERTREV - Hardware vEdge Enterprise
Cert Revoked.
EMBARGOFAIL - Embargo check failed
PEER PEER
PEER PEER PEER SITE DOMAIN PEER PRIVATE PEER PUBLIC LOCAL REMOTE REPEAT
TYPE PROTOCOL SYSTEM IP ID ID PRIVATE IP PORT PUBLIC IP PORT LOCAL COLOR STATE ERROR ERROR
 COUNT DOWNTIME
------------------------------------------------------------------------------------------------------
-------------------------------------------------------------------------------
vbond dtls 0.0.0.0 0 0 10.6.16.252 12346 10.6.16.252 12346 public-internet tear_down DISCVBD
 NOERR 0
2020-11-16T21:07:53+0000
vmanage dtls 1.1.1.254 1001 0 10.6.16.254 12346 10.6.16.254 12346 public-internet tear_down
 DISTLOC NOERR
 0 2020-11-16T21:07:34+0000
vsmart dtls 1.1.1.251 1001 1 10.6.16.251 12346 10.6.16.251 12346 public-internet tear_down
 DISTLOC NOERR
0 2020-11-16T21:07:34+0000
vsmart dtls 1.1.1.250 1001 1 10.6.16.250 12346 10.6.16.250 12346 public-internet tear_down
 DISTLOC NOERR
0 2020-11-16T21:07:34+0000
vbond dtls 0.0.0.0 0 0 10.6.16.252 12346 10.6.16.252 12346 public-internet tear_down DISCVBD
 NOERR 0
2020-11-16T13:57:52+0000
```

The following example shows how to display information about control plane connections on Cisco IOS XE SD-WAN devices.

```
Device# show sdwan control connection-info

control connections-info "Per-Control Connection Rate: 300 pps"
```

The following example shows how to display information about active control plane connections on Cisco IOS XE SD-WAN devices.

```
Device# show sdwan control connections

PEER PEER CONTROLLER
PEER PEER PEER SITE DOMAIN PEER PRIV PEER PUB GROUP
TYPE PROT SYSTEM IP ID ID PRIVATE IP PORT PUBLIC IP PORT LOCAL COLOR
PROXY STATE UPTIME ID
--------------------------------------------------------------------
------------------------------------------------------------
vsmart dtls 1.1.1.250 1001 1 10.6.16.250 12346 10.6.16.250 12346
public-internet No up 14:03:03:35 0
vsmart dtls 1.1.1.251 1001 1 10.6.16.251 12346 10.6.16.251 12346
public-internet No up 14:03:03:33 0
vmanage dtls 1.1.1.254 1001 0 10.6.16.254 12346 10.6.16.254 12346
public-internet No up 14:03:03:31 0
```

The following example shows how to display the basic configuration parameters and local properties related to the control plane on Cisco IOS XE SD-WAN devices.

```
Device# show sdwan control local-properties

personality vedge
sp-organization-name Test_Name
organization-name Test_Name
root-ca-chain-status Installed
certificate-status Installed
certificate-validity Valid
certificate-not-valid-before Aug 05 14:19:01 2019 GMT
certificate-not-valid-after May 14 20:25:41 2029 GMT
enterprise-cert-status Not-Applicable
enterprise-cert-validity Not Applicable
enterprise-cert-not-valid-before Not Applicable
enterprise-cert-not-valid-after Not Applicable
dns-name 10.6.16.252
site-id 206
domain-id 1
protocol dtls
tls-port 0
system-ip 10.3.206.1
chassis-num/unique-id ISR4331/K9-SAMPLESN123
serial-num 053DA5B7
subject-serial-num SAMPLESN123
enterprise-serial-num No certificate installed
token -NA-
keygen-interval 1:00:00:00
retry-interval 0:00:00:16
no-activity-exp-interval 0:00:00:20
dns-cache-ttl 0:00:02:00
port-hopped TRUE
time-since-last-port-hop 14:20:44:35
embargo-check success
number-vbond-peers 0
number-active-wan-interfaces 1
NAT TYPE: E -- indicates End-point independent mapping
A -- indicates Address-port dependent mapping
N -- indicates Not learned
Note: Requires minimum two vbonds to learn the NAT type
PUBLIC PUBLIC PRIVATE PRIVATE PRIVATE MAX RESTRICT/ LAST SPI TIME NAT VM
INTERFACE IPv4 PORT IPv4 IPv6 PORT VS/VM COLOR STATE CNTRL CONTROL/ LR/LB CONNECTION REMAINING
 TYPE CON
STUN PRF
--------------------------------------------------------------------------------------------------------
--------------------------------------------------------------------------------------------------------
GigabitEthernet0/0/0 10.3.6.2 12366 10.3.6.2 :: 12366 2/1 public-internet up 2 no/yes/no
```

```
No/No
14:20:44:17 0:03:15:24 N 5
```

The following example shows how to display statistics about the packets that a device has transmitted and received in the process of establishing and maintaining secure DTLS connections to devices in the overlay network on Cisco IOS XE SD-WAN devices.

```
Device# show sdwan control statistics

Tx Statistics:
--------------
packets 6544303
octets 448205710
error 0
blocked 0
hello 3947942
connects 0
registers 4
register-replies 0
dtls-handshake 8
dtls-handshake-failures 0
dtls-handshake-done 8
challenge 0
challenge-response 8
challenge-ack 0
challenge-errors 0
challenge-response-errors 0
challenge-ack-errors 0
challenge-general-errors 0
vmanage-to-peer 0
register_to_vmanage 2
Rx Statistics:
--------------
packets 5860730
octets 732977621
errors 0
hello 3947931
connects 0
registers 0
register-replies 4
dtls-handshake 0
dtls-handshake-failures 0
dtls-handshake-done 0
challenge 8
challenge-response 0
challenge-ack 8
challenge-failures 0
vmanage-to-peer 2
register_to_vmanage 0
challenge_failed_due_to_bid 0
```

The following example shows how to display a count of devices that the local device is aware of on Cisco IOS XE SD-WAN devices.

```
Device# show sdwan control summary

control summary 0
vbond_counts 0
vmanage_counts 1
vsmart_counts 2
```

The following example shows how to display the chassis number of the Cisco SD-WAN Manager instances on Cisco IOS XE SD-WAN devices.

```
Device# show sdwan control valid-vmanage-id

CHASSIS NUMBER
--------------------------------------
5271ea7c-edb1-420b-be9a-4d25756785bd
```

The following example shows how to display the serial numbers and organization names of the valid Cisco Catalyst SD-WAN Controllers in the overlay network on Cisco IOS XE SD-WAN devices.

```
Device# show sdwan control valid-vsmarts

SERIAL NUMBER ORG
----------------------------
B137996B88AA876A Test_Name
B137996B88AA876D Test_Name
B137996B88AA876E Test_Name
```

show sdwan debugs

To display the list of enabled SD-WAN debugs on Cisco IOS XE SD-WAN devices, use the **show sdwan debugs** command in privileged EXEC mode.

show sdwan debugs
[confd | config-mgr | dbgd | fpm | ftm | netconf | omp | policy-counter | ttm | vdaemon]

Syntax Description

confd	(Optional) Displays the list of enabled SD-WAN confd debugs.
config-mgr	(Optional) Displays the list of enabled D-WAN config-mgr debugs.
dbgd	(Optional) Displays the list of enabled SD-WAN dbgd debugs.
fpm	(Optional) Displays the list of enabled SD-WAN config-mgr debugs.
ftm	(Optional) Displays the list of enabled SD-WAN config-mgr debugs.
netconf	(Optional) Displays the list of enabled SD-WAN config-mgr debugs.
omp	(Optional) Displays the list of enabled SD-WAN config-mgr debugs.
policy-counter	(Optional) Displays the list of enabled SD-WAN config-mgr debugs.
ttm	(Optional) Displays the list of enabled SD-WAN config-mgr debugs.
vdaemon	(Optional) Displays the list of enabled SD-WAN config-mgr debugs.

Command Default None

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines The output from debug commands provides diagnostic information that include a variety of internet working events relating to protocol status and network activity in general.

Debug output is placed in the bootflash/tracelogs folder on the local device.

This command can be used to display the list of enabled sdwan debugs on Cisco IOS XE SD-WAN devices.

Example

The following example shows how to display the list of all enabled SD-WAN debugs on Cisco IOS XE SD-WAN devices.

```
Device# show sdwan debugs
debugs ftm nat
debugs config-mgr events low
debugs confd snmp
debugs cloudexpress omp low
debugs cloudexpress ftm high
```

The following example shows how to display the list of enabled SD-WAN debugs with only specified debug keyword on Cisco IOS XE SD-WAN devices.

```
Device# show sdwan debugs confd
debugs confd snmp
```

Related Commands

Command	Description
debug	Debugging functions.
undebug	Disables debugging functions.

show sdwan firmware-packages details

To display the details of a firmware package that has been loaded on a device but has not been activated, use the **show sdwan firmware-packages details** command in privileged EXEC mode.

show sdwan firmware-packages details

Command Modes Privileged EXEC mode

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	This command was introduced.

Usage Guidelines

The device can have one of two states:

- A single firmware package is loaded and activated: The command has no output.
- One firmware package is loaded and activated, and another package has been loaded but not activated: The command output shows the version and additional details of the loaded firmware package, designated as not active.

Example

```
Router#show sdwan firmware-packages details
                              MODEM     SUB PACKAGE
VERSION      PACKAGE TYPE    TYPE      VERSION       ACTIVE
------------------------------------------------------------
17.6.0.0.1    Modem-Firmware  EM7430    02.33.03.00   false

Total Space:387M Used Space:145M Available Space:237M
```

show sdwan firmware-packages list

To display the firmware packages loaded on a device and the status of the packages (activated or not), use the **show sdwan firmware-packages list** command in privileged EXEC mode.

show sdwan firmware-packages list

Command Default

None

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.5.1a	This command was introduced.

Usage Guidelines

The device can have one of two states:

- A single firmware package is loaded and activated: The command output shows:
  - The version of the firmware package, designated as active
  - Total and used storage space on the device
- One firmware package is loaded and activated, and another package has been loaded but not activated: The command output shows:
  - The version of the active firmware package, designated as active
  - The version of the package that has been loaded but not yet activated, designated as not active
  - Total and used storage space on the device

Example

```
Router#show sdwan firmware-packages list
VERSION       ACTIVE
----------------------
0.0.0         true
17.6.0.0.1    false

Total Space:387M Used Space:145M Available Space:237M
```

show sdwan from-vsmart commit-history

To verify the commit history for a centralized data policy on Cisco IOS XE Catalyst SD-WAN devices, use the **show sdwan from-vsmart commit-history** command in privileged EXEC mode.

show sdwan from-vsmart commit-history { **detail** | **last-xml** | **summary** }

Syntax Description

detail	Displays the commit history details based on the configuration received from the Cisco SD-WAN Controller.
last-xml	Displays the last XML received from the Cisco SD-WAN Controller.
summary	Displays the commit history summary based on the configuration received from the Cisco SD-WAN Controller.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.9.2a	This command was introduced.
Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	This command was introduced.

Usage Guidelines

Use the **show sdwan from-vsmart commit-history** command to check which peer has pushed data to the Cisco IOS XE Catalyst SD-WAN device, how much time it took to commit the centralized data policy, and the commit status. You can use the information obtained from this command for troubleshooting policy commit failures and to identity the exact reason for the commit failure.

Note Data is not retained upon a reboot of the Cisco IOS XE Catalyst SD-WAN device. Data displays for all policy-related commits until you reboot the Cisco IOS XE Catalyst SD-WAN device.

Example

The following sample output from the **show sdwan from-vsmart commit-history summary** command displays the commit history for the specified centralized data policies:

```
Device# show sdwan from-vsmart commit-history summary
Index  Tenant   Peer-IP           TIMESTAMP            TIME(secs)  TYPE           STATUS
-------------------------------------------------------------------------------------------
0      0        172.16.255.19      2022-09-21 19:00:39  0.395       POLICY         Success
1      0        172.16.255.19      2022-09-21 19:00:39  0.120       TAG-INSTANCES  Success
2      0        172.16.255.19      2022-09-21 19:07:20  0.357       POLICY         Success
```

The following sample output from the **show sdwan from-vsmart commit-history last-xml** command displays the last XML received from the Cisco SD-WAN Controller:

```
Device# show sdwan from-vsmart commit-history last-xml
vSmart Configuration Commit Last XML Details
-----------------------------------------------------
Index: 2
Peer-IP: 172.16.255.19
XML: <data-policy>
  <name>DP_CEDGE</name>
  <vpn-list>
    <name>vpn1</name>
    <sequence>
      <seq-value>11</seq-value>
      <match>
        <source-ip>10.20.24.17/32</source-ip>
        <source-ip>10.20.24.150/32</source-ip>
        <protocol>1</protocol>
      </match>
      <action>
        <action-value>accept</action-value>
        <count>count1-dp1</count>
      </action>
    </sequence>
   <default-action>accept</default-action>
  </vpn-list>
<direction>all</direction></data-policy><lists><vpn-list>
  <name>vpn1</name>
  <vpn>
    <id>1</id>
  </vpn>
</vpn-list>
</lists>
```

The following sample output from the **show sdwan from-vsmart commit-history detail** command displays the commit history details based on the configuration received from the Cisco SD-WAN Controller:

```
Device# show sdwan from-vsmart commit-history detail
vSmart Configuration Commit History Details
-----------------------------------------------------
Index: 0
    Tenant Id: 0
    Peer-IP: 172.16.255.19
    TIMESTAMP: 2022-09-21 19:00:39
    TOTAL-TIME: 0.395 secs
    TYPE: POLICY
    CHKSUM: 0x89da0ad7
    STATUS: Success
    Error-code: n/a
    Error: n/a
Index: 1
    Tenant Id: 0
    Peer-IP: 172.16.255.19
    TIMESTAMP: 2022-09-21 19:00:39
    TOTAL-TIME: 0.120 secs
    TYPE: TAG-INSTANCES
```

```
    CHKSUM: 0x9a0b0195
    STATUS: Success
    Error-code: n/a
    Error: n/a
Index: 2
    Tenant Id: 0
    Peer-IP: 172.16.255.19
    TIMESTAMP: 2022-09-21 19:07:20
    TOTAL-TIME: 0.357 secs
    TYPE: POLICY
    CHKSUM: 0x23b98c55
    STATUS: Success
    Error-code: n/a
    Error: n/a
```

show sdwan from-vsmart policy

To display a centralized data policy, an application-aware policy, or a cflowd policy that a Cisco SD-WAN Controller has pushed to the devices, use the **show sdwan from-vsmart policy** command in privileged EXEC mode. The Cisco SD-WAN Controller pushes the policy via OMP after it has been configured and activated on the controller.

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.11.1a	This command was introduced.

show sdwan from-vsmart policy [**app-route-policy**] [**cflowd-template** *template-option*] [**data-policy**] [**lists** { **data-prefix-list** | **vpn-list** }] [**policer**] [**sla-class**]

Syntax Description

None	Display all the data policies that the vSmart controller has pushed to the Cisco IOS XE Catalyst SD-WAN device.
app-route-policy	Display only the application-aware routing policies that the Cisco vSmart controller has pushed to the Cisco IOS XE Catalyst SD-WAN device.
cflowd-template [*template-option*]	Display only the cflowd template information that the Cisco vSmart controller has pushed to the Cisco IOS XE Catalyst SD-WAN device. *template-option* can be one of **collector**, **flow-active-timeout**, **flow-inactive-timeout**, and **template-refresh**.
data-policy	Display only the data policies that the Cisco vSmart controller has pushed to the Cisco IOS XE Catalyst SD-WAN device.
lists {**data-prefix-list** | **vpn-list**}	Display only the policy-related lists that the Cisco vSmart controller has pushed to the Cisco IOS XE Catalyst SD-WAN device.
policer	Display only the policers that the Cisco vSmart controller has pushed to the Cisco IOS XE Catalyst SD-WAN device.
sla-class	Display only the SLA classes for application-aware routing that the Cisco vSmart controller has pushed to the Cisco IOS XE Catalyst SD-WAN device.

Examples

The following is a sample output from the **show sdwan from-vsmart policy** command displaying policy downloaded from Cisco SD-WAN Controller:

```
Device# show sdwan from-vsmart policy
from-vsmart sla-class SLA1
 latency 100
from-vsmart data-policy DATA_POLICY
 direction from-service
 vpn-list vpn_1
  sequence 11
   match
    destination-port         5060
    protocol                 17
    source-tag-instance      DP_V4_TAG1
    destination-tag-instance DP_V4_TAG3
   action accept
    count src_dst_legacy_v4
  sequence 21
   match
    source-tag-instance DP_V4_TAG1
   action drop
    count src_v4


Device# show sdwan from-vsmart policy
from-vsmart sla-class test_sla_class
 latency 50
from-vsmart app-route-policy test_app_route_policy
 vpn-list vpn_1_list
  sequence 1
   match
    destination-ip 10.2.3.21/32
   action
    sla-class test_sla_class
    sla-class strict
  sequence 2
   match
    destination-port 80
   action
    sla-class test_sla_class
    no sla-class strict
  sequence 3
   match
    destination-data-prefix-list test_data_prefix_list
   action
    sla-class test_sla_class
    sla-class strict

from-vsmart lists vpn-list vpn_1_list
 vpn 1
 vpn 102
from-vsmart lists data-prefix-list test_data_prefix_list
 ip-prefix 10.1.1.0/8


Device# show sdwan from-vsmart policy cflowd-template
from-vsmart cflowd-template test-cflowd-template
 flow-active-timeout   30
 flow-inactive-timeout 30
 template-refresh      30
 collector vpn 1 address 172.16.255.15 port 13322
Device# show sdwan from-vsmart policy cflowd-template collector
```

```
from-vsmart cflowd-template test-cflowd-template
 collector vpn 1 address 172.16.255.15 port 13322
```

show sdwan from-vsmart tag-instances

To display the tags downloaded from the Cisco SD-WAN Controller, use the **show sdwan from-vsmart tag-instances** command in privileged EXEC mode.

show sdwan from-vsmart tag-instances

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.11.1a	This command was introduced.

Usage Guidelines

Use the **show sdwan from-vsmart tag-instances** command to show user configuration of tag-instances.

Examples

The following is a sample output from **show sdwan from-vsmart tag-instances** command, displaying tags downloaded from Cisco SD-WAN Controller:

```
Device# show sdwan from-vsmart tag-instances
tag-instances-from-vsmart
 tag-instance APP_facebook_TAG9
  id       60000
  app-list apps_facebook
 tag-instance APP_office_TAG10
  id       70000
  app-list apps_ms apps_zoom
 tag-instance APP_webex_TAG8
  id       50000
  app-list apps_webex
 tag-instance DP_V4_TAG1
  id               10000
  data-prefix-list pfx1
 lists data-prefix-list multicast_pfx
  ip-prefix 224.0.0.0/8
 lists data-prefix-list pfx1
  ip-prefix 10.20.24.0/24
 lists app-list apps_facebook
  app dns
  app facebook
 lists app-list apps_ms
  app ms-office-365
  app ms-office-web-apps
  app ms-services
```

Related Commands

Command	Description
show sdwan from-vsmart policy	Displays policy downloaded from Cisco SD-WAN Controller.

show sdwan ftm umts

To view the Underlay Measurement and Tracing Services (UMTS) probes that are active on an Cisco Catalyst SD-WAN tunnel, use the **show sdwan ftm umts** command in privileged EXEC mode.

show sdwan ftm umts

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	This command was introduced.

Example

The following example shows UMTS probes that are active on the Cisco Catalyst SD-WAN tunnels.

This command displays a summary of tunnels configured for UMTS, and the corresponding trigger. The tunnels that are enabled for the on-demand option or for the events, are displayed only for a limited period because they are nonperiodic triggers.

```
Device#show sdwan ftm umts probes
MODE     TYPE       ACTIVE   VALID

CONFIG   MONITOR    1        1

CONFIG   SLA        1        1

CONFIG   PMTU       1        1

EXEC     MONITOR    0        0

EXEC     SLA        0        0

EXEC     PMTU       0        0

EXEC     ONDEMAND   0        0

Tunnel-Idx   Src IP       Dst IP       BFD LD    Color         Trigger             Periodic
 Timer left secs
13           10.1.14.14   10.1.15.15   20013     lte           PERIODIC            3575

14           10.1.14.14   10.0.21.16   20014     lte           PERIODIC            3575

15           10.1.14.14   10.0.111.1   20015     lte           PERIODIC            0

16           10.1.14.14   10.1.16.16   20016     lte           PERIODIC            3575
```

```
17           10.1.14.14   10.0.111.2   20017     lte            PERIODIC             0
18     10.1.14.14   10.0.5.11    20018      lte           PERIODIC             3
```

show sdwan ftm umts logs

To view the logs for event-driven or on-demand options of UMTS, use the **show sdwan ftm umts logs** command in privileged EXEC mode.

show sdwan ftm umts logs

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	This command was introduced.

Example

The following example displays the logs for event-driven or on-demand options of UMTS. The **show sdwan ftm umts logs** command displays the exact path traced by a Cisco IOS XE Catalyst SD-WAN device on demand or for events. In some cases, the output is partial if the path has a large number of hops.

```
Device#show sdwan ftm umts logs
Showing 'UMTS' logs
==========================================================================================
11     Mon Oct 31 21:26:18 2022:621  UMTS       (0   ) : ON_DEMAND Stream JSON: "vip_idx":
 "1","vip_time": "1667251578621","remote_color": "lte","local_color": "3g","remote_system_ip":
 "172.16.255.11","local_system_ip": "172.16.255.15","proto": "IPSEC","sent_qos": "72","state":
 "UP","event_type": "ON_DEMAND","event_subtype": "NONE","hops": {"ip": "10.0.20.23","ip":
"10.0.5.11"}
3      Mon Oct 31 21:26:49 2022:619  UMTS       (8   ) : ON_DEMAND Stream JSON: "vip_idx":
 "9","vip_time": "1667251609619","remote_color": "lte","local_color": "3g","remote_system_ip":
 "172.16.255.21","local_system_ip": "172.16.255.15","proto": "IPSEC","sent_qos": "72","state":
 "UP","event_type": "ON_DEMAND","event_subtype": "NONE","hops": {"ip": "10.0.20.23","ip":
"0.0.0.0","ip": "0.0.0.0","ip": "0.0.0.0","ip": "0.0.0.0","ip": "0.0.0.0","ip":
"0.0.0.0","ip": "0.0.0.0","ip": "0.0.0.0","ip": "0.0.0.0","ip": "0.0.0.0","ip":
"0.0.0.0","ip": "0.0.0.0","ip": "0.0.0.0","ip": "0.0.0.0","ip": "0.0.0.0","ip":
"0.0.0.0","ip": "0.0.0.0","ip": "0.0.0.0","ip": "0.0.0.0","ip": "0.0.0.0","ip":
"0.0.0.0","ip": "0.0.0.0","ip": "0.0.0.0","ip": "0.0.0.0","ip": "0.0.0.0","ip":
"0.0.0.0","ip": "0.0.0.0","ip": "0.0.0.0","ip": "0.0.0.0","ip": "0.0.0.0","ip": "0.0.0.0"}
==========================================================================================
Idx     Date-Time:MilliSec           Log-type(Idx in log-type) :   Log-message
============================[NOTE: Read it from bottom to
top]=======================================
Displyed aggregated log cnt 37 from log-types
[ UMTS      ] Max cnt: 500   Agg cnt: 37    Rotated: NO  Curent index: 36
```

show sdwan geofence-status

To verify the geofencing status and configuration, use the **show sdwan geofence-status** command in privileged EXEC mode.

show sdwan geofence-status

Syntax Description This command has no arguments or keywords.

Command Default None

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines Use this command to display geofencing configuration and status.

Examples The following example shows that geofencing is enabled and that the device location is valid and within the defined fence:

```
Device# show sdwan geofence-status
geofence-status
 Geofence Config Status =                 Geofencing-Enabled
 Target Latitude =                        37.317342
 Target Longitude =                       -122.218170
 Geofence Range(in m) =                   100
 Current Device Location Status =         Location-Valid
 Current Latitude =                       37.317567
 Current Longitude =                      -122.218170
 Current Device Status =                  Within-defined-fence
 Distance from target location(in m) =    30
 Last updated device location timestamp =  2021-04-14T19:26:34+00:00
```

show sdwan ipsec inbound-connections

To display information about the IPsec tunnels that originate on remote routers on Cisco IOS XE SD-WAN devices, use the **show sdwan ipsec inbound-connections** command in privileged EXEC mode.

show sdwan ipsec inbound-connections [*local-TLOC-address*]

Syntax Description

local-TLOC-address	(Optional) Displays information about IPsec tunnels that originate on remote routers to the specified local TLOC address.

Command Default None

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

Cisco IOS XE Catalyst SD-WAN devices can use the standards-based Internet Key Exchange (IKE) protocol when establishing IPsec tunnels between a device within the overlay network and a device that is external to the overlay network, such as a cloud-hosted service or a remote device.

IPsec provides confidentiality, data integrity, access control, and data source authentication for the traffic being exchanged over the IPsec tunnel.

This command can be used to display information about IPsec tunnels that originate on remote routers on Cisco IOS XE SD-WAN devices.

Example

The following example shows how to display information about IPsec tunnels that originate on remote routers on Cisco IOS XE SD-WAN devices.

```
Device# show sdwan ipsec inbound-connections

SOURCE SOURCE DEST DEST REMOTE REMOTE LOCAL LOCAL NEGOTIATED
IP PORT IP PORT TLOC ADDRESS TLOC COLOR TLOC ADDRESS TLOC COLOR ENCRYPTION ALGORITHM TC
SPIs
--------------------------------------------------------------------------------------------
--------------------------------------------------------------------------------------------
-----
10.6.17.254 12346 10.3.6.2 12366 2.1.1.1 default 10.3.206.1 public-internet AES-GCM-256 8
10.6.18.254 12386 10.3.6.2 12366 2.1.1.2 default 10.3.206.1 public-internet AES-GCM-256 8
```

The following example shows how to display information about IPsec tunnels that originate on remote routers to the specified local TLOC address 10.3.206.1 on Cisco IOS XE SD-WAN devices.

```
Device# show sdwan ipsec inbound-connections 10.3.206.1
SOURCE SOURCE DEST DEST REMOTE REMOTE LOCAL LOCAL NEGOTIATED
IP PORT IP PORT TLOC ADDRESS TLOC COLOR TLOC ADDRESS TLOC COLOR ENCRYPTION ALGORITHM TC
SPIs
--------------------------------------------------------------------------------------------
--------------------------------------------------------------------------------------------
-----
10.6.17.254 12346 10.3.6.2 12366 2.1.1.1 default 10.3.206.1 public-internet AES-GCM-256 8
10.6.18.254 12386 10.3.6.2 12366 2.1.1.2 default 10.3.206.1 public-internet AES-GCM-256 8
```

Related Commands

Command	Description
show sdwan ipsec local-sa	Displays security association information for the IPsec tunnels that have been created for local TLOCs.
show sdwan ipsec outbound-connections	Displays information about the IPsec tunnels to remote routers.
show sdwan ipsec pwk inbound-connections	Displays pairwise keys information about IPsec tunnels that originate on remote routers.
show sdwan ipsec pwk local-sa	Displays security association and pairwise keys information for the IPsec tunnels that have been created for local TLOCs.

Command	Description
show sdwan ipsec pwk outbound-connections	Displays pairwise keys information about the IPsec tunnels to remote routers.

show sdwan ipsec local-sa

To display information about the IPsec tunnels that originate on remote routers on Cisco IOS XE SD-WAN devices, use the **show sdwan ipsec local-sa** command in privileged EXEC mode.

show sdwan ipsec local-sa [*local-TLOC-address*]

Syntax Description

local-TLOC-address	(Optional) Displays security association information for the IPsec tunnels that have been created for the specified local TLOC address.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

Cisco SD-WAN routers can use the standards-based Internet Key Exchange (IKE) protocol when establishing IPsec tunnels between a device within the overlay network and a device that is external to the overlay network, such as a cloud-hosted service or a remote device.

IPsec provides confidentiality, data integrity, access control, and data source authentication for the traffic being exchanged over the IPsec tunnel.

This command can be used to display security association information for the IPsec tunnels that have been created for local TLOCs on Cisco IOS XE SD-WAN devices.

Example

The following example shows how to display security association information for the IPsec tunnels that have been created for local TLOCs on Cisco IOS XE SD-WAN devices.

```
Device# show sdwan ipsec local-sa

TLOC ADDRESS TLOC COLOR SPI IPv4 IPv6 PORT KEY HASH
------------------------------------------------------------------------------
10.3.206.1 public-internet 288 10.3.6.2 :: 12366 *****8415
10.3.206.1 public-internet 289 10.3.6.2 :: 12366 *****5c2c
```

The following example shows how to display security association information for the IPsec tunnels that have been created for the specified local TLOC address 10.3.206.1 on Cisco IOS XE SD-WAN devices.

```
Device# show sdwan ipsec local-sa 10.3.206.1
SOURCE SOURCE DEST TLOC ADDRESS TLOC COLOR SPI IPv4 IPv6 PORT KEY HASH
```

```
------------------------------------------------------------------------------
10.3.206.1 public-internet 288 10.3.6.2 :: 12366 *****8415
10.3.206.1 public-internet 289 10.3.6.2 :: 12366 ***
```

Related Commands

Command	Description
show sdwan ipsec inbound-connections	Displays information about IPsec tunnels that originate on remote routers.
show sdwan ipsec outbound-connections	Displays information about the IPsec tunnels to remote routers.
show sdwan ipsec pwk inbound-connections	Displays pairwise keys information about IPsec tunnels that originate on remote routers.
show sdwan ipsec pwk local-sa	Displays security association and pairwise keys information for the IPsec tunnels that have been created for local TLOCs.
show sdwan ipsec pwk outbound-connections	Displays pairwise keys information about the IPsec tunnels to remote routers.

show sdwan ipsec outbound-connections

To view information about the IPsec tunnels to remote routers on Cisco IOS XE SD-WAN devices, use the **show sdwan ipsec outbound-connections** command in privileged EXEC mode.

show sdwan ipsec outbound-connections [*source-ip*]

Syntax Description

source-ip	(Optional) Displays information about the IPsec tunnels to remote routers for the specified source IP.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	The output of this command was modified. Starting from Cisco IOS XE Catalyst SD-WAN Release 17.6.1a, the command output replaces the `Authentication Used` column with the `Integrity Used` column. The values `null`, `ah-sha1-hmac`, `ah-no-id`, and `sha1-hmac` are replaced with `none`, `ip-udp-esp`, `ip-udp-esp-no-id`, and `esp` respectively.

Usage Guidelines

Cisco IOS XE Catalyst SD-WAN devices can use the standards-based Internet Key Exchange (IKE) protocol when establishing IPsec tunnels between a device within the overlay network and a device that is external to the overlay network, such as a cloud-hosted service or a remote device.

IPsec provides confidentiality, data integrity, access control, and data source authentication for the traffic being exchanged over the IPsec tunnel.

This command can be used to display information about the IPsec tunnels to remote routers on Cisco IOS XE SD-WAN devices.

Example

The following is a sample output of the **show sdwan ipsec outbound-connections** for Cisco IOS XE Catalyst SD-WAN Release 17.6.1a and later.

The following are sample outputs of the **show sdwan ipsec outbound-connections** command for releases prior to Cisco IOS XE Catalyst SD-WAN Release 17.6.1a.

The following example displays information about the IPsec tunnels to remote routers on Cisco IOS XE SD-WAN devices.

```
Device# show sdwan ipsec outbound-connections

SOURCE SOURCE DEST DEST REMOTE REMOTE AUTHENTICATION NEGOTIATED
IP PORT IP PORT SPI TUNNEL MTU TLOC ADDRESS TLOC COLOR USED KEY HASH ENCRYPTION ALGORITHM
TC SPIs
--------------------------------------------------------------------------------------------
--------------------------------------------------------------------------------------------
-----------
10.64.0.18 12346 10.64.0.2 12366 256 1442 10.1.0.1 mpls AH_SHA1_HMAC *****c4cc AES-GCM-256
 8
10.64.0.18 12346 10.64.0.6 12366 256 1442 10.1.0.2 mpls AH_SHA1_HMAC *****5d57 AES-GCM-256
 8
10.64.0.18 12346 10.64.0.26 12366 256 1442 10.4.0.1 mpls AH_SHA1_HMAC *****e9b4 AES-GCM-256
 8
10.64.2.38 12346 10.64.2.6 17196 256 1442 10.4.0.1 biz-internet AH_SHA1_HMAC *****4ee7
AES-GCM-256 8
10.64.2.38 12346 10.64.2.26 12366 256 1442 10.1.0.1 biz-internet AH_SHA1_HMAC *****a094
AES-GCM-256 8
10.64.2.38 12346 10.64.2.30 12366 256 1442 10.1.0.2 biz-internet AH_SHA1_HMAC *****d092
AES-GCM-256 8
```

The following example shows how to display information about the IPsec tunnels to remote routers from the specified source IP 100.64.0.18 on Cisco IOS XE SD-WAN devices.

show sdwan ipsec pwk inbound-connections

To display pairwise keys information about the IPsec tunnels that originate on remote routers on Cisco IOS XE SD-WAN devices, use the **show sdwan ipsec pwk inbound-connections** command in privileged EXEC mode.

show sdwan ipsec pwk inbound-connections [*local-TLOC-address*]

Syntax Description

local-TLOC-address	(Optional) Displays pairwise keys information about the IPsec tunnels that originate on remote routers for the specified local TLOC address.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

Cisco IOS XE Catalyst SD-WAN devices can use the standards-based Internet Key Exchange (IKE) protocol when establishing IPsec tunnels between a device within the overlay network and a device that is external to the overlay network, such as a cloud-hosted service or a remote device.

IPsec provides confidentiality, data integrity, access control, and data source authentication for the traffic being exchanged over the IPsec tunnel.

IPsec pairwise keys feature implements controller-based key exchange protocol between device and controller. A pair of IPsec session keys (one encryption key and one decryption key) are configured per pair of local and remote Transport Locations (TLOC).

This command can be used to display pairwise keys information about the IPsec tunnels that originate on remote routers on Cisco IOS XE Catalyst SD-WAN devices.

Example

The following example shows how to display pairwise keys information about the IPsec tunnels that originate on remote routers on Cisco IOS XE SD-WAN devices.

```
Device# show sdwan ipsec pwk inbound-connections

DEST        LOCAL             LOCAL             REMOTE            REMOTE
                  SA    PKEY  NONCE    PKEY    SS   D-KEY   AH
               SOURCE IP                    PORT                   DEST IP
                    PORT     TLOC ADDRESS      TLOC COLOR      TLOC ADDRESS
      TLOC COLOR     PWK-SPI  INDEX    ID    HASH   HASH   HASH   HASH  AUTH
-----------------------------------------+--------+---------------------------
-------------+--------+----------------+----------------+----------------+---
-------------+---------+------+------+------+------+------+------+----
10.6.17.254                              12346    10.3.6.2
             12366    10.3.206.1       public-internet  2.1.1.1
default          000000   9      0                                    true

10.6.18.254                              12386    10.3.6.2
             12366    10.3.206.1       public-internet  2.1.1.2
default          000000   10     0                                    true
```

The following example shows how to display pairwise keys information about the IPsec tunnels that originate on remote routers for the specified local TLOC address 10.3.206.1 on Cisco IOS XE SD-WAN devices.

```
Device# show sdwan ipsec pwk inbound-connections 10.3.206.1

DEST        LOCAL             LOCAL             REMOTE            REMOTE
      SA    PKEY  NONCE    PKEY    SS   D-KEY   AH
               SOURCE IP                    PORT                   DEST IP
             PORT     TLOC ADDRESS      TLOC COLOR      TLOC ADDRESS
TLOC COLOR     PWK-SPI  INDEX    ID    HASH   HASH   HASH   HASH  AUTH
-----------------------------------------+--------+---------------------------
--------------+--------+----------------+----------------+----------------+-
---------------+---------+------+------+------+------+------+------+----
10.6.17.254                              12346    10.3.6.2
               12366    10.3.206.1       public-internet  2.1.1.1
default          000000   9      0                                    true
10.6.18.254                              12386    10.3.6.2
```

```
                    12366    10.3.206.1       public-internet  2.1.1.2
default             000000   10     0                                  true
```

Related Commands

Command	Description
show sdwan ipsec inbound-connections	Displays information about IPsec tunnels that originate on remote routers.
show sdwan ipsec local-sa	Displays security association information for the IPsec tunnels that have been created for local TLOCs.
show sdwan ipsec outbound-connections	Displays information about the IPsec tunnels to remote routers.
show sdwan ipsec pwk local-sa	Displays security association and pairwise keys information for the IPsec tunnels that have been created for local TLOCs.
show sdwan ipsec pwk outbound-connections	Displays pairwise keys information about the IPsec tunnels to remote routers.

show sdwan ipsec pwk local-sa

To display security association and pairwise keys information for the IPsec tunnels that have been created for local TLOCs on Cisco IOS XE SD-WAN devices, use the **show sdwan ipsec pwk local-sa** command in privileged EXEC mode.

show sdwan ipsec pwk local-sa [*local-TLOC-address*]

Syntax Description

local-TLOC-address	(Optional) Displays security association and pairwise keys information for the IPsec tunnels that have been created for the specified local TLOC address

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

Cisco IOS XE Catalyst SD-WAN devices can use the standards-based Internet Key Exchange (IKE) protocol when establishing IPsec tunnels between a device within the overlay network and a device that is external to the overlay network, such as a cloud-hosted service or a remote device.

IPsec provides confidentiality, data integrity, access control, and data source authentication for the traffic being exchanged over the IPsec tunnel.

IPsec Pairwise Keys feature implements controller-based key exchange protocol between device and controller. A pair of IPsec session keys (one encryption key and one decryption key) are configured per pair of local and remote Transport Locations (TLOC).

This command can be used to display security association and pairwise keys information for the IPsec tunnels that have been created for local TLOCs on Cisco IOS XE Catalyst SD-WAN devices.

Example

The following example shows how to display security association and pairwise keys information for the IPsec tunnels that have been created for local TLOCs on Cisco IOS XE SD-WAN devices.

```
Device# show sdwan ipsec pwk local-sa

SOURCE          SA              PKEY      NONCE  PKEY TLOC-ADDRESS
TLOC-COLOR      SOURCE-IP  PORT   SPI  INDEX  ID   HASH  HASH
------------------------------------------------------------------------------
10.3.206.1   public-internet 10.3.6.2   12366  292  37     0
10.3.206.1   public-internet 10.3.6.2   12366  293  38     0
```

The following example shows how to display security association and pairwise keys information for the IPsec tunnels that have been created for local TLOCs from the specified source IP 10.3.206.1 on Cisco IOS XE SD-WAN devices.

```
Device# show sdwan ipsec pwk local-sa 10.3.206.1

SOURCE      SA    PKEY  NONCE PKEY
TLOC-ADDRESS TLOC-COLOR      SOURCE-IP  PORT   SPI  INDEX  ID   HASH  HASH
------------------------------------------------------------------------------
10.3.206.1   public-internet 10.3.6.2   12366  292  37     0
10.3.206.1   public-internet 10.3.6.2   12366  293  38     0
```

Related Commands

Command	Description
show sdwan ipsec inbound-connections	Displays information about IPsec tunnels that originate on remote routers.
show sdwan ipsec local-sa	Displays security association information for the IPsec tunnels that have been created for local TLOCs.
show sdwan ipsec outbound-connections	Displays information about the IPsec tunnels to remote routers.
show sdwan ipsec pwk inbound-connections	Displays pairwise keys information about IPsec tunnels that originate on remote routers.
show sdwan ipsec pwk outbound-connections	Displays pairwise keys information about the IPsec tunnels to remote routers.

show sdwan ipsec pwk outbound-connections

To display pairwise keys information about the IPsec tunnels to remote routers on Cisco IOS XE SD-WAN devices, use the **show sdwan ipsec pwk outbound-connections** command in privileged EXEC mode.

show sdwan ipsec pwk outbound-connections [*source-ip*]

Syntax Description

source-ip	(Optional) Displays pairwise keys information about the IPsec tunnels to remote routers from the specified source IP.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

Cisco IOS XE Catalyst SD-WAN devices can use the standards-based Internet Key Exchange (IKE) protocol when establishing IPsec tunnels between a device within the overlay network and a device that is external to the overlay network, such as a cloud-hosted service or a remote device.

IPsec provides confidentiality, data integrity, access control, and data source authentication for the traffic being exchanged over the IPsec tunnel.

IPsec Pairwise Keys feature implements controller-based key exchange protocol between device and controller. A pair of IPsec session keys (one encryption key and one decryption key) are configured per pair of local and remote Transport Locations (TLOC).

This command can be used to display pairwise keys information about the IPsec tunnels to remote routers on Cisco IOS XE SD-WAN devices.

Example

The following example shows how to display pairwise keys information about the IPsec tunnels to remote routers on Cisco IOS XE SD-WAN devices.

```
Device# show sdwan ipsec pwk outbound-connections

SOURCE      DEST        LOCAL            LOCAL            REMOTE           REMOTE
         SA
PKEY  NONCE   PKEY    SS   E-KEY   AH
               SOURCE IP                   PORT                  DEST IP

PORT     TLOC ADDRESS      TLOC COLOR      TLOC ADDRESS      TLOC COLOR     PWK-SPI  INDEX

ID    HASH   HASH   HASH   HASH  AUTH
-------------------------------------+--------+-----------------------------------------+-----
---+---------------+---------------+---------------+---------------+---------+------+------+
------+------+------+------+----
10.64.0.18                           12346    10.64.0.2
12366
10.3.0.1         mpls             10.1.0.1         mpls              000000   1      0
c4cc  true
10.64.0.18                           12346    10.64.0.6
12366
10.3.0.1         mpls             10.1.0.2         mpls              000000   3      0
5d57  true
10.64.0.18                           12346    10.64.0.26
12366
10.3.0.1         mpls             10.4.0.1         mpls              000000   5      0
e9b4  true
10.64.2.38                           12346    10.64.2.6
17196
10.3.0.1         biz-internet     10.4.0.1         biz-internet      000000   6      0
4ee7  true
10.64.2.38                           12346    10.64.2.26
12366
```

```
10.3.0.1         biz-internet     10.1.0.1         biz-internet      000000   2      0
a094  true
10.64.2.38                             12346    10.64.2.30
12366
10.3.0.1         biz-internet     10.1.0.2         biz-internet      000000   4      0
d092  true
```

The following example shows how to display pairwise keys information about the IPsec tunnels to remote routers from the specified source IP 10.64.0.18 on Cisco IOS XE SD-WAN devices.

```
Device# show sdwan ipsec pwk outbound-connections 10.3.206.1

SOURCE     DEST         LOCAL             LOCAL      REMOTE      REMOTE
SA     PKEY  NONCE    PKEY     SS    E-KEY    AH     SOURCE IP      PORT
DEST IP     PORT    TLOC ADDRESS       TLOC COLOR       TLOC ADDRESS       TLOC COLOR
PWK-SPI  INDEX     ID     HASH HASH    HASH    HASH  AUTH
-----------------------------------------+--------+--------------------------------
-+----------------+----------------+----------------+----------------+---------+--
--+------+------+------+----
10.64.0.18                         12346    10.64.0.2                          12366
10.3.0.1         mpls              10.1.0.1         mpls  00000   1      0   c4cc  true
10.64.0.18                         12346    10.64.0.6                          12366
10.3.0.1         mpls              10.1.0.2         mpls              000000   3      0
5d57  true
```

Related Commands

Command	Description
show sdwan ipsec inbound-connections	Displays information about IPsec tunnels that originate on remote routers.
show sdwan ipsec local-sa	Displays security association information for the IPsec tunnels that have been created for local TLOCs.
show sdwan ipsec outbound-connections	Displays information about the IPsec tunnels to remote routers.
show sdwan ipsec pwk inbound-connections	Displays pairwise keys information about IPsec tunnels that originate on remote routers.
show sdwan ipsec pwk local-sa	Displays security association and pairwise keys information for the IPsec tunnels that have been created for local TLOCs.

show sdwan nat-fwd ip-nat-translation

To display active NAT translations on Cisco IOS XE SD-WAN devices, use the **show sdwan nat-fwd ip-nat-translation** command in privileged EXEC mode.

show sdwan nat-fwd ip-nat-translation

Syntax Description This command has no keywords or arguments.

Command Default None

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

NAT enables private IP internetworks that use nonregistered IP addresses to connect to the internet. NAT operates on a device, usually connecting two networks. Before packets are forwarded onto another network, NAT translates the private (not globally unique) addresses in the internal network into legal addresses.

This command can be used to display active NAT translations on Cisco IOS XE SD-WAN devices.

Example

The following example shows how to display active NAT translations on Cisco IOS XE SD-WAN devices.

```
Device# show sdwan nat-fwd ip-nat-translation
nat-fwd ip-nat-translation 10.3.40.14 168.61.161.212 62244 443 3 6
 inside-global-addr  100.64.2.38
 outside-global-addr 168.61.161.212
 inside-global-port  5841
 outside-global-port 443
 flags               536887296
 application-type    0
nat-fwd ip-nat-translation 10.3.40.14 52.255.188.83 62246 443 3 6
 inside-global-addr  100.64.2.38
 outside-global-addr 52.255.188.83
 inside-global-port  5844
 outside-global-port 443
 flags               2113552
 application-type    0
```

Related Commands

Command	Description
show sdwan nat-fwd ip-nat-translation-verbose	Displays detailed active NAT translations.

show sdwan nat-fwd ip-nat-translation-verbose

To display detailed active NAT translations on Cisco IOS XE SD-WAN devices, use the **show sdwan nat-fwd ip-nat-translation-verbose** command in privileged EXEC mode.

show sdwan nat-fwd ip-nat-translation-verbose

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

NAT enables private IP internetworks that use nonregistered IP addresses to connect to the internet. NAT operates on a device, usually connecting two networks. Before packets are forwarded onto another network, NAT translates the private (not globally unique) addresses in the internal network into legal addresses.

This command can be used to display detailed active NAT translations on Cisco IOS XE Catalyst SD-WAN devices.

Example

The following example shows how to display detailed active NAT translations on Cisco IOS XE Catalyst SD-WAN devices.

```
Device# show sdwan nat-fwd ip-nat-translation-verbose

nat-fwd ip-nat-translation-verbose 10.3.40.10 198.18.1.222 43965 80 3 6
 inside-global-addr  100.64.2.38
 outside-global-addr 198.18.1.222
 inside-global-port  5280
 outside-global-port 80
 flags               1075855376
 application-type    0
 entry-id            0xea5bc6c0
 in_mapping_id       1
 out_mapping_id      0
 create_time         "Thu Dec  3 19:37:07 2020"
 last_used_time      "Thu Dec  3 19:37:59 2020"
 pkts_in             13
 pkts_out            11
 timeout             "13 seconds"
 usecount            1
 input-idb           GigabitEthernet7
 output-idb          GigabitEthernet4
 bytes_in            638
 bytes_out           11335
```

Related Commands

Command	Description
show sdwan nat-fwd ip-nat translation	Displays active NAT translations.

show sdwan omp cloudexpress

To display the available routes from each gateway device in the network, for each application configured in Cloud onRamp for SaaS, use the **show sdwan omp cloudexpress** command in privileged EXEC mode.

show sdwan omp cloudexpress

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command is supported for Cisco Catalyst SD-WAN.

Usage Guidelines

The command displays the available routes from each gateway device in the network, for each application configured in Cloud onRamp for SaaS. Cloud onRamp for SaaS sends the routes, together with service level agreement (SLA) information to the devices in the network to use to determine the best path, to the cloud server for the application. The path may be through direct internet access (DIA) or through a gateway device.

The APP ID column indicates the application, using the following codes:

APP ID	Application
1	Salesforce
2	Office 365
3	Amazon AWS
4	Oracle
6	Box
7	Dropbox
9	Intuit
10	Concur
11	Sugar CRM
12	Zoho CRM
13	Zendesk
14	GoToMeeting
15	Webex
16	Google

The STATUS column codes are as follows:

Status	Description
C	Chosen
I	Installed
Red	Redistributed
Rej	Rejected
L	Looped

Status	Description
R	Resolved
S	Stale
Ext	Extranet
Inv	Invalid

Examples

The following is an example output for the **show sdwan omp cloudexpress** command:

```
Device#show sdwan omp cloudexpress
                     APP  APP   SUBAPP
VPN  ORIGINATOR      ID   TYPE  ID      APP NAME    FROM PEER      STATUS
-------------------------------------------------------------------------
1    172.16.255.15   3    2     0       amazon_aws  172.16.255.15  C,R
                                                   172.16.255.20  C,R
1    172.16.255.15   15   4     8       webex       172.16.255.15  C,R
                                                   172.16.255.20  C,R
1    172.16.255.16   3    0     0       amazon_aws  172.16.255.16  C,R
                                                   172.16.255.20  C,R
```

show sdwan omp ipv6-routes

To display IPv6 OMP routes on Cisco IOS XE Catalyst SD-WAN devices, use the **show sdwan omp ipv6-routes** command in privileged EXEC mode.

show sdwan omp ipv6-routes [*WORD*]

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

On Cisco Catalyst SD-WAN devices, OMP advertises to its peers the routes and services that it has learned from its local site, along with their corresponding transport location mappings, which are called TLOCs.

OMP routes carry information that the device learns from the routing protocols running on its local network including routes learned from BGP and OSPF as well direct, connected, and static routes. This command can be used to display IPv6 OMP routes on Cisco IOS XE Catalyst SD-WAN devices.

Example

The following example shows how to display IPv6 OMP routes on Cisco IOS XE Catalyst SD-WAN devices.

```
Device# show sdwan omp ipv6-routes
------------------------------------------------
omp route entries for vpn 10 route 2001:db8:1::/64
------------------------------------------------
           RECEIVED FROM:
peer            0.0.0.0
path-id         66
label           1002
status          C,Red,R
loss-reason     not set
lost-to-peer    not set
lost-to-path-id not set
    Attributes:
     originator       10.3.0.2
     type             installed
     tloc             10.3.0.2, mpls, ipsec
     ultimate-tloc    not set
     domain-id        not set
     overlay-id        1
     site-id          300
     preference       not set
     tag              not set
     origin-proto     connected
     origin-metric    0
     as-path          not set
     unknown-attr-len not set
           RECEIVED FROM:
peer            0.0.0.0
path-id         68
label           1002
status          C,Red,R
loss-reason     not set
lost-to-peer    not set
lost-to-path-id not set
    Attributes:
     originator       10.3.0.2
     type             installed
     tloc             10.3.0.2, biz-internet, ipsec
     ultimate-tloc    not set
     domain-id        not set
     overlay-id        1
     site-id          300
     preference       not set
     tag              not set
     origin-proto     connected
     origin-metric    0
     as-path          not set
     unknown-attr-len not set
           ADVERTISED TO:
peer    12.12.12.12
           ADVERTISED TO:
peer    22.22.22.22
```

Related Commands

Commands	Description
show sdwan omp cloudexpress	Displays OMP routes for applications configured with Cloud OnRamp for SaaS.
show sdwan omp milticast-auto-discover	Displays the peers that support multicast.

Commands	Description
show sdwan omp multicast-routes	Displays the multicast routes that OMP has learned from PIM join messages.
show sdwan omp peers	Displays information about the OMP peering sessions that are active on the local Cisco Catalyst SD-WAN devices.
show sdwan omp routes	Displays information about OMP routes.
show sdwan omp services	Displays the services learned from OMP peering sessions.
show sdwan omp summary	Displays information about the OMP sessions running between Cisco Catalyst SD-WAN devices.
show sdwan omp tlocs-paths	Displays information about the TLOC path information.
show sdwan omp tlocs	Displays information learned from the TLOC routes advertised over the OMP sessions running between Cisco Catalyst SD-WAN devices.

show sdwan omp multicast-auto-discover

show sdwan omp multicast-auto-discover—List the peers that support multicast on Cisco IOS XE Catalyst SD-WAN device and vSmart controllers only.

Command Syntax

show sdwan omp multicast-auto-discover [**detail**]

Syntax Description

	None: List standard information about the OMP Multicast routes.
detail	Detailed Information: List detailed information.

Output Fields

The output fields are self-explanatory.

Command History

Release	Modification
17.2.1	Command introduced.

Example

```
Device# show sdwan omp multicast-auto-discover
Code:
C   -> chosen
I   -> installed
Red -> redistributed
Rej -> rejected
L   -> looped
R   -> resolved
S   -> stale
Ext -> extranet
Inv -> invalid

ADDRESS       SOURCE
FAMILY   VPN  ORIGINATOR     FROM PEER      STATUS
-----------------------------------------------------
ipv4     1    172.16.255.11  172.16.255.19  C,I,R
                             172.16.255.20  C,I,R
         1    172.16.255.14  172.16.255.19  C,I,R
                             172.16.255.20  C,I,R
         1    172.16.255.15  172.16.255.19  C,I,R
                             172.16.255.20  C,I,R
         1    172.16.255.16  0.0.0.0        C,Red,R
         1    172.16.255.21  172.16.255.19  C,I,R
                             172.16.255.20  C,I,R
```

show sdwan omp multicast-routes

show sdwan omp multicast-routes—List the multicast routes that OMP has learned from PIM join messages (on Cisco IOS XE Catalyst SD-WAN device and vSmart controllers).

Command Syntax

show sdwan omp multicast-routes [**detail**]

Syntax Description

	None: List standard information about Cisco IOS XE Catalyst SD-WAN devices supporting multicast routes.
detail	Detailed Information: List detailed information.

Output Fields

The output fields are self-explanatory.

Command History

Release	Modification
17.2.1	Command introduced.

Example

```
Device# show sdwan omp multicast-routes
Code:
C   -> chosen
I   -> installed
Red -> redistributed
Rej -> rejected
L   -> looped
R   -> resolved
S   -> stale
Ext -> extranet
Inv -> invalid

ADDRESS              SOURCE
FAMILY   TYPE   VPN  ORIGINATOR     DESTINATION    GROUP      SOURCE   FROM PEER      RP            STATUS
-------------------------------------------------------------------------------------------------------------
ipv4     (*,G)  1    172.16.255.14  172.16.255.16  225.0.0.1  0.0.0.0  172.16.255.19  10.20.25.18  C,I,R
                                                                       172.16.255.20  10.20.25.18  C,I,R
```

show sdwan omp peers

To display information about OMP peers on Cisco SD-WAN Controllers and Cisco IOS XE Catalyst SD-WAN devices, use the **show sdwan omp peers** command in privileged EXEC mode.

Command Syntax

show sdwan omp peers [**detail**]

Syntax Description

	None: List information about all OMP peering sessions on the local device.
detail	Detailed information: Display detailed information.

Output Fields

Field	Explanation
Domain ID	Identifier of the domain that the device is a member of.
downcount	Number of times an OMP peering session has gone down.
last-downtime	The last time that an OMP peering session went down.
last-uptime	The last time that an OMP peering session came up.
Peer or peer	IP address of the connected Cisco IOS XE Catalyst SD-WAN device.

Field	Explanation
Region ID	Region assigned for Hierarchical SD-WAN. For information, see Hierarchical SD-WAN.
R/I/S	Number of routes received, installed, and sent over the OMP session.
routes-installed	Number of routes installed over the OMP session.
routes-received	Number of routes received over the OMP session.
routes-sent	Number of routes sent over the OMP session.
services-installed	Number of services installed that were learned over OMP sessions.
services-received	Number of services received over OMP sessions.
services-sent	Number of services advertised over OMP sessions.
Site ID	Identifier of the Cisco IOS XE Catalyst SD-WAN device administrative site where the connected Cisco IOS XE Catalyst SD-WAN device is located.
state	Operational state of the connection to the Cisco IOS XE Catalyst SD-WAN device: • down—The connection is not functioning. • down-in-gr—A connection on which OMP grace restart is enabled is down. init—The connection is initializing. up—The connection is operating.
tlocs-installed	Number of TLOCs installed that were learned over OMP sessions.
tlocs-received	Number of TLOCs received over OMP sessions.
tlocs-sent	Number of TLOCs advertised over OMP sessions.
Type or type	Type of Cisco IOS XE Catalyst SD-WAN device • Cisco IOS XE Catalyst SD-WAN device • vsmart - vSmart controller
upcount	Number of times an OMP peering session has come up.
Uptime	How long the OMP session between the Cisco IOS XE Catalyst SD-WAN devices has been up and operational.

Command History

Release	Modification
16.12.1	Command introduced.
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	Added the Region ID column to the command output.

Examples

Example 1

```
Device# show sdwan omp peers
R -> routes received
I -> routes installed
S -> routes sent

                        DOMAIN    SITE
PEER             TYPE   ID        ID        STATE    UPTIME           R/I/S
-----------------------------------------------------------------------------
172.16.255.19    vsmart  1         100       up       0:04:09:59       7/7/3
172.16.255.20    vsmart  1         200       up       0:04:10:14       7/0/3
```

```
vEdge# show omp peers 172.16.255.19 detail

peer                     172.16.255.19
type                     vsmart
domain-id                1
site-id                  100
state                    up
version                  1
legit                    yes
upcount                  1
downcount                0
last-uptime              2014-11-12T14:52:19+00:00
last-downtime            0000-00-00T00:00:00+00:00
uptime                   0:04:12:30
hold-time                15
graceful-restart         supported
graceful-restart-interval 300
hello-sent               3032
hello-received           3030
handshake-sent           1
handshake-received       1
alert-sent               0
alert-received           0
inform-sent              5
inform-received          5
update-sent              8
update-received          27
policy-sent
policy-received
total-packets-sent       3046
total-packets-received   3063
routes-received          7
routes-installed         7
routes-sent              3
tlocs-received           4
tlocs-installed          4
tlocs-sent               1
services-received        0
services-installed       0
services-sent            1
mcast-routes-received    0
```

```
mcast-routes-installed    0
mcast-routes-sent         0
```

Example 2

```
vSmart# show sdwan omp peers
R -> routes received
I -> routes installed
S -> routes sent
                         DOMAIN    SITE
PEER             TYPE    ID        ID        STATE    UPTIME           R/I/S
-------------------------------------------------------------------------------
172.16.255.11    vedge   1         100       up       0:00:38:20       3/0/9
172.16.255.14    vedge   1         400       up       0:00:38:22       0/0/11
172.16.255.15    vedge   1         500       up       0:00:38:22       3/0/8
172.16.255.16    vedge   1         600       up       0:00:38:21       4/0/7
172.16.255.20    vsmart  1         200       up       0:00:38:24       11/0/11
172.16.255.21    vedge   1         100       up       0:00:38:20       3/0/9
```

Example 3

```
vSmart# show sdwan omp peers
R -> routes received
I -> routes installed
S -> routes sent

                         DOMAIN    SITE
PEER             TYPE    ID        ID        STATE     UPTIME           R/I/S
-------------------------------------------------------------------------------
172.16.255.11    vedge   1         100       up        0:05:19:17       3/0/5
172.16.255.14    vedge   1         400       up        0:05:19:17       0/0/7
172.16.255.15    vedge   1         500       down-in-gr                 3/0/0
172.16.255.16    vedge   1         600       down                       0/0/0
172.16.255.20    vsmart  1         200       up        0:05:19:21       7/0/7
172.16.255.21    vedge   1         100       up        0:05:19:20       3/0/5
```

Example 4

Beginning with Cisco IOS XE Catalyst SD-WAN Release 17.7.1a, the command output includes the Region ID column.

```
Device# show sdwan omp peers
R -> routes received
I -> routes installed
S -> routes sent

TENANT                           DOMAIN    OVERLAY   SITE      REGION
ID        PEER              TYPE    ID        ID        ID        ID        STATE    UPTIME           R/I/S
-------------------------------------------------------------------------------------------------------------------
0         172.24.121.10     vsmart  1         1         100       0         up       12:04:39:41      32/28/16
0         172.24.122.10     vsmart  1         1         200       2         up       0:09:36:45       12/10/32
0         172.24.123.10     vsmart  1         1         300       2         up       12:04:44:52      12/0/32
0         172.24.124.10     vsmart  1         1         400       0         up       12:04:39:41      32/0/16
```

show sdwan omp routes

To display information about OMP routes on Cisco Catalyst SD-WAN Controllers and Cisco IOS XE Catalyst SD-WAN devices, use the command **show sdwan omp routes** in the privileged EXEC mode. OMP routes carry information that the device learns from the routing protocols running on its local network, including routes learned from BGP and OSPF, as well as direct, connected, and static routes.

Command Syntax

show sdwan omp routes [*prefix/length*] [**family** *family address*] [**vpn** *vpn-id*] [**tenant** *tenant-id*] [**verify**] [**detail**]

Syntax Description

None	Lists the routing information about all OMP peering sessions on the local device.
prefix	Displays the route prefix. Lists OMP route information for the specified route prefix.
length	Displays the route length. Lists OMP route information for the specified route prefix.
family *family address*	Displays the family. Lists OMP route information for the specified IP family.
vpn *vpn-id*	Displays VPN-specific routes. Lists the OMP routes for the specified VPN.
tenant *tenant-id*	Displays tenant ID. Specify tenant-id value within the range, 0 to 65534.
verify	Displays end-to-end verification information of a prefix availability, while keeping track of received and installed prefixes into RIB and FIB, TLOCs, and BFD sessions established.
detail	Displays detailed output information.

Output Fields

The output fields are self-explanatory.

Command Default

NA

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 17.2	This command is introduced.
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	Added **REGION ID** to the output to show the Hierarchical SD-WAN region ID. Added **TENANT ID** to the output to show the tenant ID.
Cisco IOS XE Catalyst SD-WAN Release 17.8.1a	Added **PREFERENCE** and **AFFINITY GROUP NUMBER** to the output to indicate the affinity group preference order and the affinity ID.

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	Added **VERIFY** to the output to verify the OMP routes.
Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	Added Multi-Region Fabric subregion information to the output. For information about subregions, see the Cisco SD-WAN Multi-Region Fabric (also Hierarchical SD-WAN) Configuration Guide.

Examples

In the following sample output, the **Region ID** column indicates either **1** for region 1, or **1.5** for subregion 5 of region 1.

```
Device#show sdwan omp routes

                AFFINITY
                                          PATH                    ATTRIBUTE
                GROUP
TENANT VPN   PREFIX        FROM PEER  ID     LABEL STATUS    TYPE        TLOC IP     COLOR
ENCAP  PREFERENCE  NUMBER    REGION ID   REGION PATH
-------------------------------------------------------------------------------------------
0      1    10.1.1.0/24  0.0.0.0    70     1003  C,Red,R   installed  192.0.5.0   lte
ipsec  -           None       1.5         1
                         0.0.0.0    71     1003  C,Red,R   installed  192.0.5.0   3g
ipsec  -           None       1.5         1
                         0.0.0.0    72     1003  C,Red,R   installed  192.0.5.0   red
ipsec  -           None       1.5         1
0      1    10.1.2.0/24  192.0.2.0  2      1003  C,I,R     installed  192.0.6.0   lte
ipsec  -           None       1.5         1
                         192.0.2.0  4      1003  C,I,R     installed  192.0.6.0   3g
ipsec  -           None       1.5         1
                         192.0.2.0  5      1003  C,I,R     installed  192.0.6.0   red
ipsec  -           None       1.5         1
                         192.0.3.0  1      1003  C,R       installed  192.0.6.0   lte
ipsec  -           None       1.5         1
                         192.0.3.0  3      1003  C,R       installed  192.0.6.0   3g
ipsec  -           None       1.5         1
                         192.0.3.0  6      1003  C,R       installed  192.0.6.0   red
ipsec  -           None       1.5         1
0      1    10.1.3.0/24  192.0.2.0  35     1003  C,I,R     installed  192.0.7.0   lte
ipsec  -           None       1           1
                         192.0.2.0  36     1003  C,I,R     installed  192.0.7.0   3g
ipsec  -           None       1           1
                         192.0.3.0  35     1003  C,R       installed  192.0.7.0   lte
ipsec  -           None       1           1
                         192.0.3.0  36     1003  C,R       installed  192.0.7.0   3g
ipsec  -           None       1           1


Device# show sdwan omp routes

Code:
C -> chosen
I -> installed
Red -> redistributed
Rej -> rejected
L -> looped
R -> resolved
```

```
S -> stale
Ext -> extranet
Inv -> invalid
Stg -> staged
U -> TLOC unresolved
                                                PATH                        ATTRIBUTE
VPN    PREFIX              FROM PEER        ID     LABEL    STATUS    TYPE       TLOC IP
       COLOR            ENCAP  PREFERENCE
--------------------------------------------------------------------------------------------
1      192.0.2.0/24      192.168.1.3      1      1001     C,I,R     installed  192.168.1.152
    biz-internet     ipsec  -
202    192.0.2.1/24      192.168.1.3      2      1002     C,I,R     installed  192.168.1.152
    biz-internet     ipsec  -
202    192.0.2.0/24      0.0.0.0          68     1002     C,Red,R   installed  192.168.1.121
    biz-internet     ipsec  -
```

```
Device# show sdwan omp routes vpn 202 192.0.2.0/24
-------------------------------------------------
omp route entries for vpn 202 route 192.0.2.0/24
-------------------------------------------------
            RECEIVED FROM:
peer            0.0.0.0
path-id         68
label           1002
status          C,Red,R
loss-reason     not set
lost-to-peer    not set
lost-to-path-id not set
    Attributes:
     originator       192.168.1.121
     type             installed
     tloc             192.168.1.121, biz-internet, ipsec
     domain-id        not set
     site-id          121
     overlay-id        1
     preference       not set
     tag              not set
     origin-proto     connected
     origin-metric    0
     as-path          not set
     unknown-attr-len not set
            ADVERTISED TO:
peer    192.168.1.3
advertise-id    68
    Attributes:
     originator       192.168.1.121
     label            1002
     path-id          68
     tloc             192.168.1.121, biz-internet, ipsec
     domain-id        not set
     site-id          121
     overlay-id        1
     preference       not set
     tag              not set
     origin-proto     connected
     origin-metric    0
     as-path          not set
     unknown-attr-len not set
```

```
Device# show sdwan omp routes vpn 202
-------------------------------------------------
omp route entries for vpn 202 route 192.0.2.1/24
-------------------------------------------------
            RECEIVED FROM:
peer            0.0.0.0
```

```
path-id         68
label           1002
status          C,Red,R
loss-reason     not set
lost-to-peer    not set
lost-to-path-id not set
    Attributes:
     originator       192.168.1.121
     type             installed
     tloc             192.168.1.121, biz-internet, ipsec
     ultimate-tloc    not set
     domain-id        not set
     overlay-id        1
     site-id          121
     preference       not set
     tag              not set
     origin-proto     connected
     origin-metric    0
     as-path          not set
     unknown-attr-len not set
            ADVERTISED TO:
peer    192.168.1.3
    Attributes:
     originator       192.168.1.121
     label            1002
     path-id          68
     tloc             192.168.1.121, biz-internet, ipsec
     ultimate-tloc    not set
     domain-id        not set
     site-id          121
     overlay-id        1
     preference       not set
     tag              not set
     origin-proto     connected
     origin-metric    0
     as-path          not set
     unknown-attr-len not set
```

```
Device# show sdwan omp tenant 0 vpn 1 10.20.24.0/24 verify
------------------------------------------------------------------------------
omp route entries for tenant-id 0 vpn 1 route 10.20.24.0/24
------------------------------------------------------------------------------
            RECEIVED FROM:
peer            172.16.255.19
path-id         780
label           1003
status          C,I,R
loss-reason     not set
lost-to-peer    not set
lost-to-path-id not set
    Attributes:
     originator       172.16.255.15
     type             installed
     tloc             172.16.255.15, lte, ipsec
     ultimate-tloc    not set
     domain-id        not set
     overlay-id        1
     site-id          500
     preference       not set
     affinity-group  None
     region-id        None
     region-path      not set
     route-reoriginator      not set
     tag              not set
     origin-proto     connected
```

```
     origin-metric    0
     as-path          not set
     community        not set
     unknown-attr-len not set
     tloc-status      C,I,R
     bfd-status       up
     rib-status       rib-installed
            RECEIVED FROM:
peer            172.16.255.20
path-id         119
label           1003
status          C,R
loss-reason     not set
lost-to-peer    not set
lost-to-path-id not set
    Attributes:
     originator       172.16.255.15
     type             installed
     tloc             172.16.255.15, lte, ipsec
     ultimate-tloc    not set
     domain-id        not set
     overlay-id        1
     site-id          500
     preference       not set
     affinity-group  None
     region-id        None
     region-path      not set
     route-reoriginator      not set
     tag              not set
     origin-proto     connected
     origin-metric    0
     as-path          not set
     community        not set
     unknown-attr-len not set
     tloc-status      C,R
    bfd-status       up
     rib-status       rib-not-installed
```

show sdwan omp l2-routes

To display OMP L2VPN routes on a Cisco Catalyst SD-WAN Controller and Cisco IOS XE Catalyst SD-WAN device, use the command **show sdwan omp l2-routes** in the privileged EXEC mode.

Command Syntax

show sdwan omp l2-routes [**vpn** *vpn-id*] [**vc** *vc-id*]

Syntax Description

vpn *vpn-id*	Displays L2VPN-specific routes. Lists the OMP routes for the specified L2VPN.
vc *vc-id*	Displays Virtual Circuit (VC) ID that is used to identify a particular bridge domain. Specify bridge-domain vc-id value. Range: 1 to 4294967295

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.14.1a	This command is introduced.

Usage Guidelines

These commands are only used on Cisco Catalyst SD-WAN Controllers and Cisco IOS XE Catalyst SD-WAN devices.

Examples

The following shows a sample output of OMP information on Cisco IOS XE Catalyst SD-WAN devices:

```
Device# show sdwan omp l2-routes

Code:
C   -> chosen
I   -> installed
Red -> redistributed
Rej -> rejected
L   -> looped
R   -> resolved
S   -> stale
Ext -> extranet
Inv -> invalid
Stg -> staged
IA  -> On-demand inactive
U   -> TLOC unresolved

                                                REMOTE
                                      ROUTE                   IP                    SITE
                PATH                      SITE
VPN     VC ID         ORIGINATOR        TYPE    MAC ADDRESS       ADDRESS  VPN TYPE     ID
FROM PEER         ID      LABEL     STATUS     ID
-------------------------------------------------------------------------------------------
12      12            172.16.255.15     vpn     0000.0000.0000    ::       p2p         500
0.0.0.0           66      1004      C,Red,R    501

0.0.0.0           69      1004      C,Red,R    501
12      12            172.16.255.27     vpn     0000.0000.0000    ::       p2p         501
172.16.255.19     2       1014      C,I,R      500

172.16.255.20     1       1014      C,R        500
13      13            172.16.255.15     vpn     0000.0000.0000    ::       multipoint  500
0.0.0.0           66      1006      C,Red,R    -

0.0.0.0           69      1006      C,Red,R    -
13      13            172.16.255.27     vpn     0000.0000.0000    ::       multipoint  501
172.16.255.19     2       1016      C,I,R      -

172.16.255.20     1       1016      C,R        -
13      13            172.16.255.32     vpn     0000.0000.0000    ::       multipoint  503
172.16.255.19     1       1007      C,I,R      -
```

```
172.16.255.20    1      1007     C,R       -
15     1           172.16.255.15    vpn    0000.0000.0000   ::       p2p         500
0.0.0.0          66     1020     C,Red,R   501

0.0.0.0          69     1020     C,Red,R   501
15     1           172.16.255.27    vpn    0000.0000.0000   ::       p2p         501
172.16.255.19    2      1020     C,I,R     500

172.16.255.20    1      1020     C,R       500
```

```
Device# show sdwan omp l2-routes vpn 13

Code:
C   -> chosen
I   -> installed
Red -> redistributed
Rej -> rejected
L   -> looped
R   -> resolved
S   -> stale
Ext -> extranet
Inv -> invalid
Stg -> staged
IA  -> On-demand inactive
U   -> TLOC unresolved
                                                                    REMOTE
                                      ROUTE                         IP                    SITE
               PATH                       SITE
VPN    VC ID        ORIGINATOR        TYPE   MAC ADDRESS      ADDRESS  VPN TYPE    ID
FROM PEER        ID     LABEL    STATUS    ID
-------------------------------------------------------------------------------------------
13     13           172.16.255.15    vpn    0000.0000.0000   ::       multipoint  500
0.0.0.0          66     1006     C,Red,R   -

0.0.0.0          69     1006     C,Red,R   -
13     13           172.16.255.27    vpn    0000.0000.0000   ::       multipoint  501
172.16.255.19    2      1016     C,I,R     -

172.16.255.20    1      1016     C,R       -
13     13           172.16.255.32    vpn    0000.0000.0000   ::       multipoint  503
172.16.255.19    1      1007     C,I,R     -

172.16.255.20    1      1007     C,R       -
```

```
Device# show sdwan omp l2-routes vpn 13 vc-id 13

Code:
C   -> chosen
I   -> installed
Red -> redistributed
Rej -> rejected
L   -> looped
R   -> resolved
S   -> stale
Ext -> extranet
Inv -> invalid
Stg -> staged
IA  -> On-demand inactive
U   -> TLOC unresolved
                                                                    REMOTE
                                      ROUTE                         IP                    SITE
               PATH                       SITE
VPN    VC ID        ORIGINATOR        TYPE   MAC ADDRESS      ADDRESS  VPN TYPE    ID
FROM PEER        ID     LABEL    STATUS    ID
-------------------------------------------------------------------------------------------
```

```
13     13           172.16.255.15    vpn    0000.0000.0000   ::       multipoint  500
0.0.0.0          66     1006     C,Red,R   -

0.0.0.0          69     1006     C,Red,R   -
13     13           172.16.255.27    vpn    0000.0000.0000   ::       multipoint  501
172.16.255.19    2      1016     C,I,R     -

172.16.255.20    1      1016     C,R       -
13     13           172.16.255.32    vpn    0000.0000.0000   ::       multipoint  503
172.16.255.19    1      1007     C,I,R     -

172.16.255.20    1      1007     C,R       -

               1      1007     C,R       -
```

The following shows a sample output of OMP information on Cisco Catalyst SD-WAN Controllers:

```
Device# show omp l2-routes | tab

Code:
C   -> chosen
I   -> installed
Red -> redistributed
Rej -> rejected
L   -> looped
R   -> resolved
S   -> stale
Ext -> extranet
Inv -> invalid
Stg -> staged
IA  -> On-demand inactive
U   -> TLOC unresolved


                                                    REMOTE
                                    ROUTE                    IP                    SITE
               PATH                     SITE
VPN    VC ID        ORIGINATOR       TYPE   MAC ADDRESS      ADDRESS  VPN TYPE    ID
FROM PEER        ID     LABEL    STATUS    ID
-------------------------------------------------------------------------------------------
12     12           172.16.255.15    vpn    0000.0000.0000   ::       p2p         500
172.16.255.15    66     1004     C,R       501

172.16.255.15    69     1004     C,R       501

172.16.255.20    1      1004     C,R       501

172.16.255.20    2      1004     C,R       501
12     12           172.16.255.27    vpn    0000.0000.0000   ::       p2p         501
172.16.255.20    1      1014     C,R       500

172.16.255.27    70     1014     C,R       500
13     13           172.16.255.15    vpn    0000.0000.0000   ::       multipoint  500
172.16.255.15    66     1006     C,R       -

172.16.255.15    69     1006     C,R       -

172.16.255.20    1      1006     C,R       -

172.16.255.20    2      1006     C,R       -
13     13           172.16.255.27    vpn    0000.0000.0000   ::       multipoint  501
172.16.255.20    1      1016     C,R       -

172.16.255.27    70     1016     C,R       -
13     13           172.16.255.32    vpn    0000.0000.0000   ::       multipoint  503
```

```
172.16.255.20    1      1007     C,R       -

172.16.255.32    71     1007     C,R       -
14     1            172.16.255.27    vpn    0000.0000.0000   ::       multipoint  501
172.16.255.20    1      1018     C,R       -

172.16.255.27    70     1018     C,R       -
15     1            172.16.255.15    vpn    0000.0000.0000   ::       p2p         500
172.16.255.15    66     1020     C,R       501

172.16.255.15    69     1020     C,R       501

172.16.255.20    1      1020     C,R       501

172.16.255.20    2      1020     C,R       501
15     1            172.16.255.27    vpn    0000.0000.0000   ::       p2p         501
172.16.255.20    1      1020     C,R       500

172.16.255.27    70     1020     C,R       500
```

```
Device# show omp l2-routes vpn 13 | tab

Code:
C   -> chosen
I   -> installed
Red -> redistributed
Rej -> rejected
L   -> looped
R   -> resolved
S   -> stale
Ext -> extranet
Inv -> invalid
Stg -> staged
IA  -> On-demand inactive
U   -> TLOC unresolved

                                                    REMOTE
                                    ROUTE                    IP                    SITE
               PATH                     SITE
VPN    VC ID        ORIGINATOR       TYPE   MAC ADDRESS      ADDRESS  VPN TYPE    ID
FROM PEER        ID     LABEL    STATUS    ID
-------------------------------------------------------------------------------------------
12     12           172.16.255.15    vpn    0000.0000.0000   ::       p2p         500
172.16.255.15    66     1004     C,R       501

172.16.255.15    69     1004     C,R       501

172.16.255.20    1      1004     C,R       501

172.16.255.20    2      1004     C,R       501
12     12           172.16.255.27    vpn    0000.0000.0000   ::       p2p         501
172.16.255.20    1      1014     C,R       500

172.16.255.27    70     1014     C,R       500
13     13           172.16.255.15    vpn    0000.0000.0000   ::       multipoint  500
172.16.255.15    66     1006     C,R       -

172.16.255.15    69     1006     C,R       -

172.16.255.20    1      1006     C,R       -
```

```
172.16.255.20    2      1006     C,R       -
13     13           172.16.255.27    vpn    0000.0000.0000   ::       multipoint  501
172.16.255.20    1      1016     C,R       -

172.16.255.27    70     1016     C,R       -
13     13           172.16.255.32    vpn    0000.0000.0000   ::       multipoint  503
172.16.255.20    1      1007     C,R       -

172.16.255.32    71     1007     C,R       -
14     1            172.16.255.27    vpn    0000.0000.0000   ::       multipoint  501
172.16.255.20    1      1018     C,R       -

172.16.255.27    70     1018     C,R       -
15     1            172.16.255.15    vpn    0000.0000.0000   ::       p2p         500
172.16.255.15    66     1020     C,R       501

172.16.255.15    69     1020     C,R       501

172.16.255.20    1      1020     C,R       501

172.16.255.20    2      1020     C,R       501
15     1            172.16.255.27    vpn    0000.0000.0000   ::       p2p         501
172.16.255.20    1      1020     C,R       500

172.16.255.27    70     1020     C,R       500
```

```
Device# show omp l2-routes vpn 13 vc-id 13 | tab

Code:
C   -> chosen
I   -> installed
Red -> redistributed
Rej -> rejected
L   -> looped
R   -> resolved
S   -> stale
Ext -> extranet
Inv -> invalid
Stg -> staged
IA  -> On-demand inactive
U   -> TLOC unresolved

                                                                REMOTE
                                      ROUTE                      IP                    SITE
                PATH                      SITE
VPN    VC ID        ORIGINATOR        TYPE   MAC ADDRESS       ADDRESS  VPN TYPE     ID
FROM PEER        ID     LABEL     STATUS    ID
-------------------------------------------------------------------------------------------
13     13           172.16.255.15    vpn    0000.0000.0000   ::       multipoint  500
172.16.255.15    66     1006     C,R       -

172.16.255.15    69     1006     C,R       -

172.16.255.20    1      1006     C,R       -

172.16.255.20    2      1006     C,R       -
13     13           172.16.255.27    vpn    0000.0000.0000   ::       multipoint  501
172.16.255.20    1      1016     C,R       -

172.16.255.27    70     1016     C,R       -
13     13           172.16.255.32    vpn    0000.0000.0000   ::       multipoint  503
172.16.255.20    1      1007     C,R       -

172.16.255.32    71     1007     C,R       -
```

show sdwan omp services

show sdwan omp services—Display the services learned from OMP peering sessions (on vSmart controllers and Cisco IOS XE Catalyst SD-WAN devices only).

Command Syntax

show sdwan omp services [**detail**]

Syntax Description

	None: List information about the services learned from OMP peering sessions.
detail	Detailed Information: Display detailed information.

Output Fields

The output fields are self-explanatory.

Command History

Release	Modification
16.12.1	Command introduced.

Usage Guidelines

The OMP services are not supported on IPv6 routes.

Example

```
vSmart# show sdwan omp services (command issued from a vSmart controller)
C   -> chosen
I   -> installed
Red -> redistributed
Rej -> rejected
L   -> looped
R   -> resolved
S   -> stale
Ext -> extranet
Inv -> invalid
                                                PATH
VPN  SERVICE  ORIGINATOR     FROM PEER      ID    LABEL  STATUS
-----------------------------------------------------------------
1    VPN      172.16.255.11  172.16.255.11  3     32772  C,I,R
                             172.16.255.20  4     32772  R
1    VPN      172.16.255.14  172.16.255.14  3     18978  C,I,R
                             172.16.255.20  2     18978  R
1    VPN      172.16.255.15  172.16.255.15  3     19283  C,I,R
```

```
                                172.16.255.20  1     19283  R
1    VPN      172.16.255.16     172.16.255.16  3     3272   C,I,R
                                172.16.255.20  3     3272   R
1    VPN      172.16.255.21     172.16.255.20  5     53645  R
                                172.16.255.21  3     53645  C,I,R
```

show sdwan omp summary

Use the **show sdwan omp summary** to display information about the OMP sessions running between Cisco SD-WAN Controllers and Cisco IOS XE Catalyst SD-WAN devices (on Cisco SD-WAN Controllers and Cisco IOS XE Catalyst SD-WAN devices only).

Command Syntax

show sdwan omp summary [*parameter-name*]

Syntax Description

	None: List information about the OMP peering sessions running on the local device
parameter-name	Information about a Specific Parameter: Display configuration information about a specific OMP peering session parameter. *parameter-name* can be one of the following: **adminstate**, **devicetype**, **ompdowntime**, **ompuptime**, **operstate**, **peers**, **routes-installed**, **routes-received**, **routes-sent**, **services-installed**, **services-sent**, **tlocs-installed**, **tlocs-received**, **tlocs-sent**, and **vsmart-peers**. For an explanation of these parameters, see the Output Fields below.

Output Fields

Field	Explanation
admin-state	Administrative state of the OMP session. It can be UP or DOWN.
omp-uptime	How long the OMP session has been up and operational.
oper-state	Operational status of the OMP session. It can be UP or DOWN.
personality	Cisco IOS XE Catalyst SD-WAN device personality.
region-id	Region ID, for the Multi-Region Fabric feature.
routes-installed	Number of routes installed over the OMP session.
routes-received	Number of routes received over the OMP session.
routes-sent	Number of routes sent over the OMP session.

Field	Explanation
services-installed	Number of services installed that were learned over OMP sessions.
services-received	Number of services received over OMP sessions.
services-sent	Number of services advertised over OMP sessions.
sub-region-id	Subregion ID, for the Multi-Region Fabric feature.
tlocs-installed	Number of TLOCs installed that were learned over OMP sessions.
tlocs-received	Number of TLOCs received over OMP sessions.
tlocs-sent	Number of TLOCs advertised over OMP sessions.
transport-gateway	Indicates the enabled/disabled status of the transport gateway feature.
vsmart-peers	Number of vSmart peers that are up.

Command History

Release	Modification
16.12.1	Command introduced.
Cisco IOS XE Catalyst SD-WAN Release 17.8.1a	Added **transport-gateway** to the output to indicate the enabled/disabled status.
Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	Added Multi-Region Fabric subregion information to the output. For information about subregions, see the Cisco SD-WAN Multi-Region Fabric (also Hierarchical SD-WAN) Configuration Guide.

Example

The following sample output includes the **region-id** and **sub-region-id** of a device. These fields are relevant for a device operating in a network using Multi-Region Fabric.

```
Device#show sdwan omp summary
oper-state              UP
admin-state             UP
personality             vedge
device-role             Edge-Router
omp-uptime              0:00:56:17
routes-received         194
routes-installed        58
routes-sent             12
tlocs-received          25
tlocs-installed         11
tlocs-sent              6
services-received       3
```

```
services-installed     0
services-sent          6
mcast-routes-received  0
mcast-routes-installed 0
mcast-routes-sent      0
hello-sent             1351
hello-received         1344
handshake-sent         2
handshake-received     2
alert-sent             0
alert-received         0
inform-sent            26
inform-received        26
update-sent            30
update-received        254
policy-sent            0
policy-received        0
total-packets-sent     1409
total-packets-received 1628
vsmart-peers           2
region-id              1
sub-region-id          5
secondary-region-id    None


Device# show sdwan omp summary
oper-state             UP
admin-state            UP
personality            vedge
omp-uptime             0:19:05:45
routes-received        16
routes-installed       8
routes-sent            0
tlocs-received         7
tlocs-installed        3
tlocs-sent             2
services-received      1
services-installed     0
services-sent          2
mcast-routes-received  0
mcast-routes-installed 0
mcast-routes-sent      0
hello-sent             27471
hello-received         27460
hsndshake-sent         6
handshake-received     6
alert-sent             2
alert-received         2
inform-sent            8
inform-received        8
update-sent            48
update-received        213
policy-sent            0
policy-received        0
total-packets-sent     27535
total-packets-received 27689
vsmart-peers           2

vSmart# show sdwan omp summary
oper-state             UP
admin-state            UP
personality            vsmart
omp-uptime             0:19:07:20
routes-received        18
```

```
routes-installed       0
routes-sent            32
tlocs-received         8
tlocs-installed        4
tlocs-sent             16
services-received      8
services-installed     4
services-sent          4
mcast-routes-received  0
mcast-routes-installed 0
mcast-routes-sent      0
hello-sent             80765
hello-received         80782
hsndshake-sent         13
handshake-received     13
alert-sent             4
alert-received         4
inform-sent            24
inform-received        24
update-sent            633
update-received        278
policy-sent            0
policy-received        0
total-packets-sent     81439
total-packets-received 81101
vsmart-peers           1
vedge-peers            4
```

show sdwan omp tlocs

Use the **show sdwan omp tlocs** to display information learned from the TLOC routes advertised over the OMP sessions running between Cisco SD-WAN Controllers and Cisco IOS XE Catalyst SD-WAN devices (on Cisco SD-WAN Controllers and Cisco IOS XE Catalyst SD-WAN devices only).

Command Syntax

show sdwan omp tlocs [**detail**]

Syntax Description

	None: List information about all TLOCs that the local device has learned about.
detail	Detailed Information: Show detailed information.

Output Fields

The output fields are self-explanatory.

Command History

Release	Modification
16.12	Command introduced.
Cisco IOS XE Catalyst SD-WAN Release 17.10.1a	Added Multi-Region Fabric subregion information to the output. For information about subregions, see the Cisco SD-WAN Multi-Region Fabric (also Hierarchical SD-WAN) Configuration Guide.

Example

In the following sample output, the **Region ID** column indicates either **1** for region 1, or **1.5** for subregion 5 of region 1.

```
Device#show sdwan omp tlocs table

                                        PUBLIC            PRIVATE                          AFFINITY
ADDRESS                                 TENANT                                PSEUDO                    PUBLIC
                        PRIVATE  PUBLIC IPV6    PRIVATE  IPV6     BFD                     GROUP
FAMILY   TLOC IP        COLOR    ENCAP  ID      FROM PEER        STATUS   KEY     PUBLIC IP         PORT
   PRIVATE IP           PORT     IPV6   PORT    IPV6     PORT    STATUS  REGION ID  NUMBER
-------------------------------------------------------------------------------------------------------
ipv4     175.1.11.10  lte    ipsec  0       175.0.122.10     C,I,R    1       172.1.11.11      12366
   172.1.11.11       12366  ::     0       ::       0       up       1.5       None
                                    0       175.0.123.10     C,R      1       172.1.11.11      12366
   172.1.11.11       12366  ::     0       ::       0       up       1.5       None
         175.1.11.10  3g     ipsec  0       175.0.122.10     C,I,R    1       173.1.11.11      12366
   173.1.11.11       12366  ::     0       ::       0       up       1.5       None
                                    0       175.0.123.10     C,R      1       173.1.11.11      12366
   173.1.11.11       12366  ::     0       ::       0       up       1.5       None
         175.1.11.10  red    ipsec  0       175.0.122.10     C,I,R    1       172.1.12.11      5062
   173.174.11.1      12366  ::     0       ::       0       up       1.5       None
                                    0       175.0.123.10     C,R      1       172.1.12.11      5062
   173.174.11.1      12366  ::     0       ::       0       up       1.5       None
         175.1.12.10  lte    ipsec  0       175.0.122.10     C,I,R    1       172.1.12.11      12366
   172.1.12.11       12366  ::     0       ::       0       up       1         None
                                    0       175.0.123.10     C,R      1       172.1.12.11      12366
   172.1.12.11       12366  ::     0       ::       0       up       1         None
         175.1.12.10  3g     ipsec  0       175.0.122.10     C,I,R    1       173.1.12.11      12366
   173.1.12.11       12366  ::     0       ::       0       up       1         None
                                    0       175.0.123.10     C,R      1       173.1.12.11      12366
   173.1.12.11       12366  ::     0       ::       0       up       1         None
         175.1.12.10  red    ipsec  0       175.0.122.10     C,I,R    1       172.1.11.11      5062
   173.174.12.1      12366  ::     0       ::       0       up       1         None
                                    0       175.0.123.10     C,R      1       172.1.11.11      5062
   173.174.12.1      12366  ::     0       ::       0       up       1         None
         175.1.51.10  lte    ipsec  0       0.0.0.0          C,Red,R  1       172.1.1.11       12366
   172.1.1.11        12366  ::     0       ::       0       up       1.5       None
         175.1.51.10  3g     ipsec  0       0.0.0.0          C,Red,R  1       173.1.1.11       12366
   173.1.1.11        12366  ::     0       ::       0       up       1.5       None
         175.1.51.10  red    ipsec  0       0.0.0.0          C,Red,R  1       172.1.2.11       5062
   173.174.1.1       12366  ::     0       ::       0       up       1.5       None
         175.1.52.10  lte    ipsec  0       175.0.122.10     C,I,R    1       172.1.2.11       12366
   172.1.2.11        12366  ::     0       ::       0       up       1.5       None
                                    0       175.0.123.10     C,R      1       172.1.2.11       12366
   172.1.2.11        12366  ::     0       ::       0       up       1.5       None
```

```
Device# show sdwan omp tlocs
Code:
C   -> chosen
I   -> installed
Red -> redistributed
Rej -> rejected
L   -> looped
R   -> resolved
```

```
S   -> stale
Ext -> extranet
Inv -> invalid

          PUBLIC           PRIVATE                                                                  PSEUDO                  PUBLIC                  PRIVATE
  PUBLIC  IPV6    PRIVATE  IPV6     BFD
TLOC IP           COLOR            ENCAP  FROM PEER        STATUS    KEY     PUBLIC IP        PORT    PRIVATE IP       PORT
  IPV6    PORT    IPV6     PORT      STATUS
-------------------------------------------------------------------------------------------------------------------------------------------------
172.16.254.1      lte              ipsec  172.16.254.1     C,I,R     1       10.102.2.2       12366   10.102.2.2       12366
  ::      0       ::       0        -
                                          172.16.255.132   C,R       1       10.102.2.2       12366   10.102.2.2       12366
  ::      0       ::       0        -
172.16.254.1      3g               ipsec  172.16.254.1     C,I,R     1       10.101.2.2       12366   10.101.2.2       12366
  ::      0       ::       0        -
                                          172.16.255.132   C,R       1       10.101.2.2       12366   10.101.2.2       12366
  ::      0       ::       0        -
172.16.254.2      lte              ipsec  172.16.254.2     C,I,R     1       10.102.3.3       12366   10.102.3.3       12366
  ::      0       ::       0        -
                                          172.16.255.132   C,R       1       10.102.3.3       12366   10.102.3.3       12366
  ::      0       ::       0        -
172.16.254.2      3g               ipsec  172.16.254.2     C,I,R     1       10.101.3.3       12366   10.101.3.3       12366
  ::      0       ::       0        -
                                          172.16.255.132   C,R       1       10.101.3.3       12366   10.101.3.3       12366
  ::      0       ::       0        -
172.16.254.3      lte              ipsec  172.16.254.3     C,I,R     1       10.102.4.4       12366   10.102.4.4       12366
  ::      0       ::       0        -
                                          172.16.255.132   C,R       1       10.102.4.4       12366   10.102.4.4       12366
  ::      0       ::       0        -
172.16.254.3      3g               ipsec  172.16.254.3     C,I,R     1       10.101.4.4       12366   10.101.4.4       12366
  ::      0       ::       0        -
                                          172.16.255.132   C,R       1       10.101.4.4       12366   10.101.4.4       12366
  ::      0       ::       0        -
172.16.254.4      lte              ipsec  172.16.254.4     C,I,R     1       10.102.5.5       12366   10.102.5.5       12366
  ::      0       ::       0        -
                                          172.16.255.132   C,R       1       10.102.5.5       12366   10.102.5.5       12366
  ::      0       ::       0        -
172.16.254.4      3g               ipsec  172.16.254.4     C,I,R     1       10.101.5.5       12366   10.101.5.5       12366
  ::      0       ::       0        -
                                          172.16.255.132   C,R       1       10.101.5.5       12366   10.101.5.5       12366
  ::      0       ::       0        -
172.16.254.5      lte              ipsec  172.16.254.5     C,I,R     1       10.102.6.6       12366   10.102.6.6       12366
  ::      0       ::       0        -
                                          172.16.255.132   C,R       1       10.102.6.6       12366   10.102.6.6       12366
  ::      0       ::       0        -
172.16.254.5      3g               ipsec  172.16.254.5     C,I,R     1       10.101.6.6       12366   10.101.6.6       12366
  ::      0       ::       0        -
                                          172.16.255.132   C,R       1       10.101.6.6       12366   10.101.6.6       12366
  ::      0       ::       0        -

vEdge# show sdwan omp tlocs advertised
Code:
C   -> chosen
I   -> installed
Red -> redistributed
Rej -> rejected
L   -> looped
R   -> resolved
S   -> stale
Ext -> extranet
Inv -> invalid

          PUBLIC           PRIVATE                                                                  PSEUDO                  PUBLIC                  PRIVATE
  PUBLIC  IPV6    PRIVATE  IPV6     BFD
TLOC IP           COLOR            ENCAP  FROM PEER        STATUS    KEY     PUBLIC IP        PORT    PRIVATE IP       PORT
  IPV6    PORT    IPV6     PORT      STATUS
-------------------------------------------------------------------------------------------------------------------------------------------------
172.16.254.1      lte              ipsec  172.16.254.1     C,I,R     1       10.102.2.2       12366   10.102.2.2       12366
  ::      0       ::       0        -
                                          172.16.255.132   C,R       1       10.102.2.2       12366   10.102.2.2       12366
  ::      0       ::       0        -
```

```
172.16.254.1     3g              ipsec  172.16.254.1     C,I,R     1       10.101.2.2       12366   10.101.2.2       12366
  ::      0       ::       0        -
                                        172.16.255.132   C,R       1       10.101.2.2       12366   10.101.2.2       12366
  ::      0       ::       0        -
172.16.254.2     lte             ipsec  172.16.254.2     C,I,R     1       10.102.3.3       12366   10.102.3.3       12366
  ::      0       ::       0        -
                                        172.16.255.132   C,R       1       10.102.3.3       12366   10.102.3.3       12366
  ::      0       ::       0        -
172.16.254.2     3g              ipsec  172.16.254.2     C,I,R     1       10.101.3.3       12366   10.101.3.3       12366
  ::      0       ::       0        -
                                        172.16.255.132   C,R       1       10.101.3.3       12366   10.101.3.3       12366
  ::      0       ::       0        -
172.16.254.3     lte             ipsec  172.16.254.3     C,I,R     1       10.102.4.4       12366   10.102.4.4       12366
  ::      0       ::       0        -
                                        172.16.255.132   C,R       1       10.102.4.4       12366   10.102.4.4       12366
  ::      0       ::       0        -
172.16.254.3     3g              ipsec  172.16.254.3     C,I,R     1       10.101.4.4       12366   10.101.4.4       12366
  ::      0       ::       0        -
                                        172.16.255.132   C,R       1       10.101.4.4       12366   10.101.4.4       12366
  ::      0       ::       0        -
172.16.254.4     lte             ipsec  172.16.254.4     C,I,R     1       10.102.5.5       12366   10.102.5.5       12366
  ::      0       ::       0        -
                                        172.16.255.132   C,R       1       10.102.5.5       12366   10.102.5.5       12366
  ::      0       ::       0        -
172.16.254.4     3g              ipsec  172.16.254.4     C,I,R     1       10.101.5.5       12366   10.101.5.5       12366
  ::      0       ::       0        -
                                        172.16.255.132   C,R       1       10.101.5.5       12366   10.101.5.5       12366
  ::      0       ::       0        -
172.16.254.5     lte             ipsec  172.16.254.5     C,I,R     1       10.102.6.6       12366   10.102.6.6       12366
  ::      0       ::       0        -
                                        172.16.255.132   C,R       1       10.102.6.6       12366   10.102.6.6       12366
  ::      0       ::       0        -
172.16.254.5     3g              ipsec  172.16.254.5     C,I,R     1       10.101.6.6       12366   10.101.6.6       12366
  ::      0       ::       0        -
                                        172.16.255.132   C,R       1       10.101.6.6       12366   10.101.6.6       12366
  ::      0       ::       0        -
```

```
vEdge# show sdwan omp tlocs received
Code:
C   -> chosen
I   -> installed
Red -> redistributed
Rej -> rejected
L   -> looped
R   -> resolved
S   -> stale
Ext -> extranet
Inv -> invalid
```

```
          PUBLIC           PRIVATE                                                                PSEUDO                  PUBLIC                  PRIVATE
  PUBLIC  IPV6    PRIVATE  IPV6     BFD
TLOC IP           COLOR            ENCAP  FROM PEER        STATUS    KEY     PUBLIC IP        PORT    PRIVATE IP       PORT
  IPV6    PORT    IPV6     PORT     STATUS
--------------------------------------------------------------------------------------------------------------------------------------
172.16.254.1     lte             ipsec  172.16.254.1     C,I,R     1       10.102.2.2       12366   10.102.2.2       12366
  ::      0       ::       0        -
                                        172.16.255.132   C,R       1       10.102.2.2       12366   10.102.2.2       12366
  ::      0       ::       0        -
172.16.254.1     3g              ipsec  172.16.254.1     C,I,R     1       10.101.2.2       12366   10.101.2.2       12366
  ::      0       ::       0        -
                                        172.16.255.132   C,R       1       10.101.2.2       12366   10.101.2.2       12366
  ::      0       ::       0        -
172.16.254.2     lte             ipsec  172.16.254.2     C,I,R     1       10.102.3.3       12366   10.102.3.3       12366
  ::      0       ::       0        -
                                        172.16.255.132   C,R       1       10.102.3.3       12366   10.102.3.3       12366
  ::      0       ::       0        -
172.16.254.2     3g              ipsec  172.16.254.2     C,I,R     1       10.101.3.3       12366   10.101.3.3       12366
  ::      0       ::       0        -
                                        172.16.255.132   C,R       1       10.101.3.3       12366   10.101.3.3       12366
  ::      0       ::       0        -
172.16.254.3     lte             ipsec  172.16.254.3     C,I,R     1       10.102.4.4       12366   10.102.4.4       12366
  ::      0       ::       0        -
```

```
                                          172.16.255.132   C,R       1       10.102.4.4       12366   10.102.4.4       12366
  ::      0       ::       0        -
172.16.254.3     3g               ipsec  172.16.254.3     C,I,R     1       10.101.4.4       12366   10.101.4.4       12366
  ::      0       ::       0        -
                                          172.16.255.132   C,R       1       10.101.4.4       12366   10.101.4.4       12366
  ::      0       ::       0        -
172.16.254.4     lte              ipsec  172.16.254.4     C,I,R     1       10.102.5.5       12366   10.102.5.5       12366
  ::      0       ::       0        -
                                          172.16.255.132   C,R       1       10.102.5.5       12366   10.102.5.5       12366
  ::      0       ::       0        -
172.16.254.4     3g               ipsec  172.16.254.4     C,I,R     1       10.101.5.5       12366   10.101.5.5       12366
  ::      0       ::       0        -
                                          172.16.255.132   C,R       1       10.101.5.5       12366   10.101.5.5       12366
  ::      0       ::       0        -
172.16.254.5     lte              ipsec  172.16.254.5     C,I,R     1       10.102.6.6       12366   10.102.6.6       12366
  ::      0       ::       0        -
                                          172.16.255.132   C,R       1       10.102.6.6       12366   10.102.6.6       12366
  ::      0       ::       0        -
172.16.254.5     3g               ipsec  172.16.254.5     C,I,R     1       10.101.6.6       12366   10.101.6.6       12366
  ::      0       ::       0        -
                                          172.16.255.132   C,R       1       10.101.6.6       12366   10.101.6.6       12366
  ::      0       ::       0        -
vEdge# show sdwan omp tlocs detail

----------------------------------------------------
tloc entries for 172.16.254.1
                 lte
                 ipsec
----------------------------------------------------
            RECEIVED FROM:
peer            172.16.254.1
status          C,I,R
loss-reason     not set
lost-to-peer    not set
lost-to-path-id not set
    Attributes:
     attribute-type    installed
     encap-key         not set
     encap-proto       0
     encap-spi         376
     encap-auth        sha1-hmac,ah-sha1-hmac
     encap-encrypt     aes256
     public-ip         10.102.2.2
     public-port       12366
     private-ip        10.102.2.2
     private-port      12366
     public-ip         ::
     public-port       0
     private-ip        ::
     private-port      0
     domain-id         not set
     site-id           2
     overlay-id        not set
     preference        0
     tag               not set
     stale             not set
     weight            1
     version           2
    gen-id             0x80000000
     carrier           default
     restrict          0
     groups            [ 0 ]
     border             not set
     unknown-attr-len  not set
            RECEIVED FROM:
peer            172.16.255.132
status          C,R
loss-reason     not set
lost-to-peer    not set
lost-to-path-id not set
    Attributes:
     attribute-type    installed
     encap-key         not set
```

```
     encap-proto       0
     encap-spi         376
     encap-auth        sha1-hmac,ah-sha1-hmac
     encap-encrypt     aes256
     public-ip         10.102.2.2
     public-port       12366
     private-ip        10.102.2.2
     private-port      12366
     public-ip         ::
     public-port       0
     private-ip        ::
     private-port      0
     domain-id         not set
     site-id           2
     overlay-id        not set
     preference        0
     tag               not set
     stale             not set
     weight            1
     version           2
    gen-id             0x80000000
     carrier           default
     restrict          0
     groups            [ 0 ]
     border             not set
     unknown-attr-len  not set
           ADVERTISED TO:
peer    172.16.254.2
    Attributes:
     encap-key         not set
     encap-proto       0
     encap-spi         376
     encap-auth        sha1-hmac,ah-sha1-hmac
     encap-encrypt     des,des3
     public-ip         10.102.2.2
     public-port       12366
     private-ip        10.102.2.2
     private-port      12366
     public-ip       ::
     public-port     0
     private-ip      ::
     private-port     0
     domain-id         not set
     site-id           2
     overlay-id        not set
     preference        0
     tag               not set
     stale             not set
     weight            1
     version           2
     gen-id            0x80000000
     carrier           default
     restrict          0
     groups            [ 0 ]
     border              not set
     unknown-attr-len  not set
           ADVERTISED TO:
peer    172.16.254.3
    Attributes:
     encap-key         not set
     encap-proto       0
     encap-spi         376
     encap-auth        sha1-hmac,ah-sha1-hmac
     encap-encrypt     des,des3
     public-ip         10.102.2.2
     public-port       12366
     private-ip        10.102.2.2
     private-port      12366
     public-ip       ::
     public-port     0
     private-ip      ::
     private-port     0
     domain-id         not set
```

```
     site-id           2
     overlay-id        not set
     preference        0
     tag               not set
     stale             not set
     weight            1
     version           2
     gen-id            0x80000000
     carrier           default
     restrict          0
     groups            [ 0 ]
     border              not set
     unknown-attr-len  not set
           ADVERTISED TO:
peer    172.16.254.4
    Attributes:
     encap-key         not set
     encap-proto       0
     encap-spi         376
     encap-auth        sha1-hmac,ah-sha1-hmac
     encap-encrypt     des,des3
     public-ip         10.102.2.2
     public-port       12366
     private-ip        10.102.2.2
     private-port      12366
     public-ip       ::
     public-port     0
     private-ip      ::
     private-port     0
     domain-id         not set
     site-id           2
     overlay-id        not set
     preference        0
     tag               not set
     stale             not set
     weight            1
     version           2
     gen-id            0x80000000
     carrier           default
     restrict          0
     groups            [ 0 ]
     border              not set
     unknown-attr-len  not set
           ADVERTISED TO:
peer    172.16.254.5
    Attributes:
     encap-key         not set
     encap-proto       0
     encap-spi         376
     encap-auth        sha1-hmac,ah-sha1-hmac
     encap-encrypt     des,des3
     public-ip         10.102.2.2
     public-port       12366
     private-ip        10.102.2.2
     private-port      12366
     public-ip       ::
     public-port     0
     private-ip      ::
     private-port     0
     domain-id         not set
     site-id           2
     overlay-id        not set
     preference        0
     tag               not set
     stale             not set
     weight            1
     version           2
     gen-id            0x80000000
     carrier           default
     restrict          0
     groups            [ 0 ]
     border              not set
     unknown-attr-len  not set
```

```
            ADVERTISED TO:
peer    172.16.255.132
    Attributes:
     encap-key          not set
     encap-proto        0
     encap-spi          376
     encap-auth         sha1-hmac,ah-sha1-hmac
     encap-encrypt      des,des3
     public-ip          10.102.2.2
     public-port        12366
     private-ip         10.102.2.2
     private-port       12366
     public-ip         ::
     public-port      0
     private-ip       ::
     private-port      0
     domain-id          not set
     site-id            2
     overlay-id         not set
     preference         0
     tag                not set
     stale              not set
     weight             1
     version            2
     gen-id             0x80000000
     carrier            default
     restrict           0
     groups             [ 0 ]
     border               not set
     unknown-attr-len   not set
...
```

show sdwan policy access-list-associations

Display the IPv4 access lists that are operating on each interface.

show sdwan policy access-list-associations [*access-list-name*]

Syntax Description

None	Display all access lists operating on the router's interfaces.
Specific Access List	*access-list-name* Display the interfaces on which the specific access list is operating.

Examples

Show sdwan policy access-list-associations

```
Device# show running-config policy
policy
 access-list ALLOW_OSPF_PACKETS
  sequence 65535
   match
    protocol 89
   !
   action accept
    count count_OSPF_PACKETS
   !
  !
  default-action accept
```

```
 !
!

Device# show policy access-list-associations

                    INTERFACE  INTERFACE
NAME                NAME       DIRECTION
-----------------------------------------
ALLOW_OSPF_PACKETS  ge0/0      in
```

show sdwan policy access-list-counters

Display the IPv4 access lists that are operating on each interface.

show sdwan policy access-list-counters [*access-list-name*]

Syntax Description

None	Display all access lists operating on the router's interfaces.
Specific Access List	*access-list-name* Display the interfaces on which the specific access list is operating.

Examples

Show sdwan policy access-list-counters

```
Device# show running-config policy
policy
 access-list ALLOW_OSPF_PACKETS
  sequence 65535
   match
    protocol 89
   !
   action accept
    count count_OSPF_PACKETS
   !
  !
  default-action accept
 !
!

Device# show policy access-list-associations

                    INTERFACE  INTERFACE
NAME                NAME       DIRECTION
-----------------------------------------
ALLOW_OSPF_PACKETS  ge0/0      in
```

show sdwan policy data-policy-filter

show sdwan policy access-list-names

Display the names of the IPv4 access lists configured on the devices.

show sdwan policy access-list-names

Syntax Description

Syntax Description None

Examples

Show sdwan policy access-list-names

```
Device# show running-config policy
policy
 access-list ALLOW_OSPF_PACKETS
  sequence 65535
   match
    protocol 89
   !
   action accept
    count count_OSPF_PACKETS
   !
  !
  default-action accept
 !
!
Device# show policy access-list-names

NAME
--------------------
ALLOW_OSPF_PACKETS
```

show sdwan policy access-list-policers

Display information about the policers configured in IPv4 access lists.

show sdwan policy access-list-policers

Syntax Description

None

Example

Display a list of policers configured in access lists. This output shows that the policer named "p1_police" was applied in sequence 10 in the access list "acl_p1" in sequences 10, 20, and 30 in the "acl_plp" access list.

```
Device# show sdwan policy access-list-policers
                                    OOS
NAME                POLICER NAME    PACKETS
-------------------------------------------
acl_p1              10.p1_police    0
acl_plp             10.p1_police    0
                    20.p1_police    0
                    30.p2_police    0
```

show sdwan policy app-route-policy-filter

To display information about application-aware routing policy matched packet counts on Cisco IOS XE SD-WAN devices, use the **show sdwan policy app-route-policy-filter** command in privileged EXEC mode.

show sdwan policy app-route-policy-filter [*policy-name*]

Syntax Description

policy-name	(Optional) Displays information about the application-aware routing policy matched packet counts for the specified policy.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

Application-aware routing tracks network and path characteristics of the data plane tunnels between Cisco IOS XE SD-WAN devices, and uses the collected information to compute optimal paths for data traffic.

An application-aware routing policy matches applications with an SLA, that is, with the data plane tunnel performance characteristics that are necessary to transmit the applications' data traffic. When a data packet matches one of the match conditions, an SLA action is applied to the packet to determine the data plane tunnel to transmit the packet.

This command can be used to display information about application-aware routing policy matched packet counts on Cisco IOS XE SD-WAN devices.

Example

The following example shows how to display information about application-aware routing policy matched packet counts on Cisco IOS XE SD-WAN devices.

```
Device# show sdwan policy app-route-policy-filter
NAME               NAME     COUNTER NAME          PACKETS       BYTES
-------------------------------------------------------------------------
_ALLVPNs_Test-AAR  ALLVPNs  default_action_count  12            2936
```

The following example shows how to display information about application-aware routing policy matched packet counts for the specified policy on Cisco IOS XE SD-WAN devices.

```
Device# show sdwan policy app-route-policy-filter _ALLVPNs_Test-AAR
NAME               NAME     COUNTER NAME          PACKETS       BYTES
-------------------------------------------------------------------------
_ALLVPNs_Test-AAR  ALLVPNs  default_action_count  12            2936
```

Related Commands

Command	Description
show sdwan ipsec inbound-connections	Displays SD-WAN policy access-list-associations.
show sdwan ipsec inbound-connections	Displays SD-WAN policy access-list-counters.
show sdwan ipsec inbound-connections	Displays SD-WAN policy access-list-names.
show sdwan ipsec inbound-connections	Displays SD-WAN policy access-list-policers.
show sdwan ipsec inbound-connections	Displays SD-WAN policy data-policy-filter.
show sdwan policy from-vsmart	Displays SD-WAN policy from Cisco Catalyst SD-WAN Controller.
show sdwan policy ipv6	Displays SD-WAN policy IPv6.
show sdwan policy rewrite-associations	Displays SD-WAN policy rewrite-associations.
show sdwan policy service-path	Displays next-hop information for packet coming from service side.
show sdwan policy tunnel-path	Displays next-hop information for packet coming over the WAN tunnel.

show sdwan policy data-policy-filter

Display information about data policy filters for configured counters.

show sdwan policy data-policy-filter

Syntax Description

None

Examples

Example 1

Display the number of packets and bytes for four configured data policy counters:

```
vSmart# show running-config policy data-policy
policy
 data-policy Local-City-Branch
   vpn-list-Guest-VPN
    sequence 10
      action accetp
        count Guest-Wifi-Traffic
        cflod
      !
    !
    default-action accept
  !
  vpn-list Service-VPN
    sequence 10
      match
```

```
        destination-data-prefix-list Business-Prefixes
        destination-port 80
      !
      action accept
        count Business-Traffic
        cflowd
      !
    !
    sequence 20
      match
        destination-port 10090
        protocol 6
      !
      action accept
        count Other-Branch-Traffic
        cflowd
      !
    !
    sequence 30
      action accept
        count Misc-Traffic
        cflowd
      !
    !
    default-action accept
  !
!
```

```
vEdge# show policy data-policy-filter
                                                                                    POLICER    OOS      OOS
NAME                    NAME         COUNTER NAME          PACKETS     BYTES        NAME       PACKETS  BYTES
-------------------------------------------------------------------------------------------------------------
Local-City-Branch       Guest-VPN    Guest-Wifi-Traffic    18066728    12422330320
                        Service-VPN  Business-Traffic      92436       7082643
                                     Other-Branch-Traffic  1663339139  163093277861
                                     Misc-Traffic          32079661    5118593007
```

Example 3

For a data policy that includes a policer, display the policers:

```
Device# show policy from-vsmart
from-vsmart data-policy dp1
 direction from-service
 vpn-list vpn_1_list
  sequence 10
   match
    protocol 1
   action accept
    count police_count
    set
     policer police
  sequence 20
   action accept
    count police_count20
    set
     policer police
  sequence 30
   action accept
    set
     policer police
  default-action accept
from-vsmart policer police
 rate   10000000
 burst  1000000
 exceed remark
from-vsmart lists vpn-list vpn_1_list
```

```
 vpn 1

Device# show sdwan policy data-policy-filter

                                                    POLICER    OOS      OOS
NAME  NAME        COUNTER NAME    PACKETS  BYTES    NAME       PACKETS  BYTES
------------------------------------------------------------------------------
dp1   vpn_1_list  police_count    0        0
                  police_count20  0        0        10.police  0
                                                    20.police  0
                                                    30.police  0
```

show sdwan policy from-vsmart

To display a centralized data policy, an application-aware policy, or a cflowd policy that a Cisco SD-WAN Controller has pushed to the devices, use the **show sdwan policy from-vsmart** command in privileged EXEC mode. The Cisco SD-WAN Controller pushes the policy via OMP after it has been configured and activated on the controller.

show sdwan policy from-vsmart [**app-route-policy**] [**cflowd-template** *template-option*] [**data-policy**] [**lists** { **data-prefix-list** | **vpn-list** }] [**policer**] [**sla-class**]

Syntax Description

None	Display all the data policies that the vSmart controller has pushed to the Cisco IOS XE Catalyst SD-WAN device.
app-route-policy	Display only the application-aware routing policies that the Cisco vSmart controller has pushed to the Cisco IOS XE Catalyst SD-WAN device.
cflowd-template [*template-option*]	Display only the cflowd template information that the Cisco vSmart controller has pushed to the Cisco IOS XE Catalyst SD-WAN device. *template-option* can be one of **collector**, **flow-active-timeout**, **flow-inactive-timeout**, and **template-refresh**.
data-policy	Display only the data policies that the Cisco vSmart controller has pushed to the Cisco IOS XE Catalyst SD-WAN device.
lists {**data-prefix-list** | **vpn-list**}	Display only the policy-related lists that the Cisco vSmart controller has pushed to the Cisco IOS XE Catalyst SD-WAN device.
policer	Display only the policers that the Cisco vSmart controller has pushed to the Cisco IOS XE Catalyst SD-WAN device.
sla-class	Display only the SLA classes for application-aware routing that the Cisco vSmart controller has pushed to the Cisco IOS XE Catalyst SD-WAN device.

Examples

The following is a sample output from the **show sdwan policy from-vsmart** command displaying policy downloaded from Cisco SD-WAN Controller:

```
Device# show sdwan policy from-vsmart
from-vsmart sla-class SLA1
 latency 100
```

```
from-vsmart data-policy DATA_POLICY
 direction from-service
 vpn-list vpn_1
  sequence 11
   match
    destination-port         5060
    protocol                 17
    source-tag-instance      DP_V4_TAG1
    destination-tag-instance DP_V4_TAG3
   action accept
    count src_dst_legacy_v4
  sequence 21
   match
    source-tag-instance DP_V4_TAG1
   action drop
    count src_v4


Device# show sdwan policy from-vsmart
from-vsmart sla-class test_sla_class
 latency 50
from-vsmart app-route-policy test_app_route_policy
 vpn-list vpn_1_list
  sequence 1
   match
    destination-ip 10.2.3.21/32
   action
    sla-class test_sla_class
    sla-class strict
  sequence 2
   match
    destination-port 80
   action
    sla-class test_sla_class
    no sla-class strict
  sequence 3
   match
    destination-data-prefix-list test_data_prefix_list
   action
    sla-class test_sla_class
    sla-class strict

from-vsmart lists vpn-list vpn_1_list
 vpn 1
 vpn 102
from-vsmart lists data-prefix-list test_data_prefix_list
 ip-prefix 10.60.1.0/24


Device# show sdwan policy from-vsmart cflowd-template
from-vsmart cflowd-template test-cflowd-template
 flow-active-timeout   30
 flow-inactive-timeout 30
 template-refresh      30
 collector vpn 1 address 172.16.255.15 port 13322
Device# show policy from-vsmart cflowd-template collector
from-vsmart cflowd-template test-cflowd-template
 collector vpn 1 address 172.16.255.15 port 13322
```

show sdwan policy ipv6 access-list-associations

show sdwan policy ipv6 access-list-associations—Display the IPv6 access lists that are operating on each interface.

Command Syntax

show sdwan policy ipv6 access-list-associations

Syntax Description

None

Output Fields

The output fields are self-explanatory.

Command History

Release	Modification
16.3	Command introduced.

Example

```
Device# show sdwan policy ipv6 access-list-associations

             INTERFACE  INTERFACE
NAME         NAME       DIRECTION
------------------------------------------
ipv6-policy  ge0/2      out
```

show sdwan policy ipv6 access-list-counters

show sdwan policy ipv6 access-list-counters—Display the number of packets counted by IPv6 access lists configured on the Cisco IOS XE Catalyst SD-WAN device.

Command Syntax

show sdwan policy ipv6 access-list-counters

Syntax Description

None

Output Fields

The output fields are self-explanatory.

Command History

Release	Modification
16.3	Command introduced.

Example

```
Device# show sdwan policy ipv6 access-list-counters

NAME         COUNTER NAME  PACKETS  BYTES
------------------------------------------------------------
ipv6-policy  ipv6-counter  1634     135940
```

show sdwan policy ipv6 access-list-names

show sdwan policy ipv6 access-list-names—Display the names of the IPv6 access lists configured on the Cisco IOS XE Catalyst SD-WAN device.

Command Syntax

show sdwan policy ipv6 access-list-names

Syntax Description

None

Output Fields

The output fields are self-explanatory.

Command History

Release	Modification
16.3	Command introduced.

Examples

```
Device# show sdwan policy ipv6 access-list-names

NAME
--------------------
ipv6-policy
```

show sdwan policy ipv6 access-list-policers

show sdwan policy ipv6 access-list-policers—Display information about the policers configured in IPv6 access lists.

Command Syntax

show sdwan policy ipv6 access-list-policers

Syntax Description

None

Output Fields

The output fields are self-explanatory.

Command History

Release	Modification
16.3	Command introduced.

Examples

Display a list of policers configured in access lists. This output shows that the policer named "p1_police" was applied in sequence 10 in the access list "ipv6_p1" in sequences 10, 20, and 30 in the "ipv6_plp" access list.

```
Device# show sdwan policy ipv6 access-list-policers
                                    OOS
NAME                 POLICER NAME   PACKETS
-------------------------------------------
ipv6_p1              10.p1_police   0
ipv6_plp             10.p1_police   0
                     20.p1_police   0
                     30.p2_police   0
```

show sdwan policy rewrite-associations

To display information about rewrite rules to interface bindings on Cisco IOS XE SD-WAN devices, use the **show sdwan policy rewrite-associations** command in privileged EXEC mode.

show sdwan policy rewrite-associations

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE SD-WAN Release 17.2.1v	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Usage Guidelines

The QoS feature on Cisco IOS XE SD-WAN devices works by examining packets entering at the edge of the network.

Generally, each router on the local service-side network examines the QoS settings of the packets that enter it, determines which class of packets are transmitted first, and processes the transmission based on those settings. As packets leave the network on the remote service-side network, you can rewrite the QoS bits of the packets before transmitting them to meet the policies of the targeted peer router.

You can configure and apply rewrite rules on the egress interface to overwrite the Differentiated Services Code Point (DSCP) value for packets entering the network.

This command can be used to display information about rewrite rules to interface bindings on Cisco IOS XE SD-WAN devices.

Example

The following example shows how to display information about rewrite rules to interface bindings on Cisco IOS XE SD-WAN devices.

```
Device# show sdwan policy rewrite-associations
NAME INTERFACE NAME
transport1 GigabitEthernet0/0/0
transport2 GigabitEthernet0/0/1
```

Related Commands

Command	Description
show sdwan policy access-list-associations	Displays SD-WAN policy access-list-associations.
show sdwan policy access-list-counters	Displays SD-WAN policy access-list-counters.
show sdwan policy access-list-names	Displays SD-WAN policy access-list-names.
show sdwan policy access-list-policers	Displays SD-WAN policy access-list-policers.
show sdwan app-route-policy-filter	Displays information about application-aware routing policy matched packet counts.
show sdwan policy data-policy-filter	Displays SD-WAN policy data-policy-filter.
show sdwan policy from-vsmart	Displays SD-WAN policy from Cisco Catalyst SD-WAN Controller.
show sdwan policy ipv6	Displays SD-WAN policy IPv6.
show sdwan policy service-path	Displays next-hop information for packet coming from service side.
show sdwan policy tunnel-path	Displays next-hop information for packet coming over the WAN tunnel.

show sdwan reboot history

To display the history of when the Cisco vManage device is rebooted, use the **show reboot history** command in privileged EXEC mode. The command displays only the latest 20 reboots.

show sdwan reboot history

Syntax Description

None

Command History

Release	Modification
16.9	Command introduced.

Example

```
Device# show sdwan reboot history
REBOOT DATE TIME           REBOOT REASON
---------------------------------------------------------------------------
2016-03-14T23:24:43+00:00  Initiated by user - patch
2016-03-14T23:36:20+00:00  Initiated by user
2016-03-15T21:06:56+00:00  Initiated by user - activate next-1793
2016-03-15T21:10:11+00:00  Software initiated - USB controller disabled
2016-03-15T21:12:53+00:00  Initiated by user
2016-03-15T23:47:59+00:00  Initiated by user
2016-03-15T23:54:49+00:00  Initiated by user
2016-03-15T23:58:28+00:00  Initiated by user
2016-03-16T00:01:32+00:00  Initiated by user
2016-03-16T00:11:02+00:00  Initiated by user
2016-03-16T00:14:42+00:00  Initiated by user
2016-03-16T00:20:30+00:00  Initiated by user
2016-03-16T00:27:11+00:00  Initiated by user
2016-03-16T00:38:46+00:00  Software initiated - watchdog expired
2016-03-16T00:49:25+00:00  Software initiated - watchdog expired
2016-03-16T01:00:07+00:00  Software initiated - watchdog expired
2016-03-16T03:22:05+00:00  Initiated by user
2016-03-16T03:35:40+00:00  Initiated by user
2016-03-16T21:42:19+00:00  Initiated by user
2016-03-16T22:00:25+00:00  Initiated by user
```

show sdwan running-config

To display the active configuration that is running on devices, use the **details** filter with this command to display the default values for configured components.

show sdwan running-config [*configuration-hierarchy*]

Syntax Description

None	Display the full active configuration.
configuration-hierarchy	Specific Configuration Hierarchy: Display the active configuration for a specific hierarchy in the configuration.

Command History

Release	Modification
16.9	Command introduced.
Cisco IOS XE Catalyst SD-WAN Release 17.8.1a	Added **secondary-region** to the output to show the Hierarchical SD-WAN region ID, and **region** to show the secondary region mode. Added **transport-gateway** to the output to indicate the enabled/disabled status. Added **affinity-group** and **affinity-group preference** to the output to indicate the affinity group ID assigned to the device and the preference order.

Usage Guidelines

Starting from Cisco IOS XE Catalyst SD-WAN Release 17.6.1a, edge device accepts template push from Cisco vManage Release 20.6.1 with **integrity-type** configuration. The **show sdwan running-config diff** command fails if the template with **integrity-type** config is pushed from Cisco vManage Release 20.6.1 to older edge devices. Edge device needs to be upgraded to Cisco IOS XE Catalyst SD-WAN Release 17.6.1a or higher version before receiving a template-push from Cisco vManage Release 20.6.1.

Examples

Example 1

```
Device# show sdwan running-config
system
host-name vedge1
system-ip 172.16.255.1
domain-id 1
site-id   1
clock timezone America/Los_Angeles
vbond 10.0.14.4
aaa
  auth-order local radius
  usergroup basic
   task system read write
   task interface read write
  !
  usergroup netadmin
  !
  usergroup operator
   task system read
   task interface read
   task policy read
   task routing read
   task security read
  !
  user admin
   password $1$zvOh58pk$QLX7/RS/F0c6ar94.xl2k.
  !
  user eve
   password $1$aLEJ6jve$aBpPQpkl3h.SvA2dt4/6E/
   group    operator
  !
!
logging
  disk
   enable
  !
```

```
 !
!
```

Example 2

```
Device# show sdwan running-config vpn 1
vpn 1
 name ospf_and_bgp_configs
 router
  ospf
   router-id 172.16.255.15
   timers spf 200 1000 10000
   redistribute static
   redistribute omp
   area 0
    interface ge0/4
    exit
   exit
  !
  pim
   interface ge0/5
   exit
  exit
 !
 interface ge0/4
  ip address 10.20.24.15/24
  no shutdown
 !
 interface ge0/5
  ip address 56.0.1.15/24
  no shutdown
 !
!
Device# show running-config vpn 1
vpn 1
 name ospf_and_bgp_configs
 no ecmp-hash-key layer4
 router
  ospf
   router-id 172.16.255.15
   auto-cost reference-bandwidth 100
   compatible rfc1583
   distance external 0
   distance inter-area 0
   distance intra-area 0
   timers spf 200 1000 10000
   redistribute static
   redistribute omp
   area 0
    interface ge0/4
     hello-interval      10
     dead-interval       40
     retransmit-interval 5
     priority            1
     network             broadcast
    exit
   exit
  !
  pim
   no shutdown
   no auto-rp
   interface ge0/5
```

```
    hello-interval      30
    join-prune-interval 60
   exit
  exit
 !
 interface ge0/4
  ip address 10.20.24.15/24
  flow-control        autoneg
  no clear-dont-fragment
  no pmtu
  mtu                 1500
  no shutdown
  arp-timeout         1200
 !
 interface ge0/5
  ip address 56.0.1.15/24
  flow-control        autoneg
  no clear-dont-fragment
  no pmtu
  mtu                 1500
  no shutdown
  arp-timeout         1200
 !
!
```

show sdwan security-info

To view the security information configured for IPsec tunnel connections, use the **show sdwan security-info** command in privileged EXEC mode.

show sdwan security-info

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	The output of this command was modified. The `security-info authentication-type` field in the output of this command is deprecated. A new field `security-info integrity-type` field is added to the command output.

Example

The following is a sample output from the **show sdwan security-info** command:

```
Device# show sdwan security-info
security-info authentication-type deprecated
security-info rekey  86400
security-info replay-window 512
security-info encryption-supported "AES_GCM_256 (and AES_256_CBC for multicast)"
security-info fips-mode Disabled
security-info pairwise-keying Disabled
security-info pwk-sym-rekey Enabled
security-info extended-ar-window Disabled
security-info integrity-type ip-udp-esp
```

show sdwan secure-internet-gateway tunnels

To view information about the automatic SIG tunnels that you have configured from a Cisco IOS XE SD-WAN device to Cisco Umbrella or Zscaler SIG, use the **show sdwan secure-internet-gateway tunnels** command in the privileged EXEC mode.

show sdwan secure-internet-gateway tunnels

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 17.9.1a	This command is introduced.

Examples

```
Device# show sdwan secure-internet-gateway tunnels
TUNNEL IF     TUNNEL                                                    HA      DEVICE  SIG
   TRACKER              DESTINATION            TUNNEL
NAME          ID        TUNNEL NAME                                   PAIR    STATE   STATE
  STATE    SITE ID     DATA CENTER  PROVIDER  TYPE    TIMESTAMP
-------------------------------------------------------------------------------------------
Tunnel100001  52615809  site1820851800sys172x16x255x15ifTunnel100001  Active  Up      NA
   Enabled  1820851800  NA           zScaler   IPsec   NA
Tunnel100002  52615814  site1820851800sys172x16x255x15ifTunnel100002  Backup  Up      NA
   Enabled  1820851800  NA           zScaler   IPsec   NA
```

Table 42: Output Columns

Column	Description
TUNNEL IF NAME	Tunnel name configured on the device.
TUNNEL ID	Unique ID for the tunnel defined by the SIG provider.
TUNNEL NAME	Unique name for the tunnel that can be used to identify the tunnel at both the local and remote ends. On the SIG provider portal, you can use the tunnel name to find details about a particular tunnel.
HA PAIR	Active or Backup.
DEVICE STATE	Tunnel status as perceived by the device.
SIG STATE	Tunnel status as perceived by the SIG endpoint. **Note** Supported for Cisco Umbrella SIG endpoints only.

Column	Description
TRACKER STATE	Whether enabled or disabled during tunnel configuration.
SITE ID	ID of the site where the WAN edge device is deployed
DESTINATION DATA CENTER	SIG provider data center to which the tunnel is connected **Note** Supported for Cisco Umbrella SIG endpoints only.
PROVIDER	Cisco Umbrella or Zscaler.
TUNNEL TYPE	IPSec or GRE

show sdwan secure-internet-gateway umbrella tunnels

To view information about the automatic SIG tunnels that you have configured from a Cisco IOS XE SD-WAN device to Cisco Umbrella, use the **show sdwan secure-internet-gateway umbrella tunnels** command in the privileged EXEC mode.

show sdwan secure-internet-gateway umbrella tunnels

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 17.5.1a	This command is introduced.

Examples

```
Device# show sdwan secure-internet-gateway umbrella tunnels
                                                                                                                API
 LAST
TUNNEL IF                                                                                                       HTTP
 SUCCESSFUL    TUNNEL
NAME          TUNNEL ID  TUNNEL NAME                                  FSM STATE             CODE
 REQ           STATE
-------------------------------------------------------------------------------------------------------------------
Tunnel17447  527398582  SITE10005SYS172x16x255x88IFTunnel17447  st-tun-create-notif  200
 rekey-tunnel  -
Tunnel22427  527398577  SITE10005SYS172x16x255x88IFTunnel22427  st-tun-create-notif  200
 rekey-tunnel  -
Tunnel22457  527398373  SITE10005SYS172x16x255x88IFTunnel22457  st-tun-create-notif  200
 rekey-tunnel  -
```

Table 43: Output Columns

Column	Description
TUNNEL IF NAME	Tunnel name configured on the device.
TUNNEL ID	Unique ID for the tunnel defined by the SIG provider.
TUNNEL NAME	Unique name for the tunnel that can be used to identify the tunnel at both the local and remote ends. On the SIG provider portal, you can use the tunnel name to find details about a particular tunnel.
FSM STATE	The current state of the finite state machine (FSM) when a tunnel is being created to the SIG endpoint.
API HTTP CODE	The last HTTP code received from the SIG endpoint in response to an API request.
LAST SUCCESSFUL REQ	The last API request to the SIG endpoint that was successful.
TUNNEL STATE	Yet to be supported.

show sdwan secure-internet-gateway zscaler tunnels

To view information about the automatic SIG tunnels that you have configured from a Cisco IOS XE SD-WAN device to Zscaler SIG, use the **show sdwan secure-internet-gateway zscaler tunnels** command in the privileged EXEC mode.

show sdwan secure-internet-gateway zscaler tunnels

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Release 17.5.1a	This command is introduced.

Examples

```
Device# show sdwan secure-internet-gateway zscaler tunnels

                          HTTP
TUNNEL IF                                                 TUNNEL
                                                               LOCATION
                          RESP
NAME          TUNNEL NAME                                 ID        FQDN
                                       TUNNEL FSM STATE         ID        LOCATION FSM
```

```
STATE   LAST HTTP REQ     CODE
-------------------------------------------------------------------------------------------------------------------------------
Tunnel100001  site1820851800sys172x16x255x15ifTunnel100001  52615809
site1820851800sys172x16x255x15iftunnel100001@example.com  add-vpn-credential-info  52615819
  location-init-state  get-data-centers  200
Tunnel100002  site1820851800sys172x16x255x15ifTunnel100002  52615814
site1820851800sys172x16x255x15iftunnel100002@example.com  add-vpn-credential-info  52615819
  location-init-state  get-data-centers  200
```

Table 44: Output Columns

Column	Description
TUNNEL IF NAME	Tunnel name configured on the device.
TUNNEL NAME	Unique name for the tunnel that can be used to identify the tunnel at both the local and remote ends. On the SIG provider portal, you can use the tunnel name to find details about a particular tunnel.
TUNNEL ID	Unique ID for the tunnel defined by the SIG provider
FQDN	The fully qualified domain name (FQDN) that the device uses to interact with the Zscaler SIG endpoint.
TUNNEL FSM STATE	The current state of the tunnel finite state machine (FSM) when a tunnel is being created to the SIG endpoint.
LOCATION ID	ID provided by Zscaler after the location is set up successfully.
LOCATION FSM STATE	The current state of the location finite state machine (FSM) when a lcation is being set up using Zscaler endpoint APIs.
LAST HTTP REQ	The last API request to the SIG endpoint.
HTTP RESP CODE	The last HTTP code received from the SIG endpoint in response to an API request.

show sdwan software

List the software images that are installed on the local device (on Cisco IOS XE Catalyst SD-WAN devices and vSmart controllers).

show sdwan software *image-name*

show sdwan software

Syntax Description

None	List information about all software images installed on the local device.

image-name	Specific Software Image: List information about a specific software image.

Command History

Release	Modification
16.9	Command introduced.
16.11	Version string displays 5-tuples.
16.12	Includes installer space usage.

Example

Example 1

Release 16.9

```
Device# show sdwan software

VERSION   ACTIVE  DEFAULT  PREVIOUS  CONFIRMED  TIMESTAMP
-------------------------------------------------------------------------------
16.10.2e  true    true     false     user       2022-07-07T23:47:18-00:0
16.9.3    false   true     true      auto       2020-04-08T19:39:36-00:00
```

Example 2

Release 16.12

```
Device# show sdwan software

VERSION          ACTIVE  DEFAULT  PREVIOUS  CONFIRMED  TIMESTAMP
-------------------------------------------------------------------------------
16.10.3.0.0      false   true     true      user       2020-06-08T13:32:21-00:00
17.03.05.0.6600  true    false    false     user       2022-07-19T23:35:54-00:00

Total Space:387M Used Space:130M Available Space:253M
```

show sdwan system status

Display time and process information for the device, as well as CPU, memory, and disk usage data.

show sdwan system status

Syntax Description

None

Command History

Release	Modification
16.9	Command introduced.
17.2	Model name changed to display Cisco IOS XE Catalyst SD-WAN device Product ID.
17.3	Included Hypervisor details.

Examples

Example 1

Release 16.12.4

```
Device# show sdwan system status
Viptela (tm) vedge Operating System Software
Copyright (c) 2013-2020 by Viptela, Inc.
Controller Compatibility: 19.2
Version: 16.12.4.0.4457
Build: Not applicable

System logging to host is disabled
System logging to disk is enabled

System state: GREEN. All daemons up
System FIPS state: Disabled
Testbed mode: Enabled

Last reboot: Image Install .
CPU-reported reboot: Image
Boot loader version: Not applicable
System uptime: 0 days 02 hrs 18 min 08 sec
Current time: Wed Dec 23 15:26:46 UTC 2020

Load average: 1 minute: 0.15, 5 minutes: 0.12, 15 minutes: 0.13
Processes: 560 total
CPU allocation: 8 total, 1 control, 7 data
CPU states: 1.18% user, 1.39% system, 97.30% idle
Memory usage: 16425460K total, 2302960K used, 14122500K free
330540K buffers, 2548048K cache

Disk usage: Filesystem Size Used Avail Use % Mounted on
/dev/bootflash1 29469M 17656M 10316M 63% /bootflash
/dev/loop18 388M 105M 279M 28% /bootflash/.sdwaninstaller


Personality: vedge
Model name: vedge-ISR-4451-X
Services: None
vManaged: false
Commit pending: false
Configuration template: None
Chassis serial number: FGL174411F8
```

Example 2

Release 17.2.1v

```
Device# show sdwan system status
Viptela (tm) vEdge Operating System Software
Copyright (c) 2013-2020 by Viptela, Inc.
Controller Compatibility: 20.1
Version: 17.02.01v.0.75
Build: Not applicable

System logging to host is disabled
System logging to disk is enabled

System state: GREEN. All daemons up
System FIPS state: Disabled
Testbed mode: Enabled

Last reboot: .
CPU-reported reboot:
Boot loader version: Not applicable
System uptime: 0 days 00 hrs 01 min 38 sec
Current time: Wed Dec 23 16:03:11 UTC 2020

Load average: 1 minute: 2.16, 5 minutes: 1.65, 15 minutes: 0.70
Processes: 515 total
CPU allocation: 8 total, 8 control, 0 data
CPU states: 11.23% user, 11.19% system, 68.65% idle
Memory usage: 16417952K total, 2432636K used, 13985316K free
305852K buffers, 2573596K cache

Disk usage: Filesystem Size Used Avail Use % Mounted on
/dev/bootflash1 29469M 18987M 8985M 68% /bootflash
387M 140M 242M 37 /bootflash/.installer


Personality: vEdge
Model name: ISR4451-X/K9
Services: None
vManaged: false
Commit pending: false
Configuration template: None
Chassis serial number: FGL174411F8
```

Example 3

17.3.1a

```
Device# show sdwan system status
Viptela (tm) vEdge Operating System Software
Copyright (c) 2013-2020 by Viptela, Inc.
Controller Compatibility: 20.3
Version: 17.03.01a.0.354
Build: Not applicable

System logging to host is disabled
System logging to disk is enabled

System state: GREEN. All daemons up
System FIPS state: Disabled
Testbed mode: Enabled
```

```
Last reboot: .
CPU-reported reboot:
Boot loader version: Not applicable
System uptime: 0 days 00 hrs 02 min 13 sec
Current time: Wed Dec 23 16:20:54 UTC 2020

Hypervisor Type: None
Cloud Hosted Instance: false

Load average: 1 minute: 0.94, 5 minutes: 1.64, 15 minutes: 0.81
Processes: 522 total
CPU allocation: 8 total, 8 control, 223 data
CPU states: 10.47% user, 10.48% system, 72.01% idle
Memory usage: 16417952K total, 2245016K used, 14172936K free
316244K buffers, 2566252K cache

Disk usage: Filesystem Size Used Avail Use % Mounted on
/dev/bootflash1 29469M 20330M 7642M 73% /bootflash
387M 159M 224M 41 /bootflash/.installer


Personality: vEdge
Model name: ISR4451-X/K9
Services: None
vManaged: false
Commit pending: false
Configuration template: None
Chassis serial number: FGL174411F8
```

show sdwan tag-instances from-vsmart

To display the tags downloaded from the Cisco SD-WAN Controller, use the **show sdwan tag-instances from-vsmart** command in privileged EXEC mode.

show sdwan tag-instances from-vsmart

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	This command was introduced.

Usage Guidelines

Use the **show sdwan tag-instances from-vsmart** command to show user configuration of tag-instances.

Examples

The following is a sample output from **show sdwan tag-instances from-vsmart** command, displaying tags downloaded from Cisco SD-WAN Controller:

```
Device# show sdwan tag-instances from-vsmart
tag-instances-from-vsmart
 tag-instance APP_facebook_TAG9
```

```
 id       60000
 app-list apps_facebook
tag-instance APP_office_TAG10
 id       70000
 app-list apps_ms apps_zoom
tag-instance APP_webex_TAG8
 id       50000
 app-list apps_webex
tag-instance DP_V4_TAG1
 id               10000
 data-prefix-list pfx1
lists data-prefix-list multicast_pfx
 ip-prefix 224.0.0.0/8
lists data-prefix-list pfx1
 ip-prefix 10.20.24.0/24
lists app-list apps_facebook
 app dns
 app facebook
lists app-list apps_ms
 app ms-office-365
 app ms-office-web-apps
 app ms-services
```

Related Commands

Command	Description
show sdwan policy from-vsmart	Displays policy downloaded from Cisco SD-WAN Controller.

show sdwan version

Display the active version of the Cisco SD-WAN software running on the device.

```
show sdwan version
```

Syntax Description

None

Command History

Release	Modification
16.9	Command introduced.

Example

Example

```
Device# show sdwan version
17.02.01r.0.32
```

show sdwan zbfw drop-statistics

To display zone based firewall drop statistic, use the **show sdwan zbfw drop-statistics** command in privileged EXEC mode.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.11.1a	This command is supported in Cisco Catalyst SD-WAN

Example

The following example displays the zone based firewall drop statistic.

```
Device#show sdwan zbfw drop-statistics
zbfw drop-statistics catch-all                 0
zbfw drop-statistics l4-max-halfsession        0
zbfw drop-statistics l4-too-many-pkts          0
zbfw drop-statistics l4-session-limit          0
zbfw drop-statistics l4-invalid-hdr            0
zbfw drop-statistics l4-internal-err-undefined-dir 0
zbfw drop-statistics l4-scb-close              0
zbfw drop-statistics l4-tcp-invalid-ack-flag   0
zbfw drop-statistics l4-tcp-invalid-ack-num    0
zbfw drop-statistics l4-tcp-invalid-tcp-initiator 0
zbfw drop-statistics l4-tcp-syn-with-data      0
zbfw drop-statistics l4-tcp-invalid-win-scale-option 0
zbfw drop-statistics l4-tcp-invalid-seg-synsent-state 0
zbfw drop-statistics l4-tcp-invalid-seg-synrcvd-state 0
zbfw drop-statistics l4-tcp-invalid-seg-pkt-too-old 0
zbfw drop-statistics l4-tcp-invalid-seg-pkt-win-overflow 0
zbfw drop-statistics l4-tcp-invalid-seg-pyld-after-fin-send 0
zbfw drop-statistics l4-tcp-invalid-flags      0
zbfw drop-statistics l4-tcp-invalid-seq        0
zbfw drop-statistics l4-tcp-retrans-invalid-flags 0
zbfw drop-statistics l4-tcp-l7-ooo-seg         0
zbfw drop-statistics l4-tcp-syn-flood-drop     0
zbfw drop-statistics l4-tcp-internal-err-synflood-alloc-hostdb-fail 0
zbfw drop-statistics l4-tcp-synflood-blackout-drop 0
zbfw drop-statistics l4-tcp-unexpect-tcp-payload 0
zbfw drop-statistics l4-tcp-syn-in-win         0
zbfw drop-statistics l4-tcp-rst-in-win         0
zbfw drop-statistics l4-tcp-stray-seg          0
zbfw drop-statistics l4-tcp-rst-to-resp        0
zbfw drop-statistics insp-pam-lookup-fail      0
zbfw drop-statistics insp-internal-err-get-stat-blk-fail 0
zbfw drop-statistics insp-dstaddr-lookup-fail  0
zbfw drop-statistics insp-policy-not-present   0
zbfw drop-statistics insp-sess-miss-policy-not-present 0
zbfw drop-statistics insp-classification-fail  0
zbfw drop-statistics insp-class-action-drop    0
zbfw drop-statistics insp-policy-misconfigure  0
zbfw drop-statistics l4-icmp-too-many-err-pkts 0
zbfw drop-statistics l4-icmp-internal-err-no-nat 0
zbfw drop-statistics l4-icmp-internal-err-alloc-fail 0
```

```
zbfw drop-statistics l4-icmp-internal-err-get-stat-blk-fail 0
zbfw drop-statistics l4-icmp-internal-err-dir-not-identified 0
zbfw drop-statistics l4-icmp-scb-close         0
zbfw drop-statistics l4-icmp-pkt-no-ip-hdr     0
zbfw drop-statistics l4-icmp-pkt-too-short     0
zbfw drop-statistics l4-icmp-err-no-ip-no-icmp 0
zbfw drop-statistics l4-icmp-err-pkts-burst    0
zbfw drop-statistics l4-icmp-err-multiple-unreach 0
zbfw drop-statistics l4-icmp-err-l4-invalid-seq 0
zbfw drop-statistics l4-icmp-err-l4-invalid-ack 0
zbfw drop-statistics l4-icmp-err-policy-not-present 0
zbfw drop-statistics l4-icmp-err-classification-fail 0
zbfw drop-statistics syncookie-max-dst         0
zbfw drop-statistics syncookie-internal-err-alloc-fail 0
zbfw drop-statistics syncookie-trigger         0
zbfw drop-statistics policy-fragment-drop      0
zbfw drop-statistics policy-action-drop        11
zbfw drop-statistics policy-icmp-action-drop   0
zbfw drop-statistics l7-type-drop              0
zbfw drop-statistics l7-no-seg                 0
zbfw drop-statistics l7-no-frag                0
zbfw drop-statistics l7-unknown-proto          0
zbfw drop-statistics l7-alg-ret-drop           0
zbfw drop-statistics l7-promote-fail-no-zone-pair 0
zbfw drop-statistics l7-promote-fail-no-policy 0
zbfw drop-statistics no-session                0
zbfw drop-statistics no-new-session            0
zbfw drop-statistics not-initiator             0
zbfw drop-statistics invalid-zone              18
zbfw drop-statistics ha-ar-standby             0
zbfw drop-statistics no-forwarding-zone        0
zbfw drop-statistics backpressure              0
zbfw drop-statistics zone-mismatch             0
zbfw drop-statistics fdb-err                   0
zbfw drop-statistics lisp-header-restore-fail  0
zbfw drop-statistics lisp-inner-pkt-insane     0
zbfw drop-statistics lisp-inner-ipv4-insane    0
zbfw drop-statistics lisp-inner-ipv6-insane    0
zbfw drop-statistics policy-avc-action-drop    0
zbfw drop-statistics l4-icmp-invalid-seq       0
zbfw drop-statistics l4-udp-max-halfsession    0
zbfw drop-statistics l4-icmp-max-halfsession   0
zbfw drop-statistics no-zone-pair-present      0
```

show sdwan zbfw zonepair-statistics

Display zone based firewall zonepair statistics, use the **show sdwan zbfw zonepair-statistics** command in privileged EXEC mode.

show sdwan zbfw zonepair-statistics

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.11.1a	This command is supported in Cisco Catalyst SD-WAN

Example

The following example displays the zone based firewall zonepair statistics.

```
Device#show sdwan zbfw zonepair-statistics
zbfw zonepair-statistics ZP_zone1_zone1_seq_1
 src-zone-name zone1
 dst-zone-name zone1
 policy-name   seq_1
 fw-traffic-class-entry seq_1-seq-1-cm_
  zonepair-name                 ZP_zone1_zone1_seq_1
  class-action                  Inspect
  pkts-counter                  7236
  bytes-counter                 4573618
  attempted-conn                9
  current-active-conn           0
  max-active-conn               1
  current-halfopen-conn         0
  max-halfopen-conn             1
  current-terminating-conn      0
  max-terminating-conn          0
  time-since-last-session-create 4373
  fw-tc-match-entry seq_1-seq-rule1-v6-acl_ 3
   match-type "access-group name"
  fw-tc-proto-entry 1
   protocol-name tcp
   byte-counters 4545768
   pkt-counters  7037
  fw-tc-proto-entry 4
   protocol-name icmp
   byte-counters 27850
   pkt-counters  199
  l7-policy-name                NONE
 fw-traffic-class-entry seq_1-seq-11-cm_
  zonepair-name                 ZP_zone1_zone1_seq_1
  class-action                  Inspect
  pkts-counter                  4947
  bytes-counter                 3184224
  attempted-conn                5
  current-active-conn           0
  max-active-conn               1
  current-halfopen-conn         0
  max-halfopen-conn             0
  current-terminating-conn      0
  max-terminating-conn          0
  time-since-last-session-create 4480
  fw-tc-match-entry seq_1-seq-Rule_3-acl_ 3
   match-type "access-group name"
  fw-tc-proto-entry 1
   protocol-name tcp
   byte-counters 3184224
   pkt-counters  4947
  l7-policy-name                NONE
 fw-traffic-class-entry class-default
  zonepair-name                 ZP_zone1_zone1_seq_1
  class-action                  "Inspect Drop"
  pkts-counter                  11
  bytes-counter                 938
  attempted-conn                0
  current-active-conn           0
  max-active-conn               0
  current-halfopen-conn         0
  max-halfopen-conn             0
```

```
current-terminating-conn       0
max-terminating-conn           0
time-since-last-session-create 0
l7-policy-name                 NONE
```

show sdwan zonebfwdp sessions

To display the existing zone-based firewall sessions on Cisco IOS XE SD-WAN devices, use the **show sdwan zonebfwdp sessions** command in privileged EXEC mode.

show sdwan zonebfwdp sessions

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE SD-WAN Release 17.2.1v	This command is supported in Cisco Catalyst SD-WAN.

Usage Guidelines

Secure SD-WAN brings key security capabilities embedded natively in SD-WAN solution with cloud-based single-pane of management for both SD-WAN and security capabilities. The security capabilities include enterprise firewall with application awareness, intrusion prevention systems with Cisco Talos signatures, URL-Filtering, and DNS/web-layer security.

The Enterprise Firewall with Application Awareness uses a flexible and easily understood zone-based model for traffic inspection.

A firewall policy is a type of localized security policy that allows stateful inspection of TCP, UDP, and ICMP data traffic flows. Traffic flows that originate in a given zone are allowed to proceed to another zone based on the policy between the two zones. A zone is a grouping of one or more VPNs. Grouping VPNs into zones allows you to establish security boundaries in your overlay network so that you can control all data traffic that passes between zones.

Firewall policies can match IP prefixes, IP ports, the protocols TCP, UDP, and ICMP, and applications. Matching flows for prefixes, ports, and protocols can be accepted or dropped, and the packet headers can be logged. Nonmatching flows are dropped by default. Matching applications are denied.

A zone pair is a container that associates a source zone with a destination zone and that applies a firewall policy to the traffic that flows between the two zones.

This command can be used to display the existing zone-based firewall sessions on Cisco IOS XE SD-WAN devices.

Example

The following example shows how to display the existing zone-based firewall sessions on Cisco IOS XE SD-WAN devices.

```
Device# show sdwan zonebfwdp sessions

   SRC  DST                                          TOTAL      TOTAL                    UTD

SESSION                                         SRC    DST                            SRC  DST
  VPN  VPN  ZP      CLASSMAP    NAT    INTERNAL  INITIATOR  RESPONDER  APPLICATION  POLICY

ID       STATE   SRC IP        DST IP        PORT   PORT  PROTOCOL                VRF  VRF
  ID   ID   NAME    NAME        FLAGS  FLAGS     BYTES      BYTES      TYPE         NAME

-------------------------------------------------------------------------------------------------------------
136      open    10.20.24.150  10.1.15.150   39662  1719  PROTO_L7_H225_RAS       1    1
   1    0    in2out  fw-traffic  -      0         166        6                        -

134      open    10.1.15.151   10.20.24.150  5013   5001  PROTO_L7_H323_RTCP_DATA  1    1
   1    0    in2out  fw-traffic  -      0         276        184                      -

132      closed  10.20.24.150  10.1.15.151   48330  1720  PROTO_L7_H323            1    1
   1    0    in2out  fw-traffic  -      65543     506        552                      -

133      open    10.1.15.151   10.20.24.150  5012   5000  PROTO_L7_H323_RTP_DATA   1    1
   1    0    in2out  fw-traffic  -      0         396976     396804                   -
```

show service-insertion type appqoe

To view detailed information about service controllers, service node groups, and individual service nodes, use the **show service-insertion type appqoe** command in privileged EXEC mode.

show service-insertion type appqoe { **status** | **alarms** | **config** | **token** | **cluster-summary** | **appnav-controller-group** | **service-node-group** [*name*] | **service-context** [*service-context-name*] }

Syntax Description

status	Displays the general status of the AppNav-XE controller.
alarms	Displays information about various AppNav-XE controller alarms.
config	Displays AppNav-XE controller configuration.
token	Displays information about the AppNav-XE controller token.
cluster-summary	Displays the summary of the AppNav-XE cluster.
appnav-controller-group	Displays membership details of the AppNav controller group and service nodes configured and registered with the controller group.
service-node-group	Displays configuration details for all service nodes within a service node group.
name	(Optional) Name of the service node group
service-context *service-context-name*	Displays information about all or the specified service context.

Command Default

This command has no default behavior.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	This command was introduced.
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	The output of this command was modified to include sub-service health for AppQoE using the keyword **service-node-group**.

Usage Guidelines

Starting from Cisco IOS XE Catalyst SD-WAN Release 17.6.1a the output of the **show service-insertion type appqoe service-node-group** command shows the sub-service health for AppQoE. However, if the service node runs a version prior to Cisco IOS XE Catalyst SD-WAN Release 17.6.1a, the sub-service health information is unavailable to the service controller. In such cases, the health markers for various AppQoE services show as green with 0% utilization even though not all services may be available to the service nodes.

The following is the sample output from **show service-insertion type appqoe service-node-group** command when the service nodes aren't upgraded to Cisco IOS XE Catalyst SD-WAN Release 17.6.1a:

```
Device# show service-insertion type appqoe service-node-group
Service Node Group name         : SNG-APPQOE
    Service Context             : appqoe/1
    Member Service Node count   : 2


Service Node (SN)                   : 192.0.2.254
Auto discovered                     : No
SN belongs to SNG                   : SNG-APPQOE
Current status of SN                : Alive
System IP                           : 1.0.0.33
Site ID                             : 10050
Time current status was reached              : Tue Apr 20 17:08:29 2021

Cluster protocol VPATH version               : 1 (Bitmap recvd: 1)
Cluster protocol incarnation number          : 1
Cluster protocol last sent sequence number   : 1618944623
Cluster protocol last received sequence number: 392504
Cluster protocol last received ack number    : 1618944622

Health Markers:
              AO       Load State

             tcp          GREEN 0%
             ssl          GREEN 0%
             dre          GREEN 0%
            http          GREEN 0%
```

Example

The following sample output shows the configuration details of service nodes in a service node group:

```
Device# show service-insertion type appqoe service-node-group
Service Node Group name : SNG-APPQOE
Service Context : appqoe/1
Member Service Node count : 2


Service Node (SN) : 10.1.1.1
Auto discovered : No
SN belongs to SNG : SNG-APPQOE
Current status of SN : Alive
```

```
System IP : 192.168.1.11
Site ID : 101
Time current status was reached : Wed Sep 23 11:01:49 2020

Cluster protocol VPATH version : 1 (Bitmap recvd: 1)
Cluster protocol incarnation number : 1
Cluster protocol last sent sequence number : 1601432656
Cluster protocol last received sequence number: 715749
Cluster protocol last received ack number : 1601432655
```

The following sample output shows the traffic statistics for service nodes in a service node group:

```
Device# show service-insertion type appqoe statistics service-node-group
Service Node Group: SNG-APPQOE
Number of Service Node(s): 2
Member Service Nodes:
IP Address
10.1.1.1
10.1.1.2

Aggregate of statistics from all SNs of the SNG:
------------------------------------------------
Time since statistics were last reset/cleared:

Aggregate number of probe requests sent to SN : 1435070
Aggregate number of probe responses received from SN: 715915
Aggregate number of invalid probe responses received
Total : 0
Incompatible version : 0
Authentication failed : 0
Stale response : 0
Malformed response : 0
Unknown response : 0
Aggregate number of times liveliness was lost with the SN : 1
Aggregate number of times liveliness was regained with the SN:2
Aggregare number of version probes sent to SN: 719033
Aggregate number of version probes received from SN: 2
Aggregate number of healthprobes sent to SN: 716037
Aggregate number of healthprobes received from SN: 715913


Aggregate traffic distribution statistics
-----------------------------------------
Packet and byte counts-
----------------------
Redirected Bytes : 1558757923174
Redirected Packets : 1945422189
Received Bytes : 1582477555093
Received Packets : 1908965233
```

The following sample output shows the configuration details of service controllers in a controller group:

```
Device# show service-insertion type appqoe appnav-controller-group
All AppNav Controller Groups in service context
Appnav Controller Group : ACG-APPQOE
Member Appnav Controller Count : 1
Members:
IP Address
10.1.1.100

AppNav Controller : 192.0.2.1
Local AppNav Controller : Yes
Current status of AppNav Controller : Alive
Time current status was reached : Mon Sep 21 19:09:08 2020
```

```
Current AC View of AppNav Controller
IP Address
10.1.1.100

Current SN View of AppNav Controller
IP Address
10.1.1.1
```

show sslproxy statistics

To view SSL proxy statistics and TLS flow counters, use the **show sslproxy statistics** command in privileged EXEC mode.

show sslproxy statistics

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1v	This command was introduced.
Cisco IOS XE Catalyst SD-WAN Release 17.13.1a	This command was modified to include the TLS flow counters in Cisco IOS XE Catalyst SD-WAN Release 17.13.1a.

Example

The following is a sample output from the **show ssl proxy statistics** command showcases SSL statistics and TLS flow counters. The fields are self-explanatory. The count for the TLS flow counter for version 1.3 is shown as 8.

```
Device# show sslproxy statistics
=========================================================
SSL Statistics:
=========================================================
Flow Selected SSL/TLS version:
TLS 1.0 Flows : 0
TLS 1.1 Flows : 0
TLS 1.2 Flows : 0
TLS 1.3 Flows : 8
```

show sslproxy status

To view the status of SSL Proxy, use the **show sslproxy status** command in privileged EXEC mode.

show sslproxy status

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	The command was introduced.
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	The output of this command was modified to remove the fields SSL Proxy Operational State and TCP Proxy Operational State.

Usage Guidelines

Example

The following is sample output from the **show sslproxy status** command.

```
Device# show sslproxy status

=========================================================

               SSL Proxy Status

=========================================================


Configuration

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

CA Cert Bundle                : /bootflash/vmanage-admin/bengaluru.pem

CA TP Label                   : PROXY-SIGNING-CA

Cert Lifetime                 : 730

EC Key type                   : P256

RSA Key Modulus               : 2048

Cert Revocation               : NONE

Expired Cert                  : drop

Untrusted Cert                : drop

Unknown Status                : drop

Unsupported Protocol Ver      : drop

Unsupported Cipher Suites     : drop

Failure Mode Action           : close

Min TLS Ver                   : TLS Version 1


Status

------
```

```
Clear Mode                    : FALSE
```

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

Field	Description
CA TP label	Default Trustpoint label for SSL proxy.
Cert Lifetime	Certificate lifetime in days.
EC Key type	Enterprise certificate key type for SSL proxy.
RSA Key Modulus	The length of the RSA key. The default key length is 2048.

show standby

To display Hot Standby Router Protocol (HSRP) information, use the **show standby** command in user EXEC or privileged EXEC mode.

show standby [**all** | **brief**]

Syntax Description

all	(Optional) Displays information for groups that are learned or don't have the **standby ip** command configured.
brief	(Optional) Displays a single-line output summarizing each standby group.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE show standby command.

The **no standby** or **no standby version** commands resets the version to 1. If standby IPv6 groups are present on the interface, then the **no standby** command is rejected because v6 groups are not supported with version 1.

You may also observe errors for the standby authentication command with version 1 because authentication isn't supported with the default version.

Examples

The following is a sample output from the **show standby** command:

```
Device# show standby

GigabitEthernet3 - Group 1
 State is Active
   8 state changes, last state change 00:30:53
```

```
 Virtual IP address is 12.1.1.100
 Active virtual MAC address is 0000.0c07.ac01 (MAC In Use)
   Local virtual MAC address is 0000.0c07.ac01 (v1 default)
 Hello time 3 sec, hold time 10 sec
   Next hello sent in 0.592 secs
 Preemption disabled
 Active router is local
 Standby router is unknown
 Priority 100 (default 100)
 Group name is "Leader" (cfgd)
 FLAGS: 1/1
 Followed by groups:
   Gi3.1 Grp 1 Active 13.1.1.100 0000.0c07.ac01 refresh 10 secs (expires in 5.728 sec)
```

The following is a sample output from the **show standby** command when HSRP version 2 is configured:

```
Device# show standby
GigabitEthernet0/0/1 - Group 94 (version 2)
  State is Active
    2 state changes, last state change 01:06:01
    Track object 8 state Up
  Virtual IP address is 10.96.194.1
  Active virtual MAC address is 0000.0c9f.f05e (MAC In Use)
    Local virtual MAC address is 0000.0c9f.f05e (v2 default)
  Hello time 1 sec, hold time 4 sec
    Next hello sent in 0.400 secs
  Authentication MD5, key-string
  Preemption enabled, delay min 180 secs
  Active router is local
  Standby router is 10.96.194.3, priority 105 (expires in 3.616 sec)
  Priority 110 (configured 110)
  Group name is "hsrp-Gi0/0/1.94-94" (default)
  FLAGS: 1/1
GigabitEthernet0/0/1 - Group 194 (version 2)
  State is Active
    2 state changes, last state change 01:06:01
    Track object 80 state Up
  Link-Local Virtual IPv6 address is FE80::5:73FF:FEA0:C2 (impl auto EUI64)
    Virtual IPv6 address 2001:10:96:194::1/64
  Active virtual MAC address is 0005.73a0.00c2 (MAC In Use)
    Local virtual MAC address is 0005.73a0.00c2 (v2 IPv6 default)
  Hello time 1 sec, hold time 4 sec
    Next hello sent in 0.352 secs
  Authentication MD5, key-string
  Preemption enabled, delay min 180 secs
  Active router is local
  Standby router is FE80::2E73:A0FF:FEB3:4AC1, priority 105 (expires in 3.888 sec)
  Priority 110 (configured 110)
  Group name is "hsrp-Gi0/0/1.94-194" (default)
  FLAGS: 1/1
```

The following is a sample output from the **show standby** command using the **brief** keyword:

```
Device# show standby brief
Interface   Grp  Pri P State   Active   Standby           Virtual IP
Gi0/0/1     94   110 P Active  local    10.96.194.3       10.96.194.1
Gi0/0/1     194  110 P Active  local    FE80::2E73:A0FF:FEB3:4AC1    FE80::5:73FF:FEA0:C2
```

The following is a sample output from the **show standby** command when HSRP MD5 authentication is configured:

```
Device# show standby

GigabitEthernet0/0/1 - Group 94 (version 2)
```

```
  State is Standby
    1 state change, last state change 01:06:09
    Track object 8 state Up
  Virtual IP address is 10.96.194.1
  Active virtual MAC address is 0000.0c9f.f05e (MAC Not In Use)
    Local virtual MAC address is 0000.0c9f.f05e (v2 default)
  Hello time 1 sec, hold time 4 sec
    Next hello sent in 0.688 secs
  Authentication MD5, key-string
  Preemption enabled, delay min 180 secs
  Active router is 10.96.194.2, priority 110 (expires in 4.272 sec)
    MAC address is cc16.7e8c.6dd1
  Standby router is local
  Priority 105 (configured 105)
  Group name is "hsrp-Gi0/0/1.94-94" (default)
```

The following is a sample output from the **show standby** command when HSRP group shutdown is configured:

```
Device# show standby

Ethernet0/0 - Group 1
State is Init (tracking shutdown)
3 state changes, last state change 00:30:59
Track object 100 state Up
Track object 101 state Down
Track object 103 state Up
```

The following is a sample output from the **show standby** command when HSRP BFD peering is enabled:

```
Device# show standby

Ethernet0/0 - Group 2
  State is Listen
    2 state changes, last state change 01:18:18
  Virtual IP address is 10.0.0.1
  Active virtual MAC address is 0000.0c07.ac02
    Local virtual MAC address is 0000.0c07.ac02 (v1 default)
  Hello time 3 sec, hold time 10 sec
  Preemption enabled
  Active router is 10.0.0.250, priority 120 (expires in 9.396 sec)
  Standby router is 10.0.0.251, priority 110 (expires in 8.672 sec)
    BFD enabled
  Priority 90 (configured 90)
  Group name is "hsrp-Et0/0-1" (default)
```

The following is a sample output from the **show standby** command displaying the state of the standby RP:

```
Device# show standby

GigabitEthernet3/25 - Group 1
State is Init (standby RP, peer state is Active)
Virtual IP address is 10.0.0.1
Active virtual MAC address is unknown
Local virtual MAC address is 0000.0c07.ac01 (v1 default)
Hello time 3 sec, hold time 10 sec
Preemption disabled
Active router is unknown
Standby router is unknown
Priority 100 (default 100)
Group name is "hsrp-Gi3/25-1" (default)
```

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

Table 45: show standby command Field Descriptions

Field	Description
Active router is	Value can be **local**, **unknown**, or an **IP address**. Address (and the expiration date of the address) of the current active hot standby router.
Active virtual MAC address	Virtual MAC address being used by the current active router.
Authentication	Authentication type configured based on the **standby authentication** command.
BFD enabled	Indicates that BFD peering is enabled on the router.
Ethernet - Group	Interface type and number and hot standby group number for the interface.
expires in	Time (in hours:minutes:seconds) in which the standby router will no longer be the standby router if the local router receives no hello packets from it.
Followed by groups:	Indicates the client HSRP groups that have been configured to follow this HSRP group.
Gratuitous ARP 14 sent, next in 7.412 secs	Number of the gratuitous ARP packet HSRP has sent and the time, in seconds, when HSRP sends the next gratuitous ARP packet. This output appears only when HSRP sends gratuitous ARP packets.
Group name is	Name of the HSRP group.
Hello time, hold time	Hello time is the time between hello packets, in seconds, based on the command. The holdtime is the time, in seconds, before other routers declare the active or standby router to be down, based on the **standby timers** command. All the routers in an HSRP group use the hello and hold- time values of the current active router. If the locally configured values are different, the variance appears in parentheses after the hello time and hold-time values.
key-string	Indicates that a key string is used for authentication. Configured key chains aren't displayed.
Local virtual MAC address	Virtual MAC address that will be used if this router became the active router. The origin of this address (displayed in parentheses) can be **default**, **bia** (burned-in address), or **confgd** (configured).
Next hello sent in	Time at which the Cisco IOS software sends the next hello packet (in hours:minutes:seconds).
P	Indicates that the router is configured to preempt.
Preemption enabled, sync delay	Indicates whether preemption is enabled or disabled. If enabled, the minimum delay is the time a higher-priority nonactive router waits before preempting the lower-priority active router. The sync delay is the maximum time a group waits for to synchronize with the IP redundancy clients.

Field	Description
Standby router is	Value can be **local**, **unknown**, or an **IP address**. IP address is the address (and the expiry date of the address) of the "standby" router (the router that is next in line to be the hot standby router).
State is	State of local router. Can be one of the following: • Active: Indicates the current hot standby router. • Standby: Indicates the router that is next in line to be the hot standby router. • Speak: Router is sending packets to claim the active or standby role. • Listen: Router is not in the active or standby state. However, if no messages are received from the active or standby router, it starts to speak. • Init or Disabled: Router isn't yet ready or able to participate in HSRP, possibly because the associated interface isn't up. HSRP groups configured on the other routers on the network, which are learned through snooping, are displayed as being in the initState. Locally configured groups with an interface that is down or groups without a specified interface IP address appear in the initState. For these cases, the Active address and Standby address fields show **unknown**. The state is listed as disabled in the fields when the **standby ip** command hasn't been specified. • Init (tracking shutdown): HSRP groups appear in the initState when HSRP group shutdown is configured and a tracked object goes down.
timeout	Duration (in seconds) for which HSRP accepts message digests based on both the old and new keys.
Tracking	Displays the list of interfaces that are being tracked and their corresponding states based on the configurations, using the **standby track** command.
Virtual IP address is, Secondary virtual IP addresses	All secondary virtual IP addresses are listed on separate lines. If one of the virtual IP addresses is a duplicate of an address configured for another device, it will be marked as **duplicate**. A duplicate address indicates that the router has failed to defend its Address Resolution Protocol (ARP) cache entry.

show standby neighbors

To display information about Hot Standby Router Protocol (HSRP) peer routers on an interface, use the **show standby neighbors** command in privileged EXEC mode.

show standby neighbors [*interface-type interface-number*]

Syntax Description

interface-type interface-number	(Optional) Interface type and number for which output is displayed.

Command Default

HSRP neighbor information is displayed for all the interfaces.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE show standby neighbors command.

Examples

The following is a sample output from the **show standby neighbors** *Ethernet0/0* command displaying the HSRP neighbors on Ethernet interface 0/0. Neighbor 10.0.0.250 is active for group 2 and standby for groups 1 and 8, and is registered with BFD.

```
Device# show standby neighbors Ethernet0/0

HSRP neighbors on Ethernet0/0
  10.0.0.250
    Active groups: 2
    Standby groups: 1, 8
    BFD enabled
  10.0.0.251
    Active groups: 5, 8
    Standby groups: 2
    BFD enabled
  10.0.0.253
    No Active groups
    No Standby groups
    BFD enabled
```

The following is a sample output from the **show standby neighbors** command displaying information for all the HSRP neighbors:

```
Device# show standby neighbors

HSRP neighbors on FastEthernet2/0
  10.0.0.2
    No active groups
    Standby groups: 1
    BFD enabled
HSRP neighbors on FastEthernet2/0
  10.0.0.1
    Active groups: 1
    No standby groups
    BFD enabled
```

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

Table 46: show standby neighbors command Field Descriptions

Field	Description
Active groups	Indicates the HSRP groups for which an interface is acting as the active peer.
Standby groups	Indicates the HSRP groups for which an interface is acting as the standby peer.
BFD enabled	Indicates that HSRP BFD peering is enabled.

show support policy route-policy

To display the control policies configured on a Cisco SD-WAN Controller, use the **show support policy route-policy** command in privileged EXEC mode.

show support policy route-policy

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
	This command was introduced.

Usage Guidelines

Use the command on a Cisco SD-WAN Controller. The command output shows the control policies configured on the Cisco SD-WAN Controller, and the TLOCs associated with each control policy.

Example

The following example shows information for a single policy, including the TLOCs of interest.

```
vsmart# show support policy route-policy

================================
  ROUTE POLICIES
================================

route-policy hub-and-spoke-v1
seq-num 46
users-count 1
action srvc/srvc-chain/tloc/tloc-list/affinity counts: 0/0/0/1/0
Policy TLOC-Interest Database:
   TLOC:172.16.255.11 : lte : ipsec Ref-Count: 1

    sequence: 1
        match tloc [SITE-LIST  (0x1) ]
            site-list: HUB (0x1234567890ab)
        action: accept
        set: [ (0x0) ]
    sequence: 11
        match route [PFX-LIST  (0x10) ]
            IPv4 prefix-list: ALL-ROUTES (0x2345678901ab)
        action: accept
        set: [TLOC-LIST  (0x20) ]
            tloc-list: HUB-TLOCS [none]
    default-action: reject, fetch_xml: 1

  Users:
  172.16.255.14, type: route, dir: out, policy: hub-and-spoke-v1 (0x3456789012ab), ctx:
0x4567890123ab, cb: 0x5678901234ab, change: no
```

show tech-support sdwan bfd

To display BFD information on Cisco IOS XE Catalyst SD-WAN devices, use the **show tech-support sdwan bfd** command in privileged EXEC mode.

show tech-support sdwan bfd [detail]

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.11.1a	This command was introduced.

Usage Guidelines

The **show tech-support sdwan bfd** command displays BFD information about devices for troubleshooting. The command displays the output of the following **show** commands:

- show sdwan bfd summary
- show platform software sdwan session
- show platform software bfd f0 summary
- show platform hardware qfp active feature bfd datapath sdwan summary
- show platform hardware qfp active feature sdwan datapath session summary

The **show tech-support sdwan bfd detail** command displays detailed BFD information about devices for troubleshooting. With the **detail** keyword, the command displays the output of the following commands:

- show sdwan bfd sessions
- show platform software sdwan session
- show platform software sdwan session adj
- show platform software ipsec ftm-msg-stats
- show platform software bfd f0
- show platform software object-manager f0 statistics
- show platform software ipsec f0 flow table
- show platform hardware qfp active feature bfd datapath sdwan all
- show platform hardware qfp active feature bfd datapath statistics

Example 1

The following is a sample output from the **show tech-support sdwan bfd** command.

```
Device#show tech-support sdwan bfd

------------------ show sdwan bfd summary ------------------

sessions-total           12
sessions-up              12
sessions-max             12
sessions-flap            2
poll-interval            600000
sessions-up-suspended    0
sessions-down-suspended  0

------------------ show platform software sdwan session ------------------
======Session Database=====
RemoteSysIP         Color               Proto SrcIp              SPort DstIp
  DPort DPubIp              PPort BFD-LD TUN-ID SA-ID     WAN-Intf (nexthop)
10.1.1.21           metro-ethernet      IPSEC 10.10.1.129         12346 10.10.1.121
  12386 10.10.1.121        12386 20011  11     603979798 GigabitEthernet0/0/1 (10.10.1.121)
10.1.1.23           metro-ethernet      IPSEC 10.10.1.129         12346 10.10.1.123
  12426 10.10.1.123        12426 20009  9      603979794 GigabitEthernet0/0/1 (10.10.1.123)
...

------------------ show platform software bfd f0 ------------------
Forwarding Manager BFD Information
Local Discri   If Handle         Src IP            Dst IP        Encap      AOM ID    Status

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

   20001          0x8         10.10.1.129       10.10.1.130      IPSEC       403      Done

   20002          0x8         10.10.1.129       10.10.1.135      IPSEC       404      Done

...

------------------ show platform hardware qfp active feature bfd datapath sdwan summary
-----------
Total number of session: 12
LD       SrcIP             DstIP         TX          RX      Encap      State     AppProbe
    AdjId
20001  10.10.1.129     10.10.1.130     23973      23971      IPSEC      Up        YES
 GigabitEthernet0/0/1 (0xf800005f)
20002  10.10.1.129     10.10.1.135     22769      22766      IPSEC      Up        YES
 GigabitEthernet0/0/1 (0xf800006f)
...

------------------ show platform hardware qfp active feature sdwan datapath session summary
 ---------
Src IP          Dst IP          Src Port Dst Port   Encap    Uidb     Bfd Discrim PMTU
 Flags
------          ------          -------- -------    ------   -------  ----------- -----
 -----
10.10.1.129     10.10.1.71      12346    12346      CTRL     0        0           0
 0x0
10.10.1.129     10.10.1.125     12346    12406      IPSEC    65527    20004       1442
 0x0
...
```

Example 2

The following is a sample output from the **show tech-support sdwan bfd detail** command.

```
Device#show tech-support sdwan bfd detail

------------------ show sdwan bfd sessions ------------------
                                       SOURCE TLOC      REMOTE TLOC
             DST PUBLIC                        DST PUBLIC         DETECT      TX

SYSTEM IP        SITE ID     STATE       COLOR            COLOR            SOURCE IP
                                 IP                                              PORT
   ENCAP  MULTIPLIER  INTERVAL(msec  UPTIME          TRANSITIONS
-------------------------------------------------------------------------------------
10.1.1.21        121         up          metro-ethernet   default          10.10.1.129
                                 10.10.1.121                                     12386
   ipsec  7           1000           0:01:30:24      1
10.1.1.23        123         up          metro-ethernet   public-internet  10.10.1.129
                                 10.10.1.123                                     12426
   ipsec  7           1000           0:02:50:15      0
...

------------------ show platform software sdwan session ------------------

======Session Database=====
RemoteSysIP         Color               Proto SrcIp               SPort DstIp
  DPort DPubIp              PPort BFD-LD TUN-ID SA-ID     WAN-Intf (nexthop)
10.1.1.21           metro-ethernet      IPSEC 10.10.1.129         12346 10.10.1.121
  12386 10.10.1.121        12386 20011  11     603979798 GigabitEthernet0/0/1 (10.10.1.121)
10.1.1.23           metro-ethernet      IPSEC 10.10.1.129         12346 10.10.1.123
  12426 10.10.1.123        12426 20009  9      603979794 GigabitEthernet0/0/1 (10.10.1.123)
...

------------------ show platform software sdwan session adj ------------------

============  Adjacency Database =============
Index  Interface           IP address       Same-Cable  is-p2p  adj-exist resolved
ref-count      handle
(0):   GigabitEthernet0/0/1(8),       10.10.1.130,     1,          0,       1,       1,
       1,             0x7F543F07B518
(1):   GigabitEthernet0/0/1(8),       10.10.1.135,     1,          0,       1,       1,
       1,             0x7F543F07A5C8
...

------------------ show platform software ipsec ftm-msg-stats ------------------

            MSG Type   From FTM   Suppressed        OK        ERR
            CREATE         12            0         12         0
            DELETE          0            0          0         0
         REKEY(IN)          0            0          0         0
        REKEY(OUT)          1            0          1         0

           Ring Name      Read    Write   ReadERR  WriteERR ItemCount
           DCR Ring          0        0         0         0         0
           DDM Ring          0        0         0         0         0
 ftm_msg_rate(per second) 100

------------------ show platform software bfd f0 ------------------

Forwarding Manager BFD Information

Local Discri   If Handle         Src IP            Dst IP        Encap      AOM ID    Status

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

   20001          0x8         10.10.1.129       10.10.1.130      IPSEC       403       Done

   20002          0x8         10.10.1.129       10.10.1.135      IPSEC       404       Done
```

```
...

------------------ show platform software object-manager f0 statistics ------------------

Forwarding Manager Asynchronous Object Manager Statistics

Object update: Pending-issue: 0, Pending-acknowledgement: 0
Batch begin:   Pending-issue: 0, Pending-acknowledgement: 0
Batch end:     Pending-issue: 0, Pending-acknowledgement: 0
Command:       Pending-acknowledgement: 0
Total-objects: 560
Stale-objects: 0
Resolve-objects: 0
Childless-delete-objects: 0
Backplane-objects: 0
Error-objects: 0
Number of bundles: 0
Paused-types: 3

------------------ show platform software ipsec f0 flow table ------------------

Flow id  QFP SA hdl  SPI         local IP                                lport  remote IP
                                rport  dir       proto  mode
-------------------------------------------------------------------------------------------
1        6           0x000102    10.10.1.129                           12346  10.10.1.130
                               12406  inbound   esp    transport
2        26          0x000255    10.10.1.129                           12346  10.10.1.130
                               12406  outbound  esp    transport
...

------------------ show platform hardware qfp active feature bfd datapath sdwan all
------------------

Total number of session: 12

LD                    : 20001
My Private IP         : 10.10.1.129
Remote Private IP     : 10.10.1.130
Tx Stats              : 24060
Rx Stats              : 24058
Encap Type            : IPSEC
State                 : Up
AppProbe              : YES
IPSec Out SA ID       : 603979778
Tunnel Rec ID         : 1
IfName                : GigabitEthernet0/0/1 (0xf800005f)
Uidb                  : 65528
Config Tx Timer       : 1000000
Conig Detect Timer    : 7000000
Actual Tx Timer       : 1000000
Actual Detect Timer   : 7000000
My Pub IP             : 10.10.1.129
My Pub Port           : 12346
My Symmetric NAT IP   : 0.0.0.0
My Symmetric NAT Port : 0
Remote public IP      : 10.10.1.130
Remote public Port    : 12406
MTU(config), Actual   : 1442, 1442
Farend PMTU           : 1442
My Capabilities       : 0x160
Remote Capabilities   : 0x160
SDWAN BFD flags       : ||||
local_color           : 3
```

```
Ipsec Overhead        : 38
PFR stats for SLA default (addr:df297530)
 Number of pkts  : 30
 Loss Count      : 0
 Latency(1/16ms) : 416
 Jitter(1/16ms)  : 96
Following are SDWAN stats
 Echo Tx         : 23829
 Echo Rx         : 23827
 PMTU Tx         : 231
 PMTU RX         : 231
AppProbeID  Valid  NextProbeID    StatAddr    #Packets    Loss   Latency(1/16ms)
Jitter(1/16ms)
    1         N         0         df297548           0       0                 0
       0
    2         N         0         df297560           0       0                 0
       0
...

------------------ show platform hardware qfp active feature bfd datapath statistics
------------------
QFP BFD global statistics

CPP num: 0
 Data Path IPC Statistics:
  IPC Tx: 31, IPC Rx: 31

 Data Path Session Statistics:
  Session Added: 12, Removed: 0
  Session Up: 12, Down: 0, Init: 0

 Data Path Memory Chunk Statistics:
  Alloc: 12, Free: 0, Fail: 0
  Chunk Add: 0, Return: 0

 Data Path BFD ingress packets Statistics:
  Total receive: 272567, Punt to PI: 0
  Drop due to error: 0, Consume normally: 0

 Data Path BFD SDWAN packets Statistics:
  PktSb Not Found: 0, No Bfd session: 0, Bfd AdminDown: 0
  BFD Corrupted TLV: 0, BFD No TLV: 0
  No Tunnel Adj: 0, Invalid Adj2: 0, Physical Adj Invalid: 0
  Pmtu tx error: 0, Pmtu rx error: 0, Pmtu disabled: 14
  Echo Tx error: 0, Echo Rx error: 0
  tloc ipc: 0, Pmtu ipc: 12, Bfd state ipc: 16, bfd timer ipc: 0
  Oce chain invalid: 0
```

show track

To display information about objects that are tracked by the tracking process, use the **show track** command in privileged EXEC mode.

show track *track-number* [**brief** | **interface** [**brief**] | **ip** [**route** | **sla**] [**brief**] | **application** [**brief**] | **WORD** [**map**] | **stub-object** [**brief**] | **service** [**brief**] | **resolution** | **summary** | **timers**]

Syntax Description

track-number	(Optional) Specifies the track number that is being tracked. The range is from 1 to 1000.
WORD	(Optional) Displays track object string.
map	(Optional) Displays track object map information.
application	(Optional) Displays application objects.
brief	(Optional) Displays a single line of information related to the preceding argument or keyword.
endpoint-tracker	(Optional) Displays endpoint object tracker.
interface	(Optional) Displays interface objects.
iproutesla	(Optional) Displays tracked IP route or sla objects.
ipv6route	(Optional) Displays tracked IPv6 route objects.
resolution	(Optional) Displays resolution of ipv4 or ipv6 tracked parameters.
service	(Optional) Displays service objects.
timers	(Optional) Displays polling interval timers.

Command Default

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command was introduced.

Usage Guidelines

For usage guidelines, see the Cisco IOS XE show track command.

Example

The following is a sample output from the **show track** command:

```
Device# show track 8
Track 8
  IP route 0.0.0.0 0.0.0.0 reachability
  Reachability is Up (OMP)
    10 changes, last change 1w3d
  VPN Routing/Forwarding table "509"
  First-hop interface is Sdwan-system-intf
  Tracked by:
    HSRP GigabitEthernet0/0/1.94 94
    Track List 7
```

show uidp statistics

To display UIDP statistics, use the **show uidp statistics** command in privileged EXEC mode.

show uidp statistics

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	This command was introduced.

Examples

The following sample output displays UIDP statistics.

```
Device# show uidp statistics
Add/Delete Stats
---------------------------------------
Total Users added            : 22
Total Usergroups added       : 12
Total SGT added              : 0
Total Users deleted          : 0
Total Usergroups deleted     : 0
Total SGT deleted            : 0
---------------------------------------
 Add/Delete Error Stats
---------------------------------------
 User add error              : 0
 Usergroup add error         : 0
 SGT add error               : 0
 User delete error           : 0
 Usergroups delete error     : 0
 SGT delete error            : 0
---------------------------------------
 Memory allocation error Stats
---------------------------------------
 ipvrf key list create error : 0
 Index list create error     : 0
 Memory allocation error     : 0
 Invalid binding event       : 0
-----------------------------------------------
 DB Add/Delete Bindings stats
-----------------------------------------------
 Total IP User binding added             : 341
 Total IP User binding delete            : 0
 Total IP User binding add error         : 0
 Total IP User binding delete error      : 0
 Total User Usergroups binding added        : 20
 Total User Usergroups binding deleted      : 0
 Total User Usergroups binding add error    : 0
 Total User Usergroups binding delete error : 0
```

Related Commands

Command	Description
show uidp user-group all	Displays UIDP user group info.
show uidp user ip	Displays the user information by IP address.

show uidp user-group all

To display UIDP user group information, use the **show uidp user-group all** command in privileged EXEC mode.

show uidp user-group all

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	This command was introduced.

Examples

The following sample output displays UIDP user group info.

```
Device# show uidp user-group all
Total Usergroups : 12
-------------------------
SDWAN-IDENTITY.CISCO.COM/Builtin/Users
User Identity Groups:Employee
User Identity Groups:TestUserGroup-1
null
Unknown
sdwan-identity.cisco.com/S-1-5-32-545
S-1-5-21-787885371-2815506856-1818290038-513
SDWAN-IDENTITY.CISCO.COM/Users/Domain Users
cisco
eng
dev
mgmt
cEdge-identity#
cEdge-identity#sh uidp user-group us
cEdge-identity#sh uidp user ?
  all   Show all users info
  ip    Show user info by ip
  name  Show user info by user name
```

Related Commands

Command	Description
show uidp statistics	Displays UIDP statistics.
show uidp user ip	Displays the user information by IP address.

show uidp user ip

To display the user information by IP address, use the **show uidp user ip** command in privileged EXEC mode.

show uidp user ip

Command Default None

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.9.1a	This command was introduced.

Examples

The following sample output displays the user information by IP address.

```
Device# show uidp user ip
 User Info 1 : TestUser0@SDWAN-IDENTITY.CISCO.COM
cEdge-identity#sh uidp user name TestUser0@SDWAN-IDENTITY.CISCO.COM
------------------------------------------------------------------------------
User Id    User Name                          IP address
    VRF   Usergroup  Usergroup Name
------------------------------------------------------------------------------
1          TestUser0@SDWAN-IDENTITY.CISCO.COM   72.1.1.7
    0     1          SDWAN-IDENTITY.CISCO.COM/Builtin/Users

          5          Unknown

          6          sdwan-identity.cisco.com/S-1-5-32-545

          7          S-1-5-21-787885371-2815506856-1818290038-513

          8          SDWAN-IDENTITY.CISCO.COM/Users/Domain Users
```

Related Commands

Command	Description
show uidp statistics	Displays UIDP statistics.
show uidp user-group all	UIDP user group information.

show utd engine standard config

To display the Unified Threat Defense (UTD) configuration, use the **show utd engine standard config** command in user EXEC mode.

show utd engine standard config

Command Default None

Command Modes

User EXEC (>)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	This command was introduced.

Examples

The following sample output displays the unified threat defense (UTD) configuration.

```
Device# show utd engine standard config
TD Engine Standard Configuration:


Unified Policy: Enabled


URL-Filtering Cloud Lookup: Enabled


URL-Filtering On-box Lookup: Disabled


File-Reputation Cloud Lookup: Disabled


File-Analysis Cloud Submission: Disabled


UTD TLS-Decryption Dataplane Policy: Enabled


Flow Logging: Disabled


UTD VRF table entries:

Policy: uni-utd

 Threat Profile: uips


VirtualPortGroup Id: 1


UTD threat-inspection profile table entries:

Threat profile: uips

 Mode: Intrusion Prevention
```

```
 Policy: Balanced
 Logging level: Error

UTD threat-inspection whitelist profile table entries:
 UTD threat-inspection whitelist profile table is empty

UTD web-filter profile table entries
 UTD web-filter profile table is empty

UTD TLS-Decryption profile table entries
 UTD TLS-Decryption profile table is empty

UTD File analysis table entries
 UTD File analysis profile table is empty

UTD File reputation table entries
 UTD File reputation profile table is empty
```

show utd unified-policy

To display the unified policy configuration, use the **show utd unified-policy** command in user EXEC mode.

show utd unified-policy

Command Default

None

Command Modes

User EXEC (>)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	This command was introduced.

Examples

The following sample output displays the unified policy configuration.

```
Device# show utd unified-policy
Unified Policy is enabled
```

```
Config State : MT Config Sync Complete

Bulk download Timer State  : Stopped

Messages sent in current transaction: 0

Config download queue size: 0

UTD TLS-decryption dataplane policy is enabled
```

show vrrp

To display the status of configured Virtual Router Redundancy Protocol (VRRP) groups on a device, use the **show vrrp** command in privileged EXEC mode.

show vrrp *group number* [**GigabitEthernet** | **ipv4** | **all** | **brief** | **detail** | **statistics**]

Syntax Description

group number	VRRP group number. The range is from 1–255.
GigabitEthernet	(Optional) Displays GigabitEthernet information for IEEE 802.3z.
ipv4	(Optional) Displays information about IPv4 groups.
all	(Optional) Displays information about all VRRP groups, including groups in a disabled state.
brief	(Optional) Displays a summary view of the VRRP group information.
detail	(Optional) Displays information about all VRRP groups, including statistical information.
statistics	(Optional) Displays statistical information about the VRRP groups.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.7.1a	This command is supported for Cisco Catalyst SD-WAN.

Usage Guidelines

If no group is specified, the status for all groups is displayed.

For usage guidelines, see the Cisco IOS XE show vrrp command.

Examples

The following is a sample output from the **show vrrp detail** command:

```
Device# show vrrp detail
GigabitEthernet2 - Group 1 - Address-Family IPv4
 State is BACKUP
 State duration 2 hours 13 mins 4 secs
 Virtual IP address is 10.10.1.10
 Virtual MAC address is 0000.5E00.0101
 Advertisement interval is 1000 msec
```

```
 Preemption enabled
 Priority is 100
    Track object 1 state UNDEFINED decrement 10
 Router is 10.1.1.1, priority is 180
 Master Advertisement interval is 1000 msec (learned)
 Master Down interval is 3609 msec (expires in 3319 msec)
 tloc-change increase-preference 333 configured
 FLAGS: 1/1
```

The following is a sample output from the **show vrrp** command:

```
Device# show vrrp
Ethernet1/0 - Group 1
State is Master
Virtual IP address is 10.2.0.10
Virtual MAC address is 0000.5e00.0101
Advertisement interval is 3.000 sec
Preemption is enabled
 min delay is 0.000 sec
Priority 100
 Track object 1 state down decrement 15
Master Router is 10.2.0.1 (local), priority is 100
Master Advertisement interval is 3.000 sec
Master Down interval is 9.609 sec
Ethernet1/0 - Group 2
State is Master
Virtual IP address is 10.0.0.20
Virtual MAC address is 0000.5e00.0102
Advertisement interval is 1.000 sec
Preemption is enabled
 min delay is 0.000 sec
Priority 95
Master Router is 10.0.0.1 (local), priority is 95
Master Advertisement interval is 1.000 sec
Master Down interval is 3.628 sec
```

The following is a sample output from the **show vrrp** command, displaying peer RP state information:

```
Device# show vrrp
Ethernet0/0 - Group 1
  State is Init (standby RP, peer state is Master)
  Virtual IP address is 172.24.1.1
  Virtual MAC address is 0000.5e00.0101
  Advertisement interval is 1.000 sec
  Preemption enabled
  Priority is 255
  Master Router is 172.24.1.1 (local), priority is 255
  Master Advertisement interval is 1.000 sec
  Master Down interval is 3.003 sec
```

The following is a sample output from the **show vrrp** command, displaying information about a configured VRRS group name:

```
Device# show vrrp
GigabitEthernet0/0/0 - Group 1
 State is Master
 Virtual IP address is 10.0.0.7
 Virtual MAC address is 0000.5e00.0101
 Advertisement interval is 1.000 sec
 Preemption enabled
 Priority is 100
 VRRS Group name CLUSTER1 ! Configured VRRS Group Name
```

```
 Master Router is 10.0.0.1 (local), priority is 100
 Master Advertisement interval is 1.000 sec
 Master Down interval is 3.609 sec
```

The following is a sample output from the **show vrrp** command, displaying information when an object is being tracked:

```
Device# show vrrp
Ethernet0/0 - Group 1 - Address-Family IPv4
  State is BACKUP
  State duration 1 mins 41.856 secs
  Virtual IP address is 172.24.1.253
  Virtual MAC address is 0000.5E00.0101
  Advertisement interval is 1000 msec
  Preemption enabled
  Priority is 80 (configured 100)
    Track object 1 state Down decrement 20
  Master Router is 172.24.1.2, priority is 100
  Master Advertisement interval is 1000 msec (learned)
  Master Down interval is 3609 msec (expires in 3297 msec)
```

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

Table 47: show vrrp command Field Descriptions

Field	Description
Ethernet1/0 - Group	Interface type and number, and VRRP group number.
State is	Role this interface plays within VRRP (master or backup).
Advertisement interval is	Interval at which the device sends VRRP advertisements when it is the master virtual device. This value is configured with the **vrrp timers advertise** command.
Priority	Priority of the interface.
Track object	Object number representing the object to be tracked.
state	State value (up or down) of the object being tracked.
decrement	Amount by which the priority of the device is decremented (or incremented) when the tracked object goes down (or comes back up).
Master Router is	IP address of the current master virtual device.
priority is	Priority of the current master virtual device.
Master Advertisement interval is	Advertisement interval, in seconds, of the master virtual device.

Field	Description
Master Down interval is	Calculated time, in seconds, that the master virtual device can be down before the backup virtual device takes over.

The following is a sample output from the **show vrrp brief** command:

```
Device# show vrrp brief
Interface    Grp  A-F Pri   Time Own Pre  State   Master addr/Group addr
  Et1/0       1   IPv4 150    0   N   Y   MASTER  10.0.0.1(local) 10.0.0.10
  Et1/0       1   IPv6 100    0   N   Y   INIT    AF-UNDEFINED no address
  Et1/0       6   IPv6 150    0   N   Y   MASTER  FE80::1(local) FE80::100
```

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

Table 48: show vrrp brief command Field Descriptions

Field	Description
Interface	Interface type and number.
Grp	VRRP group to which this interface belongs.
Pri	VRRP priority number for this group.
Time	Calculated time that the master virtual device can be down before the backup virtual device takes over.
Own	IP address owner.
Pre	Preemption status. Y indicates that preemption is enabled. If this field is empty, preemption is disabled.
State	Role this interface plays within VRRP (master or backup).
Master addr	IP address of the master virtual device.
Group addr	IP address of the virtual device.

show wireless-lan radio

To display the radio parameters of the wireless LAN, use the **show wireless-lan radio** command in user EXEC mode.

show wireless-lan radio

Syntax Description This command has no keywords or arguments.

Command Default None

Command Modes User EXEC (>)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	This command was introduced.

Examples

The following sample output displays the radio parameters of the wireless LAN.

```
Device# show wireless-lan radio

band  admin  oper  TxPwr  Channel
 ----  -----  ----  -----  --------------------
 2.4g     on    up   2dbm  1
  5g      on    up   2dbm  100,104,108,112
```

show wireless-lan wlan

To display information about the wireless SSID, use the **show wireless-lan wlan** command in user EXEC mode.

show wireless-lan wlan

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

User EXEC (>)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	This command was introduced.

Examples

The following sample output displays information about the wireless SSID.

```
Device# show wireless-lan wlan

  wlan  oper  vlan  #client  SSID
 ----  ----  ----  -------  -----------------
    1    up    19        0  119
    2    up   105        0  122
    3    up    23        0  123
    4    up   100        0  hello
    5    up    22        0  hello2
```

show wireless-lan client

To display information about the wireless clients in a wireless LAN, use the **show wireless-lan client** command in user EXEC mode.

show wireless-lan client

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command Modes

User EXEC (>)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	This command was introduced.

Examples

The following sample output displays information about the wireless clients in the wireless LAN.

```
Device# show wireless-lan client

 Client-MAC-Addr    band  status         SSID
 -----------------  ----  -------------  -------------
 64:BC:0C:65:8B:4C    5g  Associated     hello
```

show zone-pair security

To display the source zone, destination zone, and policy attached to the zone-pair, use the **show zone-pair security** command in privileged EXEC mode.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.11.1a	This command is supported in Cisco Catalyst SD-WAN

Usage Guidelines

For usage guidelines, see the Cisco IOS XE show zone-pair security command.

Example

The following example displays the source zone, destination zone, and policy attached to the zone-pair.

```
Device#show zone-pair security
Zone-pair name ZP_zone1_zone1_seq_1 1
```

```
Source-Zone zone1  Destination-Zone zone1
service-policy seq_1
```

verify

To verify the file integrity of a software image stored in the device bootflash, use the **verify** command in privileged EXEC mode.

verify *image*

Syntax Description

image	Software image stored in the device bootflash. Specify the file as follows: **bootflash:***filename*

Command Default

This command has no default behavior.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.6.1a	Command qualified for use in Cisco SD-WAN Manager CLI templates.

Example

```
Device# verify bootflash:image.bin
Verifying file integrity of
bootflash:image.bin.....................................................................

Embedded Hash   SHA1 : 0123456789ABCDEF0123456789ABCDEF01234567
Computed Hash   SHA1 : 0123456789ABCDEF0123456789ABCDEF01234567
Starting image verification
Hash Computation:    100%Done!
Computed Hash   SHA2: 0123456789abcdef0123456789abcdef
                      0123456789abcdef0123456789abcdef
                       0123456789abcdef0123456789abcdef
                       0123456789abcdef0123456789abcdef

Embedded Hash   SHA2: 0123456789abcdef0123456789abcdef
                       0123456789abcdef0123456789abcdef
                       0123456789abcdef0123456789abcdef
                       0123456789abcdef0123456789abcdef

Digital signature successfully verified in file bootflash:image.bin
```

vdiagnose vmanage cluster

To run diagnostics on a Cisco SD-WAN Manager cluster, use the **vdiagnose vmanage cluster** command in privileged EXEC mode on Cisco SD-WAN Manager.

vdiagnose vmanage cluster [*verbose*]

Syntax Description

cluster	Run diagnostics on a Cisco SD-WAN Managercluster.
verbose	(Optional) View a verbose version of the **vdiagnose vmanage cluster** command.

Command Default

None

Command Modes

Privileged EXEC mode (#)

Command History

Release	Modification
Cisco IOS XE Catalyst SD-WAN Release 17.12.1a	This command is supported in Cisco Catalyst SD-WAN.

Usage Guidelines

Run the **vdiagnose vmanage cluster** command directly from the CLI on any Cisco SD-WAN Manager node in a cluster.

The **vdiagnose vmanage cluster** command tests the following for a Cisco SD-WAN Manager cluster:

- **Mandatory interfaces operational status**: Tests the operational status of the cluster interface on a Cisco SD-WAN Manager node.
- **Cluster interface reachability:** Runs a ping test on all cluster node interfaces in a network, verifying full interface reachability across all Cisco SD-WAN Manager nodes.
- **Cluster services health status:** Provides the health status of cluster services running on one or more Cisco SD-WAN Manager nodes.
- **Cluster service reachability:** Performs nping test for cluster services running on Cisco SD-WAN Manager nodes in the cluster.
- **Current node container status:** Provides the docker container status of cluster services running on the current Cisco SD-WAN Manager node.

Perform the following steps to run the **vdiagnose vmanage cluster** diagnostics command from the CLI on any Cisco SD-WAN Manager node in a cluster:

1. From the Cisco SD-WAN Manager menu, choose **Tools** > **SSH Terminal**.
2. Choose **vManage** as the device in the left pane. The **SSH Terminal** window opens in the right pane.
3. Enter the username and password to log in to Cisco SD-WAN Manager.
4. Enter the **vdiagnose vmanage cluster** command to run a diagnostic test on a Cisco SD-WAN Manager cluster.
5. (Optional) Enter the **vdiagnose vmanage cluster verbose** command to view the verbose of the diagnostic test executed on a Cisco SD-WAN Manager cluster.

Example

The following example shows the results of the diagnostics run on a Cisco SD-WAN Manager controller to test a Cisco SD-WAN Manager cluster:

```
Device#vdiagnose vmanage cluster
Running vdiagnostics, this can take some time...
Current Date and time is 2023-08-03 15:37:02.897422


Personality is Vmanage
Running vdiagnostics for Cluster, this can take some time..

Current node: 10.0.105.39

Checking interfaces operational status
======================================
        eth5 - Cluster                                                  PASS

Checking cluster interface reachability
=======================================
        Full interface reachability across all nodes                    PASS

Checking services health status
===============================
        Services healthy across all nodes                               PASS

Checking service reachability
=============================
        Full service reachability across all nodes                      PASS

Checking current node container status
======================================
        All cluster services containers are up                          PASS
```