System Management Commands

arp

To display the contents of the Address Resolution Protocol (ARP) table, use the **arp** command in boot loader mode.

arp [*ip_address*]

Syntax Description

ip_address	(Optional) Shows the ARP table or the mapping for a specific IP address.

Command Default

No default behavior or values.

Command Modes

Boot loader

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

The ARP table contains the IP-address-to-MAC-address mappings.

Examples

This example shows how to display the ARP table:

```
Device: arp 172.20.136.8
arp'ing 172.20.136.8...
172.20.136.8 is at 00:1b:78:d1:25:ae, via port 0
```

boot

To load and boot an executable image and display the command-line interface (CLI), use the **boot** command in boot loader mode.

boot *flag* *filesystem:/file-url...*

Syntax Description

filesystem:	Alias for a file system. Use **flash:** for the system board flash device; use **usbflash0:** for USB memory sticks.
/file-url	Path (directory) and name of a bootable image. Separate image names with a semicolon.

Command Default

No default behavior or values.

Command Modes

Boot loader

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

When you enter the **boot** command without any arguments, the device attempts to automatically boot the system by using the information in the BOOT environment variable, if any.

If you supply an image name for the *file-url* variable, the **boot** command attempts to boot the specified image.

When you specify boot loader **boot** command options, they are executed immediately and apply only to the current boot loader session.

These settings are not saved for the next boot operation.

Filenames and directory names are case sensitive.

Example

This example shows how to boot the device using the *new-image.bin* image:

```
Device: set BOOT flash:/new-images/new-image.bin
Device: boot
```

After entering this command, you are prompted to start the setup program.

boot system

To specify which system image to load during the next boot cycle, use the **boot system** command in global configuration mode. To remove the startup system image specification, use the **no** form of this command.

boot system {*filesystem: /file-url* | **switch all** *filesystem: /file-url*}
no boot system [{*filesystem: /file-url* | **switch all [***filesystem: /file-url***]**}]

Syntax Description

filesystem:	Specifies a file system. The options are *bootflash:*, *flash:*, *ftp:*, *http:*, *sftp:*, and *tftp:*.
switch all	Sets the system image for all devices in the stack.
/file-url	The URL of the system image to load at system startup.

Command Default

No default behavior or values.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Examples

This example shows how to boot the system image file named cat9k_lite_iosxe.16.09.03.SPA.bin from the bootflash:

```
Device(config)# boot system bootflash:cat9k_lite_iosxe.16.09.03.SPA.bin
```

This example shows how to boots all devices in the stack from a network server with an IP address:

```
Device(config)# boot system switch all tftp://10.11.15.10/cat9k_lite_iosxe.16.09.03.SPA.bin
```

cat

To display the contents of one or more files, use the **cat** command in boot loader mode.

cat *filesystem:/file-url...*

Syntax Description

filesystem:	Specifies a file system.
/file-url	Specifies the path (directory) and name of the files to display. Separate each filename with a space.

Command Default

No default behavior or values.

Command Modes

Boot loader

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Filenames and directory names are case sensitive.

If you specify a list of files, the contents of each file appears sequentially.

Examples

This example shows how to display the contents of an image file:

```
Device: cat flash:image_file_name
version_suffix: universal-122-xx.SEx
version_directory: image_file_name
image_system_type_id: 0x00000002
image_name: image_file_name.bin
ios_image_file_size: 8919552
total_image_file_size: 11592192
image_feature: IP|LAYER_3|PLUS|MIN_DRAM_MEG=128
image_family: family
stacking_number: 1.34
board_ids: 0x00000068 0x00000069 0x0000006a 0x0000006b
info_end:
```

copy

To copy a file from a source to a destination, use the **copy** command in boot loader mode.

copy *filesystem:/source-file-url filesystem:/destination-file-url*

Syntax Description

filesystem:	Alias for a file system. Use **usbflash0:** for USB memory sticks.
/source-file-url	Path (directory) and filename (source) to be copied.
/destination-file-url	Path (directory) and filename of the destination.

Command Default

No default behavior or values.

Command Modes

Boot loader

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Filenames and directory names are case sensitive.

Directory names are limited to 127 characters between the slashes (/); the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.

Filenames are limited to 127 characters; the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.

If you are copying a file to a new directory, the directory must already exist.

Examples

This example shows how to copy a file at the root:

```
Device: copy usbflash0:test1.text usbflash0:test4.text
File "usbflash0:test1.text" successfully copied to "usbflash0:test4.text"
```

You can verify that the file was copied by entering the **dir** *filesystem:* boot loader command.

copy startup-config tftp:

To copy the configuration settings from a switch to a TFTP server, use the **copy startup-config tftp:** command in Privileged EXEC mode.

copy startup-config tftp: *remote host {ip-address}/{name}*

Syntax Description

remote host {ip-address}/{name}	Host name or IP-address of Remote host.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Release 16.1	This command was introduced.

Usage Guidelines

To copy your current configurations from the switch, run the command **copy startup-config tftp:** and follow the instructions. The configurations are copied onto the TFTP server.

Then, login to another switch and run the command **copy tftp: startup-config** and follow the instructions. The configurations are now copied onto the other switch.

Examples

This example shows how to copy the configuration settings onto a TFTP server:

```
Device: copy startup-config tftp:
Address or name of remote host []?
```

copy tftp: startup-config

To copy the configuration settings from a TFTP server onto a new switch, use the **copy tftp: startup-config** command in Privileged EXEC mode on the new switch.

copy tftp: startup-config *remote host {ip-address}/{name}*

Syntax Description

remote host {ip-address}/{name}	Host name or IP-address of Remote host.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Release 16.1	This command was introduced.

Usage Guidelines

After the configurations are copied, to save your configurations, use **write memory** command and then either reload the switch or run the **copy startup-config running-config** command.

Examples

This example shows how to copy the configuration settings from the TFTP server onto a switch:

```
Device: copy tftp: startup-config
Address or name of remote host []?
```

debug voice diagnostics mac-address

To enable debugging of voice diagnostics for voice clients, use the **debug voice diagnostics mac-address** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug voice diagnostics mac-address *mac-address1* **verbose mac-address** *mac-address2* **verbose**
nodebug voice diagnostics mac-address *mac-address1* **verbose mac-address** *mac-address2* **verbose**

Syntax Description

voice diagnostics	Configures voice debugging for voice clients.
mac-address *mac-address1* **mac-address** *mac-address2*	Specifies MAC addresses of the voice clients.
verbose	Enables verbose mode for voice diagnostics.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

The following is sample output from the **debug voice diagnostics mac-address** command and shows how to enable debugging of voice diagnostics for voice client with MAC address of 00:1f:ca:cf:b6:60:

```
Device# debug voice diagnostics mac-address 00:1f:ca:cf:b6:60
```

debug platform condition feature multicast controlplane

To enable radioactive tracing for the Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) snooping features, use the **debug platform condition feature multicast controlplane** command in privileged EXEC mode. To disable radioactive tracing, use the **no** form of this command.

debug platform condition feature multicast controlplane {{igmp-debug | pim} group-ip {*ipv4 address* | *ipv6 address***} | {mld-snooping | igmp-snooping} mac** *mac-address* **ip {***ipv4 address* | *ipv6 address***} vlan** *vlan-id* **} level {debug | error | info | verbose | warning}**
no debug platform condition feature multicast controlplane {{igmp-debug | pim} group-ip {*ipv4 address* | *ipv6 address***} | {mld-snooping | igmp-snooping} mac** *mac-address* **ip {***ipv4 address* | *ipv6 address***} vlan** *vlan-id* **} level {debug | error | info | verbose | warning}**

Syntax Description

igmp-debug	Enables IGMP control radioactive tracing.
pim	Enables Protocol Independent Multicast (PIM) control radioactive tracing.
mld-snooping	Enables MLD snooping control radioactive tracing.
igmp-snooping	Enables IGMP snooping control radioactive tracing.
mac *mac-address*	MAC address of the receiver.
group-ip {*ipv4 address* | *ipv6 address***}**	IPv4 or IPv6 address of the igmp-debug or pim group.
ip {*ipv4 address* | *ipv6 address***}**	IPv4 or IPv6 address of the mld-snooping or igmp-snooping group.
vlan *vlan-id*	VLAN ID. The range is from 1 to 4094.
level	Enables debug severity levels.
debug	Enables debugging level.
error	Enables error debugging.
info	Enables information debugging.
verbose	Enables detailed debugging.
warning	Enables warning debugging.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

The following example shows how to enable radioactive tracing for IGMP snooping:

```
Device# debug platform condition feature multicast controlplane igmp-snooping mac
000a.f330.344a ip 10.1.1.10 vlan 550 level warning
```

Related Commands

Command	Description
clear debug platform condition all	Removes the debug conditions applied to a platform.
debug platform condition	Filters debugging output for **debug** commands on the basis of specified conditions.
debug platform condition start	Starts conditional debugging on a system.
debug platform condition stop	Stops conditional debugging on a system.
show platform condition	Displays the currently active debug configuration.

debug platform condition mac

To enable radioactive tracing for MAC learning, use the **debug platform condition mac** command in privileged EXEC mode. To disable radioactive tracing for MAC learning, use the **no** form of this command.

debug platform condition mac **{***mac-address* **{control-plane | egress | ingress} | access-list** *access-list name* **{egress | ingress}}**
no debug platform condition mac **{***mac-address* **{control-plane | egress | ingress} | access-list** *access-list name* **{egress | ingress}}**

Syntax Description

mac *mac-address*	Filters output on the basis of the specified MAC address.
access-list *access-list name*	Filters output on the basis of the specified access list.
control-plane	Displays messages about the control plane routines.
egress	Filters output on the basis of outgoing packets.
ingress	Filters output on the basis of incoming packets.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

The following example shows how to filter debugging output on the basis of a MAC address:

```
Device# debug platform condition mac bc16.6509.3314 ingress
```

Related Commands

Command	Description
show platform condition	Displays the currently active debug configuration.
debug platform condition	Filters debugging output for **debug** commands on the basis of specified conditions.
debug platform condition start	Starts conditional debugging on a system.
debug platform condition stop	Stops conditional debugging on a system.
clear debug platform condition all	Removes the debug conditions applied to a platform.

debug platform rep

To enable debugging of Resilient Ethernet Protocol (REP) functions, use the **debug platform rep** command in privileged EXEC mode. To remove the specified condition, use the **no** form of this command.

debug platform rep {all | error | event | packet | verbose}
no debug platform rep {all | error | event | packet | verbose}

Syntax Description

all	Enables all REP debugging functions.
error	Enables REP error debugging.
event	Enables REP event debugging.
packet	Enables REP packet debugging.
verbose	Enables REP verbose debugging.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

The following example shows how to enable debugging for all functionss:

```
Device# debug platform rep all

debug platform rep verbose debugging is on
debug platform rep control pkt handle debugging is on
debug platform rep error debugging is on
debug platform rep event debugging is on
```

Related Commands

Command	Description
show platform condition	Displays the currently active debug configuration.
debug platform condition	Filters debugging output for **debug** commands on the basis of specified conditions.
debug platform condition start	Starts conditional debugging on a system.
debug platform condition stop	Stops conditional debugging on a system.
clear debug platform condition all	Removes the debug conditions applied to a platform.

debug ilpower powerman

To enable debugging of the power controller and Power over Ethernet (PoE) system, use the **debug ilpower powerman** command in privileged EXEC mode. Use the no form of this command to disable debugging.

Command Default

This command has no arguments or keywords.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

This example shows the output for the **debug ilpower powerman** command for releases prior to Cisco IOS XE Gibraltar 16.10.1:

```
Device# debug ilpower powerman
1. %ILPOWER-3-CONTROLLER_PORT_ERR: Controller port error, Interface
Gix/y/z: Power Controller reports power Imax error detected
Mar 8 16:35:17.801: ilpower_power_assign_handle_event: event 0, pwrassign
 is done by proto CDP
Port Gi1/0/48: Selected Protocol CDP
Mar 8 16:35:17.801: Ilpowerinterface (Gi1/0/48) process tlvfrom cdpINPUT:

Mar 8 16:35:17.801: power_consumption= 2640, power_request_id= 1,
power_man_id= 2,
Mar 8 16:35:17.801: power_request_level[] = 2640 0 0 0 0
Mar 8 16:35:17.801:
Mar 8 16:35:17.801: ILP:: Sending icutoffcurrent msgto slot:1 port:48
Mar 8 16:35:17.802: Ilpowerinterface (Gi1/0/48) power negotiation:
consumption = 2640, alloc_power= 2640
Mar 8 16:35:17.802: Ilpowerinterface (Gi1/0/48) setting ICUT_OFF threshold
 to 2640.
Mar 8 16:35:17.802: ILP:: Sending icutoffcurrent msgto slot:1 port:48
Mar 8 16:35:17.802: ILP:: Sending icutoffcurrent msgto slot:1 port:48
Mar 8 16:35:17.803: ILP:: Sending icutoffcurrent msgto slot:1 port:48
Mar 8 16:35:17.803: ILP:: Sending icutoffcurrent msgto slot:1 port:48
Mar 8 16:35:17.803: ILP:: Sending icutoffcurrent msgto slot:1 port:48
Mar 8 16:35:18.115: ILP:: posting ilpslot 1 port 48 event 5 class 0
Mar 8 16:35:18.115: ILP:: Gi1/0/48: State=NGWC_ILP_LINK_UP_S-6,
Event=NGWC_ILP_IMAX_FAULT_EV-5
Mar 8 16:35:18.115: ilpowerdelete power from pdlinkdownGi1/0/48
Mar 8 16:35:18.115: Ilpowerinterface (Gi1/0/48), delete allocated power
2640
Mar 8 16:35:18.116: Ilpowerinterface (Gi1/0/48) setting ICUT_OFF threshold
 to 0.
Mar 8 16:35:18.116: ILP:: Sending icutoffcurrent msgto slot:1 port:48
Mar 8 16:35:18.116: ilpower_notify_lldp_power_via_mdi_tlvGi1/0/48 pwralloc0
Mar 8 16:35:18.116: Gi1/0/48 AUTO PORT PWR Alloc130 Request 130
Mar 8 16:35:18.116: Gi1/0/48: LLDP NOTIFY TLV:
```

```
(curr/prev) PSE Allocation: 13000/0
(curr/prev) PD Request : 13000/0
(curr/prev) PD Class : Class 4/
(curr/prev) PD Priority : low/unknown
(curr/prev) Power Type : Type 2 PSE/Type 2 PSE
(curr/prev) mdi_pwr_support: 7/0
(curr/prevPower Pair) : Signal/
(curr/prev) PSE PwrSource : Primary/Unknown
```

This example shows the output for the **debug ilpower powerman** command starting Cisco IOS XE Gibraltar 16.10.1. Power Unit (mW) has been added to the power_request_level, PSE Allocation and PD Request. Power_request_level has been enhanced to display only non-zero values.

```
Device# debug ilpower powerman
1. %ILPOWER-3-CONTROLLER_PORT_ERR: Controller port error, Interface
Gix/y/z: Power Controller reports power Imax error detected
Mar 8 16:35:17.801: ilpower_power_assign_handle_event: event 0, pwrassign
 is done by proto CDP
Port Gi1/0/48: Selected Protocol CDP
Mar 8 16:35:17.801: Ilpowerinterface (Gi1/0/48) process tlvfrom cdpINPUT:

Mar 8 16:35:17.801: power_consumption= 2640, power_request_id= 1,
power_man_id= 2,
Mar 8 16:35:17.801: power_request_level(mW) = 2640
<------------------------- mW unit added, non-zero value display
Mar 8 16:35:17.801:
Mar 8 16:35:17.801: ILP:: Sending icutoffcurrent msgto slot:1 port:48
Mar 8 16:35:17.802: Ilpowerinterface (Gi1/0/48) power negotiation:
consumption = 2640, alloc_power= 2640
Mar 8 16:35:17.802: Ilpowerinterface (Gi1/0/48) setting ICUT_OFF threshold
 to 2640.
Mar 8 16:35:17.802: ILP:: Sending icutoffcurrent msgto slot:1 port:48
Mar 8 16:35:17.802: ILP:: Sending icutoffcurrent msgto slot:1 port:48
Mar 8 16:35:17.803: ILP:: Sending icutoffcurrent msgto slot:1 port:48
Mar 8 16:35:17.803: ILP:: Sending icutoffcurrent msgto slot:1 port:48
Mar 8 16:35:17.803: ILP:: Sending icutoffcurrent msgto slot:1 port:48
Mar 8 16:35:18.115: ILP:: posting ilpslot 1 port 48 event 5 class 0
Mar 8 16:35:18.115: ILP:: Gi1/0/48: State=NGWC_ILP_LINK_UP_S-6,
Event=NGWC_ILP_IMAX_FAULT_EV-5
Mar 8 16:35:18.115: ilpowerdelete power from pdlinkdownGi1/0/48
Mar 8 16:35:18.115: Ilpowerinterface (Gi1/0/48), delete allocated power
2640
Mar 8 16:35:18.116: Ilpowerinterface (Gi1/0/48) setting ICUT_OFF threshold
 to 0.
Mar 8 16:35:18.116: ILP:: Sending icutoffcurrent msgto slot:1 port:48
Mar 8 16:35:18.116: ilpower_notify_lldp_power_via_mdi_tlvGi1/0/48 pwralloc0
Mar 8 16:35:18.116: Gi1/0/48 AUTO PORT PWR Alloc130 Request 130
Mar 8 16:35:18.116: Gi1/0/48: LLDP NOTIFY TLV:
(curr/prev) PSE Allocation (mW): 13000/0
<------------------------- mW unit added
(curr/prev) PD Request (mW) : 13000/0
<------------------------- mW unit added
```

```
(curr/prev) PD Class : Class 4/
(curr/prev) PD Priority : low/unknown
(curr/prev) Power Type : Type 2 PSE/Type 2 PSE
(curr/prev) mdi_pwr_support: 7/0
(curr/prevPower Pair) : Signal/
(curr/prev) PSE PwrSource : Primary/Unknown
```

delete

To delete one or more files from the specified file system, use the **delete** command in boot loader mode.

delete *filesystem:/file-url...*

Syntax Description

filesystem:	Alias for a file system. Use **usbflash0:** for USB memory sticks.
/file-url...	Path (directory) and filename to delete. Separate each filename with a space.

Command Default

No default behavior or values.

Command Modes

Boot loader

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Filenames and directory names are case sensitive.

The device prompts you for confirmation before deleting each file.

Examples

This example shows how to delete two files:

```
Device: delete usbflash0:test2.text usbflash0:test5.text
Are you sure you want to delete "usbflash0:test2.text" (y/n)?y
File "usbflash0:test2.text" deleted
Are you sure you want to delete "usbflash0:test5.text" (y/n)?y
File "usbflash0:test2.text" deleted
```

You can verify that the files were deleted by entering the **dir usbflash0:** boot loader command.

dir

To display the list of files and directories on the specified file system, use the **dir** command in boot loader mode.

dir *filesystem:/file-url*

Syntax Description

filesystem:	Alias for a file system. Use **flash:** for the system board flash device; use **usbflash0:** for USB memory sticks.
/file-url	(Optional) Path (directory) and directory name that contain the contents you want to display. Separate each directory name with a space.

Command Default

No default behavior or values.

Command Modes

Boot Loader

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Directory names are case sensitive.

Examples

This example shows how to display the files in flash memory:

```
Device: dir flash:
Directory of flash:/
    2  -rwx        561   Mar 01 2013 00:48:15  express_setup.debug
    3  -rwx    2160256   Mar 01 2013 04:18:48  c2960x-dmon-mz-150-2r.EX
    4  -rwx       1048   Mar 01 2013 00:01:39  multiple-fs
    6  drwx        512   Mar 01 2013 23:11:42  c2960x-universalk9-mz.150-2.EX
  645  drwx        512   Mar 01 2013 00:01:11  dc_profile_dir
  647  -rwx       4316   Mar 01 2013 01:14:05  config.text
  648  -rwx          5   Mar 01 2013 00:01:39  private-config.text

   96453632 bytes available (25732096 bytes used)
```

Table 1: dir Field Descriptions

Field	Description
2	Index number of the file.
-rwx	File permission, which can be any or all of the following: • d—directory • r—readable • w—writable • x—executable

Field	Description
1644045	Size of the file.
<date>	Last modification date.
env_vars	Filename.

exit

To return to the previous mode or exit from the CLI EXEC mode, use the **exit** command.

exit

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Global configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

This example shows how to exit the configuration mode:

```
Device(config)# exit
Device#
```

factory-reset

To erase all customer-specific data and restore a device to its factory configuration, use the **factory-reset** command in privileged EXEC mode.

Note The erasure is consistent with the clear method, as described in NIST SP 800-88 Rev. 1.

Standalone Device
factory-reset { **all** **[secure 3-pass]** | **boot-vars** | **config** }

Stacked Device
factory-reset { **all** **[secure 3-pass]** | **boot-vars** | **config** | **switch** *switch_number* | **all** { **all** **[secure 3-pass]** | **boot-vars** | **config** } }

Syntax Description

all	Erases all the content from the NVRAM, all Cisco IOS images, including the current boot image, boot variables, startup and running configuration data, and user data.
secure 3-pass	Erases all the content from the device with 3-pass overwrite. • Pass 1: Overwrites all addressable locations with binary zeroes. • Pass 2: Overwrites all addressable locations with binary ones. • Pass 3: Overwrites all addressable locations with a random bit pattern.
boot-vars	Erases only the user-added boot variables.
config	Erases only the startup configurations.
switch {*switch_number* | **all**}	Erases content on the selected switch: • *switch-number*: Specifies the switch number. The range is from 1 to 16. • **all**: Selects all the switches in the stack.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.
Cisco IOS XE Amsterdam 17.2.1	The **secure 3-pass** and **switch** keyword was i

Usage Guidelines

The **factory-reset** command is used in the following scenarios:

- To return a device to Cisco for Return Material Authorization (RMA), use this command to remove all the customer-specific data before obtaining an RMA certificate for the device.
- If the key information or credentials that are stored on a device is compromised, use this command to reset the device to factory configuration, and then reconfigure the device.

After the factory reset process is successfully completed, the device reboots and enters ROMMON mode.

Examples

The following example shows how to erase all the content from a device using the **factory-reset all** command:

```
Device> enable
Device# factory-reset all

The factory reset operation is irreversible for all operations. Are you sure? [confirm]
The following will be deleted as a part of factory reset:
1: Crash info and logs
2: User data, startup and running configuration
3: All IOS images, including the current boot image
4: OBFL logs
5: User added rommon variables
6: Data on Field Replaceable Units(USB/SSD/SATA)
The system will reload to perform factory reset.
It will take some time to complete and bring it to rommon.
You will need to load IOS image using USB/TFTP from rommon after
this operation is completed.
DO NOT UNPLUG THE POWER OR INTERRUPT THE OPERATION
Are you sure you want to continue? [confirm]
```

The following examples show how to perform a factory reset on stacked devices:

```
Device> enable
Device# factory-reset switch all all
The factory reset operation is irreversible for all operations. Are you sure? [confirm]
 The following will be deleted as a part of factory reset:
 1: Crash info and logs
 2: User data, startup and running configuration
 3: All IOS images, including the current boot image
 4: OBFL logs
 5: User added rommon variables
 6: Data on Field Replaceable Units(USB/SSD/SATA)
 The system will reload to perform factory reset.
 It will take some time to complete and bring it to rommon.
 You will need to load IOS image using USB/TFTP from rommon after
 this operation is completed.
 DO NOT UNPLUG THE POWER OR INTERRUPT THE OPERATION
 Are you sure you want to continue? [confirm]
Chassis 1 reloading, reason - Factory Reset

 Protection key not found
9300L#Oct 25 09:53:05.740: %PMAN-5-EXITACTION: F0/0: pvp: Process manager is exiting: reload
 fp action requested
Oct 25 09:53:07.277: %PMAN-5-EXITACTION:vp: Process manager is exiting: rp processes exit
with reload switch code


Enabling factory reset for this reload cycle
 Switch booted with
tftp://10.5.40.45/cat9k_iosxe.BLD_POLARIS_DEV_LATEST_20191007_224933_V17_2_0_21_2.SSA.bin
 Switch booted via
//10.5.40.45/cat9k_iosxe.BLD_POLARIS_DEV_LATEST_20191007_224933_V17_2_0_21_2.SSA.bin
% FACTORYRESET - Started Cleaning Up...
% FACTORYRESET - Unmounting sd1
% FACTORYRESET - Cleaning Up sd1 [0]
% FACTORYRESET - erase In progress.. please wait for completion...
% FACTORYRESET - write zero...
% FACTORYRESET - finish erase

% FACTORYRESET - Making File System sd1 [0]
Discarding device blocks: done
Creating filesystem with 409600 4k blocks and 102544 inodes
Filesystem UUID: fcf01664-7c6f-41ce-99f0-6df1d941701e
Superblock backups stored on blocks:
 32768, 98304, 163840, 229376, 294912

Allocating group tables: done
Writing inode tables: done
Writing superblocks and filesystem accounting information: done

% FACTORYRESET - Mounting Back sd1 [0]
% FACTORYRESET - Handling Mounted sd1
% FACTORYRESET - Factory Reset Done for sd1

% FACTORYRESET - Unmounting sd3
% FACTORYRESET - Cleaning Up sd3 [0]
% FACTORYRESET - erase In progress.. please wait for completion...
% FACTORYRESET - write zero...



Chassis 2 reloading, reason - Factory Reset
Dec 12 01:02:12.500: %PMAN-5-EXITACTION: F0/0: pvp: Process manager is exiting: reload fp
action requested
De
Enabling factory reset for this reload cycle
 Switch booted with
tftp://10.5.40.45/cat9k_iosxe.BLD_POLARIS_DEV_LATEST_20191007_224933_V17_2_0_21_2.SSA.bin
 Switch booted via
//10.5.40.45/cat9k_iosxe.BLD_POLARIS_DEV_LATEST_20191007_224933_V17_2_0_21_2.SSA.bin
% FACTORYRESET - Started Cleaning Up...
% FACTORYRESET - Unmounting sd1
% FACTORYRESET - Cleaning Up sd1 [0]
% FACTORYRESET - erase In progress.. please wait for completion...
% FACTORYRESET - write zero...



After this the switch will come to boot prompt. Then the customer has to boot the device
from TFTP.
```

flash_init

To initialize the flash: file system, use the **flash_init** command in boot loader mode.

flash_init

Syntax Description

This command has no arguments or keywords.

Command Default

The flash: file system is automatically initialized during normal system operation.

Command Modes

Boot loader

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

During the normal boot process, the flash: file system is automatically initialized.

Use this command to manually initialize the flash: file system. For example, you use this command during the recovery procedure for a lost or forgotten password.

help

To display the available commands, use the **help** command in boot loader mode.

help

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Boot loader

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Example

This example shows how to display a list of available boot loader commands:

```
Device:help
? -- Present list of available commands
arp -- Show arp table or arp-resolve an address
boot -- Load and boot an executable image
cat -- Concatenate (type) file(s)
copy -- Copy a file
delete -- Delete file(s)
dir -- List files in directories
emergency-install -- Initiate Disaster Recovery
...
...
...
unset -- Unset one or more environment variables
version -- Display boot loader version
```

hostname

To specify or modify the hostname for the network server, use the **hostname** command in global configuration mode.

hostname *name*

Syntax Description

name	New hostname for the network server.

Command Default

The default hostname is switch.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

The hostname is used in prompts and default configuration filenames.

Do not expect case to be preserved. Uppercase and lowercase characters look the same to many internet software applications. It may seem appropriate to capitalize a name the same way you might do in English, but conventions dictate that computer names appear all lowercase. For more information, refer to RFC 1178, *Choosing a Name for Your Computer* .

The name must also follow the rules for ARPANET hostnames. They must start with a letter, end with a letter or digit, and have as interior characters only letters, digits, and hyphens. Names must be 63 characters or fewer. Creating an all numeric hostname is not recommended but the name will be accepted after an error is returned.

```
Device(config)#hostname 123
% Hostname contains one or more illegal characters.
123(config)#
```

A hostname of less than 10 characters is recommended. For more information, refer to RFC 1035, *Domain Names--Implementation and Specification* .

On most systems, a field of 30 characters is used for the hostname and the prompt in the CLI. Note that the length of your hostname may cause longer configuration mode prompts to be truncated. For example, the full prompt for service profile configuration mode is:

```
(config-service-profile)#
```

However, if you are using the hostname of “Switch,” you will only see the following prompt (on most systems):

```
Switch(config-service-profil)#
```

If the hostname is longer, you will see even less of the prompt:

```
Basement-rtr2(config-service)#
```

Keep this behavior in mind when assigning a name to your system (using the **hostname** global configuration command). If you expect that users will be relying on mode prompts as a CLI navigation aid, you should assign hostnames of no more than nine characters.

The use of a special character such as '\'(backslash) and a three or more digit number for the character setting like **hostname**, results in incorrect translation:

```
Device(config)#
Device(config)#hostname \99
% Hostname contains one or more illegal characters.
```

Examples

The following example changes the hostname to “host1”:

```
Device(config)# hostname host1
host1(config)#
```

install

To install Software Maintenance Upgrade (SMU) packages, use the **install** command in privileged EXEC mode.

```
install {abort | activate | file {bootflash: | flash: | harddisk: | webui:} [{auto-abort-timer timer timer
prompt-level {all | none}}] | add file {bootflash: | flash: | ftp: | harddisk: | http: | https: | rcp: | scp:
| tftp: | webui:} [{activate [{auto-abort-timer timer prompt-level {all | none}commit}]}] | commit |
auto-abort-timer stop | deactivate file {bootflash: | flash: | harddisk: | webui:} | label id{description
description | label-name name} | remove {file {bootflash: | flash: | harddisk: | webui:} | inactive } |
rollback to {base | committed | id {install-ID } | label {label-name}}}
```

Syntax Description

abort	Terminates the current install operation.
activate	Validates whether the SMU is added through the **install add** command. This keyword runs a compatibility check, updates package status, and if the package can be restarted, triggers post-install scripts to restart the necessary processes, or triggers a reload for nonrestartable packages.
file	Specifies the package to be activated.
{**bootflash:** | **flash:** | **harddisk:** | **webui:**}	Specifies the location of the installed package.
auto-abort-timer *timer*	(Optional) Installs an auto-abort timer.
prompt-level {**all** | **none**}	(Optional) Prompts a user about installation activities. For example, the **activate** keyword automatically triggers a reload for packages that require a reload. Before activating the package, a message prompts users about wanting to continue or not. The **all** keyword allows you to enable prompts. The **none** keyword disables prompts.
add	Copies files from a remote location (through FTP or TFTP) to a device and performs SMU compatibility check for the platform and image versions. This keyword runs base compatibility checks to ensure that a specified package is supported on a platform.
{ **bootflash:** | **flash:** |**ftp:** |**harddisk:** |**http:** |**https:** | **rcp:** | **scp:** | **tftp:** |**webui:**}	Specifies the package to be added.

commit	Makes SMU changes persistent over reloads. You can perform a commit after activating a package while the system is up, or after the first reload. If a package is activated, but not committed, it remains active after the first reload, but not after the second reload.
auto-abort-timer stop	Stops the auto-abort timer.
deactivate	Deactivates an installed package. **Note** Deactivating a package also updates the package status and might trigger a process restart or reload.
label *id*	Specifies the ID of the install point to label.
description	Adds a description to the specified install point.
label-name *name*	Adds a label name to the specified install point.
remove	Removes the installed packages. The **remove** keyword can only be used on packages that are currently inactive.
inactive	Removes all the inactive packages from the device.
rollback	Rolls back the data model interface (DMI) package SMU to the base version, the last committed version, or a known commit ID.
to base	Returns to the base image.
committed	Returns to the installation state when the last commit operation was performed.
id *install-ID*	Returns to the specific install point ID. Valid values are from 1 to 4294967295.

Command Default

Packages are not installed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.4	This command was introduced on the C9200L models of the series.
Cisco IOS XE Gibraltar 16.12.1	This command was introduced on the C9200 models of the series.

Usage Guidelines

An SMU is a package that can be installed on a system to provide a patch fix or security resolution to a released image. This package contains a minimal set of files for patching the release along with metadata that describes the contents of the package.

Packages must be added before the SMU is activated.

A package must be deactivated before it is removed from Flash. A removed packaged must be added again.

You can install, activate, and commit an SMU package using a single command (1-step process) or using separate commands (3-step process). Use the 1-step process when you have to install just one SMU package file and use the 3-step process when you have to install multiple SMUs. The 3-step process minimises the number of reloads required when you have more than one SMU package file to install. The examples below show both methods.

Example: Installing an SMU (3-Step Process, Using flash:)

The following example shows how to install a SMU package by using the 3-step process. Here the SMU package file is saved in the device's flash.

1. Copying the SMU package file from flash and installing it.

```
Device# install add file flash:cat9k_lite_iosxe.16.09.04.CSCvk70181.SPA.smu.bin
install_add: START Wed Jun 10 14:17:45 IST 2020
install_add: Adding SMU

--- Starting initial file syncing ---
Info: Finished copying flash:cat9k_lite_iosxe.16.09.04.CSCvk70181.SPA.smu.bin to the
selected switch(es)
Finished initial file syncing


*Jun 10 14:17:48.128 IST: %INSTALL-5-INSTALL_START_INFO: Switch 1 R0/0: install_engine:
 Started install add flash:cat9k_lite_iosxe.16.09.04.CSCvk70181.SPA.smu.binExecuting pre
 scripts....
Executing pre sripts done.
--- Starting SMU Add operation ---
Performing SMU_ADD on all members
  [1] SMU_ADD package(s) on switch 1
  [1] Finished SMU_ADD on switch 1
Checking status of SMU_ADD on [1]
SMU_ADD: Passed on [1]
Finished SMU Add operation

SUCCESS: install_add /flash/cat9k_lite_iosxe.16.09.04.CSCvk70181.SPA.smu.bin Wed Jun 10
 14:18:00 IST 2020
```

Verifying the addition and installation of the SMU package file by using the **show install summary** command. The status of the SMU package file is `I`, because it has not been activated and committed yet.

```
Device# show install summary

[ Switch 1 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
            C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type  St   Filename/Version
--------------------------------------------------------------------------------
SMU   I    flash:cat9k_lite_iosxe.16.09.04.CSCvk70181.SPA.smu.bin
IMG   C    16.9.4.0.3431
```

```
--------------------------------------------------------------------------------
Auto abort timer: inactive
--------------------------------------------------------------------------------
```

2. Activating the SMU package file.

```
Device# install activate file flash:cat9k_lite_iosxe.16.09.04.CSCvk70181.SPA.smu.bin

install_activate: START Wed Jun 10 14:19:59 IST 2020
install_activate: Activating SMU

*Jun 10 14:20:01.513 IST: %INSTALL-5-INSTALL_START_INFO: Switch 1 R0/0: install_engine:
 Started install activate flash:cat9k_lite_iosxe.16.09.04.CSCvk70181.SPA.smu.bin

This operation requires a reload of the system. Do you want to proceed? [y/n]y
Executing pre scripts....
Executing pre sripts done.

--- Starting SMU Activate operation ---
Performing SMU_ACTIVATE on all members
  [1] SMU_ACTIVATE package(s) on switch 1
  [1] Finished SMU_ACTIVATE on switch 1
Checking status of SMU_ACTIVATE on [1]
SMU_ACTIVATE: Passed on [1]
Finished SMU Activate operation

install_activate: Reloading the box to complete activation of the SMU...
install_activate will reload the system now!

*Jun 10 14:20:22.258 IST: %INSTALL-5-INSTALL_AUTO_ABORT_TIMER_PROGRESS: Switch 1 R0/0:
rollback_timer: Install auto abort timer will expire in 7200 seconds
     Chassis 1 reloading, reason - Reload command
Jun 10 14:20:28.291: %PMAN-5-EXITACTION: F0/0: pvp: Process manager is exiting: reload
fp action requested
Jun 10 14:20:30.718: %PMAN-5-EXITACTION: R0/0: pvp: Proce
Jun 10 14:20:34.834: %PMAN-5-EXITACTION: C0/0: pvp: Process manager is exiting:
Jun 10 14:20:36.053: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine: Completed
 install activate SMU flash:cat9k_lite_iosxe.16.09.04.CSCvk70181.SPA.smu.bin
watchdog watchdog0: watchdog did not stop!
reboot: Restarting system

Initializing Hardware...
<output truncated>

###########
Jun 10 08:52:01.806: %BOOT-5-BOOTTIME_SMU_TEMP_ACTIVE_DETECTED: R0/0: install_engine:
SMU file /flash/cat9k_lite_iosxe.16.09.04.CSCvk70181.SPA.smu.bin active temporary...
SMU commit is pending

Cisco IOS Software [Fuji], Catalyst L3 Switch Software (CAT9K_LITE_IOSXE), Version 16.9.4,
 RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2019 by Cisco Systems, Inc.
Compiled Thu 22-Aug-19 17:30 by mcpre

<output truncated>
```

Verifying activation of the SMU package file by using the **show install summary** command. The status of the SMU package file is `U`, because it has not been committed yet.

```
[ Switch 1 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
            C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
```

```
Type  St   Filename/Version
--------------------------------------------------------------------------------
SMU   U    flash:cat9k_lite_iosxe.16.09.04.CSCvk70181.SPA.smu.bin
IMG   C    16.9.4.0.3431

--------------------------------------------------------------------------------
Auto abort timer: active on install_activate, time before rollback - 01:41:52
--------------------------------------------------------------------------------
```

3. Committing the SMU package file

```
Device# install commit
install_commit: START Wed Jun 10 14:38:42 IST 2020
install_commit: Committing SMU

*Jun 10 14:38:44.906 IST: %INSTALL-5-INSTALL_START_INFO: Switch 1 R0/0: install_engine:
 Started install commitExecuting pre scripts....
Executing pre sripts done.
--- Starting SMU Commit operation ---
Performing SMU_COMMIT on all members
  [1] SMU_COMMIT package(s) on switch 1
  [1] Finished SMU_COMMIT on switch 1
Checking status of SMU_COMMIT on [1]
SMU_COMMIT: Passed on [1]
Finished SMU Commit operation

SUCCESS: install_commit /flash/cat9k_lite_iosxe.16.09.04.CSCvk70181.SPA.smu.bin Wed Jun
 10 14:38:58 IST 2020
*Jun 10 14:38:59.385 IST: %INSTALL-5-INSTALL_COMPLETED_INFO: Switch 1 R0/0:
install_engine: Completed install commit SMU
```

Verifying the commit by using the **show install summary** command. The SMU package file has been installed, activated and committed and the status is `C`.

```
Device# show install summary
[ Switch 1 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
            C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type  St   Filename/Version
--------------------------------------------------------------------------------
SMU   C    flash:cat9k_lite_iosxe.16.09.04.CSCvk70181.SPA.smu.bin
IMG   C    16.9.4.0.3431

--------------------------------------------------------------------------------
Auto abort timer: inactive
--------------------------------------------------------------------------------
```

Verifying active packages by using the **show install active** command

```
Device# show install active
[ Switch 1 ] Active Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
            C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type  St   Filename/Version
--------------------------------------------------------------------------------
SMU   C    flash:cat9k_lite_iosxe.16.09.04.CSCvk70181.SPA.smu.bin
IMG   C    16.9.4.0.3431
```

Checking the version, by using the **show version** command:

```
Device# show version
Cisco IOS XE Software, Version 16.09.04
Cisco IOS Software [Fuji], Catalyst L3 Switch Software (CAT9K_LITE_IOSXE), Version 16.9.4,
 RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2019 by Cisco Systems, Inc.
Compiled Thu 22-Aug-19 17:30 by mcpre
...
```

Example: Installing Multiple SMUs (3-Step Process, Using flash:)

The following example shows how to install multiple SMU package files by using the 3-step process. Here the SMU package files are saved in the device's flash.

The SMU files being installed on the switch stack are: `cat9k_lite_iosxe.16.12.03.CSCvt22238.SPA.smu.bin` and `cat9k_lite_iosxe.16.12.03.CSCvt72427.SPA.smu.bin`

1. (Optional) Checking that the switch stack is ready and that the SMU package files are in the device's flash.

   ```
   Device# show switch
   Switch/Stack Mac Address : 08ec.f586.aa80 - Local Mac Address
   Mac persistency wait time: Indefinite
                                                  H/W   Current
   Switch#   Role    Mac Address     Priority Version  State
   -----------------------------------------------------------------------------------------
   *1       Active   08ec.f586.aa80     1      V01      Ready
    2       Member   7488.bb3c.f600     1      V01      Ready
    3       Member   7488.bb3f.9c00     1      V01      Ready
    4       Member   08ec.f5ee.1080     1      V01      Ready
    5       Standby  08ec.f589.7c80     1      V01      Ready
   ```

   ```
   Device# dir flash: | i smu

   89075  -rw-  79256 Oct 26 2035 07:07:42 +00:00
   cat9k_lite_iosxe.16.12.03.CSCvt22238.SPA.smu.bin
   89082  -rw-  9656  Oct 26 2035 07:08:08 +00:00
   cat9k_lite_iosxe.16.12.03.CSCvt72427.SPA.smu.bin
   ```

2. Copying the SMU package files from flash and adding them.

   Only one SMU package file is added at a time; no reload is required between the addition of the SMU package files.

   ```
   Device# install add file flash:cat9k_lite_iosxe.16.12.03.CSCvt22238.SPA.smu.bin
   install_add: START Fri Oct 26 07:10:59 UTC 2035
   Oct 26 07:11:01.695 %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install
    add flash:cat9k_lite_iosxe.16.12.03.CSCvt22238.SPA.smu.bin
   install_add: Adding SMU
   install_add: Checking whether new add is allowed ....

   --- Starting initial file syncing ---

   *Oct 26 07:11:01.643: %INSTALL-5-INSTALL_START_INFO: Switch 1 R0/0: install_engine:
   Started install add flash:cat9k_lite_iosxe.16.12.03.CSCvt22238.SPA.smu.bin[1]: Copying
   flash:cat9k_lite_iosxe.16.12.03.CSCvt22238.SPA.smu.bin from switch 1 to switch 2 3 4 5
   [2 3 4 5]: Finished copying to switch 2 switch 3 switch 4 switch 5
   Info: Finished copying flash:cat9k_lite_iosxe.16.12.03.CSCvt22238.SPA.smu.bin to the
   selected switch(es)
   Finished initial file syncing
   ```

```
--- Starting SMU Add operation ---
Performing SMU_ADD on all members
  [1] SMU_ADD package(s) on switch 1
  [1] Finished SMU_ADD on switch 1
  [2] SMU_ADD package(s) on switch 2
  [2] Finished SMU_ADD on switch 2
  [3] SMU_ADD package(s) on switch 3
  [3] Finished SMU_ADD on switch 3
  [4] SMU_ADD package(s) on switch 4
  [4] Finished SMU_ADD on switch 4
  [5] SMU_ADD package(s) on switch 5
  [5] Finished SMU_ADD on switch 5
Checking status of SMU_ADD on [1 2 3 4 5]
SMU_ADD: Passed on [1 2 3 4 5]
Finished SMU Add operation

SUCCESS: install_add  Fri Oct 26 07:11:45 UTC 2035
Oct 26 07:11:46.695 %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine: Completed
install add SMU flash:cat9k_lite_iosxe.16.12.03.CSCvt22238.SPA.smu.bin
Device#
*Oct 26 07:11:46.656: %INSTALL-5-INSTALL_COMPLETED_INFO: Switch 1 R0/0: install_engine:
 Completed install add SMU flash:cat9k_lite_iosxe.16.12.03.CSCvt22238.SPA.smu.bin
```

Verifying the additiong of the first SMU package file by using the **show install summary** command.

```
Device# show install summary
[ Switch 1 2 3 4 5 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
            C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type  St   Filename/Version
--------------------------------------------------------------------------------
SMU   I    flash:cat9k_lite_iosxe.16.12.03.CSCvt22238.SPA.smu.bin
IMG   C    16.12.3.0.3752

--------------------------------------------------------------------------------
Auto abort timer: inactive
--------------------------------------------------------------------------------
```

Adding the second SMU package file.

```
Device# install add file flash:cat9k_lite_iosxe.16.12.03.CSCvt72427.SPA.smu.bin

install_add: START Fri Oct 26 07:12:38 UTC 2035
Oct 26 07:12:40.782 %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install
 add flash:cat9k_lite_iosxe.16.12.03.CSCvt72427.SPA.smu.bin
install_add: Adding SMU
install_add: Checking whether new add is allowed ....

--- Starting initial file syncing ---

*Oct 26 07:12:40.743: %INSTALL-5-INSTALL_START_INFO: Switch 1 R0/0: install_engine:
Started install add flash:cat9k_lite_iosxe.16.12.03.CSCvt72427.SPA.smu.bin[1]: Copying
flash:cat9k_lite_iosxe.16.12.03.CSCvt72427.SPA.smu.bin from switch 1 to switch 2 3 4 5
[2 3 4 5]: Finished copying to switch 2 switch 3 switch 4 switch 5
Info: Finished copying flash:cat9k_lite_iosxe.16.12.03.CSCvt72427.SPA.smu.bin to the
selected switch(es)
Finished initial file syncing

--- Starting SMU Add operation ---
Performing SMU_ADD on all members
  [1] SMU_ADD package(s) on switch 1
  [1] Finished SMU_ADD on switch 1
  [2] SMU_ADD package(s) on switch 2
  [2] Finished SMU_ADD on switch 2
  [3] SMU_ADD package(s) on switch 3
  [3] Finished SMU_ADD on switch 3
  [4] SMU_ADD package(s) on switch 4
  [4] Finished SMU_ADD on switch 4
  [5] SMU_ADD package(s) on switch 5
  [5] Finished SMU_ADD on switch 5
Checking status of SMU_ADD on [1 2 3 4 5]
SMU_ADD: Passed on [1 2 3 4 5]
Finished SMU Add operation

SUCCESS: install_add  Fri Oct 26 07:13:24 UTC 2035
Oct 26 07:13:25.656 %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine: Completed
install add SMU flash:cat9k_lite_iosxe.16.12.03.CSCvt72427.SPA.smu.bin
 Decive#
*Oct 26 07:13:25.616: %INSTALL-5-INSTALL_COMPLETED_INFO: Switch 1 R0/0: install_engine:
 Completed install add SMU flash:cat9k_lite_iosxe.16.12.03.CSCvt72427.SPA.smu.bin
```

Verifying the addition and installation of both the SMU package files by using the **show install summary** command. The status of both package files is `I`, because they have not been activated and committed yet.

```
Device# show install summary

[ Switch 1 2 3 4 5 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
            C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type  St   Filename/Version
--------------------------------------------------------------------------------
SMU   I    flash:cat9k_lite_iosxe.16.12.03.CSCvt22238.SPA.smu.bin
SMU   I    flash:cat9k_lite_iosxe.16.12.03.CSCvt72427.SPA.smu.bin
IMG   C    16.12.3.0.3752

--------------------------------------------------------------------------------
Auto abort timer: inactive
--------------------------------------------------------------------------------
```

3. Activating the SMU package files.

   When entering multiple SMUs, use a comma (without a space before or after), to separate file names. Also ensure that total number of characters does not exceed 128. This step involves a reload.

```
Device# install activate file
flash:cat9k_lite_iosxe.16.12.03.CSCvt22238.SPA.smu.bin,cat9k_lite_iosxe.16.12.03.CSCvt72427.SPA.smu.bin


install_activate: START Sun Oct 28 13:23:42 UTC 2035
Oct 28 13:23:44.620 %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install
 activate
flash:cat9k_lite_iosxe.16.12.03.CSCvt22238.SPA.smu.bin,cat9k_lite_iosxe.16.12.03.CSCvt72427.SPA.smu.bin
install_activate: Activating SMU

*Oct 28 13:23:44.581: %INSTALL-5-INSTALL_START_INFO: Switch 1 R0/0: install_engine:
Started install activate
flash:cat9k_lite_iosxe.16.12.03.CSCvt22238.SPA.smu.bin,cat9k_lite_iosxe.16.12.03.CSCvt72427.SPA.smu.bin

This operation may require a reload of the system. Do you want to proceed? [y/n]y
Executing pre scripts....

Executing pre sripts done.
```

```
--- Starting SMU Activate operation ---
Performing SMU_ACTIVATE on all members

*Oct 28 13:24:41.563: %INSTALL-5-INSTALL_AUTO_ABORT_TIMER_PROGRESS: Switch 1 R0/0:
rollback_timer: Install auto abort timer will expire in 7200 secondsOct 28 13:24:43.259:
 %INSTALL-5-INSTALL_AUTO_ABORT_TIMER_PROGRESS: R0/0: rollback_timer: Install auto abort
 timer will expire in 7200 seconds
*Oct 28 13:24:43.222: %INSTALL-5-INSTALL_AUTO_ABORT_TIMER_PROGRESS: Switch 4 R0/0:
rollback_timer: Install auto abort timer will expire in 7200 seconds
*Oct 28 13:24:43.192: %INSTALL-5-INSTALL_AUTO_ABORT_TIMER_PROGRESS: Switch 3 R0/0:
rollback_timer: Install auto abort timer will expire in 7200 seconds
*Oct 28 13:24:43.134: %INSTALL-5-INSTALL_AUTO_ABORT_TIMER_PROGRESS: Switch 2 R0/0:
rollback_timer: Install auto abort timer will expire in 7200 seconds
*Oct 28 13:24:43.825: %INSTALL-5-INSTALL_AUTO_ABORT_TIMER_PROGRESS: Switch 5 R0/0:
rollback_timer: Install auto abort timer will expire in 7200 seconds  [1] SMU_ACTIVATE
package(s) on switch 1
  [1] Finished SMU_ACTIVATE on switch 1
  [2] SMU_ACTIVATE package(s) on switch 2
  [2] Finished SMU_ACTIVATE on switch 2
  [3] SMU_ACTIVATE package(s) on switch 3
  [3] Finished SMU_ACTIVATE on switch 3
  [4] SMU_ACTIVATE package(s) on switch 4
  [4] Finished SMU_ACTIVATE on switch 4
  [5] SMU_ACTIVATE package(s) on switch 5
  [5] Finished SMU_ACTIVATE on switch 5
Checking status of SMU_ACTIVATE on [1 2 3 4 5]
SMU_ACTIVATE: Passed on [1 2 3 4 5]
Finished SMU Activate operation

install_activate: Reloading the box to complete activation of the SMU...
install_activate will reload the system now!

Chassis 4 reloading, reason - Reload command
reload fp action requested
rp processes exit with reload switch code



watchdog watchdog0: watchdog did not stop!
reboot: Restarting system

Initializing Hardware...

System Bootstrap, Version 16.12.1r [FC6], RELEASE SOFTWARE (P)
Compiled Thu 02/13/2020 12:36:08 by rel

Current ROMMON image : Primary
C9200L-24T-4G platform with 2097152 Kbytes of main memory

boot: attempting to boot from [flash:packages.conf]
boot: reading file packages.conf

#############
Oct 28 13:26:55.653: %BOOT-5-BOOTTIME_SMU_TEMP_ACTIVE_DETECTED: R0/0: install_engine:
SMU file /flash/cat9k_lite_iosxe.16.12.03.CSCvt72427.SPA.smu.bin active temporary... SMU
 commit is pending
Oct 28 13:26:55.912: %BOOT-5-BOOTTIME_SMU_TEMP_ACTIVE_DETECTED: R0/0: install_engine:
SMU file /flash/cat9k_lite_iosxe.16.12.03.CSCvt22238.SPA.smu.bin active temporary... SMU
 commit is pending

Waiting for 120 seconds for other switches to boot
##########
Switch number is 4
All switches in the stack have been discovered. Accelerating discovery
```

Verifying activation of the SMU package files by using the **show install summary** command. The status of both files is `U`, because they have not been committed yet.

```
Device# show install summary
[ Switch 1 2 3 4 5 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
            C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type  St   Filename/Version
--------------------------------------------------------------------------------
SMU   U    flash:cat9k_lite_iosxe.16.12.03.CSCvt22238.SPA.smu.bin
SMU   U    flash:cat9k_lite_iosxe.16.12.03.CSCvt72427.SPA.smu.bin
IMG   C    16.12.3.0.3752

--------------------------------------------------------------------------------
Auto abort timer: active on install_activate, time before rollback - 01:50:16
--------------------------------------------------------------------------------
```

4. Committing the SMU package file

```
Device# install commit
install_commit: START Sun Oct 28 13:34:42 UTC 2035
Oct 28 13:34:45.202 %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install
 commit

*Oct 28 13:34:45.146: %INSTALL-5-INSTALL_START_INFO: Switch 1 R0/0: install_engine:
Started install commitinstall_commit: Committing SMU
Executing pre scripts....
Executing pre sripts done.
--- Starting SMU Commit operation ---
Performing SMU_COMMIT on all members

*Oct 28 13:35:24.436: %PLATFORM-4-ELEMENT_WARNING: Switch 1 R0/0: smand: 5/RP/0: limited
 space - copy files out of flash: directory. flash: value 84% (1599 MB) exceeds warning
 level 70% (1337 MB).
*Oct 28 13:35:30.587: %PLATFORM-4-ELEMENT_WARNING: Switch 1 R0/0: smand: 2/RP/0: limited
 space - copy files out of flash: directory. flash: value 74% (1412 MB) exceeds warning
 level 70% (1337 MB).  [1] SMU_COMMIT package(s) on switch 1
  [1] Finished SMU_COMMIT on switch 1
  [2] SMU_COMMIT package(s) on switch 2
  [2] Finished SMU_COMMIT on switch 2
  [3] SMU_COMMIT package(s) on switch 3
  [3] Finished SMU_COMMIT on switch 3
  [4] SMU_COMMIT package(s) on switch 4
  [4] Finished SMU_COMMIT on switch 4
  [5] SMU_COMMIT package(s) on switch 5
  [5] Finished SMU_COMMIT on switch 5
Checking status of SMU_COMMIT on [1 2 3 4 5]
SMU_COMMIT: Passed on [1 2 3 4 5]
Finished SMU Commit operation

SUCCESS: install_commit /flash/cat9k_lite_iosxe.16.12.03.CSCvt72427.SPA.smu.bin
/flash/cat9k_lite_iosxe.16.12.03.CSCvt22238.SPA.smu.bin
Sun Oct 28 13:35:52 UTC 2035
Oct 28 13:35:53.789 %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine: Completed
install commit SMU

JJ22-Vore_stack-24TE#
*Oct 28 13:35:53.749: %INSTALL-5-INSTALL_COMPLETED_INFO: Switch 1 R0/0: install_engine:
 Completed install commit SMU
```

Verifying the commit by using the **show install summary** command. The SMU package files have been installed, activated and committed, and the status is `C`.

```
Device# show install summary
[ Switch 1 2 3 4 5 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
            C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type  St   Filename/Version
--------------------------------------------------------------------------------
SMU   C    flash:cat9k_lite_iosxe.16.12.03.CSCvt22238.SPA.smu.bin
SMU   C    flash:cat9k_lite_iosxe.16.12.03.CSCvt72427.SPA.smu.bin
IMG   C    16.12.3.0.3752

--------------------------------------------------------------------------------
Auto abort timer: inactive
--------------------------------------------------------------------------------
```

Example: Installing an SMU (3-Step Process, Using TFTP)

The following example shows how to install a SMU package by using the 3-step process. Here the SMU package file is saved in a remote (TFTP) location.

1. Adding the SMU package file.

```
Device# install add file
tftp://172.16.0.1//tftpboot/folder1/cat9k_lite_iosxe.16.09.04.CSCvk70181.SPA.smu.bin

Jun 22 11:32:27.035: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install
 add tftp://172.16.0.1//tftpboot/folder1/cat9k_lite_iosxe.16.09.04.CSCvk70181.SPA.smu.bin
Jun 22 11:32:27.035 %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install
 add tftp://172.16.0.1//tftpboot/folder1/cat9k_lite_iosxe.16.09.04.CSCvk70181.SPA.smu.bin
Downloading file
tftp://172.16.0.1//tftpboot/folder1/cat9k_lite_iosxe.16.09.04.CSCvk70181.SPA.smu.bin
Finished downloading file
tftp://172.16.0.1//tftpboot/folder1/cat9k_lite_iosxe.16.09.04.CSCvk70181.SPA.smu.bin to
 flash:cat9k_lite_iosxe.16.09.04.CSCvk70181.SPA.smu.bin
install_add: Adding SMU
install_add: Checking whether new add is allowed ....

--- Starting initial file syncing ---

025335: *Jun 22 2020 11:32:26 UTC: %INSTALL-5-INSTALL_START_INFO: Switch 1 R0/0:
install_engine: Started install add
tftp://172.16.0.1//tftpboot/folder1/cat9k_lite_iosxe.16.09.04.CSCvk70181.SPA.smu.bin[1]:
 Copying flash:cat9k_lite_iosxe.16.09.04.CSCvk70181.SPA.smu.bin from switch 1 to switch
 2
[2]: Finished copying to switch 2
Info: Finished copying flash:cat9k_lite_iosxe.16.09.04.CSCvk70181.SPA.smu.bin to the
selected switch(es)
Finished initial file syncing

--- Starting SMU Add operation ---
Performing SMU_ADD on all members
[1] SMU_ADD package(s) on switch 1
[1] Finished SMU_ADD on switch 1
[2] SMU_ADD package(s) on switch 2
[2] Finished SMU_ADD on switch 2
Checking status of SMU_ADD on [1 2]
SMU_ADD: Passed on [1 2]
Finished SMU Add operation
```

```
SUCCESS: install_add Mon Jun 22 11:32:56 UTC 2020
Jun 22 11:32:57.598: %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine: Completed
 install add SMU flash:cat9k_lite_iosxe.16.09.04.CSCvk70181.SPA.smu.bin
Jun 22 11:32:57.598 %INSTALL-5-INSTALL_COMPLETED_INFO: R0/0: install_engine: Completed
install add SMU flash:cat9k_lite_iosxe.16.09.04.CSCvk70181.SPA.smu.bin

ECSG-SEC-C9200-24P#
025336: *Jun 22 2020 11:32:57 UTC: %INSTALL-5-INSTALL_COMPLETED_INFO: Switch 1 R0/0:
install_engine: Completed install add SMU
flash:cat9k_lite_iosxe.16.09.04.CSCvk70181.SPA.smu.bin
```

Verifying addition by using the **show install summary** command.

```
Device# show install summary
[ Switch 1 2 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type St Filename/Version
--------------------------------------------------------------------------------
SMU I flash:cat9k_lite_iosxe.16.09.04.CSCvk70181.SPA.smu.bin
IMG C 16.12.02.0.6

--------------------------------------------------------------------------------
Auto abort timer: inactive
--------------------------------------------------------------------------------
```

2. Activating the SMU package file.

Note You use TFTP to add the SMU package file (in the previous step) and *flash*, to activate - not TFTP.

```
Device# install activate file flash:cat9k_lite_iosxe.16.09.04.CSCvk70181.SPA.smu.bin

install_activate: START Mon Jun 22 11:37:17 UTC 2020

Jun 22 11:37:37.582: %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install
 activate flash:cat9k_lite_iosxe.16.09.04.CSCvk70181.SPA.smu.bin
Jun 22 11:37:37.582 %INSTALL-5-INSTALL_START_INFO: R0/0: install_engine: Started install
 activate flash:cat9k_lite_iosxe.16.09.04.CSCvk70181.SPA.smu.bin
install_activate: Activating SMU

025337: *Jun 22 2020 11:37:37 UTC: %INSTALL-5-INSTALL_START_INFO: Switch 1 R0/0:
install_engine: Started install activate
flash:cat9k_lite_iosxe.16.09.04.CSCvk70181.SPA.smu.bin
This operation may require a reload of the system. Do you want to proceed? [y/n]n
```

Checking the version, by using the **show version** command:

```
Device# show version
Cisco IOS XE Software, Version 16.09.04
Cisco IOS Software [Fuji], Catalyst L3 Switch Software (CAT9K_LITE_IOSXE), Version 16.9.4,
 RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2019 by Cisco Systems, Inc.
Compiled Thu 22-Aug-19 17:30 by mcpre
<output truncated>
```

3. Committing the SMU package file.

```
Device# install commit

install_commit: START Mon Jun 22 11:38:48 UTC 2020
SUCCESS: install_commit Mon Jun 22 11:38:52 UTC 2020
Device#
```

Verifying that the update package is now committed, and that it will be persistent across reloads:

```
Device# show install summary

Active Packages:
tftp:cat9k_lite_iosxe.16.09.04.CSCvk70181.SPA.smu.bin
Inactive Packages:
No packages
Committed Packages:
tftp:cat9k_lite_iosxe.16.09.04.CSCvk70181.SPA.smu.bin
Uncommitted Packages:
No packages
Device#
```

Related Commands

Command	Description
show install	Displays information about the install packages.

ip ssh bulk-mode

To enable the Secure Shell (SSH) bulk data transfer mode, use the **ip ssh bulk-mode** command in global configuration mode. To disable this mode, use the **no** form of this command.

ip ssh bulk-mode [*window-size*]
no ip ssh bulk-mode [*window-size*]

Syntax Description

window-size	(Optional) The SSH window size. The range is from 131072 to 1073741824. The default is 131072.

Command Default

SSH bulk mode is not enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.2.1	This command was introduced.
Cisco IOS XE Bengaluru 17.6.1	This command was modified. The *window-size* variable option was introduced.

Usage Guidelines

SSH bulk mode enables optimizing the throughput performance of procedures that involve the transfer of large amounts of data. The Secure Copy feature has been enhanced to leverage bulk mode optimizations. We recommend that you enable the **ip ssh bulk-mode** command for transferring large files only because this operation consumes more system resources, such as, CPU and memory, compared to other file transfer operations. Do not use this command when the system resources are heavily loaded, and disable this command after the required file transfers are completed.

Note

- Bulk data transfer mode does not support the time or volume-based SSH rekey functionality.
- Bulk data transfer mode is not supported with SSH Version 1.

Examples

The following example shows how to enable bulk data transfer mode on an SSH server:

```
Device> enable
Device# configure terminal
Device(config)# ip ssh bulk-mode
Device(config)# exit
```

l2 traceroute

To enable the Layer 2 traceroute server, use the **l2 traceroute** command in global configuration mode. Use the **no** form of this command to disable the Layer 2 traceroute server.

l2 traceroute
no l2 traceroute

Syntax Description

This command has no arguments or keywords.

Command Modes

Global configuration (config#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	The command was introduced.

Usage Guidelines

Layer 2 traceroute is enabled by default and opens a listening socket on User Datagram Protocol (UDP) port 2228. To close the UDP port 2228 and disable Layer 2 traceroute, use the **no l2 traceroute** command in global configuration mode.

The following example shows how to configure Layer 2 traceroute using the **l2 traceroute** command.

```
Device# configure terminal
Device(config)# l2 traceroute
```

license air level

To configure AIR licenses on a wireless controller that is connected to Cisco Catalyst Access, Core, and Aggregation Switches, enter the **license air level** command in global configuration mode. To revert to the default setting, use the **no** form of this command.

license air level { **air-network-advantage** [**addon air-dna-advantage**] | **air-network-essentials** [**addon air-dna-essentials**] }

no license air level

Syntax Description

air-network-advantage	Configures the AIR network advantage license level.
addon air-dna-advantage	(Optional) Configures the add-on AIR DNA advantage license level. This add-on option is available with the AIR network advantage license, and is the default license.
air-network-essentials	Configures the AIR network essential license level.
addon air-dna-essentials	(Optional) Configures the add-on AIR DNA essentials license level. This add-on option is available with the AIR network essential license.

Command Default

AIR DNA Advantage is the default license

Command Modes

Global configuration (Device(config)#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.
Cisco IOS XE Amsterdam 17.3.2a	This command continues to be available and applicable with the introduction of Smart Licensing Using Policy in this release. See the *Usage Guidelines* section below for details.

Usage Guidelines

In the Smart Licensing Using Policy environment, you can use the **license air level** command to change the license level being used on the product instance, or to additionally configure an add-on license on the product instance. The change is effective after a reload.

The licenses that can be configured are:

- AIR Network Essential
- AIR Network Advantage
- AIR DNA Essential
- AIR DNA Advantage

You can configure AIR DNA Essential or AIR DNA Advantage license level, and on term expiry, you can move to the Network Advantage or Network Essentials license level, if you do not want to renew the DNA license.

Every connecting Access Point requires a Cisco DNA Center License to leverage the unique value properties of the controller.

For more information, see the Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide for the required release.

Examples

The following example shows how to configure the AIR DNA Essential license level:

```
Device# configure terminal
Device(config)# license air level network-essentials addon air-dna-essentials
```

The following example shows how to configure the AIR DNA Advantage license level:

```
Device# configure terminal
Device(config)# license air level air-network-advantage addon air-dna-advantage
```

license boot level

To boot a new software license on the device, use the **license boot level** command in global configuration mode. Use the **no** form of this command to remove all software licenses from the device.

license boot level { **network-advantage** [**addon dna-advantage**] | **network-essentials** [**addon dna-essentials**] }

no license boot level

Syntax Description

network-advantage [**addon dna-advantage**]	Configures the Network Advantage license. Optionally, you can also configure the Digital Networking Architecture (DNA) Advantage license.
network-essentials [**addon dna-essentials**]	Configures the Network Essentials license. Optionally, you can also configure the Digital Networking Architecture (DNA) Essentials license.

Command Default

Network Essentials

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.
Cisco IOS XE Amsterdam 17.3.2a	This command continues to be available and applicable with the introduction of Smart Licensing Using Policy in this release. See the *Usage Guidelines* section below for details.

Usage Guidelines

The software features available on Cisco Catalyst 9000 Series Switches fall under these base or add-on license levels:

Base Licenses:

- Network Essentials
- Network Advantage—Includes features available with the Network Essentials license and more.

Add-on Licenses:

- DNA Essentials
- DNA Advantage—Includes features available with the Network Essentials license and more.

Base licenses are permanent or perpetual licenses.

Add-on licenses are subscription or term licenses and can be purchased for a three, five, or seven year period. Base licenses are a prerequite for add-on licenses. See the release notes for more information about this.

The sections below provide information about using the **license boot level** command in the earlier Smart Licensing environment, and in the Smart Licensing Using Policy environment.

Smart Licensing: If the software version on the device is Cisco IOS XE Amsterdam 17.3.1 or an earlier release, Smart Licensing is enabled by default and you can use the **license boot level** command for these purposes:

- Downgrade or upgrade licenses
- Enable or disable an evaluation or extension license
- Clear an upgrade license

This command forces the licensing infrastructure to boot the configured license level instead of the license hierarchy maintained by the licensing infrastructure for a given module:

- When the switch reloads, the licensing infrastructure checks the configuration in the startup configuration for licenses, if any. If there is a license in the configuration, the switch boots with that license. If there is no license, the licensing infrastructure follows the image hierarchy to check for licenses.
- If the forced boot evaluation license expires, the licensing infrastructure follows the regular hierarchy to check for licenses.
- If the configured boot license has already expired, the licensing infrastructure follows the hierarchy to check for licenses.

Smart Licensing Using Policy: If the software version on the device (also referred to as a product instance) is Cisco IOS XE Amsterdam 17.3.2a or a later release, Smart Licensing Using Policy is enabled by default and you can use the **license boot level** command for these purposes:

- To change the base or add-on license levels being used on the product instance.

  For example, if you are using Network Essentials and you want to use Network Advantage with the next reload, or if you are using DNA Advantage and you want to use DNA Essentials with the next reload.

- To add or remove add-on license levels being used on the product instance.

  For example, if you are using only Network Essentials and you want to use DNA Essentials with the next reload, or if you are using DNA Advantage and you do not want to use the add-on after the next reload.

The notion of evaluation or expired licenses does not exist in Smart Licensing Using Policy.

After the command is configured, the configured license is effective after the next reload. License usage continues to be recorded on device and this changed licensing consmption information may have to be sent via the next Resource Utilization Measurement Report (RUM report), to CSSM. The reporting requirements and frequency are determined by the policy that is applied. See the `Usage Reporting:` section of the **show license status** command output. For more information about Smart Licensing Using Policy, in the software configuration guide of the required release, see *System Management* > *Smart Licensing Using Policy*.

Examples

The following example shows how to configure the Network Essentials license at the next reload:

```
Device# configure terminal
Device(config)# license boot level network-essentals
Device(config)# exit
Device# copy running-config startup-config
Device# reload
```

The following example shows how to activate the DNA Essentials license at the next reload:

```
Device# configure terminal
Device(config)# license boot level network-essentals add-on dna-essentials
Device(config)# exit
Device# copy running-config startup-config
Device# reload
```

license smart (global config)

To configure licensing-related settings such as the mode of transport and the URL that the product instance uses to communicate with Cisco Smart Software Manager (CSSM), or Cisco Smart Licensing Utility (CSLU), or Smart Software Manager On-Prem (SSM On-Prem), to configure the usage reporting interval, to configure the information that must be exluded or included in a license usage report (RUM report), enter the **license smart** command in global configuration mode. Use the **no** form of the command to revert to default values.

license smart { **custom_id** *ID* | **enable** | **privacy** { **all** | **hostname** | **version** } | **proxy** { **address** *address_hostname* | **port** *port* } | **reservation** | **server-identity-check** | **transport** { **automatic** | **callhome** | **cslu** | **off** | **smart** } | **url** { *url* | **cslu** *cslu_or_on-prem_url* | **default** | **smart** *smart_url* | **utility** *secondary_url* } | **usage** { **customer-tags** { **tag1** | **tag2** | **tag3** | **tag4** } *tag_value* | **interval** *interval_in_days* } | **utility** [**customer_info** { **city** *city* | **country** *country* | **postalcode** *postalcode* | **state** *state* | **street** *street* }] }

no license smart { **custom_id** | **enable** | **privacy** { **all** | **hostname** | **version** } | **proxy** { **address** *address_hostname* | **port** *port* } | **reservation** | **server-identity-check** | **transport** | **url** { *url* | **cslu** *cslu_or_on-prem_url* | **default** | **smart** *smart_url* | **utility** *secondary_url* } | **usage** { **customer-tags** { **tag1** | **tag2** | **tag3** | **tag4** } *tag_value* | **interval** *interval_in_days* } | **utility** [**customer_info** { **city** *city* | **country** *country* | **postalcode** *postalcode* | **state** *state* | **street** *street* }] }

Syntax Description

custom_id *ID*	Although available on the CLI, this option is not supported.
enable	Although visible on the CLI, configuring this keyword has no effect. Smart licensing is always enabled.
privacy { **all** | **hostname** | **version** }	Enables you to *leave out* certain information from the usage reports that are send to CSSM. Choose from the following options: • **all**: Sends only the minimal licensing information in any communication. • **hostname**: Excludes the hostname from any communication. • **version**: Excludes the product instance agent version from any communication.

proxy { **address** *address_hostname* | **port** *port* }	Configures a proxy for license usage synchronization with CSLU or CSSM. This means that you can use this option to configure a proxy only if the transport mode is **license smart transport smart** (CSSM), or **license smart transport cslu** (CSLU). However, you cannot configure a proxy for license usage synchronization in an SSM On-Prem deployment, which also uses **license smart transport cslu** as the transport mode. Configure the following options: • **address** *address_hostname*: Configures the proxy address. For *address_hostname*, enter the enter the IP address or hostname of the proxy. • **port***port*: Configures the proxy port. For *port*, enter the proxy port number.
reservation	Enables or disables a license reservation feature. **Note** Although available on the CLI, this option is not applicable because license *reservation* is not applicable in the Smart Licensing Using Policy environment.
server-identity-check	Enables or disables the HTTP secure server identity check.
transport { **automatic** | **callhome** | **cslu** | **off** | **smart** }	Configures the mode of transport the product instance uses to communicate with CSSM. Choose from the following options: • **automatic**: Sets the transport mode **cslu**. • **callhome**: Enables Call Home as the transport mode. • **cslu**: Enables CSLU as the transport mode. This is the default transport mode. The same keyword applies to both CSLU *and* SSM On-Prem, but the URLs are different. See **cslu***cslu_or_on-prem_url* in the following row. • **off**: Disables all communication from the product instance. • **smart**: Enables Smart transport.

url { *url* | **cslu** *cslu_url* | **default** | **smart** *smart_url* | **utility** *secondary_url* }

Sets a URL for the configured transport mode. Choose from the following options:

- *url*: If you have configured the transport mode as **callhome**, configure this option. Enter the CSSM URL exactly as follows:

  ```
  https://tools.cisco.com/its/service/oddce/services/DDCEService
  ```

  The **no license smart url** *url* command reverts to the default URL.

- **cslu** *cslu_or_on-prem_url*: If you have configured the transport mode as **cslu**, configure this option, with the URL for CSLU or SSM On-Prem, as applicable:

  - If you are using CSLU, enter the URL as follows:

    ```
    http://<cslu_ip_or_host>:8182/cslu/v1/pi
    ```

    For `<cslu_ip_or_host>`, enter the hostname or the IP address of the windows host where you have installed CSLU. 8182 is the port number and it is the only port number that CSLU uses.

    The **no license smart url cslu** *cslu_or_on-prem_url* command reverts to `http://cslu-local:8182/cslu/v1/pi`

  - If you are using SSM On-Prem, enter the URL as follows:

    ```
    http://<ip>/cslu/v1/pi/<tenant ID>
    ```

    For <ip>, enter the hostname or the IP address of the server where you have installed SSM On-Prem. The <tenantID> must be the default local virtual account ID.

    Tip You can retrieve the entire URL from SSM On-Prem. In the software configuration guide of the required release (17.3.x onwards), see *System Management > Smart Licensing Using Policy* > Task Library for Smart Licensing Using Policy > Retrieving the Transport URL (SSM On-Prem UI).

    The **no license smart url cslu** *cslu_or_on-prem_url* command reverts to `http://cslu-local:8182/cslu/v1/pi`

- **default**: Depends on the configured transport mode. Only the **smart** and **cslu** transport modes are supported with this option.

  If the transport mode is set to **cslu**, and you configure

license smart url default, the CSLU URL is configured automatically (`https://cslu-local:8182/cslu/v1/pi`).

If the transport mode is set to **smart**, and you configure **license smart url default**, the Smart URL is configured automatically (`https://smartreceiver.cisco.com/licservice/license`).

- **smart** *smart_url*: If you have configured the transport type as **smart**, configure this option. Enter the URL exactly as follows:

  ```
  https://smartreceiver.cisco.com/licservice/license
  ```

  When you configure this option, the system automatically creates a duplicate of the URL in **license smart url** *url*. You can ignore the duplicate entry, no further action is required.

  The **no license smart url smart***smart_url* command reverts to the default URL.

- **utility** *smart_url*: Although available on the CLI, this option is not supported.

usage { **customer-tags** { **tag1** | **tag2** | **tag3** | **tag4** } *tag_value* | **interval** *interval_in_days* }	Configures usage reporting settings. You can set the following options: • **customer-tags** { **tag1** | **tag2** | **tag3** | **tag4** } *tag_value*: Defines strings for inclusion in data models, for telemetry. Up to 4 strings (or tags) may be defined. For *tag_value*, enter the string value for each tag that you define. • **interval** *interval_in_days*: Sets the reporting interval in days. By default the RUM report is sent every 30 days. The valid value range is 1 to 3650. If you set the value to zero, RUM reports are not sent, regardless of what the applied policy specifies - this applies to topologies where CSLU or CSSM may be on the receiving end. If you set a value that is greater than zero and the transport type is set to **off**, then, between the *interval_in_days* and the policy value for `Ongoing reporting frequency(days):`, the lower of the two values is applied. For example, if *interval_in_days* is set to 100, and the value in the in the policy says `Ongoing reporting frequency (days):90`, RUM reports are sent every 90 days. If you do not set an interval, and the default is effective, the reporting interval is determined entirely by the policy value. For example, if the default value is effective and only unenforced licenses are in use, if the policy states that reporting is not required, then RUM reports are not sent.
utility [**customer_info** { **city** *city* | **country** *country* | **postalcode** *postalcode* | **state** *state* | **street** *street* }]	Although visible on the CLI, this option is not supported.

Command Default

Cisco IOS XE Amsterdam 17.3.1 or earlier: Smart Licensing is enabled by default

Cisco IOS XE Amsterdam 17.3.2a and later: Smart Licensing Using Policy is enabled by default.

Command Modes

Global config (Device(config)#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Release	Modification
Cisco IOS XE Amsterdam 17.3.2a	The following keywords and variables were introduced with Smart Licensing Using Policy: • Under the **url**keyword, these options were introduced: { **cslu** *cslu_url* | **smart** *smart_url* } • Under the **transport** keyword, these options were introduced: { **cslu** | **off** } Further, the default transport type was changed from **callhome**, to **cslu**. • **usage** { **customer-tags** { **tag1** | **tag2** | **tag3** | **tag4** } *tag_value* | **interval** *interval_in_days* } The following keywords and variables under the **license smart** global command are deprecated and no longer available on the CLI: **enable**and **conversion automatic**.
Cisco IOS XE Amsterdam 17.3.3	SSM On-Prem support was introduced. For product instance-initiated communication in an SSM On-Prem deployment, the existing [**no**]**license smart url cslu***cslu_or_on-prem_url* command supports the configuration of a URL for SSM On-Prem as well. But the required URL format for SSM On-Prem is: `http://<ip>/cslu/v1/pi/<tenant ID>`. The corresponding transport mode that must be configured is also an existing command (**license smart transport cslu**).

Usage Guidelines

Communication failure and reporting

The reporting interval that you configure (**license smart usage interval** *interval_in_days* command), determines the date and time at which the product instance sends out the RUM report. If the scheduled interval coincides with a communication failure, the product instance attempts to send out the RUM report for up to four hours after the scheduled time has expired. If it is still unable to send out the report (because the communication failure persists), the system resets the interval to 15 minutes. Once the communication failure is resolved, the system reverts the reporting interval to the value that you last configured.

The system message you may see in case of a communicatin failure is %SMART_LIC-3-COMM_FAILED. For information about resolving this error and restoring the reporting interval value, in the software configuration guide of the required release (17.3.x onwards), see *System Management* > *Smart Licensing Using Policy* > *Troubleshooting Smart Licensing Using Policy*.

Proxy server acceptance

When configuring the **license smart proxy** {**address** *address_hostname* | **port***port*} command, note the change in the criteria for the acceptance of proxy servers, starting with Cisco IOS XE Bengaluru 17.6.1: only the status code of the proxy server response is verified by the system and not the reason phrase. The RFC format is `status-line = HTTP-version SP status-code SP reason-phrase CRLF`, where the status code is a three-digit numeric code. For more information about the status line, see section 3.1.2 of RFC 7230.

- Examples for Data Privacy, on page 57
- Examples for Transport Type and URL, on page 57

- Examples for Usage Reporting Options, on page 58

Examples for Data Privacy

The following examples show how to configure data privacy related information using **license smart privacy** command in global configuration mode. The accompanying **show license status** output displays configured information.

No private information is sent:

```
Device# configure terminal
Device(config)# license smart privacy all
Device(config)# license smart transport callhome
Device(config)# license smart url
https://tools.cisco.com/its/service/oddce/services/DDCEService
Device(config)# exit
Device# show license status
<output truncated>
Data Privacy:
  Sending Hostname: no
    Callhome hostname privacy: ENABLED
    Smart Licensing hostname privacy: ENABLED
  Version privacy: ENABLED

Transport:
  Type: Callhome
<output truncated>
```

Agent version on the product instance is not sent:

```
Device# configure terminal
Device(config)# license smart privacy version
Device(config)# license smart transport callhome
Device(config)# license smart url
https://tools.cisco.com/its/service/oddce/services/DDCEService
Device(config)# exit
Device# show license status
<output truncated>
Data Privacy:
  Sending Hostname: yes
    Callhome hostname privacy: DISABLED
    Smart Licensing hostname privacy: DISABLED
  Version privacy: ENABLED

Transport:
  Type: Callhome
<output truncated>
```

Examples for Transport Type and URL

The following examples show how to configure some of the transport types using the **license smart transport** and the **license smart url** commands in global configuration mode. The accompanying **show license all** output displays configured information.

Transport: **cslu**:

```
Device# configure terminal
Device(config)# license smart transport cslu
Device(config)# license smart url default
Device(config)# exit
Device# show license all
```

```
<output truncated>
Transport:
  Type: cslu
  Cslu address: http://192.168.0.1:8182/cslu/v1/pi
  Proxy:
    Not Configured
<output truncated>
```

Transport: **smart**:

```
Device# configure terminal
Device(config)# license smart transport smart
Device(config)# license smart url smart https://smartreceiver.cisco.com/licservice/license
Device(config)# exit
Device# show license all
<output truncated>
Transport:
  Type: Smart
  URL: https://smartreceiver-stage.cisco.com/licservice/license
  Proxy:
    Not Configured
<output truncated>
```

Examples for Usage Reporting Options

The following examples show how to configure some of the usage reporting settings using the **license smart usage** command in global configuration mode. The accompanying **show running-config** output displays configured information.

Configuring the **customer-tag** option:

```
Device# configure terminal
Device(config)# license smart usage customer-tags tag1 SA/VA:01
Device(config)# exit
Device# show running-config | include tag1
license smart usage customer-tags tag1 SA/VA:01
```

Configuring a narrower reporting interval than the currently applied policy:

```
Device# show license status
<output truncated>
Usage Reporting:
Last ACK received: Sep 22 13:49:38 2020 PST
Next ACK deadline: Dec 21 12:02:21 2020 PST
Reporting push interval: 30 days
Next ACK push check: Sep 22 12:20:34 2020 PST
Next report push: Oct 22 12:05:43 2020 PST
Last report push: Sep 22 12:05:43 2020 PST
Last report file write: <none>
<output truncated>

Device# configure terminal
Device(config)# license smart usage interval 20
Device(config)# exit
Device# show license status
<output truncated>

Usage Reporting:
Last ACK received: Sep 22 13:49:38 2020 PST
Next ACK deadline: Nov 22 12:02:21 2020 PST
Reporting push interval: 20 days
Next ACK push check: Sep 22 12:20:34 2020 PST
Next report push: Oct 12 12:05:43 2020 PST
Last report push: Sep 22 12:05:43 2020 PST
Last report file write: <none>
<output truncated>
```

license smart (privileged EXEC)

To configure licensing functions such as requesting or returning authorization codes, saving Resource Utilization Measurement reports (RUM reports), importing a file on to a product instance, establishing trust with Cisco Smart Software Manager (CSSM), synchronizing the product instance with CSSM, or Cisco Smart License Utility (CSLU), or Smart Software Manager On-Prem (SSM On-Prem), and removing licensing information from the product instance, enter the **license smart** command in privileged EXEC mode with the corresponding keyword or argument.

license smart { **authorization** { **request** { **add** | **replace** } *feature_name* { **all** | **local** } | **return** { **all** | **local** } { **offline** [*path*] | **online** } } | **clear eventlog** | **export return** { **all** | **local** } *feature_name* | **factory reset** | **import** *file_path* | **save** { **trust-request** *filepath_filename* | **usage** { **all** | **days** *days* | **rum-id** *rum-ID* | **unreported** } { **file** *file_path* } } | **sync** { **all** | **local** } | **trust idtoken** *id_token_value* { **local** | **all** } [{ **force** }] }

Syntax Description

smart	Provides options for Smart Licensing.
authorization	Provides the option to request for, or return, authorization codes. Authorization codes are required *only* if you use licenses with enforcement type: export-controlled or enfored.
request	Requests an authorization code from CSSM, CSLU (CSLU in-turn fetches it from CSSM), or SSM On-Prem and installs it on the product instance.
add	Adds the requested license to the existing authorization code. The new authorization code will contain all the licenses of the existing authorization code and the requested license.
replace	Replaces the existing authorization code. The new authorization code will contain only the requested license. All licenses in the current authorization code are returned. When you enter this option, the product instance verifies if licenses that correspond to the authorization codes that will be removed, are in-use. If licenses are being used, an error message tells you to first disable the corresponding features.
feature_name	Name of the license for which you are requesting an authorization code.
all	Performs the action for all product instances in a High Availability or stacking set-up.
local	Performs the action for the *active* product instance. This is the default option.
return	Returns an authorization code back to the license pool in CSSM.
offline *file_path*	Means the product instance is not connected to CSSM. The authorization code is returned offline. This option requires you to print the return code to a file. Optionally, you can also specify a path to save the file. The file format can be any readable format, such as `.txt` If you choose the offline option, you must complete the additional step of copying the return code from the CLI or the saved file and entering it in CSSM.

online	Means that the product instance is in a connected mode. The authorization code is returned to CSLU or CSSM directly.
clear eventlog	Clears all event log files from the product instance.
export return	Although visible on the CLI, this command is not applicable in the Smart Licensing Using Policy environment. Use the **license smart authorization return** privileged EXEC command to return an authorization code instead.
factory reset	Clears all saved licensing information from the product instance.
import *filepath_filename*	Imports a file on to the product instance. The file may be that of an authorization code, a trust code, or, or a policy. For *filepath_filename*, specify the location, including the filename.
save	Provides options to save RUM reports or trust code requests.
trust-request *filepath_filename*	Saves the trust code request for the active product instance in the specified location. For *filepath_filename*, specify the absolute path to the file, including the filename.
usage { **all** | **days** *days* | **rum-id** *rum-ID* | **unreported** } { **file** *file_path* }	Saves RUM reports (license usage information) in the specified location. You must specify one of these options: • **all**: Saves all RUM reports. • **days** *days*: Saves RUM report for the last *n* number of days (excluding the current day). Enter a number. The valid range is 0 to 4294967295. For example, if you enter 3, RUM reports of the last three days are saved. • **rum-Id** *rum-ID*: Saves a specified RUM ID. The valid value range is 0 to 18446744073709551615. • **unreported**: Saves all unreported RUM reports. **file** *filepath_filename*: Saves the specified usage information to a file. Specify the absolute path to the file, including the filename.
sync { **all** | **local** }	Synchronizes with CSSM or CSLU, or SSM On-Prem, to send and receive any pending data. This includes uploading pending RUM reports, downloading the ACK response, any pending authorization codes, trust codes, and policies for the product instance. Specify the product instance by entering one of these options: • **all**: Performs synchronization for all the product instances in a High Availability or stacking set-up. If you choose this option, the product instance also sends the list of all the UDIs in the synchronization request. • **local**: Performs synchronization only for the active product instance sending the request, that is, its own UDI. This is the default option.

trust idtoken *id_token_value*	Establishes a trusted connection with CSSM. To use this option, you must first generate a token in the CSSM portal. Provide the generated token value for *id_token_value*.
force	Submits a trust code request even if a trust code already exists on the product instance. A trust code is node-locked to the UDI of a product instance. If the UDI is already registered, CSSM does not allow a new registration for the same UDI. Entering the **force** keyword overrides this behavior.

Command Default

Cisco IOS XE Amsterdam 17.3.1 and earlier: Smart Licensing is enabled by default.

Cisco IOS XE Amsterdam 17.3.2a and later: Smart Licensing Using Policy is enabled by default.

Command Modes

Privileged EXEC (Device#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.
Cisco IOS XE Amsterdam 17.3.2a	The following keywords and variables were introduced with Smart Licensing Using Policy: • **authorization** { **request** { **add** | **replace** } *feature_name* { **all** | **local** } | **return** { **all** | **local** } { **offline** [*path*] | **online** } } • **import** *file_path* • **save** { **trust-request** *filepath_filename* | **usage** { **all** | **days** *days* | **rum-id** *rum-ID* | **unreported** } { **file** *file_path* } } • **sync** { **all** | **local** } • **trust idtoken** *id_token_value* { **local** | **all** } [**force**] The following keywords and variables under the **license smart** command are deprecated and no longer available on the CLI: • **register idtoken** *token_id* [**force**] • **deregister** • **renew id** { **ID** | **auth** } • **debug** { **error** | **debug** | **trace** | **all** } • **mfg reservation** { **request** | **install** | **install file** | **cancel** } • **conversion** { **start** | **stop** }

Release	Modification
Cisco IOS XE Amsterdam 17.3.3	Support for SSM On-Prem was introduced. You can perform licensing-related tasks such as saving Resource Utilization Measurement reports (RUM reports), importing a file on to a product instance, synchronizing the product instance, returning authorization codes, and removing licensing information from the product instance in an SSM On-Prem deployment.
Cisco IOS XE Bengaluru 17.6.2	Support for the Export Control Key for High Security (HSECK9), was introduced on the Cisco Catalyst 9300X Series Switches. The authorization code related commands (**license smart authorization request** and **license smart authorization return**) can be used to request and return the Smart Licensing Authorization Code (SLAC) for the HSECK9 key, on supported platforms.

Usage Guidelines

Overwriting a Trust Code

Use case for the **force** option when configuring the **license smart trust idtoken** command: You use same token for all the product instances that are part of one Virtual Account. If the product instance has moved from one account to another (for instance, because it was added to a High Availability set-up, which is part of another Virtual Account), then there may be an existing trust code you have to overwrite.

Removing Licensing Information

Entering the **licence smart factory reset** command removes all licensing information (except the licenses in-use) from the product instance, including any authorization codes, RUM reports etc. Therefore, we recommend the use of this command only if the product instance is being returned (Return Material Authrization, or RMA), or being decommissioned permanently. We also recommend that you return any authorization codes and send a RUM report to CSSM, before you remove licensing information from the product instance - this is to ensure that CSSM has up-to-date usage information.

Requesting and Returning Authorization Codes:

- Use the following command to request SLAC on supported product instances. In a stacking set-up, you can request SLAC for either the active (**local**), or the entire stack (**all**). You cannot request SLAC for just one member or standby.

  license smart authorization request { **add** | **replace** } *feature_name* { **all** | **local** }

- Use the following command to return a SLAC or an SLR authorization code:

  license smart authorization return { **all** | **local** } { **offline** [*path*] | **online** }

  While you can return an SLR authorization code in the Smart Licensing Using Policy environment, you cannot request a new SLR in the Smart Licensing Using Policy environment, because the notion of “reservation” does not apply. If you are in an air-gapped network, the *No Connectivity to CSSM and No CSLU* topology applies instead.

Examples

- Example for Requesting SLAC, on page 64
- Example for Saving Licensing Usage Information, on page 64
- Example for Installing a Trust Code, on page 65

- Example for Returning an SLR Authorization Code, on page 65

Example for Requesting SLAC

The following example shows how you can request and install SLAC on a product instance that is directly connected to CSSM. This example is of a stacking set-up with an active, a standby, and a member - all the devices in the stack are C9300X and support the HSECK9 key and IPSec. IPsec is a cryptographic feature which requires an HSECK9 key. A SLAC is requested for all the product instances in the set-up.

```
Device# license smart authorization request add hseck9 all
Device#
Oct 19 15:49:47.888: %SMART_LIC-6-AUTHORIZATION_INSTALL_SUCCESS: A new licensing authorization
 code was successfully installed on PID:C9300X-24HX,SN:FOC2519L8R7
Oct 19 15:49:47.946: %SMART_LIC-6-AUTHORIZATION_INSTALL_SUCCESS: A new licensing authorization
 code was successfully installed on PID:C9300X-48HXN,SN:FOC2524L39P
Oct 19 15:49:48.011: %SMART_LIC-6-AUTHORIZATION_INSTALL_SUCCESS: A new licensing authorization
 code was successfully installed on PID:C9300X-48HX,SN:FOC2516LC92

Device# show license authorization
Overall status:
  Active: PID:C9300X-24HX,SN:FOC2519L8R7
      Status: SMART AUTHORIZATION INSTALLED on Oct 19 15:49:47 2021 UTC
      Last Confirmation code: 4e740fb8
  Standby: PID:C9300X-48HXN,SN:FOC2524L39P
      Status: SMART AUTHORIZATION INSTALLED on Oct 19 15:49:47 2021 UTC
      Last Confirmation code: 086d28d7
  Member: PID:C9300X-48HX,SN:FOC2516LC92
      Status: SMART AUTHORIZATION INSTALLED on Oct 19 15:49:48 2021 UTC
      Last Confirmation code: beb51aa1

Authorizations:
  C9K HSEC (Cat9K HSEC):
    Description: HSEC Key for Export Compliance on Cat9K Series Switches
    Total available count: 3
    Enforcement type: EXPORT RESTRICTED
    Term information:
      Active: PID:C9300X-24HX,SN:FOC2519L8R7
        Authorization type: SMART AUTHORIZATION INSTALLED
        License type: PERPETUAL
          Term Count: 1
      Standby: PID:C9300X-48HXN,SN:FOC2524L39P
        Authorization type: SMART AUTHORIZATION INSTALLED
        License type: PERPETUAL
          Term Count: 1
      Member: PID:C9300X-48HX,SN:FOC2516LC92
        Authorization type: SMART AUTHORIZATION INSTALLED
        License type: PERPETUAL
          Term Count: 1

Purchased Licenses:
  No Purchase Information Available
```

Example for Saving Licensing Usage Information

The following example shows how you can save license usage information on the product instance. You can use this option to fulfil reporting requirements in an air-gapped network. In the example, the file is first save to flash memory and then copied to a TFTP location:

```
 Device> enable
Device# license smart save usage unreported file flash:RUM-unrep.txt
Device# copy flash:RUM-unrep.txt tftp://192.168.0.1//auto/tftp-user/user01/
```

```
Address or name of remote host [192.168.0.1]?
Destination filename [//auto/tftp-user/user01/RUM-unrep.txt]?
!!
15128 bytes copied in 0.161 secs (93963 bytes/sec)
```

After you save RUM reports to a file, you must upload it to CSSM (from a workstation that has connectivity to the internet, and Cisco).

Example for Installing a Trust Code

The following example shows how to install a trust code even if one is already installed on the product instance. This requires connectivity to CSSM. The accompanying **show license status** output shows sample output after successful installation:

Before you can install a trust code, you must generate a token and download the corresponding file from CSSM.

Use the **show license status** command (`Trust Code Installed:`) to verify results.

```
Device> enable
Device# license smart trust idtoken
NGMwMjk5mYtNZaxMS00NzMZmtgWm local force
Device# show license status
<output truncated>
Trust Code Installed:
  Active: PID:C9500-24Y4C,SN:CAT2344L4GH
    INSTALLED on Sep 04 01:01:46 2020 EDT
  Standby: PID:C9500-24Y4C,SN:CAT2344L4GJ
    INSTALLED on Sep 04 01:01:46 2020 EDT
<output truncated>
```

Example for Returning an SLR Authorization Code

The following example shows how to remove and return an SLR authorization code. Here the code is returned offline (no connectivity to CSSM). The accompanying **show license all** output shows sample output after successful return:

```
Device> enable
Device# license smart authorization return local offline
Enter this return code in Cisco Smart Software Manager portal:
UDI: PID:C9500-16X,SN:FCW2233A5ZV
Return code: Cr9JHx-L1x5Rj-ftwzg1-h9QZAU-LE5DT1-babWeL-FABPt9-Wr1Dn7-Rp7
Device# configure terminal
Device(config)# no license smart reservation

Device# show license all
<output truncated>
License Authorizations
======================
Overall status:
  Active: UDI: PID:C9500-16X,SN:FCW2233A5ZV
      Status: NOT INSTALLED
      Last return code: Cr9JHx-L1x5Rj-ftwzg1-h9QZAU-LE5DT1-babWeL-FABPt9-Wr1Dn7-Rp7
<output truncated>
```

Since the product instance is in an air-gapped network, you must copy the return code from the CLI, locate the product instance in the CSSM Web UI and enter the return code there to complete the return process.

line auto-consolidation

To consolidate multiple line configurations of the same submode into a single line, use the **line auto-consolidation** command in global configuration mode. Auto-consolidation of line configurations is enabled by default. Starting with the Cisco IOS XE Bengaluru 17.4.1 you can disable auto consolidation by using the **no** form of the command.

line auto-consolidation
no line auto-consolidation

Syntax Description

auto-consolidation	Consolidates multiple line configurations of the same submode into a single line.

Command Default

Autoconsolidation is enabled by default.

Command Modes

Global configuration mode (config)

Command History

Release	Modification
Cisco IOS XE Bengaluru 17.4.1	The command was introduced.

The following example shows the nonvolatile generation (NVGEN) process output with **line auto-consolidation** configured:

```
Device# show run | sec line
line con 0
stopbits 1
line vty 0 4
transport input ssh
line vty 5 9
transport input all
Device# configure terminal
Device(config)# line vty 10 15
Device(config-line)# transport input all
Device(config-line)# end
Device# show run | sec line
line con 0
stopbits 1
line vty 0 4
transport input ssh
line vty 5 15
transport input all
```

The following example shows the nonvolatile generation (NVGEN) process output after **no line auto-consolidation** is configured:

```
Device# show run | sec line
line con 0
stopbits 1
line vty 0 4
transport input ssh
line vty 5 9
transport input all
Device# configure terminal
```

```
Device(config)#no line auto-consolidation
Device(config)# line vty 10 15
Device(config-line)# transport input all
Device(config-line)# end
Device# show run | sec line
no line auto-consolidation
line con 0
stopbits 1
line vty 0 4
transport input ssh
line vty 5 9
transport input all
line vty 10 15
transport input all
```

location

To configure location information for an endpoint, use the **location** command in global configuration mode. To remove the location information, use the **no** form of this command.

location {**admin-tag** *string* | **civic-location identifier** {**host***id*} | **civic-location identifier** {**host***id*} | **elin-location** {*string* | **identifier** *id*} | **geo-location identifier** {**host***id*} | **prefer**{**cdp weight** *priority-value* | **lldp-med weight** *priority-value* | **static config weight** *priority-value*}
no location {**admin-tag** *string* | **civic-location identifier** {**host***id*} | **civic-location identifier** {**host***id*} | **elin-location** {*string* | **identifier** *id*} | **geo-location identifier** {**host***id*} | **prefer**{**cdp weight** *priority-value* | **lldp-med weight** *priority-value* | **static config weight** *priority-value*}

Syntax Description

admin-tag*string*	Configures administrative tag or site information. Site or location information in alphanumeric format.
civic-location	Configures civic location information.
identifier	Specifies the name of the civic location, emergency, or geographical location.
host	Defines the host civic or geo-spatial location.
id	Name of the civic, emergency, or geographical location. **Note** The identifier for the civic location in the LLDP-MED switch TLV is limited to 250 bytes or less. To avoid error messages about available buffer space during switch configuration, be sure that the total length of all civic-location information specified for each civic-location identifier does not exceed 250 bytes.
elin-location	Configures emergency location information (ELIN).
geo-location	Configures geo-spatial location information.
prefer	Sets location information source priority.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

After entering the **location civic-location identifier** global configuration command, you enter civic location configuration mode. After entering the **location geo-location identifier** global configuration command, you enter geo location configuration mode.

The civic-location identifier must not exceed 250 bytes.

The host identifier configures the host civic or geo-spatial location. If the identifier is not a host, the identifier only defines a civic location or geo-spatial template that can be referenced on the interface.

The **host** keyword defines the device location. The civic location options available for configuration using the **identifier** and the **host** keyword are the same. You can specify the following civic location options in civic location configuration mode:

- **additional-code**—Sets an additional civic location code.
- **additional-location-information**—Sets additional civic location information.
- **branch-road-name**—Sets the branch road name.
- **building**—Sets building information.
- **city**—Sets the city name.
- **country**—Sets the two-letter ISO 3166 country code.
- **county**—Sets the county name.
- **default**—Sets a command to its defaults.
- **division**—Sets the city division name.
- **exit**—Exits from the civic location configuration mode.
- **floor**—Sets the floor number.
- **landmark**—Sets landmark information.
- **leading-street-dir**—Sets the leading street direction.
- **name**—Sets the resident name.
- **neighborhood**—Sets neighborhood information.
- **no**—Negates the specified civic location data and sets the default value.
- **number**—Sets the street number.
- **post-office-box**—Sets the post office box.
- **postal-code**—Sets the postal code.
- **postal-community-name**—Sets the postal community name.
- **primary-road-name**—Sets the primary road name.
- **road-section**—Sets the road section.
- **room**—Sets room information.
- **seat**—Sets seat information.
- **state**—Sets the state name.
- **street-group**—Sets the street group.
- **street-name-postmodifier**—Sets the street name postmodifier.
- **street-name-premodifier**—Sets the street name premodifier.
- **street-number-suffix**—Sets the street number suffix.
- **street-suffix**—Sets the street suffix.
- **sub-branch-road-name**—Sets the sub-branch road name.
- **trailing-street-suffix**—Sets the trailing street suffix.
- **type-of-place**—Sets the type of place.
- **unit**—Sets the unit.

You can specify the following geo-spatial location information in geo-location configuration mode:

- **altitude**—Sets altitude information in units of floor, meters, or feet.
- **latitude**—Sets latitude information in degrees, minutes, and seconds. The range is from -90 degrees to 90 degrees. Positive numbers indicate locations north of the equator.

- **longitude**—Sets longitude information in degrees, minutes, and seconds. The range is from -180 degrees to 180 degrees. Positive numbers indicate locations east of the prime meridian.
- **resolution**—Sets the resolution for latitude and longitude. If the resolution value is not specified, default value of 10 meters is applied to latitude and longitude resolution parameters. For latitude and longitude, the resolution unit is measured in meters. The resolution value can also be a fraction.
- **default**—Sets the geographical location to its default attribute.
- **exit**—Exits from geographical location configuration mode.
- **no**—Negates the specified geographical parameters and sets the default value.

Use the **no lldp med-tlv-select location information** interface configuration command to disable the location TLV. The location TLV is enabled by default.

This example shows how to configure civic location information on the switch:

```
Device(config)# location civic-location identifier 1
Device(config-civic)# number 3550
Device(config-civic)# primary-road-name “Cisco Way”
Device(config-civic)# city “San Jose”
Device(config-civic)# state CA
Device(config-civic)# building 19
Device(config-civic)# room C6
Device(config-civic)# county “Santa Clara”
Device(config-civic)# country US
Device(config-civic)# end
```

You can verify your settings by entering the **show location civic-location** privileged EXEC command.

This example shows how to configure the emergency location information on the switch:

```
Device(config)# location elin-location 14085553881 identifier 1
```

You can verify your settings by entering the **show location elin** privileged EXEC command.

The example shows how to configure geo-spatial location information on the switch:

```
Device(config)# location geo-location identifier host
Device(config-geo)# latitude 12.34
Device(config-geo)# longitude 37.23
Device(config-geo)# altitude 5 floor
Device(config-geo)# resolution 12.34
```

You can use the **show location geo-location identifier** command to display the configured geo-spatial location details.

location plm calibrating

To configure path loss measurement (CCX S60) request for calibrating clients, use the **location plm calibrating** command in global configuration mode.

location plm calibrating {**multiband** | **uniband**}

Syntax Description

multiband	Specifies the path loss measurement request for calibrating clients on the associated 802.11a or 802.11b/g radio.
uniband	Specifies the path loss measurement request for calibrating clients on the associated 802.11a/b/g radio.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

The uniband is useful for single radio clients (even if the radio is a dual band and can operate in the 2.4-GHz and the 5-GHz bands). The multiband is useful for multiple radio clients.

This example shows how to configure the path loss measurement request for calibrating clients on the associated 802.11a/b/g radio:

```
Device# configure terminal
Device(config)# location plm calibrating uniband
Device(config)# end
```

mgmt_init

To initialize the Ethernet management port, use the **mgmt_init** command in boot loader mode.

mgmt_init

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Boot loader

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Use the **mgmt_init** command only during debugging of the Ethernet management port.

Examples

This example shows how to initialize the Ethernet management port:

```
Device: mgmt_init
```

mkdir

To create one or more directories on the specified file system, use the **mkdir** command in boot loader mode.

mkdir *filesystem:/directory-url...*

Syntax Description

filesystem:	Alias for a file system. Use **usbflash0:** for USB memory sticks.
/directory-url...	Name of the directories to create. Separate each directory name with a space.

Command Default

No default behavior or values.

Command Modes

Boot loader

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Directory names are case sensitive.

Directory names are limited to 127 characters between the slashes (/); the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.

Example

This example shows how to make a directory called Saved_Configs:

```
Device: mkdir usbflash0:Saved_Configs
Directory "usbflash0:Saved_Configs" created
```

more

To display the contents of one or more files, use the **more** command in boot loader mode.

more *filesystem:/file-url...*

Syntax Description

filesystem:	Alias for a file system. Use **flash:** for the system board flash device.
/file-url...	Path (directory) and name of the files to display. Separate each filename with a space.

Command Default

No default behavior or values.

Command Modes

Boot loader

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Filenames and directory names are case sensitive.

If you specify a list of files, the contents of each file appears sequentially.

Examples

This example shows how to display the contents of a file:

```
Device: more flash:image_file_name
version_suffix: universal-122-xx.SEx
version_directory: image_file_name
image_system_type_id: 0x00000002
image_name: image_file_name.bin
ios_image_file_size: 8919552
total_image_file_size: 11592192
image_feature: IP|LAYER_3|PLUS|MIN_DRAM_MEG=128
image_family: family
stacking_number: 1.34
board_ids: 0x00000068 0x00000069 0x0000006a 0x0000006b
info_end:
```

no debug all

To disable debugging on a switch, use the **no debug all** command in Privileged EXEC mode.

no debug all

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Release 16.1	This command was introduced.

Examples

This example shows how to disable debugging on a switch.

```
Device: no debug all
All possible debugging has been turned off.
```

rename

To rename a file, use the **rename** command in boot loader mode.

rename *filesystem:/source-file-url filesystem:/destination-file-url*

Syntax Description

filesystem:	Alias for a file system. Use **usbflash0:** for USB memory sticks.
/source-file-url	Original path (directory) and filename.
/destination-file-url	New path (directory) and filename.

Command Default

No default behavior or values.

Command Modes

Boot loader

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Filenames and directory names are case sensitive.

Directory names are limited to 127 characters between the slashes (/); the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.

Filenames are limited to 127 characters; the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.

Examples

This example shows a file named *config.text* being renamed to *config1.text*:

```
Device: rename usbflash0:config.text usbflash0:config1.text
```

You can verify that the file was renamed by entering the **dir** *filesystem:* boot loader command.

request consent-token accept-response shell-access

To submit the Consent Token response to a previously generated challenge, use the **request consent-token accept-response shell-access** command.

request consent-token accept-response shell-access *response-string*

Syntax Description

Syntax	Description
response-string	Specifies the character string representing the response.

Command Modes

Privileged EXEC mode (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

Usage Guidelines

You must enter the response string within 30 minutes of challenge generation. If it is not entered, the challenge expires and a new challenge must be requested.

Example

The following is sample output from the **request consent-token accept-response shell-access** *response-string* command:

```
Device# request consent-token accept-response shell-access
[illegible]
% Consent token authorization success
*Jan 18 02:51:37.807: %CTOKEN-6-AUTH_UPDATE: Consent Token Update (authentication success:
 Shell access 0).
```

request consent-token generate-challenge shell-access

To generate a Consent Token challenge for system shell access, use the **request consent-token generate-challenge shell-access** command.

request consent-token generate-challenge shell-access auth-timeout *time-validity-slot*

Syntax Description

Syntax	Description
auth-timeout *time-validity-slot*	Specifies the time slot in minutes for which shell-access is requested.

Command Modes

Privileged EXEC mode (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

Usage Guidelines

When the requested time-slot for system shell expires, the session gets terminated automatically.

The maximum authorization timeout for system shell access is seven days.

Example

The following is sample output from the **request consent-token generate-challenge shell-access auth-timeout** *time-validity-slot* command:

```
Device# request consent-token generate-challenge shell-access auth-timeout 900
zSSdrAAAAQEBAAQAAAABAgAEAAAAAAMACH86csUhmDl0BAAQ0Fvd7CxqRYUeoD7B4AwW7QUABAAAAG8GAAhDVEFfREVNTwAGENUQV9ERU1PX0NUQV9TSUdOSU5HX0tFWQgAC0M5ODAwLUNMLU5CQALOVpQUEVESE5KRkI=
Device#
*Jan 18 02:47:06.733: %CTOKEN-6-AUTH_UPDATE: Consent Token Update (challenge generation
attempt: Shell access 0).
```

request consent-token terminate-auth

To terminate the Consent Token based authorization to system shell, use the **request consent-token terminate-auth** command.

request consent-token terminate-auth

Command Modes

Privileged EXEC mode (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.11.1	This command was introduced.

Usage Guidelines

In system shell access scenario, exiting the shell does not terminate authorization until the authorization timeout occurs.

We recommend that you force terminate system shell authorization by explicitly issuing the **request consent-token terminate-auth** command once the purpose of system shell access is complete.

If the current authentication is terminated using the **request consent-token terminate-auth** command, the user will have to repeat the authentication process to gain access to system shell.

Example

The following is sample output from the **request consent-token terminate-auth** command:

```
Device# request consent-token terminate-auth shell-access
% Consent token authorization termination success

Device#
*Mar 13 01:45:39.197: %CTOKEN-6-AUTH_UPDATE: Consent Token Update (terminate authentication:
 Shell access 0).
Device#
```

request platform software console attach switch

To start a session on a member switch, use the **request platform software console attach switch** command in privileged EXEC mode.

Note On stacking switches (Catalyst 3650/3850/9200/9300 switches), this command can only be used to start a session on the standby console. On Catalyst 9500 switches, this command is supported only in a stackwise virtual setup. You cannot start a session on member switches. By default, all consoles are already active, so a request to start a session on the active console will result in an error.

request platform software console attach switch { *switch-number* **| active | standby } { 0/0 | R0 }**

Syntax Description

switch-number	Specifies the switch number. The range is from 1 to 9.
active	Specifies the active switch. **Note** This argument is not supported on Catalyst 9500 switches.
standby	Specifies the standby switch.
0/0	Specifies that the SPA-Inter-Processor slot is 0, and bay is 0. **Note** Do not use this option with stacking switches. It will result in an error.
R0	Specifies that the Route-Processor slot is 0.

Command Default

By default, all switches in the stack are active.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

To start a session on the standby switch, you must first enable it in the configuration.

Examples

This example shows how to session to the standby switch:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# redundancy
Device(config-red)# main-cpu
Device(config-r-mc)# standby console enable
Device(config-r-mc)# end
```

```
Device# request platform software console attach switch standby R0
#
# Connecting to the IOS console on the route-processor in slot 0.
# Enter Control-C to exit.
#
Device-stby> enable
Device-stby#
```

reset

To perform a hard reset on the system, use the **reset** command in boot loader mode. A hard reset is similar to power-cycling the device; it clears the processor, registers, and memory.

reset

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Boot loader

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Examples

This example shows how to reset the system:

```
Device: reset
Are you sure you want to reset the system (y/n)? y
System resetting...
```

rmdir

To remove one or more empty directories from the specified file system, use the **rmdir** command in boot loader mode.

rmdir *filesystem:/directory-url...*

Syntax Description

filesystem:	Alias for a file system. Use **usbflash0:** for USB memory sticks.
/directory-url...	Path (directory) and name of the empty directories to remove. Separate each directory name with a space.

Command Default

No default behavior or values.

Command Modes

Boot loader

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Directory names are case sensitive and limited to 45 characters between the slashes (/); the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.

Before removing a directory, you must first delete all of the files in the directory.

The device prompts you for confirmation before deleting each directory.

Example

This example shows how to remove a directory:

```
Device: rmdir usbflash0:Test
```

You can verify that the directory was deleted by entering the **dir** *filesystem:* boot loader command.

sdm prefer

To specify the SDM template for use on the switch, use the **sdm prefer** command in global configuration mode.

sdm prefer
{**advanced**}

Syntax Description

advanced	Supports advanced features such as NetFlow.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

In a stack, all stack members must use the same SDM template that is stored on the active .

When a new is added to a stack, the SDM configuration that is stored on the active overrides the template configured on an individual .

Example

This example shows how to configure the advanced template:

```
Device(config)# sdm prefer advanced
Device(config)# exit
Device# reload
```

service private-config-encryption

To enable private configuration file encryption, use the **service private-config-encryption** command. To disable this feature, use the **no** form of this command.

service private-config-encryption
no service private-config-encryption

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Examples

The following example shows how to enable private configuration file encryption:

```
Device> enable
Device# configure terminal
Device(config)# service private-config-encryption
```

Related Commands

Command	Description
show parser encrypt file status	Displays the private configuration encryption status.

set

To set or display environment variables, use the **set** command in boot loader mode. Environment variables can be used to control the boot loader or any other software running on the device.

set *variable* *value*

Syntax Description

variable *value*	Use one of the following keywords for *variable* and the appropriate value for *value*: **MANUAL_BOOT**—Decides whether the device boots automatically or manually. Valid values are 1/Yes and 0/No. If it is set to 0 or No, the boot loader attempts to automatically boot the system. If it is set to anything else, you must manually boot the device from the boot loader mode.
	BOOT *filesystem:/file-url*—Identifies a semicolon-separated list of executable files to try to load and execute when automatically booting. If the BOOT environment variable is not set, the system attempts to load and execute the first executable image it can find by using a recursive, depth-first search through the flash: file system. If the BOOT variable is set but the specified images cannot be loaded, the system attempts to boot the first bootable file that it can find in the flash: file system.
	ENABLE_BREAK—Allows the automatic boot process to be interrupted when the user presses the **Break** key on the console. Valid values are 1, Yes, On, 0, No, and Off. If set to 1, Yes, or On, you can interrupt the automatic boot process by pressing the **Break** key on the console after the flash: file system has initialized.
	HELPER *filesystem:/file-url*—Identifies a semicolon-separated list of loadable files to dynamically load during the boot loader initialization. Helper files extend or patch the functionality of the boot loader.
	PS1 *prompt*—Specifies a string that is used as the command-line prompt in boot loader mode.
	CONFIG_FILE flash: */file-url*—Specifies the filename that Cisco IOS uses to read and write a nonvolatile copy of the system configuration.
	BAUD *rate*—Specifies the number of bits per second (b/s) that is used for the baud rate for the console. The Cisco IOS software inherits the baud rate setting from the boot loader and continues to use this value unless the configuration file specifies another setting. The range is from 0 to 128000 b/s. Valid values are 50, 75, 110, 150, 300, 600, 1200, 1800, 2000, 2400, 3600, 4800, 7200, 9600, 14400, 19200, 28800, 38400, 56000, 57600, 115200, and 128000. The most commonly used values are 300, 1200, 2400, 9600, 19200, 57600, and 115200.
	SWITCH_NUMBER *stack-member-number*—Changes the member number of a stack member.
	SWITCH_PRIORITY *priority-number*—Changes the priority value of a stack member.

Command Default

The environment variables have these default values:

MANUAL_BOOT: No (0)

BOOT: Null string

ENABLE_BREAK: No (Off or 0) (the automatic boot process cannot be interrupted by pressing the **Break** key on the console).

HELPER: No default value (helper files are not automatically loaded).

PS1 device:

CONFIG_FILE: config.text

BAUD: 9600 b/s

SWITCH_NUMBER: 1

SWITCH_PRIORITY: 1

Note Environment variables that have values are stored in the flash: file system in various files. Each line in the files contains an environment variable name and an equal sign followed by the value of the variable.

A variable has no value if it is not listed in these files; it has a value if it is listed even if the value is a null string. A variable that is set to a null string (for example, “ ”) is a variable with a value.

Many environment variables are predefined and have default values.

Command Modes

Boot loader

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Environment variables are case sensitive and must be entered as documented.

Environment variables that have values are stored in flash memory outside of the flash: file system.

Under typical circumstances, it is not necessary to alter the setting of the environment variables.

The MANUAL_BOOT environment variable can also be set by using the **boot manual** global configuration command.

The BOOT environment variable can also be set by using the **boot system** *filesystem:/file-url* global configuration command.

The ENABLE_BREAK environment variable can also be set by using the **boot enable-break** global configuration command.

The HELPER environment variable can also be set by using the **boot helper** *filesystem: / file-url* global configuration command.

The CONFIG_FILE environment variable can also be set by using the **boot config-file flash:** */file-url* global configuration command.

The SWITCH_NUMBER environment variable can also be set by using the **switch** *current-stack-member-number* **renumber** *new-stack-member-number* global configuration command.

The SWITCH_PRIORITY environment variable can also be set by using the device *stack-member-number* **priority** *priority-number* global configuration command.

The boot loader prompt string (PS1) can be up to 120 printable characters not including the equal sign (=).

Example

This example shows how to set the SWITCH_PRIORITY environment variable:

```
Device: set SWITCH_PRIORITY 2
```

You can verify your setting by using the **set** boot loader command.

show avc client

To display information about top number of applications, use the **show avc client** command in privileged EXEC mode.

show **avc** **client** *client-mac* **top** *n* **application** [**aggregate** | **upstream** | **downstream**]

Syntax Description

client *client-mac*	Specifies the client MAC address.
top *n* **application**	Specifies the number of top "N" applications for the given client.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
	This command was introduced.

The following is sample output from the **show avc client** command:

```
# sh avc client 0040.96ae.65ec top 10 application aggregate

Cumulative Stats:

No.  AppName      Packet-Count    Byte-Count       AvgPkt-Size     usage%
---------------------------------------------------------------------------
1    skinny         7343           449860           61              94
2    unknown        99             13631            137             3
3    dhcp           18             8752             486             2
4    http           18             3264             181             1
5    tftp           9              534              59              0
6    dns            2              224              112             0

Last Interval(90 seconds) Stats:

No.  AppName     Packet-Count     Byte-Count       AvgPkt-Size      usage%
----------------------------------------------------------------------------
1    skinny         9              540              60               100
```

show bootflash:

To display information about the bootflash: file system, use the **show bootflash:** command in user EXEC or privileged EXEC mode.

show bootflash: [{**all** | **filesys** | **namesort** | **sizesort** | **timesort** }]

Syntax Description

all	(Optional) Displays all possible Flash information.
filesys	(Optional) Displays Flash system information.
namesort	(Optional) Sorts the output by file name.
sizesort	(Optional) Sorts the output by file size.
timesort	(Optional) Sorts the output by time stamp.

Command Default

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.
Cisco IOS XE Amsterdam 17.3.1	The following keywords were introduced: • **namesort** • **sizesort** • **timesort**

Example:

The following is a sample output from the **show bootflash: all** command:

```
Device# show bootflash: all
-#- --length-- ---------date/time--------- path

2       4096 May 11 2020 16:49:01.0000000000 +00:00 .installer

3       4096 Feb 27 2020 15:03:50.0000000000 +00:00 .installer/issu_crash

4         12 May 05 2020 22:06:48.0000000000 +00:00 .installer/issu_crash/fru_crash

5         50 May 11 2020 16:40:40.0000000000 +00:00 .installer/last_pkgconf_shasum

6          6 Feb 27 2020 16:33:59.0000000000 +00:00 .installer/install_issu_pid

7         13 Feb 27 2020 21:05:35.0000000000 +00:00 .installer/install_issu_prev_state

8         17 Feb 27 2020 21:05:36.0000000000 +00:00 .installer/install_issu_state

9         13 May 11 2020 16:41:12.0000000000 +00:00 .installer/watchlist
```

```
10          8 Feb 28 2020 18:04:31.0000000000 +00:00 .installer/crdu_frus
11        0 Mar 01 2020 18:01:09.0000000000 +00:00 .installer/.install_add_pkg_list.prev.txt
12       1729 Mar 01 2020 18:02:54.0000000000 +00:00 .installer/install_add_oper.log
13          5 May 11 2020 16:40:40.0000000000 +00:00 .installer/install_global_trans_lock
14         10 May 11 2020 16:40:40.0000000000 +00:00 .installer/install_state
15   33554432 May 11 2020 16:42:37.0000000000 +00:00 nvram_config
16        396 May 11 2020 16:41:02.0000000000 +00:00 boothelper.log
17       4096 May 11 2020 16:40:42.0000000000 +00:00 rpr
18         80 May 11 2020 16:40:42.0000000000 +00:00 rpr/RPR_log.txt
19         80 May 05 2020 22:10:45.0000000000 +00:00 rpr/RPR_log_prev.txt
20       2183 May 11 2020 16:40:42.0000000000 +00:00 bootloader_evt_handle.log
21       4096 Mar 06 2020 21:00:51.0000000000 +00:00 .ssh
22        965 Dec 24 2019 15:23:55.0000000000 +00:00 .ssh/ssh_host_key
23        630 Dec 24 2019 15:23:55.0000000000 +00:00 .ssh/ssh_host_key.pub
24       1675 Dec 24 2019 15:23:56.0000000000 +00:00 .ssh/ssh_host_rsa_key
25        382 Dec 24 2019 15:23:56.0000000000 +00:00 .ssh/ssh_host_rsa_key.pub
26        668 Dec 24 2019 15:23:56.0000000000 +00:00 .ssh/ssh_host_dsa_key
27        590 Dec 24 2019 15:23:56.0000000000 +00:00 .ssh/ssh_host_dsa_key.pub
28        492 Mar 06 2020 21:00:51.0000000000 +00:00 .ssh/ssh_host_ecdsa_key
29        162 Mar 06 2020 21:00:51.0000000000 +00:00 .ssh/ssh_host_ecdsa_key.pub
30        387 Mar 06 2020 21:00:51.0000000000 +00:00 .ssh/ssh_host_ed25519_key
31         82 Mar 06 2020 21:00:51.0000000000 +00:00 .ssh/ssh_host_ed25519_key.pub
32       4096 Dec 24 2019 15:24:41.0000000000 +00:00 core
33       4096 May 11 2020 16:41:29.0000000000 +00:00 core/modules
34       4096 May 05 2020 22:11:47.0000000000 +00:00 .prst_sync
35       4096 Mar 01 2020 18:17:15.0000000000 +00:00 .rollback_timer
36       4096 Mar 06 2020 21:01:11.0000000000 +00:00 gs_script
37       4096 Mar 06 2020 21:01:11.0000000000 +00:00 gs_script/sss
38       4096 Apr 24 2020 18:56:40.0000000000 +00:00 tech_support
39      15305 May 11 2020 16:41:01.0000000000 +00:00 tech_support/igmp-snooping.tcl
40       1612 May 11 2020 16:41:01.0000000000 +00:00 tech_support/igmpsn_dump.tcl
.
```

```
.
.
```

The following is a sample output from the **show bootflash: sizesort** command:

```
Device# show bootflash: sizesort

-#- --length-- ---------date/time--------- path

126  968337890 Mar 27 2020 18:06:17.0000000000 +00:00 cat9k_iosxe.CSCvt37598.bin

136  967769293 May 05 2020 21:50:33.0000000000 +00:00 cat9k_iosxe.CSCvu05574

124  967321806 Mar 23 2020 18:48:45.0000000000 +00:00 cat9k_ts_2103.bin

133  951680494 Apr 13 2020 19:46:35.0000000000 +00:00
cat9k_iosxe.2020-04-13_17.34_rakoppak.SSA.bin
130  950434163 Apr 09 2020 09:03:47.0000000000 +00:00
cat9k_iosxe.2020-04-09_13.49_rakoppak.SSA.bin
132  950410332 Apr 09 2020 07:29:57.0000000000 +00:00
cat9k_iosxe.2020-04-09_12.28_rakoppak.SSA.bin
134  948402972 Apr 17 2020 23:02:04.0000000000 +00:00 cat9k_iosxe.tla.bin

77  810146146 Feb 27 2020 15:41:42.0000000000 +00:00 cat9k_iosxe.16.12.01c.SPA.bin

88  701945494 Feb 27 2020 16:23:55.0000000000 +00:00 cat9k_iosxe.16.09.03.SPA.bin

101  535442436 Mar 01 2020 18:01:41.0000000000 +00:00 cat9k-rpbase.16.12.01c.SPA.pkg

86   88884228 Mar 01 2020 18:01:41.0000000000 +00:00 cat9k-espbase.16.12.01c.SPA.pkg

104   60167172 Mar 01 2020 18:01:41.0000000000 +00:00 cat9k-sipspa.16.12.01c.SPA.pkg

102   43111770 Mar 01 2020 18:02:07.0000000000 +00:00 cat9k-rpboot.16.12.01c.SPA.pkg

15   33554432 May 11 2020 16:42:37.0000000000 +00:00 nvram_config

131   33554432 May 11 2020 16:42:39.0000000000 +00:00 nvram_config_bkup

103   31413252 Mar 01 2020 18:01:41.0000000000 +00:00 cat9k-sipbase.16.12.01c.SPA.pkg

105   22676484 Mar 01 2020 18:01:41.0000000000 +00:00 cat9k-srdriver.16.12.01c.SPA.pkg

85   14226440 Mar 01 2020 18:01:41.0000000000 +00:00 cat9k-cc_srdriver.16.12.01c.SPA.pkg

.
.
.
```

show consistency-checker mcast l2m

To run a consistency-checker and detect inconsistent states of software entries on the Layer 2 multicast forwarding tables, run the **show consistency-checker mcast l2m** command in privileged EXEC mode.

show consistency-checker mcast l2m start { **all** | **vlan** *vlan-id* { *ipv4-address* | *ipv6-adddress* } } [{ **recursive** }]

Syntax Description

start	Starts the consistency-checker for Layer 2 multicast. • **all** : Starts the checker for entire table • **vlan** *vlan-id* { *ipv4-address* | *ipv6-address* }: Starts the checker for the specified VLAN.
all	Starts the checker for entire table.
vlan *vlan-id* { *ipv4-address* | *ipv6-address* }	Starts the checker for the specified VLAN.
recursive	Runs a recursive consistency-checker.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Bengaluru 17.6.1	This command was introduced.

Usage Guidelines

The consistency checker has the following limitations:

- There is no command to abort or terminate the consistency checker. It will stop only once the full report has been displayed.
- FED hardware checks are partially implemented. Only errors in programming hardware will be reported.
- False Positive cases: When the consistency checker is running and a large number of feature table entry delete/add/modify actions occur (triggered via clear * or relearn), the consistency checker may report inconsistent or missing entries across processes. It can also switch off the stale reporting due to a large number of changes in table entries.

Example

The following is a sample output for the **show consistency-checker mcast l2m** command:

```
Device# show consistency-checker mcast l2m start vlan 900 229.1.1.1 recursive
Single entry scan started with Run_id: 2

*Feb 17 06:54:09.880: %IOSXE_FMANRP_CCK-6-FMANRP_COMPLETED: Consistency Check for Run-Id 2
```

```
 is completed. Check 'show consistency-checker run-id 2'.
Device#
Device# show consistency-checker run 2
Process: IOSD
  Object-Type    Start-time              Entries       Exceptions
  l2m_vlan       2021/02/17 06:54:01           1                0
  l2m_group      2021/02/17 06:54:01           1                0

Process: FMAN-FP
  *Statistics(A/I/M/S/O): Actual/Inherited/Missing/Stale/Others

  Object-Type    Start-time              State            A / I / M / S / O
  l2m_vlan       1970/01/01 00:10:03     Consistent        0/  0/  0/  0/  0
  l2m_group      1970/01/01 00:10:03     Consistent        0/  0/  0/  0/  0


Process: FED
  *Statistics(A/I/M/S/HW/O): Actual/Inherited/Missing/Stale/Hardware/Others

  Object-Type    Start-time              State             A / I / M / S / HW/ O
  l2m_vlan       2021/02/17 06:54:01     Inconsistent       1/  0/  0/  0/  0/  0
  l2m_group      2021/02/17 06:54:01     Inconsistent       0/  1/  0/  0/  0/  0

Device#
```

show consistency-checker objects

To run a consistency-checker and detect inconsistent states of software entries on objects, run the **show consistency-checker objects** command in privileged EXEC mode.

show consistency-checker objects { **adjacency** | | **interface** | | **l2m_group** | | **l2m_vlan** | | **l3_entry** | | **l3m_entry** } [{ *run-id* }] [{ **detail** }]

Syntax Description

adjacency	Runs the consistenc-checker on adjacency entries.
interface	Runs the consistenc-checker on interface entries.
l2m_group	Runs the consistenc-checker on Layer 2 Multicast group entries.
l2m_vlan	Runs the consistenc-checker on Layer 2 Multicast VLAN entries.
l3_entry	Runs the consistenc-checker on Layer 3 Unicast entries.
l3m_entry	Runs the consistenc-checker on Layer 3 Multicast entries.
run-id	Runs the consistency-checker by run ID.
detail	Displays detailed output for the run ID.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Bengaluru 17.6.1	This command was introduced.

Usage Guidelines

The consistency checker has the following limitations:

- There is no command to abort or terminate the consistency checker. It will stop only once the full report has been displayed.
- FED hardware checks are partially implemented. Only errors in programming hardware will be reported.
- False Positive cases: When the consistency checker is running and a large number of feature table entry delete/add/modify actions occur (triggered via clear * or relearn), the consistency checker may report inconsistent or missing entries across processes. It can also switch off the stale reporting due to a large number of changes in table entries.

Example

The following is sample output for the **show consistency-checker objects l2m_group** command:

```
Device# show consistency-checker objects l2m_group
Process: IOSD
```

```
  Run-id    Start-time              Exception
  1         2021/02/17 05:20:42     0
  2         2021/02/17 06:19:05     0

Process: FMAN-FP
  *Statistics(A/I/M/S/Oth): Actual/Inherited/Missing/Stale/Others

  Run-id    Start-time              State           A/  I/  M/  S/Oth
  1         2021/02/17 05:20:42     Consistent      0/  0/  0/  0/  0
  2         2021/02/17 06:19:05     Consistent      0/  0/  0/  0/  0

Process: FED
  *Statistics(A/I/M/S/HW/Oth): Actual/Inherited/Missing/Stale/Hardware/Others

  Run-id    Start-time              State           A/  I/  M/  S/ HW/Oth
  1         2021/02/17 05:20:42     Consistent      0/  0/  0/  0/  0/  0
  2         2021/02/17 06:19:05     Inconsistent    4/  0/  2/  0/  0/  0

Device#
```

show consistency-checker run-id

To run a consistency-checker and detect inconsistent states of software entries by run ID, run the **show consistency-checker run-id** *run-id* command in privileged EXEC mode.

show consistency-checker run-id *run-id* [{ **detail** | | **status** }]

Syntax Description

run-id	Specifies the run ID.
detail	Displays detailed output for the run ID.
status	Displays the completion status of the checker.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Bengaluru 17.6.1	This command was introduced.

Usage Guidelines

The consistency checker has the following limitations:

- There is no command to abort or terminate the consistency checker. It will stop only once the full report has been displayed.
- FED hardware checks are partially implemented. Only errors in programming hardware will be reported.
- False Positive cases: When the consistency checker is running and a large number of feature table entry delete/add/modify actions occur (triggered via clear * or relearn), the consistency checker may report inconsistent or missing entries across processes. It can also switch off the stale reporting due to a large number of changes in table entries.

Example

The following is sample output for the **show consistency-checker run-id** *run-id* command:

```
Device# show consistency-checker run-id 6
Process: IOSD
Flags:    F - Full Table Scan, S - Single Entry Run
          RE -  Recursive Check, GD -  Garbage Detector
          Hw -  Hardware Check, HS - Hardware Shadow Copy
  Object-Type    Start-time             Entries  Exceptions  Flags
  l2m_vlan       2021/07/19 15:19:41         30         0    F Hw HS
  l2m_group      2021/07/19 15:19:42         10         0    F Hw HS

Process: FMAN-FP
  *Statistics(A/I/M/S/Oth): Actual/Inherited/Missing/Stale/Others

  Object-Type    Start-time             State             A/  I/  M/  S/Oth
  l2m_vlan       2021/07/19 15:19:41    Consistent        0/  0/  0/  0/  0
  l2m_group      2021/07/19 15:19:42    Consistent        0/  0/  0/  0/  0
```

```
Process: FED
  *Statistics(A/I/M/S/HW/Oth): Actual/Inherited/Missing/Stale/Hardware/Others

  Object-Type    Start-time              State              A/  I/  M/  S/ HW/Oth
  l2m_vlan       2021/07/19 15:19:41     Consistent         0/  0/  0/  0/  0/  0
  l2m_group      2021/07/19 15:19:42     Consistent         0/  0/  0/  0/  0/  0

Device#
```

The following is sample output for the **show consistency-checker run-id** *run-id* **status** command:

```
Device# show consistency-checker run-id 6 status
Process: IOSD
  Object-Type      Status           Time(sec)     Exceptions
  l2m_vlan         Completed        13            No
  l2m_group        Completed        13            No

Process: FMAN-FP
  Object-Type      Status           Time(sec)     State
  l2m_vlan         Completed        12            Consistent
  l2m_group        Completed        11            Consistent

Process: FED
  Object-Type      Status           Time(sec)     State
  l2m_vlan         Completed        12            Consistent
  l2m_group        Completed        11            Consistent

Device#
```

show debug

To display all the debug commands available on a switch, use the **show debug** command in Privileged EXEC mode.

show debug

show debug condition *Condition identifier* | *All conditions*

Syntax Description

Condition identifier	Sets the value of the condition identifier to be used. Range is between 1 and 1000.
All conditions	Shows all conditional debugging options available.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Release 16.1	This command was introduced.

Usage Guidelines

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use debug commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. Moreover, it is best to use debug commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased debug command processing overhead will affect system use.

Examples

This example shows the output of a **show debug** command:

```
Device# show debug condition all
```

To disable debugging, use the **no debug all** command.

show env xps

To display budgeting, configuration, power, and system power information for the Cisco eXpandable Power System (XPS) 2200, use the **show env xps** command in privileged EXEC mode.

show env xps { **budgeting** | **configuration** | **port** [**all** | *number*] | **power** | **system** | **thermal** | **upgrade** | **version** }

Syntax Description

budgeting	Displays XPS power budgeting, the allocated and budgeted power of all switches in the power stack.
configuration	Displays the configuration resulting from the power xps privileged EXEC commands. The XPS configuration is stored in the XPS. Enter the show env xps configuration command to retrieve the non-default configuration.
port [**all** | *number*]	Displays the configuration and status of all ports or the specified XPS port. Port numbers are from 1 to 9.
power	Displays the status of the XPS power supplies.
system	Displays the XPS system status.
thermal	Displays the XPS thermal status.
upgrade	Displays the XPS upgrade status.
version	Displays the XPS version details.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(55)SE1	This command was introduced.

Usage Guidelines

Use the **show env xps** privileged EXEC command to display the information for XPS 2200.

Examples

This is an example of output from the show env xps budgeting command:

```
Switch#
=======



XPS 0101.0100.0000 :
=========================================================
Data                 Current    Power     Power Port  Switch #  PS A  PS B  Role-State
Committed
Budget
----  --------  ----  ----  ---------- ---------  ------ 1     -        -    715  SP-PS
   223
    1543
```

```
2     -        -    -    SP-PS      223       223
3     -        -    -    -          -         -
4     -        -    -    -          -         -
5     -        -    -    -          -         -
6     -        -    -    -          -         -
7     -        -    -    -          -         -
8     -        -    -    -          -         -
9     1        1100 -    RPS-NB     223        070
XPS  -        -    1100  -          -
```

This is an example of output from the show env xps configuration command:

```
Switch# show env xps configuration
=============================================
XPS 0101.0100.0000 :
=============================================
power xps port 4 priority 5
power xps port 5 mode disable
power xps port 5 priority 6
power xps port 6 priority 7
power xps port 7 priority 8
power xps port 8 priority 9
power xps port 9 priority 4
```

This is an example of output from the show env xps port all command:

```
Switch#
XPS 010



-----------------------------------------
Port name          : -
Connected          : Yes
Mode               : Enabled (On)
Priority           : 1
Data stack switch # : - Configured role    : Auto-SP
Run mode            : SP-PS : Stack Power Power-Sharing Mode
Cable faults        : 0x0 XPS 0101.0100.0000 Port 2
-----------------------------------------
Port name          : -
Connected          : Yes
Mode               : Enabled (On)
Priority           : 2
Data stack switch # : - Configured role    : Auto-SP
Run mode            : SP-PS : Stack Power Power-Sharing Mode
Cable faults        : 0x0 XPS 0101.0100.0000 Port 3
-----------------------------------------
Port name          : -
Connected          : No
Mode               : Enabled (On)
Priority           : 3
Data stack switch # : - Configured role    : Auto-SP Run mode            : -
Cable faults
<output truncated>
```

This is an example of output from the show env xps power command:

```
=============================================================================
XPS 0101.0100.0000 :
=============================================================================
Port-Supply SW PID                Serial#     Status         Mode Watts
----------- -- ------------------  ----------- --------------  ----  -----
XPS-A           Not present
XPS-B           NG3K-PWR-1100WAC   LIT13320NTV OK             SP   1100
1-A         -  -                   -           -
```

```
1-B         -  -                   -            -               SP    715
2-A         -  -                   -            -
2-B         -  -                   -            -
9-A                       100WAC    LIT141307RK OK               RPS  1100
9-B                   esent
```

This is an example of output from the show env xps system command:

```
Switch#
=======


XPS 0101.0100.0000 :
=============================================================================
XPS                        Cfg  Cfg      RPS Switch  Current    Data Port  XPS Port Name

Mode Role    Pri Conn    Role-State  Switch #
----  --------------------  ---- -------  --- ------  ----------  --------
1     -                    On   Auto-SP  1   Yes     SP-PS      -
2     -                    On   Auto-SP  2   Yes     SP-PS      -
3     -                    On   Auto-SP  3   No      -          -
4     none                 On   Auto-SP  5   No      -          -
5     -                    Off  Auto-SP  6   No      -          -
6     -                    On   Auto-SP  7   No      -          -
7     -                    On   Auto-SP  8   No      -          -
8     -                    On   Auto-SP  9   No      -
9     test                 On   Auto-SP  4   Yes     RPS-NB
```

This is an example of output from the show env xps thermal command:

```
Switch#
=======



XPS 0101.0100.0000 :
=============================================
Fan  Status
----  -----------
1     OK
2     OK
3     NOT PRESENT PS-1  NOT PRESENT PS-2  OK Temperature is OK
```

This is an example of output from the show env xps upgrade command when no upgrade is occurring:

```
Switch# show env xps upgrade
No XPS is connected and upgrading.
```

These are examples of output from the show env xps upgrade command when an upgrade is in process:

```
Switch# show env xps upgrade
XPS Upgrade Xfer

SW Status Prog
-- ----------- ----
1 Waiting 0%
Switch#
*Mar 22 03:12:46.723: %PLATFORM_XPS-6-UPGRADE_START: XPS 0022.bdd7.9b14 upgrade has
started through the Service Port.
Switch# show env xps upgrade
XPS Upgrade Xfer
SW Status Prog
-- ----------- ----
1 Receiving 1%
Switch# show env xps upgrade
```

```
XPS Upgrade Xfer
SW Status Prog
-- ----------- ----
1 Receiving 5%
Switch# show env xps upgrade
XPS Upgrade Xfer
SW Status Prog
-- ----------- ----
1 Reloading 100%
Switch#
*Mar 22 03:16:01.733: %PLATFORM_XPS-6-UPGRADE_DONE: XPS 0022.bdd7.9b14 upgrade has
completed and the XPS is reloading.
```

This is an example of output from the show env xps version command:

```
Switch# show env xps version
=============================================
XPS 0022.bdd7.9b14:
=============================================
Serial Number: FDO13490KUT
Hardware Version: 8
Bootloader Version: 7
Software Version: 18
```

Table 2: Related Commands

Command	Description
power xps(global configuration command)	Configures XPS and XPS port names.
power xps(privileged EXEC command)	Configures the XPS ports and system.

show flow monitor

To display the status and statistics for a flow monitor, use the **show flow monitor** command in privileged EXEC mode.

Syntax Description

name	(Optional) Specifies the name of a flow monitor.
monitor-name	(Optional) Name of a flow monitor that was previously configured.
cache	(Optional) Displays the contents of the cache for the flow monitor.
format	(Optional) Specifies the use of one of the format options for formatting the display output.
csv	(Optional) Displays the flow monitor cache contents in comma-separated variables (CSV) format.
record	(Optional) Displays the flow monitor cache contents in record format.
table	(Optional) Displays the flow monitor cache contents in table format.
statistics	(Optional) Displays the statistics for the flow monitor.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

The **cache** keyword uses the record format by default.

The uppercase field names in the display output of the **show flowmonitor** *monitor-name* **cache** command are key fields that uses to differentiate flows. The lowercase field names in the display output of the **show flow monitor** *monitor-name* **cache** command are nonkey fields from which collects values as additional data for the cache.

Examples

The following example displays the status for a flow monitor:

```
# show flow monitor FLOW-MONITOR-1

Flow Monitor FLOW-MONITOR-1:
  Description:       Used for basic traffic analysis
  Flow Record:       flow-record-1
  Flow Exporter:     flow-exporter-1
                     flow-exporter-2
  Cache:
    Type:              normal
    Status:            allocated
    Size:              4096 entries / 311316 bytes
    Inactive Timeout:  15 secs
    Active Timeout:    1800 secs
```

This table describes the significant fields shown in the display.

Table 3: show flow monitor monitor-name Field Descriptions

Field	Description
Flow Monitor	Name of the flow monitor that you configured.
Description	Description that you configured or the monitor, or the default description User defined.
Flow Record	Flow record assigned to the flow monitor.
Flow Exporter	Exporters that are assigned to the flow monitor.
Cache	Information about the cache for the flow monitor.
Type	Flow monitor cache type. The value is always normal, as it is the only supported cache type.
Status	Status of the flow monitor cache. The possible values are: • allocated—The cache is allocated. • being deleted—The cache is being deleted. • not allocated—The cache is not allocated.
Size	Current cache size.
Inactive Timeout	Current value for the inactive timeout in seconds.
Active Timeout	Current value for the active timeout in seconds.

The following example displays the status, statistics, and data for the flow monitor named FLOW-MONITOR-1:

This table describes the significant fields shown in the display.

The following example displays the status, statistics, and data for the flow monitor named FLOW-MONITOR-1 in a table format:

The following example displays the status, statistics, and data for the flow monitor named FLOW-MONITOR-IPv6 (the cache contains IPv6 data) in record format:

The following example displays the status and statistics for a flow monitor:

show install

To display information about install packages, use the **show install** command in privileged EXEC mode.

show install {**active** | **committed** | **inactive** | **log** | **package** {**bootflash:** | **flash:** | **webui:**} | **rollback** | **summary** | **uncommitted**}

Syntax Description

active	Displays information about active packages.
committed	Displays package activations that are persistent.
inactive	Displays inactive packages.
log	Displays entries stored in the logging installation buffer.
package	Displays metadata information about the package, including description, restart information, components in the package, and so on.
{**bootflash:** | **flash:** | **harddisk:** |**webui:**}	Specifies the location of the install package.
rollback	Displays the software set associated with a saved installation.
summary	Displays information about the list of active, inactive, committed, and superseded packages.
uncommitted	Displays package activations that are nonpersistent.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.4	This command was introduced on the C9200L models of the series.
Cisco IOS XE Gibraltar 16.12.1	This command was introduced on the C9200 models of the series.

Usage Guidelines

Use the show commands to view the status of the install package.

Examples

The following sample output displays information about active, inactive, committed, and uncommitted packages by using the **show install summary** command. Here SMU package file `cat9k_lite_iosxe.16.09.04.CSCvk70181.SPA.smu.bin` is active and committed:

```
Device# show install summary

Active Packages:
    tftp:cat9k_lite_iosxe.16.09.04.CSCvk70181.SPA.smu.bin
```

```
Inactive Packages:
   No packages
Committed Packages:
    tftp:cat9k_lite_iosxe.16.09.04.CSCvk70181.SPA.smu.bin
Uncommitted Packages:
   No packages
Device#
```

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

Table 4: show install summary Field Descriptions

Field	Description
Active Packages	Name of the active install package.
Inactive Packages	List of inactive packages.
Committed Packages	Install packages that have saved or committed changes to the harddisk, so that the changes become persistent across reloads.
Uncommitted Packages	Intall package activations that are nonpersistent.

The following is sample output from the **show install active** command:

```
Device# show install active

Active Packages:
tftp:cat3k-universalk9.2017-01-10_13.15.1.CSCxxx.SSA.dmp.bin
```

The following is sample output from the **show install log** command:

```
Device# show install log

[0|install_op_boot]: START Wed Jun 10 19:31:50 Universal 2020
[0|install_op_boot]: END SUCCESS Wed Jun 10 19:31:56 Universal 2020
```

Related Commands

Command	Description
install	Installs SMU packages.

show license all

To display all licensing information enter the **show license all** command in privileged EXEC mode. This command displays status, authorization, UDI, and usage information, all combined.

show license all

Syntax Description

This command has no arguments or keywords.

Command Default

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.
Cisco IOS XE Amsterdam 17.3.2a	Command output was updated to display information relating to Smart Licensing Using Policy. Command output no longer displays Smart Account and Virtual account information.

Usage Guidelines

This command concatenates the output of other show license commands, enabling you to display different kinds of licensing information together. For field descriptions, refer to the corresponding commands.

Smart Licensing: If the software version on the device is Cisco IOS XE Amsterdam 17.3.1 or an earlier release, command output displays fields pertinent to Smart Licensing (whether smart licensing is enabled, all associated licensing certificates, compliance status, and so on).

Smart Licensing Using Policy: If the software version on the device (also referred to as a product instance) is Cisco IOS XE Amsterdam 17.3.2a or a later release, command output displays fields pertinent to Smart Licensing Using Policy.

- The `Smart Licensing Status` section corresponds with the output of the **show license status** command.
- The `License Usage` section corresponds with the output of the **show license usage** command.
- The `Product Information` section corresponds with the output of the **show license udi** command.
- The `Agent Version` section of the show license all command displays the Smart Agent version and is available only in this command.
- The `License Authorizations` section corresponds with the output of the **show license authorization** command.
- The `Usage Report Summary` section corresponds with the output in the **show license tech** command.

Examples

- show license all for Smart Licensing Using Policy (Cisco Catalyst 9300 Series Switches), on page 109
- show license all for Smart Licensing Using Policy (Cisco Catalyst 9500 Series Switches), on page 111
- show license all for Smart Licensing, on page 113

show license all for Smart Licensing Using Policy (Cisco Catalyst 9300 Series Switches)

The following is sample output of the **show license all** command in a stacking set-up. All the product instances in the stack are C9300X switches, which support the Export Control Key for High Security (HSECK9) starting from Cisco IOS XE Bengaluru 17.6.2. An HSECK9 key is used here and the requisite Smart Licensing Authorization Code (SLAC) is installed (SMART AUTHORIZATION INSTALLED on Oct 29 17:45:28 2021 UTC).

```
Device# show license all

Smart Licensing Status
======================

Smart Licensing is ENABLED

Export Authorization Key:
  Features Authorized:
    <none>

Utility:
  Status: DISABLED

Smart Licensing Using Policy:
  Status: ENABLED

Data Privacy:
  Sending Hostname: yes
    Callhome hostname privacy: DISABLED
    Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
  Type: cslu
  Cslu address: <empty>
  Proxy:
    Not Configured

Miscellaneous:
  Custom Id: <empty>

Policy:
  Policy in use: Installed On Oct 29 17:44:15 2021 UTC
  Policy name: Custom Policy
  Reporting ACK required: yes (Customer Policy)
  Unenforced/Non-Export Perpetual Attributes:
    First report requirement (days): 365 (Customer Policy)
    Reporting frequency (days): 0 (Customer Policy)
    Report on change (days): 90 (Customer Policy)
  Unenforced/Non-Export Subscription Attributes:
    First report requirement (days): 90 (Customer Policy)
    Reporting frequency (days): 90 (Customer Policy)
    Report on change (days): 90 (Customer Policy)
  Enforced (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 90 (Customer Policy)
    Report on change (days): 90 (Customer Policy)
  Export (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 90 (Customer Policy)
    Report on change (days): 90 (Customer Policy)

Usage Reporting:
  Last ACK received: Oct 29 17:48:51 2021 UTC
  Next ACK deadline: Jan 27 17:48:51 2022 UTC
  Reporting push interval: 30  days
  Next ACK push check: <none>
  Next report push: Oct 29 18:32:43 2021 UTC
  Last report push: Oct 29 17:44:50 2021 UTC
  Last report file write: <none>

Trust Code Installed:
  Active: PID:C9300X-24HX,SN:FOC2519L8R7
    INSTALLED on Oct 29 17:44:15 2021 UTC
  Standby: PID:C9300X-48HXN,SN:FOC2524L39P
    INSTALLED on Oct 29 17:44:15 2021 UTC
  Member: PID:C9300X-48HX,SN:FOC2516LC92
    INSTALLED on Oct 29 17:44:15 2021 UTC

License Usage
=============

network-advantage (C9300-24 Network Advantage):
  Description: C9300-24 Network Advantage
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: network-advantage
  Feature Description: C9300-24 Network Advantage
  Enforcement type: NOT ENFORCED
  License type: Perpetual

dna-advantage (C9300-24 DNA Advantage):
  Description: C9300-24 DNA Advantage
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: dna-advantage
  Feature Description: C9300-24 DNA Advantage
  Enforcement type: NOT ENFORCED
  License type: Subscription

network-advantage (C9300-48 Network Advantage):
  Description: C9300-48 Network Advantage
  Count: 2
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: network-advantage
  Feature Description: C9300-48 Network Advantage
  Enforcement type: NOT ENFORCED
  License type: Perpetual

dna-advantage (C9300-48 DNA Advantage):
  Description: C9300-48 DNA Advantage
  Count: 2
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: dna-advantage
  Feature Description: C9300-48 DNA Advantage
  Enforcement type: NOT ENFORCED
  License type: Subscription

hseck9 (Cat9K HSEC):
  Description: hseck9
  Count: 1
  Version: 1.0
  Status: IN USE
  Export status: RESTRICTED - ALLOWED
  Feature Name: hseck9
  Feature Description: hseck9
  Enforcement type: EXPORT RESTRICTED
  License type: Perpetual

Product Information
===================
UDI: PID:C9300X-24HX,SN:FOC2519L8R7

HA UDI List:
    Active:PID:C9300X-24HX,SN:FOC2519L8R7
    Standby:PID:C9300X-48HXN,SN:FOC2524L39P
    Member:PID:C9300X-48HX,SN:FOC2516LC92

Agent Version
=============
Smart Agent for Licensing: 5.1.23_rel/104

License Authorizations
======================
Overall status:
  Active: PID:C9300X-24HX,SN:FOC2519L8R7
      Status: SMART AUTHORIZATION INSTALLED on Oct 29 17:45:28 2021 UTC
      Last Confirmation code: 6746c5b5
  Standby: PID:C9300X-48HXN,SN:FOC2524L39P
      Status: NOT INSTALLED
  Member: PID:C9300X-48HX,SN:FOC2516LC92
      Status: NOT INSTALLED

Authorizations:
  C9K HSEC (Cat9K HSEC):
    Description: HSEC Key for Export Compliance on Cat9K Series Switches
    Total available count: 1
    Enforcement type: EXPORT RESTRICTED
    Term information:
      Active: PID:C9300X-24HX,SN:FOC2519L8R7
        Authorization type: SMART AUTHORIZATION INSTALLED
        License type: PERPETUAL
          Term Count: 1

Purchased Licenses:
  No Purchase Information Available
```

show license all for Smart Licensing Using Policy (Cisco Catalyst 9500 Series Switches)

The following is sample output of the **show license all** command on a Cisco Catalyst 9500 switch. Similar output is displayed on all supported Cisco Catalyst Access, Core, and Aggregation Switches.

```
Device# show license all

Smart Licensing Status
======================
Smart Licensing is ENABLED
License Reservation is ENABLED
Export Authorization Key:
  Features Authorized:
    <none>
Utility:
  Status: DISABLED
```

```
Smart Licensing Using Policy:
  Status: ENABLED
Data Privacy:
  Sending Hostname: yes
    Callhome hostname privacy: DISABLED
    Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED
Transport:
  Type: Transport Off
Miscellaneous:
  Custom Id: <empty>
Policy:
  Policy in use: Merged from multiple sources.
  Reporting ACK required: yes (CISCO default)
  Unenforced/Non-Export Perpetual Attributes:
    First report requirement (days): 365 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 90 (CISCO default)
  Unenforced/Non-Export Subscription Attributes:
    First report requirement (days): 90 (CISCO default)
    Reporting frequency (days): 90 (CISCO default)
    Report on change (days): 90 (CISCO default)
  Enforced (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 0 (CISCO default)
  Export (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 0 (CISCO default)
Usage Reporting:
  Last ACK received: <none>
  Next ACK deadline: Nov 29 10:50:05 2020 PDT
  Reporting Interval: 30
  Next ACK push check: <none>
  Next report push: Aug 31 10:52:05 2020 PDT
  Last report push: <none>
  Last report file write: <none>
Trust Code Installed: <none>
License Usage
=============
network-advantage (C9500 Network Advantage):
  Description: network-advantage
  Count: 2
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: network-advantage
  Feature Description: network-advantage
  Enforcement type: NOT ENFORCED
  License type: Perpetual
  Reservation:
    Reservation status: SPECIFIC INSTALLED
    Total reserved count: 2
dna-advantage (C9500-16X DNA Advantage):
  Description: C9500-16X DNA Advantage
  Count: 2
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: dna-advantage
  Feature Description: C9500-16X DNA Advantage
  Enforcement type: NOT ENFORCED
  License type: Subscription
  Reservation:
    Reservation status: SPECIFIC INSTALLED
    Total reserved count: 2
Product Information
===================
UDI: PID:C9500-16X,SN:FCW2233A5ZV
HA UDI List:
    Active:PID:C9500-16X,SN:FCW2233A5ZV
    Standby:PID:C9500-16X,SN:FCW2233A5ZY
Agent Version
=============
Smart Agent for Licensing: 5.0.5_rel/42
License Authorizations
======================
Overall status:
  Active: PID:C9500-16X,SN:FCW2233A5ZV
      Status: SPECIFIC INSTALLED on Aug 31 10:15:01 2020 PDT
      Last Confirmation code: 4bfbea7f
  Standby: PID:C9500-16X,SN:FCW2233A5ZY
      Status: SPECIFIC INSTALLED on Aug 31 10:15:01 2020 PDT
      Last Confirmation code: 9394f196
Specified license reservations:
  C9500 Network Advantage (C9500 Network Advantage):
    Description: C9500 Network Advantage
    Total reserved count: 2
    Enforcement type: NOT ENFORCED
    Term information:
      Active: PID:C9500-16X,SN:FCW2233A5ZV
        Authorization type: SPECIFIC INSTALLED on Aug 31 10:15:01 2020 PDT
        License type: PERPETUAL
          Term Count: 1
      Standby: PID:C9500-16X,SN:FCW2233A5ZY
        Authorization type: SPECIFIC INSTALLED on Aug 31 10:15:01 2020 PDT
        License type: PERPETUAL
          Term Count: 1
  C9500-DNA-16X-A (C9500-16X DNA Advantage):
    Description: C9500-DNA-16X-A
    Total reserved count: 2
    Enforcement type: NOT ENFORCED
    Term information:
      Active: PID:C9500-16X,SN:FCW2233A5ZV
        Authorization type: SPECIFIC INSTALLED on Aug 31 10:15:01 2020 PDT
        License type: PERPETUAL
          Term Count: 1
      Standby: PID:C9500-16X,SN:FCW2233A5ZY
        Authorization type: SPECIFIC INSTALLED on Aug 31 10:15:01 2020 PDT
        License type: PERPETUAL
          Term Count: 1
Purchased Licenses:
  No Purchase Information Available
Derived Licenses:
  Entitlement Tag:
regid.2017-03.com.cisco.advantagek9-Nyquist-C9500,1.0_f1563759-2e03-4a4c-bec5-5feec525a12c
  Entitlement Tag:
regid.2017-07.com.cisco.C9500-DNA-16X-A,1.0_ef3574d1-156b-486a-864f-9f779ff3ee49
```

show license all for Smart Licensing

The following is sample output from the **show license all** command:

```
Device# show license all
Smart Licensing Status
======================
Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Smart Account: CISCO Systems
  Virtual Account: NPR
  Export-Controlled Functionality: Allowed
  Initial Registration: First Attempt Pending
  Last Renewal Attempt: SUCCEEDED on Jul 19 14:49:49 2018 IST
  Next Renewal Attempt: Jan 15 14:49:48 2019 IST
  Registration Expires: Jul 19 14:43:48 2019 IST

License Authorization:
  Status: AUTHORIZED on Jul 28 07:02:56 2018 IST
  Last Communication Attempt: SUCCEEDED on Jul 28 07:02:56 2018 IST
  Next Communication Attempt: Aug 27 07:02:56 2018 IST
  Communication Deadline: Oct 26 06:57:50 2018 IST

Utility:
  Status: DISABLED

Data Privacy:
  Sending Hostname: yes
    Callhome hostname privacy: DISABLED
    Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
  Type: Callhome

License Usage
==============

C9200L DNA Advantage, 48-port Term license (C9200L-DNA-A-48):
  Description: C9200L DNA Advantage, 48-port Term license
  Count: 1
  Version: 1.0
  Status: AUTHORIZED

C9200L Network Advantage, 48-port license (C9200L-NW-A-48):
  Description: C9200L Network Advantage, 48-port license
  Count: 1
  Version: 1.0
  Status: AUTHORIZED

Product Information
===================
UDI: PID:C9200L-48P-4X,SN:JPG221300KP

Agent Version
=============
Smart Agent for Licensing: 4.4.13_rel/116
Component Versions: SA:(1_3_dev)1.0.15, SI:(dev22)1.2.1, CH:(rel5)1.0.3, PK:(dev18)1.0.3

Reservation Info
================
License reservation: DISABLED
```

Related Commands

Command	Description
show license status	Displays compliance status of a license.

Command	Description
show license authorization	Displays authorization code-related information.
show license summary	Displays summary of all active licenses.
show license udi	Displays UDI.
show license usage	Displays license usage information
show license tech support	Displays the debug output.

show license authorization

To display authorization-related information for (export-controlled and enforced) licenses, enter the **show license authorization** command in privileged EXEC mode.

show license authorization

This command has no arguments or keywords.

Command Modes

Privileged EXEC (Device#)

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.3.2a	This command was introduced.

Usage Guidelines

Use this command to display information about authorization codes. This includes SLR authorization codes and Smart Licensing Authorization Codes (SLAC).

Examples

For information about fields shown in the display, see Table 5: show license authorization Field Descriptions, on page 117 .

For sample outputs, see:

- Displaying SLAC, on page 119
- Displaying SLR Authorization Code, on page 119.

Table 5: show license authorization Field Descriptions

Field		Description
Overall Status	Header for UDI information for all product instances in the set-up, the type of authorization that is installed, and configuration errors, if any. In a High Availability set-up, all UDIs in the set-up are listed.	
	Active: Status:	The active product instance UDI, followed by the status of the authorization code installation for this UDI. If the status indicates that the authorization code is installed and there is a confirmation code, this is also displayed.
	Standby: Status:	The standby product instance UDI, followed by the status of the authorization code installation for this UDI. If the status indicates that the authorization code is installed and there is a confirmation code, this is also displayed.
	Member: Status:	The member product instance UDI, followed by the status of the authorization code installation for this UDI. If the status indicates that the authorization code is installed and there is a confirmation code, this is also displayed.
	ERROR:	Configuration errors or discrepancies in the High Availability set-up, if any.

Field		Description
Authorizations	Header for detailed license authorization information. All licenses, their enforcement types, and validity durations are displayed. Errors are displayed for each product instance if its authorization or mode does not match what is installed on the active. This section is displayed only if the product instance is using a license with an authorization code.	
	():	License name and a shortened form of the license name.
	Description	License description.
	Total available count:	Total count of licenses that are *available* to consume. This includes licenses of all durations (perpetual and subscription), including expired subscription licenses, for all the product instances in a High Availability setup.
	Enforcement type	Enforcement type for the license. This may be one of the following: • Enforced • Not enforced • Export-Controlled
	Term information:	Header providing license duration information. The following fields maybe included under this header: • Active: The active product instance UDI, followed by the status of the authorization code installation for this UDI. • Authorization type: Type of authorization code installed and date of installation. The type can be: SLAC, UNIVERSAL, SPECIFIED, PAK, RTU. • Start Date: Displays validity start date if the license is for a specific term or time period. • Start Date: Displays validity end date if the license is for a specific term or time period. • Term Count: License count. • Subscription ID: Displays ID if the license is for a specific term or time period. • License type: License duration. This can be: SUBSCRIPTION or PERPETUAL. • Standby: The standby product instance UDI, followed by the status of the authorization code installation for this UDI. • Member: The member product instance UDI, followed by the status of the authorization code installation for this UDI.

Field		Description
Purchased Licenses	Header for license purchase information.	
	Active:	The active product instance and its the UDI.
	Count:	License count.
	Description:	License description.
	License type:	License duration. This can be: SUBSCRIPTION or PERPETUAL.
	Standby:	The standby product instance UDI.
	Member:	The member product instance UDI.

Displaying SLAC

The following is sample output of the **show license authorization** command on a C9300X model switch. Here SLAC is installed only on the active product instance in a stacking set-up:

```
Device# show license authorization
Overall status:
  Active: PID:C9300X-24HX,SN:FOC2519L8R7
      Status: SMART AUTHORIZATION INSTALLED on Oct 29 17:45:28 2021 UTC
      Last Confirmation code: 6746c5b5
  Standby: PID:C9300X-48HXN,SN:FOC2524L39P
      Status: NOT INSTALLED
  Member: PID:C9300X-48HX,SN:FOC2516LC92
      Status: NOT INSTALLED

Authorizations:
  C9K HSEC (Cat9K HSEC):
    Description: HSEC Key for Export Compliance on Cat9K Series Switches
    Total available count: 1
    Enforcement type: EXPORT RESTRICTED
    Term information:
      Active: PID:C9300X-24HX,SN:FOC2519L8R7
        Authorization type: SMART AUTHORIZATION INSTALLED
        License type: PERPETUAL
          Term Count: 1

Purchased Licenses:
  No Purchase Information Available
```

Displaying SLR Authorization Code

The following is sample output of the **show license authorization** command showing SLR authorization codes (`Last Confirmation code:`). An SLR authorization code is supported after upgrade to Smart Licensing Using Policy. While existing SLRs are carried over after upgrade, you cannot request a new SLR in the Smart Licensing Using Policy environment. If you are in an air-gapped network, the *No Connectivity to CSSM and No CSLU* topology applies instead.

```
Device# show license authorization

Overall status:
  Active: PID:C9500-16X,SN:FCW2233A5ZV
```

```
      Status: SPECIFIC INSTALLED on Oct 29 09:44:06 2020 PST
      Last Confirmation code: 184ba6d6
  Standby: PID:C9500-16X,SN:FCW2233A5ZY
      Status: SPECIFIC INSTALLED on Oct 29 09:44:06 2020 PST
      Last Confirmation code: 961d598f

Specified license reservations:
  C9500 Network Advantage (C9500 Network Advantage):
    Description: C9500 Network Advantage
    Total reserved count: 2
    Enforcement type: NOT ENFORCED
    Term information:
      Active: PID:C9500-16X,SN:FCW2233A5ZV
        Authorization type: SPECIFIC INSTALLED on Oct 29 09:44:06 2020 PST
        License type: PERPETUAL
          Term Count: 1
      Standby: PID:C9500-16X,SN:FCW2233A5ZY
        Authorization type: SPECIFIC INSTALLED on Oct 29 09:44:06 2020 PST
        License type: PERPETUAL
          Term Count: 1
  C9500-DNA-16X-A (C9500-16X DNA Advantage):
    Description: C9500-DNA-16X-A
    Total reserved count: 2
    Enforcement type: NOT ENFORCED
    Term information:
      Active: PID:C9500-16X,SN:FCW2233A5ZV
        Authorization type: SPECIFIC INSTALLED on Oct 29 09:44:06 2020 PST
        License type: PERPETUAL
          Term Count: 1
      Standby: PID:C9500-16X,SN:FCW2233A5ZY
        Authorization type: SPECIFIC INSTALLED on Oct 29 09:44:06 2020 PST
        License type: PERPETUAL
          Term Count: 1

Purchased Licenses:
  No Purchase Information Available


Derived Licenses:
  Entitlement Tag:
regid.2017-03.com.cisco.advantagek9-Nyquist-C9500,1.0_f1563759-2e03-4a4c-bec5-5feec525a12c
  Entitlement Tag:
regid.2017-07.com.cisco.C9500-DNA-16X-A,1.0_ef3574d1-156b-486a-864f-9f779ff3ee49
```

show license data conversion

To display license data conversion information, enter the **show license data** command in privileged EXEC mode.

show license data conversion

Syntax Description

This command has no keywords or arguments

Command Modes

Privileged EXEC (Device#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.
Cisco IOS XE Amsterdam 17.3.2a	Command output was updated to display information relating to Smart Licensing Using Policy. Command output no longer displays Smart Account and Virtual account information.

Usage Guidelines

Smart Licensing: If the software version on the device is Cisco IOS XE Amsterdam 17.3.1 or an earlier release, command output displays fields pertinent to Smart Licensing.

Smart Licensing Using Policy: If the software version on the device (also referred to as a product instance) is Cisco IOS XE Amsterdam 17.3.2a or a later release, command output displays fields pertinent to Smart Licensing Using Policy.

Device-led conversion is not supported on Cisco Catalyst Access, Core, and Aggregation Switches.

show license eventlog

To display event logs relating to Smart Licensing Using Policy, enter the **show license eventlog** command in privileged EXEC mode.

show license eventlog [*days*]

Syntax Description

days	Enter the number of days for which you want to display event logs. The valid value range is from 0 to 2147483647.

Command Modes

Privileged EXEC (Device#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.
Cisco IOS XE Amsterdam 17.3.2a	Additional events were added with the introduction of Smart Licensing Using Policy: • Installation and removal of a policy • Request, installation and removal of an authorization code. • Installation and removal of a trust code. • Addition of authorization source information for license usage.

Usage Guidelines

Smart Licensing: If the software version on the device is Cisco IOS XE Amsterdam 17.3.1 or an earlier release, command output displays fields pertinent to Smart Licensing.

Smart Licensing Using Policy: If the software version on the device (also referred to as a product instance) is Cisco IOS XE Amsterdam 17.3.2a or a later release, command output displays fields pertinent to Smart Licensing Using Policy.

Examples

show license eventlog for One Day, for Smart Licensing Using Policy, on page 122

show license eventlog for All Events, for Smart Licensing Using Policy, on page 123

show license eventlog for One Day, for Smart Licensing Using Policy

The following is sample output from the **show license eventlog** command on a Cisco Catalyst 9500 switch. Similar output is displayed on all supported Cisco Catalyst Access, Core, and Aggregation Switches. The command is configured to display events for one day.

```
Device# show license eventlog 1
**** Event Log ****

2020-09-11 00:50:17.693 EDT SAEVT_PLATFORM eventSource="INFRA_SL"
eventName="INFRA_SL_EVLOG_ERM_RESET" MSG="ERM-Reset: Client 0, AP-GROUP group, 2 features
air-network-advantage,air-dna-advantage"
2020-09-11 00:50:17.695 EDT SAEVT_ENDPOINT_USAGE count="0"
```

```
entitlementTag="regid.2018-06.com.cisco.DNA_NWStack,1.0_e7244e71-3ad5-4608-8bf0-d12f67c80896"
2020-09-11 00:50:17.695 EDT SAEVT_ENDPOINT_USAGE count="0"
entitlementTag="regid.2017-08.com.cisco.AIR-DNA-A,1.0_b6308627-3ab0-4a11-a3d9-586911a0d790"
2020-09-11 00:50:50.175 EDT SAEVT_POLL_MESSAGE messageType="LICENSE_USAGE"
2020-09-11 08:50:17.694 EDT SAEVT_PLATFORM eventSource="INFRA_SL"
eventName="INFRA_SL_EVLOG_ERM_RESET" MSG="ERM-Reset: Client 0, AP-GROUP group, 2 features
air-network-advantage,air-dna-advantage"
2020-09-11 08:50:17.696 EDT SAEVT_ENDPOINT_USAGE count="0"
entitlementTag="regid.2018-06.com.cisco.DNA_NWStack,1.0_e7244e71-3ad5-4608-8bf0-d12f67c80896"
2020-09-11 08:50:17.696 EDT SAEVT_ENDPOINT_USAGE count="0"
entitlementTag="regid.2017-08.com.cisco.AIR-DNA-A,1.0_b6308627-3ab0-4a11-a3d9-586911a0d790"
2020-09-11 08:50:52.804 EDT SAEVT_POLL_MESSAGE messageType="LICENSE_USAGE"
```

show license eventlog for All Events, for Smart Licensing Using Policy

The following is sample output from the **show license eventlog** command on a Cisco Catalyst 9500 switch. Similar output is displayed on all supported Cisco Catalyst Access, Core, and Aggregation Switches. The command is configured to display all events.

```
Device# show license eventlog

**** Event Log ****

2020-09-01 15:43:42.300 UTC SAEVT_INIT_START version="4.13.14_rel/41"
2020-09-01 15:43:42.301 UTC SAEVT_INIT_CRYPTO success="False" error="Crypto Initialization
 has not been completed"
2020-09-01 15:43:42.301 UTC SAEVT_HA_EVENT eventType="SmartAgentEvtHArmfRegister"
2020-09-01 15:43:45.055 UTC SAEVT_READY
2020-09-01 15:43:45.055 UTC SAEVT_ENABLED
2020-09-01 15:43:45.088 UTC SAEVT_PLATFORM eventSource="INFRA_SL"
eventName="INFRA_SL_EVLOG_SYSDATA_FAIL" MSG="Get-SDL: not the active switch"
2020-09-01 15:43:45.089 UTC SAEVT_PLATFORM eventSource="INFRA_SL"
eventName="INFRA_SL_EVLOG_SYSDATA_FAIL" MSG="Get-SDL: not the active switch"
2020-09-01 15:43:45.089 UTC SAEVT_PLATFORM eventSource="INFRA_SL"
eventName="INFRA_SL_EVLOG_SYSDATA_FAIL" MSG="Get-SDL: not the active switch"
2020-09-01 15:43:45.089 UTC SAEVT_LICENSE_USAGE count="0" type="destroy"
entitlementTag="regid.2018-01.com.cisco.C9500-24Y4C-A,1.0_6b065611-6552-472a-8859-ab3339550166"
2020-09-01 15:43:45.098 UTC SAEVT_PLATFORM eventSource="INFRA_SL"
eventName="INFRA_SL_EVLOG_SYSDATA_FAIL" MSG="Get-SDL: not the active switch"
```

show license history message

To display communication history between the product instance and CSSM or CSLU (as the case may be), enter the **show license history message** command in privileged EXEC mode. The output of this command is used by the technical support team, for troubleshooting.

show license history message

Syntax Description

This command has no keywords or arguments.

Command Modes

Privileged EXEC (Device#)

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.3.2a	This command was introduced.

Usage Guidelines

When you encounter an error message that you are not able to resolve, along with a copy of the message that appears on the console or in the system log, provide your Cisco technical support representative with sample output of these commands: **show license tech support**, **show license history message**, and the **show platform software sl-infra all** privileged EXEC commands.

show license reservation

To display license reservation information, enter the **show license reservation** command in privileged EXEC mode.

show license reservation

This command has no arguments or keywords.

Command Modes

Privileged EXEC (Device#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.
Cisco IOS XE Amsterdam 17.3.2a	The command continues to be available on the CLI, but is no longer applicable because the notion of reserveration does not exist in the Smart Licensing Using Policy environment.

Usage Guidelines

The command continues to be available on the CLI and corresponding output is displayed, but with the introduction of Smart Licensing Using Policy, the notion of reservation is not longer applicable. Use the **show license all** command in privileged EXEC mode, to display *migrated* SLR licenses instead (the SLR authorization code is migrated to Smart Licensing Using Policy).

show license status

To display information about licensing settings such as data privacy, policy, transport, usage reporting and trust codes, enter the **show license status** command in privileged EXEC mode.

show license status

Syntax Description

This command has no arguments or keywords.

Command Default

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.
Cisco IOS XE Amsterdam 17.3.2a	Command output was updated to reflect new fields that are applicable to Smart Licensing Using Policy. This includes `Trust code installed:`, `Policy in use`, `Policy name:` , reporting requirements as in the policy, and `Usage Reporting:` . Command output no longer displays Smart Account and Virtual account information.

Usage Guidelines

Smart Licensing: If the software version on the device is Cisco IOS XE Amsterdam 17.3.1 or an earlier release, command output displays fields pertinent to Smart Licensing.

Smart Licensing Using Policy: If the software version on the device (also referred to as a product instance) is Cisco IOS XE Amsterdam 17.3.2a or a later release, command output displays fields pertinent to Smart Licensing Using Policy.

Examples

For information about fields shown in the display, see Table 6: show license status Field Descriptions for Smart Licensing Using Policy, on page 127

For sample outputs, see:

- show license status for Smart Licensing Using Policy, on page 132
- show license status for Smart Licensing, on page 133

Table 6: show license status Field Descriptions for Smart Licensing Using Policy

Field		Description
Utility	Header for utility settings that are configured on the product instance.	
	Status:	Status
	Utility report:	Last attempt:
	Customer Information:	The following fields are displayed: • Id: • Name: • Street • City: • State: • Country: • Postal Code:
Smart Licensing Using Policy:	Header for policy settings on the product instance.	
	Status:	Indicates if Smart Licensing Using Policy is enabled. Smart Licensing Using Policy is supported starting from Cisco IOS XE Amsterdam 17.3.2 and is always enabled on supported software images.
Data Privacy:	Header for privacy settings that are configured on the product instance.	
	Sending Hostname:	A *yes* or *no* value which shows if the hostname is sent in usage reports.
	Callhome hostname privacy:	Indicates if the Call Home feature is configured as the mode of transport for reporting. If configured, one of these values is displayed: • ENABLED • DISABLED
	Smart Licensing hostname privacy:	One of these values is displayed: • ENABLED • DISABLED
	Version privacy:	One of these values is displayed: • ENABLED • DISABLED

Field		Description
Transport:	Header for transport settings that are configured on the product instance.	
	Type:	Mode of transport that is in use. Additional fields are displayed for certain transport modes. For example, if transport type is set to CSLU, the CSLU address is also displayed.

Field		Description
Policy:	Header for policy information that is applicable to the product instance.	
	Policy in use:	Policy that is applied This can be one of the following: Cisco default, Product default, Permanent License Reservation, Specific License Reservation, PAK license, Installed on <date>, Controller.
	Policy name:	Name of the policy
	Reporting ACK required:	A *yes* or *no* value which specifies if the report for this product instance requires CSSM acknowledgement (ACK) or not. The default policy is always set to “yes”.
	Unenforced/Non-Export Perpetual Attributes	Displays policy values for perpetual licenses. • First report requirement (days): The maximum amount of time available before the first report must be sent, followed by policy name. • Reporting frequency (days): The maximum amount of time available before the subsequent report must be sent, followed by policy name. • Report on change (days): he maximum amount of time available to send a report in case of a change in license usage, followed by policy name
	Unenforced/Non-Export Subscription Attributes	Displays policy values for subscription licenses. • First report requirement (days): The maximum amount of time available before the first report must be sent, followed by policy name. • Reporting frequency (days): The maximum amount of time available before the subsequent report must be sent, followed by policy name. • Report on change (days): he maximum amount of time available to send a report in case of a change in license usage, followed by policy name
	Enforced (Perpetual/Subscription) License Attributes	

Field		Description
		Displays policy values for enforced licenses. • First report requirement (days): The maximum amount of time available before the first report must be sent, followed by policy name. • Reporting frequency (days): The maximum amount of time available before the subsequent report must be sent, followed by policy name. • Report on change (days): The maximum amount of time available to send a report in case of a change in license usage, followed by policy name
	Export (Perpetual/Subscription) License Attributes	Displays policy values for export-controlled licenses. • First report requirement (days): The maximum amount of time available before the first report must be sent, followed by policy name. • Reporting frequency (days): The maximum amount of time available before the subsequent report must be sent, followed by policy name. • Report on change (days): The maximum amount of time available to send a report in case of a change in license usage, followed by policy name
Miscellaneous	Header for custom ID.	
	Custom Id:	ID

Field		Description
Usage Reporting:	Header for usage reporting (RUM reports) information.	
	Last ACK received:	Date and time of last ACK received, in the local time zone.
	Next ACK deadline:	Date and time for next ACK. If the policy states that an ACK is not requires then this field displays `none`. **Note** If an ACK is required and is not received by this deadline, a syslog is displayed.
	Reporting Interval:	Reporting interval in days The value displayed here depends on what you configure in the **license smart usage interval***interval_in_days* and the policy value. For more information, see the corresponding Syntax Description: Table 6: show license status Field Descriptions for Smart Licensing Using Policy, on page 127.
	Next ACK push check:	Date and time when the product instance will submit the next polling request for an ACK. Date and time are in the local time zone. This applies only to product instance- initiated communication to CSSM or CSLU. If the reporting interval is zero, or if no ACK polling is pending, then this field displays `none`.
	Next report push:	Date and time when the product instance will send the next RUM report. Date and time are in the local time zone. If the reporting interval is zero, or if there are no pending RUM reports, then this field displays `none`.
	Last report push:	Date and time for when the product instance sent the last RUM report. Date and time are in the local time zone.
	Last report file write:	Date and time for when the product instance last saved an offline RUM report. Date and time are in the local time zone.
	Last report pull:	Date and time for when usage reporting information was retrieved using data models. Date and time are in the local time zone.

Field		Description
Trust Code Installed:	Header for trust code-related information. Displays date and time if trust code is installed. Date and time are in the local time zone. If a trust code is not installed, then this field displays `none`.	
	Active:	Active product instance. In a High Availability set-up, the the UDIs of all product instances in the set-up, along with corresponding trust code installation dates and times are displayed.
	Standby:	Standby product instance.
	Member:	Member product instance

show license status for Smart Licensing Using Policy

The following is sample output of the **show license status** command. A Cisco default policy (merged from multiple sources) is applied here, on a Cisco Catalyst 9500 switch. Similar output is displayed on all supported Cisco Catalyst Access, Core, and Aggregation Switches.

```
Device# show license status
Utility:
  Status: DISABLED
License Reservation is ENABLED
Data Privacy:
  Sending Hostname: yes
    Callhome hostname privacy: DISABLED
    Smart Licensing hostname privacy: DISABLED
   Version privacy: DISABLED
Transport:
  Type: Transport Off
Policy:
  Policy in use: Merged from multiple sources.
  Reporting ACK required: yes (CISCO default)
  Unenforced/Non-Export Perpetual Attributes:
    First report requirement (days): 365 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 90 (CISCO default)
  Unenforced/Non-Export Subscription Attributes:
    First report requirement (days): 90 (CISCO default)
    Reporting frequency (days): 90 (CISCO default)
    Report on change (days): 90 (CISCO default)
  Enforced (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 0 (CISCO default)
  Export (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 0 (CISCO default)
Miscellaneous:
  Custom Id: <empty>
Usage Reporting:
  Last ACK received: <none>
  Next ACK deadline: Nov 29 10:50:05 2020 PDT
  Reporting Interval: 30
  Next ACK push check: <none>
  Next report push: Aug 31 10:52:05 2020 PDT
  Last report push: <none>
  Last report file write: <none>
Trust Code Installed: <none>
```

show license status for Smart Licensing

The following is sample output of the **show license status** command.

```
Device# show license status

Smart Licensing is ENABLED

Utility:
  Status: DISABLED

Data Privacy:
  Sending Hostname: yes
    Callhome hostname privacy: DISABLED
    Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
  Type: Callhome

Registration:
  Status: REGISTERED
  Smart Account: Cisco Systems
  Virtual Account: NPR
  Export-Controlled Functionality: Allowed
  Initial Registration: First Attempt Pending
  Last Renewal Attempt: SUCCEEDED on Jul 19 14:49:49 2018 IST
  Next Renewal Attempt: Jan 15 14:49:47 2019 IST
  Registration Expires: Jul 19 14:43:47 2019 IST

License Authorization:
  Status: AUTHORIZED on Jul 28 07:02:56 2018 IST
  Last Communication Attempt: SUCCEEDED on Jul 28 07:02:56 2018 IST
  Next Communication Attempt: Aug 27 07:02:56 2018 IST
  Communication Deadline: Oct 26 06:57:50 2018 IST
```

Related Commands

Command	Description
show license all	Displays entitlements information.
show license authorization	Displays authorization code-related information.
show license summary	Displays summary of all active licenses.
show license udi	Displays UDI.
show license usage	Displays license usage information
show tech-support license	Displays the debug output.

show license summary

To display a brief summary of license usage, which includes information about licenses being used, the count, and status, use the **show license summary** command in privileged EXEC mode.

show license summary

Syntax Description

This command has no arguments or keywords.

Command Default

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.
Cisco IOS XE Amsterdam 17.3.2a	Command output was updated to reflect valid license status for Smart Licensing Using Policy. Valid license statuses are now only `IN USE`, `NOT IN USE`, `NOT AUTHORIZED`. Command output was also updated to remove registration and authorization information. Command output no longer displays Smart Account and Virtual account information.

Usage Guidelines

Smart Licensing: If the software version on the device is Cisco IOS XE Amsterdam 17.3.1 or an earlier release, command output displays fields pertinent to Smart Licensing.

Smart Licensing Using Policy: If the software version on the device (also referred to as a product instance) is Cisco IOS XE Amsterdam 17.3.2a or a later release, command output displays fields pertinent to Smart Licensing Using Policy.

- The **unenforced licenses** that are available on Cisco Catalyst Access, Core, and Aggregation Switches are never `NOT AUTHORIZED` or `NOT IN USE`.
- The **export-controlled license**, Export Control Key for High Security (HSECK9), which is available on the Cisco Catalyst 9300X Series Switches starting from Cisco IOS XE Bengaluru 17.6.2 can be `NOT IN USE` if an HSECK9 key is available on the product instance and the requisite Smart Licensing Authorization Code (SLAC) is installed, but the cryptographic feature that requires the HSECK9 key is not configured. Configure the cryptographic feature for the count and status fields to change to 1 and IN USE respectively.

  If you install SLAC on more than one device (in a High Availability or stacking set-up), the usage count still remains 1. This is because only one HSECK9 key is used at a given point in time - the one on the active. The license on the standby comes into effect when a switchover occurs. The count remains 1 with the new active as well, because it is still only one HSECK9 key that is being used.

For more detailed license usage information, see the **show license usage** privileged EXEC command.

Examples

For information about fields shown in the display, see Table 7: show license summary Field Descriptions for Smart Licensing Using Policy, on page 135

For sample outputs, see:

- show license summary (Cisco Catalyst 9300X Series Switches), on page 135
- show license summary (Cisco Catalyst 9500 Series Switches), on page 136

Table 7: show license summary Field Descriptions for Smart Licensing Using Policy

Field	Description
License	Name of the licenses in use
Entitlement Tag	Short name for license
Count	License count
Status	License status can be one of the following • In-Use: Valid license, and in-use. • Not In-Use: An HSECK9 key is available on the product instance and the requisite Smart Licensing Authorization Code (SLAC) is installed, but the cryptographic feature that requires the HSECK9 key is disabled or not configured. This status is a prerequisite when you want to *return* the SLAC for an HSECK9 key to CSSM. • Not Authorized: Means that the license requires installation of a SLAC before use.

show license summary (Cisco Catalyst 9300X Series Switches)

The following are sample outputs of the **show license summary** command, on a C9300X stack.

The Status and Count columns here, display `NOT IN USE` and `0` for the HSECK9 key. This means the HSECK9 key is available and SLAC is installed, but the cryptographic feature that requires the license is not configured:

```
Device# show license summary
License Usage:
  License                 Entitlement Tag              Count Status
  -----------------------------------------------------------------------------
  network-advantage       (C9300-24 Network Advan...)      1 IN USE
  dna-advantage           (C9300-24 DNA Advantage)         1 IN USE
  network-advantage       (C9300-48 Network Advan...)      2 IN USE
  dna-advantage           (C9300-48 DNA Advantage)         2 IN USE
  C9K HSEC                (Cat9K HSEC)                     0 NOT IN USE
```

The Status and Count columns here display `IN USE` and `1` for the HSECK9 key. This means the cryptographic feature, which requires an HSECK9 key, is configured.

```
Device# show license summary
License Usage:
  License                 Entitlement Tag              Count Status
  -----------------------------------------------------------------------------
  network-advantage       (C9300-24 Network Advan...)      1 IN USE
  dna-advantage           (C9300-24 DNA Advantage)         1 IN USE
  network-advantage       (C9300-48 Network Advan...)      2 IN USE
  dna-advantage           (C9300-48 DNA Advantage)          2 IN USE
  hseck9                  (Cat9K HSEC)                      1 IN USE
```

show license summary (Cisco Catalyst 9500 Series Switches)

The following is sample output of the **show license summary** command on a Cisco Catalyst 9500 switch. Similar output is displayed on all supported Cisco Catalyst Access, Core, and Aggregation Switches.

```
Device# show license summary

License Usage:
License            Entitlement tag            Count Status
-----------------------------------------------------------
network-advantage (C9500 Network Advantage)       2 IN USE
dna-advantage     (C9500-16X DNA Advantage)       2 IN USE
```

show license tech

To display licensing information to help the technical support team troubleshoot a problem, enter the **show license tech** command in privileged EXEC mode. The output for this command includes outputs of several other **show license** commands and more.

show license tech { **data conversion** | **eventlog** [*days*] | **reservation** | **support** }

Syntax Description

data conversion	Displays license data conversion information.
eventlog [*days*]	Displays event logs related to Smart Licensing Using Policy. For *days*, enter the number of days for which you want to display event logs. The valid value range is from 0 to 2147483647. The output for this option is the same as the **show license eventlog** command.
reservation	Displays license reservation information.
support	Displays licensing information that helps the technical support team to debug a problem.

Command Modes

Privileged EXEC (Device#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.
Cisco IOS XE Amsterdam 17.3.2a	Command output was updated to reflect new fields that are applicable to Smart Licensing Using Policy.

Usage Guidelines

Smart Licensing: If the software version on the device is Cisco IOS XE Amsterdam 17.3.1 or an earlier release, command output displays fields pertinent to Smart Licensing (whether smart licensing is enabled, all associated licensing certificates, compliance status, and so on).

Smart Licensing Using Policy: If the software version on the device (also referred to as a product instance) is Cisco IOS XE Amsterdam 17.3.2a or a later release, command output displays fields pertinent to Smart Licensing Using Policy.

When you encounter an error message that you are not able to resolve, along with a copy of the message that appears on the console or in the system log, provide your Cisco technical support representative with sample output of these commands: **show license tech support**, **show license history message**, and the **show platform software sl-infra all** privileged EXEC commands.

show license tech support for Smart Licensing Using Policy

The following is sample output from the **show license tech support** command on a Cisco Catalyst 9500 switch. Similar output is displayed on all supported Cisco Catalyst Access, Core, and Aggregation Switches.

```
Device# show license tech support
Smart Licensing Tech Support info
Smart Licensing Status
======================

Smart Licensing is ENABLED
License Reservation is ENABLED

Export Authorization Key:
  Features Authorized:
    <none>

Utility:
  Status: DISABLED

Smart Licensing Using Policy:
  Status: ENABLED

Data Privacy:
  Sending Hostname: yes
    Callhome hostname privacy: DISABLED
    Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
  Type: Transport Off

Miscellaneous:
  Custom Id: <empty>

Policy:
  Policy in use: Merged from multiple sources.
  Reporting ACK required: yes (CISCO default)
  Unenforced/Non-Export Perpetual Attributes:
    First report requirement (days): 365 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 90 (CISCO default)
  Unenforced/Non-Export Subscription Attributes:
    First report requirement (days): 90 (CISCO default)
    Reporting frequency (days): 90 (CISCO default)
    Report on change (days): 90 (CISCO default)
  Enforced (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 0 (CISCO default)
  Export (Perpetual/Subscription) License Attributes:
    First report requirement (days): 0 (CISCO default)
    Reporting frequency (days): 0 (CISCO default)
    Report on change (days): 0 (CISCO default)

Usage Reporting:
  Last ACK received: <none>
  Next ACK deadline: Jan 27 09:49:33 2021 PST
  Reporting push interval: 30  days State(2) InPolicy(90)
  Next ACK push check: <none>
  Next report push: Oct 29 09:51:33 2020 PST
  Last report push: <none>
  Last report file write: <none>

License Usage
=============
Handle: 1
  License: network-advantage
  Entitlement Tag:
regid.2017-03.com.cisco.advantagek9-Nyquist-C9500,1.0_f1563759-2e03-4a4c-bec5-5feec525a12c
  Description: network-advantage
  Count: 2
  Version: 1.0
  Status: IN USE(15)
  Status time: Oct 29 09:48:54 2020 PST
  Request Time: Oct 29 09:49:18 2020 PST
  Export status: NOT RESTRICTED
  Feature Name: network-advantage
  Feature Description: network-advantage
  Measurements:
    ENTITLEMENT:
      Interval: 00:15:00
      Current Value: 2
  Soft Enforced: True

Handle: 2
  License: dna-advantage
  Entitlement Tag:
regid.2017-07.com.cisco.C9500-DNA-16X-A,1.0_ef3574d1-156b-486a-864f-9f779ff3ee49
  Description: C9500-16X DNA Advantage
  Count: 2
  Version: 1.0
  Status: IN USE(15)
  Status time: Oct 29 09:48:54 2020 PST
  Request Time: Oct 29 09:49:18 2020 PST
  Export status: NOT RESTRICTED
  Feature Name: dna-advantage
  Feature Description: C9500-16X DNA Advantage
  Measurements:
    ENTITLEMENT:
      Interval: 00:15:00
      Current Value: 2
  Soft Enforced: True

Handle: 7
  License: air-network-advantage
  Entitlement Tag:
regid.2018-06.com.cisco.DNA_NWStack,1.0_e7244e71-3ad5-4608-8bf0-d12f67c80896
  Description: air-network-advantage
  Count: 0
  Version: 1.0
  Status: IN USE(15)
  Status time: Oct 29 10:49:09 2020 PST
  Request Time: None
  Export status: NOT RESTRICTED
  Feature Name: air-network-advantage
  Feature Description: air-network-advantage
  Measurements:
    ENTITLEMENT:
      Interval: 00:15:00
     Current Value: 0
  Soft Enforced: True

Handle: 8
  License: air-dna-advantage
  Entitlement Tag: regid.2017-08.com.cisco.AIR-DNA-A,1.0_b6308627-3ab0-4a11-a3d9-586911a0d790

  Description: air-dna-advantage
  Count: 0
  Version: 1.0
  Status: IN USE(15)
  Status time: Oct 29 10:49:09 2020 PST
  Request Time: None
  Export status: NOT RESTRICTED
  Feature Name: air-dna-advantage
  Feature Description: air-dna-advantage
  Measurements:
    ENTITLEMENT:
      Interval: 00:15:00
      Current Value: 0
  Soft Enforced: True

Product Information
===================
UDI: PID:C9500-16X,SN:FCW2233A5ZV

HA UDI List:
    Active:PID:C9500-16X,SN:FCW2233A5ZV
    Standby:PID:C9500-16X,SN:FCW2233A5ZY

Agent Version
=============
Smart Agent for Licensing: 5.0.5_rel/42

Upcoming Scheduled Jobs
=======================
Current time: Oct 29 11:04:46 2020 PST
Daily: Oct 30 09:48:56 2020 PST (22 hours, 44 minutes, 10 seconds remaining)
Init Flag Check: Expired Not Rescheduled
Reservation configuration mismatch between nodes in HA mode: Nov 05 09:52:25 2020 PST (6
days, 22 hours, 47 minutes, 39 seconds remaining)
Start Utility Measurements: Oct 29 11:19:09 2020 PST (14 minutes, 23 seconds remaining)
Send Utility RUM reports: Oct 30 09:53:10 2020 PST (22 hours, 48 minutes, 24 seconds
remaining)
Save unreported RUM Reports: Oct 29 12:04:19 2020 PST (59 minutes, 33 seconds remaining)
Process Utility RUM reports: Oct 30 09:49:33 2020 PST (22 hours, 44 minutes, 47 seconds
remaining)
Data Synchronization: Expired Not Rescheduled
External Event: Nov 28 09:49:33 2020 PST (29 days, 22 hours, 44 minutes, 47 seconds remaining)
Operational Model: Expired Not Rescheduled

Communication Statistics:
=======================
Communication Level Allowed: INDIRECT
Overall State: <empty>
Trust Establishment:
  Attempts: Total=0, Success=0, Fail=0  Ongoing Failure: Overall=0 Communication=0
  Last Response: <none>
    Failure Reason: <none>
  Last Success Time: <none>
  Last Failure Time: <none>
Trust Acknowledgement:
  Attempts: Total=0, Success=0, Fail=0  Ongoing Failure: Overall=0 Communication=0
  Last Response: <none>
    Failure Reason: <none>
  Last Success Time: <none>
  Last Failure Time: <none>
Usage Reporting:
  Attempts: Total=0, Success=0, Fail=0  Ongoing Failure: Overall=0 Communication=0
  Last Response: <none>
    Failure Reason: <none>
  Last Success Time: <none>
  Last Failure Time: <none>
Result Polling:
  Attempts: Total=0, Success=0, Fail=0  Ongoing Failure: Overall=0 Communication=0
  Last Response: <none>
    Failure Reason: <none>
  Last Success Time: <none>
  Last Failure Time: <none>
```

```
Authorization Request:
  Attempts: Total=0, Success=0, Fail=0  Ongoing Failure: Overall=0 Communication=0
  Last Response: <none>
    Failure Reason: <none>
  Last Success Time: <none>
  Last Failure Time: <none>
Authorization Confirmation:
  Attempts: Total=0, Success=0, Fail=0  Ongoing Failure: Overall=0 Communication=0
  Last Response: <none>
    Failure Reason: <none>
  Last Success Time: <none>
  Last Failure Time: <none>
Authorization Return:
  Attempts: Total=0, Success=0, Fail=0  Ongoing Failure: Overall=0 Communication=0
  Last Response: <none>
    Failure Reason: <none>
  Last Success Time: <none>
  Last Failure Time: <none>
Trust Sync:
  Attempts: Total=0, Success=0, Fail=0  Ongoing Failure: Overall=0 Communication=0
  Last Response: <none>
    Failure Reason: <none>
  Last Success Time: <none>
  Last Failure Time: <none>
Hello Message:
  Attempts: Total=0, Success=0, Fail=0  Ongoing Failure: Overall=0 Communication=0
  Last Response: <none>
    Failure Reason: <none>
  Last Success Time: <none>
  Last Failure Time: <none>

License Certificates
====================
Production Cert: True
Not registered. No certificates installed

HA Info
==========
RP Role: Active
Chassis Role: Active
Behavior Role: Active
RMF: True
CF: True
CF State: Stateless
Message Flow Allowed: False

Reservation Info
================
License reservation: ENABLED

Overall status:
  Active: PID:C9500-16X,SN:FCW2233A5ZV
      Reservation status: SPECIFIC INSTALLED on Oct 29 09:44:06 2020 PST
      Request code: <none>
      Last return code: <none>
      Last Confirmation code: 184ba6d6
      Reservation authorization code:
[illegible]
 Network Advantage</displayName><tagDescription>C9500 Network
[illegible]

  Standby: PID:C9500-16X,SN:FCW2233A5ZY
      Reservation status: SPECIFIC INSTALLED on Oct 29 09:44:06 2020 PST
      Request code: <none>
      Last return code: <none>
      Last Confirmation code: 961d598f
      Reservation authorization code:
[illegible]
 Network Advantage</displayName><tagDescription>C9500 Network
[illegible]


Specified license reservations:
  C9500 Network Advantage (C9500 Network Advantage):
    Description: C9500 Network Advantage
    Total reserved count: 2
    Enforcement type: NOT ENFORCED
    Term information:
      Active: PID:C9500-16X,SN:FCW2233A5ZV
        Authorization type: SPECIFIC INSTALLED on Oct 29 09:44:06 2020 PST
        License type: PERPETUAL
          Start Date: <none>
          End Date: <none>
          Term Count: 1
          Subscription ID: <none>
      Standby: PID:C9500-16X,SN:FCW2233A5ZY
        Authorization type: SPECIFIC INSTALLED on Oct 29 09:44:06 2020 PST
        License type: PERPETUAL
          Start Date: <none>
          End Date: <none>
          Term Count: 1
          Subscription ID: <none>
  C9500-DNA-16X-A (C9500-16X DNA Advantage):
    Description: C9500-DNA-16X-A
    Total reserved count: 2
    Enforcement type: NOT ENFORCED
    Term information:
      Active: PID:C9500-16X,SN:FCW2233A5ZV
        Authorization type: SPECIFIC INSTALLED on Oct 29 09:44:06 2020 PST
        License type: PERPETUAL
          Start Date: <none>
          End Date: <none>
          Term Count: 1
          Subscription ID: <none>
      Standby: PID:C9500-16X,SN:FCW2233A5ZY
        Authorization type: SPECIFIC INSTALLED on Oct 29 09:44:06 2020 PST
        License type: PERPETUAL
          Start Date: <none>
          End Date: <none>
          Term Count: 1
          Subscription ID: <none>

Purchased Licenses:
  No Purchase Information Available


Other Info
==========
Software ID: regid.2017-05.com.cisco.C9500,v1_7435cf27-0075-4bfb-b67c-b42f3054e82a
Agent State: authorized
TS enable: True
Transport: Transport Off
Locale: en_US.UTF-8
Debug flags: 0x7
Privacy Send Hostname: True
Privacy Send IP: True
Build type:: Production
sizeof(char)  : 1
sizeof(int)   : 4
sizeof(long)  : 4
sizeof(char *): 8
sizeof(time_t): 4
sizeof(size_t): 8
Endian: Big
Write Erase Occurred: False
XOS version: 0.12.0.0
Config Persist Received: False
Message Version: 1.3
connect_info.name: <empty>
connect_info.version: <empty>
connect_info.additional: <empty>
connect_info.prod: False
connect_info.capabilities: <empty>
agent.capabilities: UTILITY, DLC, AppHA, MULTITIER, EXPORT_2, OK_TRY_AGAIN, POLICY_USAGE
Check Point Interface: True
Config Management Interface: False
License Map Interface: True
HA Interface: True
Trusted Store Interface: True
Platform Data Interface: True
Crypto Version 2 Interface: False
SAPluginMgmtInterfaceMutex: True
SAPluginMgmtIPDomainName: True
SmartAgentClientWaitForServer: 2000
SmartAgentCmReTrySend: True
SmartAgentClientIsUnified: True
SmartAgentCmClient: True
SmartAgentClientName: UnifiedClient
builtInEncryption: True
enableOnInit: True
routingReadyByEvent: True
systemInitByEvent: True
SmartTransportServerIdCheck: False
SmartTransportProxySupport: False
SmartAgentMaxRumMemory: 50
SmartAgentConcurrentThreadMax: 10
SmartAgentPolicyControllerModel: False
SmartAgentPolicyModel: True
SmartAgentFederalLicense: True
SmartAgentMultiTenant: False
attr365DayEvalSyslog: True
checkPointWriteOnly: False
SmartAgentDelayCertValidation: False
enableByDefault: False
conversionAutomatic: False
conversionAllowed: False
storageEncryptDisable: False
storageLoadUnencryptedDisable: False
TSPluginDisable: False
bypassUDICheck: False
loggingAddTStamp: False
loggingAddTid: True
HighAvailabilityOverrideEvent: UnknownPlatformEvent
platformIndependentOverrideEvent: UnknownPlatformEvent
platformOverrideEvent: SmartAgentSystemDataListChanged
WaitForHaRole: False
standbyIsHot: True
chkPtType: 2
delayCommInit: False
roleByEvent: True
maxTraceLength: 150
traceAlwaysOn: True
```

```
debugFlags: 0
Event log max size: 5120 KB
Event log current size: 109 KB
P:C9500-16X,S:FCW2233A5ZV: No Trust Data
P:C9500-16X,S:FCW2233A5ZY: No Trust Data
Overall Trust: No ID

Platform Provided Mapping Table
===============================
  C9500-16X: Total licenses found: 143
Enforced Licenses:
  P:C9500-16X,S:FCW2233A5ZV:
    No PD enforced licenses
  P:C9500-16X,S:FCW2233A5ZY:
    No PD enforced licenses
```

show license udi

To display Unique Device Identifier (UDI) information for a product instance, enter the **show license udi** command in Privileged EXEC mode. In a High Availability set-up, the output displays UDI information for all connected product instances.

show license udi

Syntax Description

This command has no arguments or keywords.

Command Default

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.
Cisco IOS XE Amsterdam 17.3.2a	The command continues to be available and applicable in the Smart Licensing Using Policy environment.

Usage Guidelines

Smart Licensing: If the software version on the device is Cisco IOS XE Amsterdam 17.3.1 or an earlier release, command output displays fields pertinent to Smart Licensing.

Smart Licensing Using Policy: If the software version on the device (also referred to as a product instance) is Cisco IOS XE Amsterdam 17.3.2a or a later release, command output displays fields pertinent to Smart Licensing Using Policy.

In a High Availabilty or stacking set-up, the output of the **show license udi** command displays the UDI information for all connected product instances.

Examples

show licensing udi for Smart Licensing Using Policy, on page 145

show license udi for Smart Licensing, on page 145

show licensing udi for Smart Licensing Using Policy

The following is sample output of the **show license udi** command for a High Availability set-up on a Catalyst 9500 switch. Similar output is displayed on all supported Cisco Catalyst Access, Core, and Aggregation Switches.

```
Device# show license udi

UDI: PID:C9500-16X,SN:FCW2233A5ZV
HA UDI List:
Active:PID:C9500-16X,SN:FCW2233A5ZV
Standby:PID:C9500-16X,SN:FCW2233A5ZY
```

show license udi for Smart Licensing

The following is sample output of the **show license udi** command:

```
Device# show license udi
UDI: PID:C9200L-48P-4X,SN:JPG221300KP
```

show license usage

To display license usage information such as status, a count of licenses being used, and enforcement type, enter the **show license usage** command in privileged EXEC mode.

show license usage

This command has no arguments or keywords.

Command Default

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.
Cisco IOS XE Amsterdam 17.3.2a	Command output was updated to reflect new fields that are applicable to Smart Licensing Using Policy. This includes the `Status`, `Enforcement type` fields. Command output was also updated to remove reservation related information, authorization status information, and export status information.

Usage Guidelines

Smart Licensing: If the software version on the device is Cisco IOS XE Amsterdam 17.3.1 or an earlier release, command output displays fields pertinent to Smart Licensing.

Smart Licensing Using Policy: If the software version on the device (also referred to as a product instance) is Cisco IOS XE Amsterdam 17.3.2a or a later release, command output displays fields pertinent to Smart Licensing Using Policy.

- The **unenforced licenses** that are available on Cisco Catalyst Access, Core, and Aggregation Switches are never `NOT AUTHORIZED` or `NOT IN USE`.
- The **export-controlled license**, Export Control Key for High Security (HSECK9), which is available on the Cisco Catalyst 9300X Series Switches starting from Cisco IOS XE Bengaluru 17.6.2 can be `NOT IN USE` if an HSECK9 key is available on the product instance and the requisite Smart Licensing Authorization Code (SLAC) is installed, but the cryptographic feature that requires the HSECK9 key is not configured. Configure the cryptographic feature for the count and status fields to change to 1 and IN USE respectively.

  If you install SLAC on more than one device (in a High Availability or stacking set-up), the usage count still remains 1. This is because only one HSECK9 key is used at a given point in time - the one on the active. The license on the standby comes into effect when a switchover occurs. The count remains 1 with the new active as well, because it is still only one HSECK9 key that is being used.

Examples

See Table 8: show license usage Field Descriptions for Smart Licensing Using Policy, on page 147 for information about fields shown in the display.

show license usage for Smart Licensing Using Policy, on page 148

show license usage for Smart Licensing, on page 148

Table 8: show license usage Field Descriptions for Smart Licensing Using Policy

Field	Description
License Authorization: Status:	Displays overall authorization status.
():	Name of the license as in CSSM. If this license is one that requires an authorization code, the name of th the code.
Description	Description of the license as in CSSM.
Count	License count. If the license is not in-use, the count is reflected as ze
Version	Version.
Status	License status can be one of the following • In-Use: Valid license, and in-use. • Not In-Use: An HSECK9 key is available on the product instand Smart Licensing Authorization Code (SLAC) is installed, but the that requires the HSECK9 key is disabled or not configured. This status is a prerequisite when you want to *return* the SLAC to CSSM. • Not Authorized: The license requires installation of a SLAC bef
Export Status:	Indicates if the license is export-controlled or not. Accordingly, one of is displayed: • RESTRICTED - ALLOWED • RESTRICTED - NOT ALLOWED • NOT RESTRICTED
Feature name	Name of the feature that uses this license.
Feature Description:	Description of the feature that uses this license.
Utility Subscription id:	ID Not applicable, because the corresponding confiuration option is not

Field	Description
Enforcement type	Enforcement type status for the license. This may be one of the followin • ENFORCED: A license, which requires authorization before use. • NOT ENFORCED: A license, which does not require authorization • EXPORT RESTRICTED - ALLOWED: An export-controlled licens authorization, that is, a SLAC is installed. • EXPORT RESTRICTED - NOT ALLOWED: An export-controlled the required authorization. An export-controlled license requires au use.

show license usage for Smart Licensing Using Policy

The following is sample output of the **show license usage** command on a Cisco Catalyst 9500 switch. Unenforced licenses are in-use here. Similar output is displayed on all supported Cisco Catalyst Access, Core, and Aggregation Switches.

```
Device# show license usage
License Authorization:
  Status: Not Applicable
network-advantage (C9500 Network Advantage):
  Description: network-advantage
  Count: 2
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: network-advantage
  Feature Description: network-advantage
  Enforcement type: NOT ENFORCED
  License type: Perpetual
dna-advantage (C9500-16X DNA Advantage):
  Description: C9500-16X DNA Advantage
  Count: 2
  Version: 1.0
  Status: IN USE
  Export status: NOT RESTRICTED
  Feature Name: dna-advantage
  Feature Description: C9500-16X DNA Advantage
  Enforcement type: NOT ENFORCED
  License type: Subscription
```

show license usage for Smart Licensing

This example shows a sample output from the **show license usage** command:

```
Device# show license usage
License Authorization:
  Status: AUTHORIZED on Jul 28 07:02:56 2018 IST

C9200L DNA Advantage, 48-port Term license (C9200L-DNA-A-48):
  Description: C9200L DNA Advantage, 48-port Term license
  Count: 1
  Version: 1.0
  Status: AUTHORIZED

C9200L Network Advantage, 48-port license (C9200L-NW-A-48):
```

```
Description: C9200L Network Advantage, 48-port license
Count: 1
Version: 1.0
Status: AUTHORIZED
```

Related Commands

Command	Description
show license all	Displays entitlements information.
show license status	Displays compliance status of a license.
show license summary	Displays summary of all active licenses.
show license udi	Displays UDI.
show tech-support license	Displays the debug output.

show location

To display location information for an endpoint, use the **show location** command in privileged EXEC mode.

show location [{**admin-tag** | **civic-location**{**identifier** *identifier-string* | **interface** *type number* | **static**} | **custom-location**{**identifier** *identifier-string* | **interface** *type number* | **static**} | **elin-location**{**identifier** *identifier-string* | **interface** *type number* | **static**} | **geo-location**{**identifier** *identifier-string* | **interface** *type number* | **static**} | **host**}]

Syntax Description

admin-tag	Displays administrative tag or site information.
civic-location	Specifies civic location information.
identifier *identifier-string*	Information identifier of the civic location, custom location, or geo-spatial location.
interface *type number*	Interface type and number. For information about the numbering syntax for your device, use the question mark (?) online help function.
static	Displays configured civic, custom, or geo-spatial location information.
custom-location	Specifies custom location information.
elin-location	Specifies emergency location information (ELIN).
geo-location	Specifies geo-spatial location information.
host	Specifies the civic, custom, or geo-spatial host location information.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

The following sample output of the **show location civic-location** command displays civic location information for the specified identifier (`identifier 1`):

```
Device# show location civic-location identifier 1
Civic location information
--------------------------
Identifier              : 1
County                  : Santa Clara
Street number           : 3550
Building                : 19
Room                    : C6
Primary road name       : Example
```

```
City                     : San Jose
State                    : CA
Country                  : US
```

Related Commands

Command	Description
location	Configures location information for an endpoint.

show logging onboard switch uptime

To display a history of all reset reasons for all modules or switches in a system, use the **show logging onboard switch uptime** command.

show logging onboard switch { *switch-number* | **active** | **standby** } **uptime** [[[**continuous** | **detail**] [**start** *hour day month* [*year*] [**end** *hour day month year*]] |**summary**]

Syntax Description

switch *switch-number*	Specifies a switch. Enter the switch number.
active	Specifies the active instance.
standby	Specifies the standby instance.
continuous	(Optional) Displays continuous data.
detail	(Optional) Displays detailed data.
start *hour day month year*	(Optional) Specifies the start time to display data.
end *hour day month year*	(Optional) Specifies the end time to display data.
summary	(Optional) Displays summary data.

Command Modes

Privileged EXEC(#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was implemented on the Cisco Catalyst 9200 Series Switches
Cisco IOS XE Gibraltar 16.10.1	The output of this command was updated to display the reload reasons for members in a stack.

Examples:

The following is a sample output from the **show logging onboard switch active uptime continuous** command:

```
Device# show logging onboard switch active uptime continuous
--------------------------------------------------------------------------------
UPTIME CONTINUOUS INFORMATION
--------------------------------------------------------------------------------
Time Stamp          | Reset                       | Uptime
MM/DD/YYYY HH:MM:SS | Reason                      | years weeks days hours minutes
--------------------------------------------------------------------------------
06/17/2018 19:42:56   Reload                        0     0     0     0     5
06/17/2018 19:56:31   Reload                        0     0     0     0     5
06/17/2018 20:10:46   Reload                        0     0     0     0     5
06/17/2018 20:23:48   Reload                        0     0     0     0     5
06/17/2018 20:37:20   Reload Command                0     0     0     0     5
06/18/2018 17:09:23   Reload Command                0     0     0     20    5
06/18/2018 17:18:39   redundancy force-switchover   0     0     0     0     5
06/18/2018 18:33:33   Reload                        0     0     0     1     5
06/18/2018 19:03:05   Reload                        0     0     0     0     5
```

```
06/18/2018 19:40:30   Reload                        0     0     0     0     5
06/18/2018 20:37:47   Reload                        0     0     0     0     5
06/18/2018 20:51:13   Reload                        0     0     0     0     5
06/18/2018 21:04:08   Reload                        0     0     0     0     5
06/18/2018 21:18:23   Reload                        0     0     0     0     5
06/18/2018 21:31:25   Reload                        0     0     0     0     5
06/18/2018 21:45:15   Reload                        0     0     0     0     5
06/18/2018 21:59:02   Reload                        0     0     0     0     5
06/18/2018 22:11:41   Reload                        0     0     0     0     5
06/18/2018 22:24:27   Reload                        0     0     0     0     5
06/18/2018 22:39:14   Reload Command                0     0     0     0     4
06/19/2018 00:01:59   Reload Command                0     0     0     1     5
06/19/2018 00:13:21   redundancy force-switchover   0     0     0     0     5
06/19/2018 01:05:42   redundancy force-switchover   0     0     0     0     5
06/20/2018 02:37:16   redundancy force-switchover   0     0     1     1     5
06/20/2018 02:50:03   redundancy force-switchover   0     0     0     0     5
06/20/2018 03:02:13   redundancy force-switchover   0     0     0     0     5
06/20/2018 03:14:26   redundancy force-switchover   0     0     0     0     5
06/20/2018 03:26:44   redundancy force-switchover   0     0     0     0     5
06/20/2018 03:38:58   redundancy force-switchover   0     0     0     0     5
06/20/2018 03:52:43   redundancy force-switchover   0     0     0     0     5
06/20/2018 04:05:16   redundancy force-switchover   0     0     0     0     5
.
.
.
```

The following is a sample output from the **show logging onboard switch active uptime detail** command:

```
Device# show logging onboard switch active uptime detail

--------------------------------------------------------------------------------
UPTIME SUMMARY INFORMATION
--------------------------------------------------------------------------------
First customer power on : 06/10/2017 09:28:22
Total uptime            :  0  years  50 weeks  4  days  13 hours  38 minutes
Total downtime          :  0  years  15 weeks  4  days  11 hours  52 minutes
Number of resets        : 75
Number of slot changes  : 9
Current reset reason    : PowerOn
Current reset timestamp : 09/17/2018 10:59:57
Current slot            : 1
Chassis type            : 0
Current uptime          :  0  years  0  weeks  0  days  0  hours  0  minutes
--------------------------------------------------------------------------------

--------------------------------------------------------------------------------
UPTIME CONTINUOUS INFORMATION
--------------------------------------------------------------------------------
Time Stamp          | Reset                       | Uptime
MM/DD/YYYY HH:MM:SS | Reason                      | years weeks days hours minutes
--------------------------------------------------------------------------------
06/10/2017 09:28:22   Reload                        0     0     0     0     0
<snip>
09/17/2018 09:07:44   PowerOn                       0     0     3     15    5
09/17/2018 10:16:26   Reload Command                0     0     0     1     5
09/17/2018 10:59:57   PowerOn                       0     0     0     0     5
```

The following is a sample output from the **show logging onboard switch standby uptime detail** command:

```
Device# show logging onboard switch standby uptime detail

--------------------------------------------------------------------------------
UPTIME SUMMARY INFORMATION
--------------------------------------------------------------------------------
```

```
First customer power on : 06/10/2017 11:51:26
Total uptime           :  0  years  46 weeks  0  days  11 hours  44 minutes
Total downtime         :  0  years  20 weeks  1  days  10 hours  45 minutes
Number of resets       : 79
Number of slot changes  : 13
Current reset reason    : PowerOn
Current reset timestamp : 09/17/2018 10:59:57
Current slot            : 2
Chassis type            : 0
Current uptime         :  0  years  0  weeks  0  days  0  hours  5  minutes
--------------------------------------------------------------------------------

--------------------------------------------------------------------------------
UPTIME CONTINUOUS INFORMATION
--------------------------------------------------------------------------------
Time Stamp          | Reset                        | Uptime
MM/DD/YYYY HH:MM:SS | Reason                       | years weeks days hours minutes
--------------------------------------------------------------------------------
06/10/2017 11:51:26   Reload                         0     0     0     0     0
<snip>
08/10/2018 09:13:58   LocalSoft                      0     0     2     5     4
08/28/2018 14:21:42   Reload Slot Command            0     0     0     3     5
08/28/2018 14:34:29   System requested reload        0     0     0     0     0
09/11/2018 09:08:15   Reload                         0     0     1     8     5
09/11/2018 19:15:06   redundancy force-switchover   0     0     0     9     4
09/13/2018 16:50:18   Reload Command                 0     0     1     21    6
09/17/2018 10:55:09   PowerOn                        0     0     0     0     5
```

The following is a sample output from the **show logging onboard switch active uptime summary** command:

```
Device# show logging onboard switch active uptime summary
--------------------------------------------------------------------------------
UPTIME SUMMARY INFORMATION
--------------------------------------------------------------------------------
First customer power on : 04/26/2018 21:45:39
Total uptime           :  0  years  20 weeks  2  days  12 hours  22 minutes
Total downtime         :  0  years  2  weeks  2  days  8  hours  40 minutes
Number of resets       : 1900
Number of slot changes  : 18
Current reset reason    : Reload Command
Current reset timestamp : 09/26/2018 20:43:15
Current slot            : 1
Chassis type            : 91
Current uptime         :  0  years  0  weeks  5  days  22 hours  5  minutes
--------------------------------------------------------------------------------
```

show mac address-table

To display the MAC address table, use the **show mac address-table** command in privileged EXEC mode.

show mac address-table [{ **address** *mac-addr* [**interface** *type/number* | **vlan** *vlan-id*] | **aging-time** [**routed-mac** | **vlan** *vlan-id*] | **control-packet-learn** | **count** [**summary** | **vlan** *vlan-id*] | [**dynamic** | **secure** | **static**] [**address** *mac-addr*] [**interface** *type/number* | **vlan** *vlan-id*] | **interface** *type/number* | **learning** [**vlan** *vlan-id*] | **multicast** [**count**] [**igmp-snooping** | **mld-snooping** | **user**] [**vlan** *vlan-id*] | **notification** { **change** [**interface** [*type/number*]] | **mac-move** | **threshold** } | **vlan** *vlan-id* }]

Syntax Description

address *mac-addr*	(Optional) Displays information about the MAC address table for a specific MAC address.
interface *type/number*	(Optional) Displays addresses for a specific interface.
vlan *vlan-id*	(Optional) Displays addresses for a specific VLAN.
aging-time [**routed-mac** | **vlan** *vlan-id*]	(Optional) Displays the aging time for the routed MAC or VLAN.
control-packet-learn	(Optional) Displays the controlled packet MAC learning parameters.
count	(Optional) Displays the number of entries that are currently in the MAC address table.
dynamic	(Optional) Displays only the dynamic addresses.
secure	(Optional) Displays only the secure addresses.
static	(Optional) Displays only the static addresses.
learning	(Optional) Displays learnings of a VLAN or interface.
multicast	(Optional) Displays information about the multicast MAC address table entries only.
igmp-snooping	(Optional) Displays the addresses learned by Internet Group Management Protocol (IGMP) snooping.
mld-snooping	(Optional) Displays the addresses learned by Multicast Listener Discover version 2 (MLDv2) snooping.
user	(Optional) Displays the manually entered (static) addresses.
notification change	Displays the MAC notification parameters and history table.
notification mac-move	Displays the MAC-move notification status.
notification threshold	Displays the Counter-Addressable Memory (CAM) table utilization notification status.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.
Cisco IOS XE Gibraltar 16.12.4	The ouput of the **show mac address-table vlan** *vlan-id* command has been updated to show the MAC addresses used for Cisco Software-Defined Access (SD-Access) solution.

Usage Guidelines

The *mac-addr* value is a 48-bit MAC address. The valid format is H.H.H.

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

The following is sample output from the **show mac address-table** command:

```
Device# show mac address-table

          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
 All    0100.0ccc.cccc    STATIC      CPU
 All    0100.0ccc.cccd    STATIC      CPU
 All    0180.c200.0000    STATIC      CPU
 All    0180.c200.0001    STATIC      CPU
 All    0180.c200.0002    STATIC      CPU
 All    0180.c200.0003    STATIC      CPU
 All    0180.c200.0004    STATIC      CPU
 All    0180.c200.0005    STATIC      CPU
 All    0180.c200.0006    STATIC      CPU
 All    0180.c200.0007    STATIC      CPU
 All    0180.c200.0008    STATIC      CPU
 All    0180.c200.0009    STATIC      CPU
 All    0180.c200.000a    STATIC      CPU
 All    0180.c200.000b    STATIC      CPU
 All    0180.c200.000c    STATIC      CPU
 All    0180.c200.000d    STATIC      CPU
 All    0180.c200.000e    STATIC      CPU
 All    0180.c200.000f    STATIC      CPU
 All    0180.c200.0010    STATIC      CPU
 All    0180.c200.0021    STATIC      CPU
 All    ffff.ffff.ffff    STATIC      CPU
   1    780c.f0e1.1dc3    STATIC      Vl1
  51    0000.1111.2222    STATIC      Vl51
  51    780c.f0e1.1dc6    STATIC      Vl51
1021    0000.0c9f.f45c    STATIC      Vl1021
1021    0002.02cc.0002    STATIC      Gi6/0/2
1021    0002.02cc.0003    STATIC      Gi6/0/3
1021    0002.02cc.0004    STATIC      Gi6/0/4
1021    0002.02cc.0005    STATIC      Gi6/0/5
1021    0002.02cc.0006    STATIC      Gi6/0/6
1021    0002.02cc.0007    STATIC      Gi6/0/7
1021    0002.02cc.0008    STATIC      Gi6/0/8
1021    0002.02cc.0009    STATIC      Gi6/0/9
1021    0002.02cc.000a    STATIC      Gi6/0/10
```

```
<output truncated>
```

The following example shows how to display MAC address table information for a specific MAC address:

```
Device# show mac address-table address fc58.9a02.7382

          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    fc58.9a02.7382    DYNAMIC     Te1/0/1
Total Mac Addresses for this criterion: 1
```

The following example shows how to display the currently configured aging time for a specific VLAN:

```
Device# show mac address-table aging-time vlan 1

Global Aging Time:  300
Vlan    Aging Time
----    ----------
   1     300
```

The following example shows how to display the information about the MAC address table for a specific interface:

```
Device# show mac address-table interface TenGigabitEthernet1/0/1

          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
   1    fc58.9a02.7382    DYNAMIC     Te1/0/1
Total Mac Addresses for this criterion: 1
```

The following example shows how to display the MAC-move notification status:

```
Device# show mac address-table notification mac-move

MAC Move Notification: Enabled
```

The following example shows how to display the CAM-table utilization-notification status:

```
Device# show mac address-table notification threshold

    Status       limit        Interval
-------------+-----------+-------------
   enabled         50           120
```

The following example shows how to display the MAC notification parameters and history table for a specific interface:

```
Device# show mac address-table notification change interface tenGigabitEthernet1/0/1

MAC Notification Feature is Disabled on the switch
Interface                      MAC Added Trap MAC Removed Trap
---------                      -------------- ----------------
```

```
TenGigabitEthernet1/0/1        Disabled       Disabled
```

The following example shows how to display the information about the MAC-address table for a specific VLAN:

Note MAC addresses of the type CP_LEARN will be displayed only if Cisco SD-Access solution is used.

```
Device# show mac address-table vlan 1021

          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
1021    0000.0c9f.f45c    STATIC      Vl1021
1021    0002.02cc.0002    STATIC      Gi6/0/2
1021    0002.02cc.0003    STATIC      Gi6/0/3
1021    0002.02cc.0004    STATIC      Gi6/0/4
1021    0002.02cc.0005    STATIC      Gi6/0/5
1021    0002.02cc.0006    STATIC      Gi6/0/6
1021    0002.02cc.0007    STATIC      Gi6/0/7
1021    0002.02cc.0008    STATIC      Gi6/0/8
1021    0002.02cc.0009    STATIC      Gi6/0/9
1021    0002.02cc.000a    STATIC      Gi6/0/10
1021    0002.02cc.000b    STATIC      Gi6/0/11
1021    0002.02cc.000c    STATIC      Gi6/0/12
1021    0002.02cc.000d    STATIC      Gi6/0/13
1021    0002.02cc.000e    STATIC      Gi6/0/14
1021    0002.02cc.000f    STATIC      Gi6/0/15
1021    0002.02cc.0010    STATIC      Gi6/0/16
1021    0002.02cc.0011    STATIC      Gi6/0/17
1021    0002.02cc.0012    STATIC      Gi6/0/18
1021    0002.02cc.0013    STATIC      Gi6/0/19
1021    0002.02cc.0014    STATIC      Gi6/0/20

.
.
.

1021    0002.0100.0001    CP_LEARN    Tu0
1021    0002.0100.0002    CP_LEARN    Tu0
1021    0002.0100.0003    CP_LEARN    Tu0
1021    0002.0100.0004    CP_LEARN    Tu0
1021    0002.0100.0005    CP_LEARN    Tu0
1021    0002.0100.0006    CP_LEARN    Tu0
1021    0002.0100.0007    CP_LEARN    Tu0
1021    0002.0100.0008    CP_LEARN    Tu0
1021    0002.0100.0009    CP_LEARN    Tu0
1021    0002.0100.000a    CP_LEARN    Tu0
Total Mac Addresses for this criterion: 114
```

The table below describes the significant fields shown in the **show mac address-table** display.

Table 9: show mac address-table Field Descriptions

Field	Description
VLAN	VLAN number.
Mac Address	MAC address of the entry.
Type	Type of address.
Ports	Port type.
Total MAC addresses	Total MAC addresses in the MAC address table.

Related Commands

Command	Description
clear mac address-table	Deletes dynamic entries from the MAC address table.

show mac address-table move update

To display the MAC address-table move update information on the device, use the **show mac address-table move update** command in EXEC mode.

show mac address-table move update

Syntax Description

This command has no arguments or keywords.

Command Default

No default behavior or values.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Mo
Cisco IOS XE Fuji 16.9.2	Th

Example

This example shows the output from the **show mac address-table move update** command:

```
Device# show mac address-table move update

Switch-ID : 010b.4630.1780
Dst mac-address : 0180.c200.0010
Vlans/Macs supported : 1023/8320
Default/Current settings: Rcv Off/On, Xmt Off/On
Max packets per min : Rcv 40, Xmt 60
Rcv packet count : 10
Rcv conforming packet count : 5
Rcv invalid packet count : 0
Rcv packet count this min : 0
Rcv threshold exceed count : 0
Rcv last sequence# this min : 0
Rcv last interface : Po2
Rcv last src-mac-address : 0003.fd6a.8701
Rcv last switch-ID : 0303.fd63.7600
Xmt packet count : 0
Xmt packet count this min : 0
Xmt threshold exceed count : 0
Xmt pak buf unavail cnt : 0
Xmt last interface : None
```

show parser encrypt file status

To view the private configuration encryption status, use the **show parser encrypt file status** command.

show parser encrypt file status

Syntax Description

This command has no arguments or keywords.

Command Default

None

Command Modes

User EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Examples

The following command output indicates that the feature is available and the file is encrypted. The file is in ‘cipher text’ format.

```
Device> enable
Device# show parser encrypt file status
Feature:            Enabled
File Format:        Cipher text
Encryption Version: ver1
```

Related Commands

Command	Description
service private-config-encryption	Enables private configuration file encryption.

show platform integrity

To display checksum record for the boot stages , use the **show platform integrity** command in privileged EXEC mode.

show platform integrity [**sign** [**nonce** <*nonce*>]]

Syntax Description

sign	(Optional) Show signature
nonce	(Optional) Enter a nonce value

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
	This command was introduced.

Examples

This example shows how to view the checksum record for boot stages :

```
Device# show platform integrity sign

PCR0: EE47F8644C2887D9BD4DE3E468DD27EB93F4A606006A0B7006E2928C50C7C9AB
PCR8: E7B61EC32AFA43DA1FF4D77F108CA266848B32924834F5E41A9F6893A9CB7A38
Signature version: 1
Signature:
816C5A29741BBAC1961C109FFC36DA5459A44DBF211025F539AFB4868EF91834C05789
5DAFBC7474F301916B7D0D08ABE5E05E66598426A73E921024C21504383228B6787B74
8526A305B17DAD3CF8705BACFD51A2D55A333415CABC73DAFDEEFD8777AA77F482EC4B
731A09826A41FB3EFFC46DC02FBA666534DBEC7DCC0C029298DB8462A70DBA26833C2A
1472D1F08D721BA941CB94A418E43803699174572A5759445B3564D8EAEE57D64AE304
EE1D2A9C53E93E05B24A92387E261199CED8D8A0CE7134596FF8D2D6E6DA773757C70C
D3BA91C43A591268C248DF32658999276FB972153ABE823F0ACFE9F3B6F0AD1A00E257
4A4CC41C954015A59FB8FE
Platform: WS-C3650-12X48UZ
```

show platform software audit

To display the SE Linux Audit logs, use the **show platform software audit** command in privileged EXEC mode.

show platform software audit {**all** | **summary** | [**switch** {*switch-number* | **active** | **standby**}] {**0** | **F0** | **R0** | {**FP** | **RP**} {**active**}}}

Syntax Description

all	Shows the audit log from all the slots.
summary	Shows the audit log summary count from all the slots.
switch	Shows the audit logs for a slot on a specific switch.
switch-number	Selects the switch with the specified switch number.
switch active	Selects the active instance of the switch.
standby	Selects the standby instance of the switch.
0	Shows the audit log for the SPA-Inter-Processor slot 0.
F0	Shows the audit log for the Embedded-Service-Processor slot 0.
R0	Shows the audit log for the Route-Processor slot 0.
FP active	Shows the audit log for the active Embedded-Service-Processor slot.
RP active	Shows the audit log for the active Route-Processor slot.

Command Modes

Privileged EXEC (#)

Command History

Usage Guidelines

This command was introduced in the Cisco IOS XE Gibraltar 16.10.1 as a part of the SELinux Permissive Mode feature. The **show platform software audit** command displays the system logs containing the access violation events.

In Cisco IOS XE Gibraltar 16.10.1, operation in a permissive mode is available - with the intent of confining specific components (process or application) of the IOS-XE platform. In the permissive mode, access violation events are detected and system logs are generated, but the event or operation itself is not blocked. The solution operates mainly in an access violation detection mode.

The following is a sample output of the **show software platform software audit summary** command:

```
Device# show platform software audit summary

===================================
AUDIT LOG ON switch 1
-----------------------------------
```

```
AVC Denial count: 58
===================================
```

The following is a sample output of the **show software platform software audit all** command:

```
Device# show platform software audit all

===================================
AUDIT LOG ON switch 1
-----------------------------------
========== START ============
type=AVC msg=audit(1539222292.584:100): avc:  denied  { read } for  pid=14017
comm="mcp_trace_filte" name="crashinfo" dev="rootfs" ino=13667
scontext=system_u:system_r:polaris_trace_filter_t:s0
tcontext=system_u:object_r:polaris_disk_crashinfo_t:s0 tclass=lnk_file permissive=1
type=AVC msg=audit(1539222292.584:100): avc:  denied  { getattr } for  pid=14017
comm="mcp_trace_filte" path="/mnt/sd1" dev="sda1" ino=2
scontext=system_u:system_r:polaris_trace_filter_t:s0
tcontext=system_u:object_r:polaris_disk_crashinfo_t:s0 tclass=dir permissive=1
type=AVC msg=audit(1539222292.586:101): avc:  denied  { getattr } for  pid=14028 comm="ls"
 path="/tmp/ufs/crashinfo" dev="tmpfs" ino=58407
scontext=system_u:system_r:polaris_trace_filter_t:s0
tcontext=system_u:object_r:polaris_ncd_tmp_t:s0 tclass=dir permissive=1
type=AVC msg=audit(1539222292.586:102): avc:  denied  { read } for  pid=14028 comm="ls"
name="crashinfo" dev="tmpfs" ino=58407 scontext=system_u:system_r:polaris_trace_filter_t:s0
 tcontext=system_u:object_r:polaris_ncd_tmp_t:s0 tclass=dir permissive=1
type=AVC msg=audit(1539438600.896:119): avc:  denied  { execute } for  pid=8300 comm="sh"
name="id" dev="loop0" ino=6982 scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
 tcontext=system_u:object_r:bin_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438600.897:120): avc:  denied  { execute_no_trans } for  pid=8300
comm="sh"
path="/tmp/sw/mount/cat9k-rpbase.2018-10-02_00.13_mhungund.SSA.pkg/nyquist/usr/bin/id"
dev="loop0" ino=6982 scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:bin_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438615.535:121): avc:  denied  { name_connect } for  pid=26421
comm="nginx" dest=8098 scontext=system_u:system_r:polaris_nginx_t:s0
tcontext=system_u:object_r:polaris_caf_api_port_t:s0 tclass=tcp_socket permissive=1
type=AVC msg=audit(1539438624.916:122): avc:  denied  { execute_no_trans } for  pid=8600
comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438648.936:123): avc:  denied  { execute_no_trans } for  pid=9307
comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438678.649:124): avc:  denied  { name_connect } for  pid=26421
comm="nginx" dest=8098 scontext=system_u:system_r:polaris_nginx_t:s0
tcontext=system_u:object_r:polaris_caf_api_port_t:s0 tclass=tcp_socket permissive=1
type=AVC msg=audit(1539438696.969:125): avc:  denied  { execute_no_trans } for  pid=10057
comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438732.973:126): avc:  denied  { execute_no_trans } for  pid=10858
comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438778.008:127): avc:  denied  { execute_no_trans } for  pid=11579
comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438800.156:128): avc:  denied  { name_connect } for  pid=26421
comm="nginx" dest=8098 scontext=system_u:system_r:polaris_nginx_t:s0
tcontext=system_u:object_r:polaris_caf_api_port_t:s0 tclass=tcp_socket permissive=1
type=AVC msg=audit(1539438834.099:129): avc:  denied  { execute_no_trans } for  pid=12451
comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
```

```
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539440246.697:149): avc:  denied  { name_connect } for  pid=26421
comm="nginx" dest=8098 scontext=system_u:system_r:polaris_nginx_t:s0
tcontext=system_u:object_r:polaris_caf_api_port_t:s0 tclass=tcp_socket permissive=1
type=AVC msg=audit(1539440299.119:150): avc:  denied  { name_connect } for  pid=26421
comm="nginx" dest=8098 scontext=system_u:system_r:polaris_nginx_t:s0
tcontext=system_u:object_r:polaris_caf_api_port_t:s0 tclass=tcp_socket permissive=1
========== END ============
===================================
```

The following is a sample output of the **show software platform software audit switch** command:

```
Device# show platform software audit switch active R0

========== START ============
type=AVC msg=audit(1539222292.584:100): avc:  denied  { read } for  pid=14017
comm="mcp_trace_filte" name="crashinfo" dev="rootfs" ino=13667
scontext=system_u:system_r:polaris_trace_filter_t:s0
tcontext=system_u:object_r:polaris_disk_crashinfo_t:s0 tclass=lnk_file permissive=1
type=AVC msg=audit(1539222292.584:100): avc:  denied  { getattr } for  pid=14017
comm="mcp_trace_filte" path="/mnt/sd1" dev="sda1" ino=2
scontext=system_u:system_r:polaris_trace_filter_t:s0
tcontext=system_u:object_r:polaris_disk_crashinfo_t:s0 tclass=dir permissive=1
type=AVC msg=audit(1539222292.586:101): avc:  denied  { getattr } for  pid=14028 comm="ls"
 path="/tmp/ufs/crashinfo" dev="tmpfs" ino=58407
scontext=system_u:system_r:polaris_trace_filter_t:s0
tcontext=system_u:object_r:polaris_ncd_tmp_t:s0 tclass=dir permissive=1
type=AVC msg=audit(1539222292.586:102): avc:  denied  { read } for  pid=14028 comm="ls"
name="crashinfo" dev="tmpfs" ino=58407 scontext=system_u:system_r:polaris_trace_filter_t:s0
 tcontext=system_u:object_r:polaris_ncd_tmp_t:s0 tclass=dir permissive=1
type=AVC msg=audit(1539438624.916:122): avc:  denied  { execute_no_trans } for  pid=8600
comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438648.936:123): avc:  denied  { execute_no_trans } for  pid=9307
comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438678.649:124): avc:  denied  { name_connect } for  pid=26421
comm="nginx" dest=8098 scontext=system_u:system_r:polaris_nginx_t:s0
tcontext=system_u:object_r:polaris_caf_api_port_t:s0 tclass=tcp_socket permissive=1
type=AVC msg=audit(1539438696.969:125): avc:  denied  { execute_no_trans } for  pid=10057
comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438732.973:126): avc:  denied  { execute_no_trans } for  pid=10858
comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438778.008:127): avc:  denied  { execute_no_trans } for  pid=11579
comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438800.156:128): avc:  denied  { name_connect } for  pid=26421
comm="nginx" dest=8098 scontext=system_u:system_r:polaris_nginx_t:s0
tcontext=system_u:object_r:polaris_caf_api_port_t:s0 tclass=tcp_socket permissive=1
type=AVC msg=audit(1539438834.099:129): avc:  denied  { execute_no_trans } for  pid=12451
comm="auto_upgrade_se" path="/bin/bash" dev="rootfs" ino=7276
scontext=system_u:system_r:polaris_auto_upgrade_server_rp_t:s0
tcontext=system_u:object_r:shell_exec_t:s0 tclass=file permissive=1
type=AVC msg=audit(1539438860.907:130): avc:  denied  { name_connect } for  pid=26421
comm="nginx" dest=8098 scontext=system_u:system_r:polaris_nginx_t:s0
tcontext=system_u:object_r:polaris_caf_api_port_t:s0 tclass=tcp_socket permissive=1
```

```
========== END ============
===================================
```

show platform software fed switch punt cause

To display information about why the packets received on an interface are punted to the Router Processor (RP), use the **show platform software fed switch punt cpuq cause** command in privileged EXEC mode.

show platform software fed switch {*switch-number* | **active** | **standby**} **punt**{*cause_id* | **clear** | **summary**}

Syntax Description

switch {*switch-number* | **active** | **standby**}	Displays information about the switch. You have the following options: • *switch-number.* • **active** —Displays information relating to the active switch. • **standby**—Displays information relating to the standby switch, if available. **Note** This keyword is not supported.
cause_id	Specifies the ID of the cause for which the details have to be displayed.
clear	Clears the statistics for all the causes. Clearing the causes might result in inconsistent statistics.
summary	Displays a high-level overview of the punt reason.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Usage Guidelines

None

Example

The following is sample output from the **show platform software fed switch active punt cause summary** command.

```
Device# show platform software fed switch active punt cause summary
Statistics for all causes

Cause  Cause Info                      Rcvd                Dropped
------------------------------------------------------------------------------
7      ARP request or response         1                   0
21     RP<->QFP keepalive              22314               0
55     For-us control                  12                  0
60     IP subnet or broadcast packet   21                  0
96     Layer2 control protocols        133808              0
```

```
------------------------------------------------------------------------------
```

The following is sample output from the **show platform software fed switch active punt cause** *cause-id* command.

```
Device# show platform software fed switch active punt cause 21
Detailed Statistics

Sub Cause       Rcvd                 Dropped
--------------------------------------------
0               22363                0

--------------------------------------------
```

show platform software fed switch punt cpuq

To display information about the punt traffic on CPU queues, use the **show platform software fed switch punt cpuq** command in privileged EXEC mode.

show platform software fed switch {*switch-number* | **active** | **standby**} **punt cpuq** {*cpuq_id* | **all** | **brief** | **clear** | **rates**}

Syntax Description

switch {*switch-number* **active standby**}	Displays information about the switch. You have the following options: • *switch-number.* • **active** —Displays information relating to the active switch. • **standby**—Displays information relating to the standby switch, if available. **Note** This keyword is not supported.
punt	Displays the punt informtion.
cpuq	Displays information about the CPU receive queue.
cpuq_id	Specifies details specific to a particular CPU queue.
all	Displays the statistics for all the CPU queues.
brief	Displays summarized statistics for all the queues like details about punt packets received and dropped.
clear	Clears the statistics for all the CPU queues. Clearing the CPU queue might result in inconsistent statistics.
rates	Displays the rate at which the packets are punted.

Command Default

None

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Usage Guidelines

None

Example

The following is sample output from the **show platform software fed switch active punt cpuq brief** command.

```
Device#show platform software fed switch active punt cpuq brief

Punt CPU Q Statistics Brief
======================================================================================
 Q  |         Queue            |  Rx    |  Rx   |  Rx    |  Drop  |  Drop   |  Drop
 no |         Name             |  prev  |  cur  |  delta |  prev  |  cur    |  delta
======================================================================================
 0  CPU_Q_DOT1X_AUTH                0        0        0        0        0        0
 1  CPU_Q_L2_CONTROL                0        6772     6772     0        0        0
 2  CPU_Q_FORUS_TRAFFIC             0        0        0        0        0        0
 3  CPU_Q_ICMP_GEN                  0        0        0        0        0        0
 4  CPU_Q_ROUTING_CONTROL           0        12       12       0        0        0
 5  CPU_Q_FORUS_ADDR_RESOLUTION     0        1        1        0        0        0
 6  CPU_Q_ICMP_REDIRECT             0        0        0        0        0        0
 7  CPU_Q_INTER_FED_TRAFFIC         0        0        0        0        0        0
 8  CPU_Q_L2LVX_CONTROL_PKT         0        0        0        0        0        0
 9  CPU_Q_EWLC_CONTROL              0        0        0        0        0        0
 10 CPU_Q_EWLC_DATA                 0        0        0        0        0        0
 11 CPU_Q_L2LVX_DATA_PKT            0        0        0        0        0        0
 12 CPU_Q_BROADCAST                 0        21       21       0        0        0
 13 CPU_Q_LEARNING_CACHE_OVFL       0        0        0        0        0        0
 14 CPU_Q_SW_FORWARDING             0        0        0        0        0        0
 15 CPU_Q_TOPOLOGY_CONTROL          0        127300   127300   0        0        0
 16 CPU_Q_PROTO_SNOOPING            0        0        0        0        0        0
 17 CPU_Q_BFD_LOW_LATENCY           0        0        0        0        0        0
 18 CPU_Q_TRANSIT_TRAFFIC           0        0        0        0        0        0
 19 CPU_Q_RPF_FAILED                0        0        0        0        0        0
 20 CPU_Q_MCAST_END_STATION_SERVICE 0        0        0        0        0        0
 21 CPU_Q_LOGGING                   0        0        0        0        0        0
 22 CPU_Q_PUNT_WEBAUTH              0        0        0        0        0        0
 23 CPU_Q_HIGH_RATE_APP             0        0        0        0        0        0
 24 CPU_Q_EXCEPTION                 0        0        0        0        0        0
 25 CPU_Q_SYSTEM_CRITICAL           0        0        0        0        0        0
 26 CPU_Q_NFL_SAMPLED_DATA          0        0        0        0        0        0
 27 CPU_Q_LOW_LATENCY               0        0        0        0        0        0
 28 CPU_Q_EGR_EXCEPTION             0        0        0        0        0        0
 29 CPU_Q_FSS                       0        0        0        0        0        0
 30 CPU_Q_MCAST_DATA                0        0        0        0        0        0
 31 CPU_Q_GOLD_PKT                  0        0        0        0        0        0

-------------------------------------------------------------------------------------
```

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

*Table 10: **show platform software fed switch active punt cpuq brief** Field Descriptions*

Field	Description
Q no	ID of the queue.
Queue Name	Name of the queue.
Rx	Number of packets received.

Field	Description
Drop	Number of packets dropped.

The following is sample output from the **show platform software fed switch active punt cpuq cpuq_id** command.

```
Device#show platform software fed switch active punt cpuq 1

Punt CPU Q Statistics
===========================================

CPU Q Id                       : 1
CPU Q Name                     : CPU_Q_L2_CONTROL
Packets received from ASIC     : 6774
Send to IOSd total attempts    : 6774
Send to IOSd failed count      : 0
RX suspend count               : 0
RX unsuspend count             : 0
RX unsuspend send count        : 0
RX unsuspend send failed count : 0
RX consumed count              : 0
RX dropped count               : 0
RX non-active dropped count    : 0
RX conversion failure dropped  : 0
RX INTACK count                : 6761
RX packets dq'd after intack   : 0
Active RxQ event               : 6761
RX spurious interrupt          : 0

Replenish Stats for all rxq:
-------------------------------------------
Number of replenish            : 61969
Number of replenish suspend    : 0
Number of replenish un-suspend : 0
-------------------------------------------
```

show platform software sl-infra

To display troubleshooting information and for debugging, enter the **show platform software sl-infra** command in privileged EXEC mode. The output of this command is used by the technical support team, for troubleshooting and debugging.

show platform software sl-infra { **all** | **current** | **debug** | **stored** }

Syntax Description

all	Displays current, debugging, and stored information.
current	Displays current license-related information.
debug	Enables debugging
stored	Displays information that is stored on the product instance.

Command Modes

Privileged EXEC (Device#)

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.3.2a	This command was introduced.

Usage Guidelines

When you encounter an error message that you are not able to resolve, along with a copy of the message that appears on the console or in the system log, provide your Cisco technical support representative with sample output of these commands: **show license tech support**, **show license history message**, and the **show platform software sl-infra all** privileged EXEC commands.

show platform sudi certificate

To display checksum record for the specific SUDI, use the **show platform sudi certificate** command in privileged EXEC mode.

show platform sudi certificate [**sign** [**nonce** *<nonce>*]]

Syntax Description

sign	(Optional) Show signature
nonce	(Optional) Enter a nonce value

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
	This command was introduced.

Examples

This example shows how to view the checksum record for a specific SUDI :

```
# show platform sudi certificate

-----BEGIN CERTIFICATE-----
MIIDQzCCAiugAwIBAgIQX/h7KCtU3I1CoxW1aMmt/zANBgkqhkiG9w0BAQUFADA1
MRYwFAYDVQQKEw1DaXNjbyBTeXN0ZW1zMRswGQYDVQQDExJDaXNjbyBSb290IENB
IDIwNDgwHhcNMDQwNTE0MjAxNzEyWhcNMjkwNTE0MjAyNTQyWjA1MRYwFAYDVQQK
Ew1DaXNjbyBTeXN0ZW1zMRswGQYDVQQDExJDaXNjbyBSb290IENBIDIwNDgwggEg
MA0GCSqGSIb3DQEBAQUAA4IBDQAwggEIAoIBAQCwmrmrp68Kd6ficba0ZmKUeIhH
xmJVhEAyv8CrLqUccda8bnuoqrpu0hWISEWdovyD0My5jOAmaHBKeN8hF570YQXJ
FcjPFto1YYmUQ6iEqDGYeJu5Tm8sUxJszR2tKyS7McQr/4NEb7Y9JHcJ6r8qqB9q
VvYgDxFUl4F1pyXOWWqCZe+36ufijXWLbvLdT6ZeYpzPEApk0E5tzivMW/VgpSdH
jWn0f84bcN5wGyDWbs2mAag8EtKpP6BrXruOIIt6keO1aO6g58QBdKhTCytKmg9l
Eg6CTY5j/e/rmxrbU6YTYK/CfdfHbBcl1HP7R2RQgYCUTOG/rksc35LtLgXfAgED
o1EwTzALBgNVHQ8EBAMCAYYwDwYDVR0TAQH/BAUwAwEB/zAdBgNVHQ4EFgQUJ/PI
FR5umgIJFq0roIlgX9p7L6owEAYJKwYBBAGCNxUBBAMCAQAwDQYJKoZIhvcNAQEF
BQADggEBAJ2dhISjQal8dwy3U8pORFBi71R803UXHOjgxkhLtv5MOhmBVrBW7hmW
Yqpao2TB9k5UM8Z3/sUcuuVdJcr18JOagxEu5sv4dEX+5wW4q+ffy0vhN4TauYuX
cB7w4ovXsNgOnbFp1iqRe6lJT37mjpXYgyc81WhJDtSd9i7rp77rMKSsH0T8lasz
Bvt9YAretIpjsJyp8qS5UwGH0GikJ3+r/+n6yUA4iGe0OcaEb1fJU9u6ju7AQ7L4
CYNu/2bPPu8Xs1gYJQk0XuPL1hS27PKSb3TkL4Eq1ZKR4OCXPDJoBYVL0fdX4lId
kxpUnwVwwEpxYB5DC2Ae/qPOgRnhCzU=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIEPDCCAySgAwIBAgIKYQlufQAAAAAADDANBgkqhkiG9w0BAQUFADA1MRYwFAYD
VQQKEw1DaXNjbyBTeXN0ZW1zMRswGQYDVQQDExJDaXNjbyBSb290IENBIDIwNDgw
HhcNMTEwNjMwMTc1NjU3WhcNMjkwNTE0MjAyNTQyWjAnMQ4wDAYDVQQKEwVDaXNj
bzEVMBMGA1UEAxMMQUNUMiBTVURJIENBMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
MIIBCgKCAQEA0m5l3THIxA9tN/hS5qR/6UZRpdd+9aE2JbFkNjht6gfHKd477AkS
5XAtUs5oxDYVt/zEbslZq3+LR6qrqKKQVu6JYvH05UYLBqCj38s76NLk53905Wzp
9pRcmRCPuX+a6tHF/qRuOiJ44mdeDYZo3qPCpxzprWJDPclM4iYKHumMQMqmgmg+
xghHIooWS80BOcdiynEbeP5rZ7qRuewKMpl1TiI3WdBNjZjnpfjg66F+P4SaDkGb
BXdGj13oVeF+EyFWLrFjj97fL2+8oauV43Qrvnf3d/GfqXj7ew+z/sXlXtEOjSXJ
URsyMEj53Rdd9tJwHky8neapszS+r+kdVQIDAQABo4IBWjCCAVYwCwYDVR0PBAQD
AgHGMB0GA1UdDgQWBBRI2PHxwnDVW7t8cwmTr7i4MAP4fzAfBgNVHSMEGDAWgBQn
88gVHm6aAgkWrSugiWBf2nsvqjBDBgNVHR8EPDA6MDigNqA0hjJodHRwOi8vd3d3
LmNpc2NvLmNvbS9zZWN1cml0eS9wa2kvY3JsL2NyY2EyMDQ4LmNybDBQBggrBgEF
```

```
BQcBAQREMEIwQAYIKwYBBQUHMAKGNGh0dHA6Ly93d3cuY2lzY28uY29tL3NlY3Vy
aXR5L3BraS9jZXJ0cy9jcmNhMjA0OC5jZXIwXAYDVR0gBFUwUzBRBgorBgEEAQkV
AQwAMEMwQQYIKwYBBQUHAgEWNWh0dHA6Ly93d3cuY2lzY28uY29tL3NlY3VyaXR5
L3BraS9wb2xpY2llcy9pbmRleC5odG1sMBIGA1UdEwEB/wQIMAYBAf8CAQAwDQYJ
KoZIhvcNAQEFBQADggEBAGh1qclr9tx4hzWgDERm371yeuEmqcIfi9b9+GbMSJbi
ZHc/CcCl0lJu0a9zTXA9w47H9/t6leduGxb4WeLxcwCiUgvFtCa51Iklt8nNbcKY
/4dw1ex+7amATUQO4QggIE67wVIPu6bgAE3Ja/nRS3xKYSnj8H5TehimBSv6TECi
i5jUhOWryAK4dVo8hCjkjEkzu3ufBTJapnv89g9OE+H3VKM4L+/KdkUO+52djFKn
hyl47d7cZR4DY4LIuFM2P1As8YyjzoNpK/urSRI14WdIlplR1nH7KNDl5618yfVP
0IFJZBGrooCRBjOSwFv8cpWCbmWdPaCQT2nwIjTfY8c=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIDhjCCAm6gAwIBAgIDctWkMA0GCSqGSIb3DQEBCwUAMCcxDjAMBgNVBAoTBUNp
c2NvMRUwEwYDVQQDEwxBQ1QyIFNVREkgQ0EwHhcNMTUwODA2MDgwODI5WhcNMjUw
ODA2MDgwODI5WjBzMSwwKgYDVQQFEyNQSUQ6V1MtQzM2NTAtMTJYNDhVWiBTTjpG
RE8xOTMyWDAwQzEOMAwGA1UEChMFQ2lzY28xGDAWBgNVBAsTD0FDVC0yIExpdGUg
U1VESTEZMBcGA1UEAxMQV1MtQzM2NTAtMTJYNDhVWjCCASIwDQYJKoZIhvcNAQEB
BQADggEPADCCAQoCggEBANZxOGYI0eUl4HcSwjL4HO75qTjl9C2BHG3ufce9ikkN
xwGXi8qg8vKxuB9tRYRaJC5bP1WMoq7+ZJtQA079xE4X14soNbkq5NaUhh7RB1wD
iRUJvTfCOzVICbNfbzvtB30I75tCarFNmpd0K6AFrIa41U988QGqaCj7R1JrYNaj
nC73UXXM/hC0HtNR5mhyqer5Y2qjjzo6tHZYqrrx2eS1XOa262ZSQriAxmaH/KLC
K97ywyRBdJlxBRX3hGtKlog8nASB8WpXqB9NVCERzUajwU3L/kg2BsCqw9Y2m7HW
U1cerTxgthuyUkdNI+Jg6iGApm2+s8E9hsHPBPMCdIsCAwEAAaNvMG0wDgYDVR0P
AQH/BAQDAgXgMAwGA1UdEwEB/wQCMAAwTQYDVR0RBEYwRKBCBgkrBgEEAQkVAgOg
NRMzQ2hpcElEPVVZSk5ORmRRRlFvN1ZIVmxJRTlqZENBeU9DQXhPRG93TlRveE1T
QVg5eWc9MA0GCSqGSIb3DQEBCwUAA4IBAQBKicTRZbVCRjVIR5MQcWXUT086v6Ej
HahDHTts3YpQoyAVfioNg2x8J6EXcEau4voyVu+eMUuoNL4szPhmmDcULfiCGBcA
/R3EFuoVMIzNT0geziytsCf728KGw1oGuosgVjNGOOahUELu4+F/My7bIJNbH+PD
KjIFmhJpJg0F3q17yClAeXvd13g3W393i35d00Lm5L1WbBfQtyBaOLAbxsHvutrX
u1VZ5sdqSTwTkkO9vKMaQjh7a8J/AmJi93jvzM69pe5711P1zqZfYfpiJ3cyJ0xf
I4brQ1smdczloFD4asF7A+1vor5e4VDBP0ppmeFAJvCQ52JTpj0M0o1D
-----END CERTIFICATE-----
```

show running-config

To display the contents of the current running configuration file or the configuration for a specific module, Layer 2 VLAN, class map, interface, map class, policy map, or virtual circuit (VC) class, use the **show running-config** command in privileged EXEC mode.

show running-config [*options*]

Syntax Description

options	(Optional) Keywords used to customize output. You can enter more than one keyword. • **aaa** [**accounting** | **attribute** | **authentication** | **authorization** | **diameter** | **group** | **ldap** | **miscellaneous** | **radius-server** | **server** | **tacacs-server** | **user-name** | **username**]: Displays AAA configurations. • **all**: Expands the output to include the commands that are configured with default parameters. If the **all** keyword is not used, the output does not display commands configured with default parameters. • **bridge-domain** {**id** | **parameterized vlan**}: Displays the running configuration for bridge domains. • **brief**: Displays the configuration without certification data and encrypted filter details. • **class-map** [*name*] [**linenum**]: Displays class map information. • **cts** [**interface** | **policy-server** | **rbm-rbac** | **server** | **sxp**] : Displays Cisco TrustSec configurations. • **deprecated**: Displays deprecated configuration along with the running configuration. • **eap** {**method** | **profiles**}: Displays EAP method configurations and profiles. • **flow** {**exporter** | **monitor** | **record**}: Displays global flow configuration commands. • **full**: Displays the full configuration. • **identity** {**policy** | **profile**}: Displays identity profile or policy information.

- **interface** *type number*: Displays interface-specific configuration information. If you use the **interface** keyword, you must specify the interface type and the interface number (for example, **interface GigabitEthernet 1/0/1**). Use the **show run interface ?** command to determine the interfaces available on your system.
- **ip dhcp pool** [*name*]: Displays IPv4 DHCP pool configuration.
- **ipv6 dhcp pool** [*name*]: Displays IPv6 DHCP pool configuration.
- **linenum** [**brief** | **full** | **partition**]: Displays line numbers in the output.
- **map-class** [**atm** | **dialer** | **frame-relay**] [*name*]: Displays map class information.
- **mdns-sd** [**gateway** | **location-group** | **service-definition** | **service-list** | **service-peer** | **service-policy**]: Displays Multicast DNS Service Discovery (mDNS-SD) configurations.
- **partition** {**access-list** | **class-map** | **common** | **global-cdp** | **interface** | **ip-as-path** | **ip-community** | **ip-prefix-list** | **ip-static-routes** | **line** | **policy-map** | **route-map** | **router** | **snmp** | **tacacs**}: Displays the configuration corresponding to a partition.
- **policy-map** [*name*] [**linenum**]: Displays policy map information.
- **switch** *number*: Displays configuration for the specified switch.
- **view** [**full**]: Enables the display of a full running configuration. This is for view-based users who typically can only view the configuration commands that they are entitled to access for that particular view.
- **vlan** [*vlan-id*]: Displays the specific VLAN information; valid values are from 1 to 4094.
- **vrf** [*vrf-name*]: Displays the Virtual routing and forwarding (VRF)-aware configuration module number .

Command Default

The default syntax, **show running-config**, displays the contents of the running configuration file, except commands configured using the default parameters.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

The **show running-config** command is technically a command alias (substitute or replacement syntax) of the **more system:running-config** command. Although the use of more commands is recommended (because of their uniform structure across platforms and their expandable syntax), the **show running-config** command remains enabled to accommodate its widespread use, and to allow typing shortcuts such as **show run**.

The **show running-config interface** command is useful when there are multiple interfaces and you want to look at the configuration of a specific interface.

The **linenum** keyword causes line numbers to be displayed in the output. This option is useful for identifying a particular portion of a very large configuration.

You can enter additional output modifiers in the command syntax by including a pipe character (|) after the optional keyword. For example, **show running-config interface GigabitEthernet 1/0/1 linenum | begin 3**.

To display the output modifiers that are available for a keyword, enter **| ?** after the keyword. Depending on the platform you are using, the keywords and the arguments for the *options* argument may vary.

The **show running-config all** command displays complete configuration information, including the default settings and values. For example, if the Cisco Discovery Protocol (abbreviated as CDP in the output) hold-time value is set to its default of 180:

- The **show running-config** command does not display this value.
- The **show running-config all** displays the following output: cdp holdtime 180.

If the Cisco Discovery Protocol holdtime is changed to a nondefault value (for example, 100), the output of the **show running-config** and **show running-config all** commands is the same; that is, the configured parameter is displayed.

The **show running-config** command displays ACL information. To exclude ACL information from the output, use the **show running | section exclude ip access | access list** command.

Examples

The following example shows the configuration for GigabitEthernet0/0 interface. The fields are self-explanatory.

```
Device# show running-config interface gigabitEthernet0/0

Building configuration...

Current configuration : 130 bytes
!
interface GigabitEthernet0/0
 vrf forwarding Mgmt-vrf
 ip address 10.5.20.10 255.255.0.0
 negotiation auto
 ntp broadcast
end
```

The following example shows how to set line numbers in the command output and then use the output modifier to start the display at line 10. The fields are self-explanatory.

```
Device# show running-config linenum | begin 10

   10 : boot-start-marker
   11 : boot-end-marker
   12 : !
   13 : no logging buffered
   14 : enable password #####
   15 : !
   16 : spe 1/0 1/7
   17 :  firmware location bootflash:mica-modem-pw.10.16.0.0.bin
   18 : !
   19 : !
   20 : resource-pool disable
   21 : !
   22 : no aaa new-model
   23 : ip subnet-zero
   24 : ip domain name cisco.com
   25 : ip name-server 172.16.11.48
   26 : ip name-server 172.16.2.133
   27 : !
   28 : !
   29 : isdn switch-type primary-5ess
   30 : !
   .
```

```
.
.
126 : end
```

In the following sample output from the **show running-config** command, the **shape average** command indicates that the traffic shaping overhead accounting for ATM is enabled. The BRAS-DSLAM encapsulation type is qinq and the subscriber line encapsulation type is snap-rbe based on the ATM adaptation layer 5 (AAL5) service. The fields are self-explanatory.

```
Device# show running-config
.
.
.
subscriber policy recording rules limit 64
no mpls traffic-eng auto-bw timers frequency 0
call rsvp-sync
!
controller T1 2/0
framing sf
linecode ami
!
controller T1 2/1
framing sf
linecode ami
!
!
policy-map unit-test
class class-default
shape average percent 10 account qinq aal5 snap-rbe
!
```

The following is sample output from the **show running-config class-map** command. The fields in the display are self-explanatory.

```
Device# show running-config class-map

Building configuration...

Current configuration : 2157 bytes
!
class-map match-any system-cpp-police-ewlc-control
  description EWLC Control
class-map match-any system-cpp-police-topology-control
  description Topology control
class-map match-any system-cpp-police-sw-forward
  description Sw forwarding, L2 LVX data packets, LOGGING, Transit Traffic
class-map match-any system-cpp-default
  description EWLC Data, Inter FED Traffic
class-map match-any system-cpp-police-sys-data
  description Openflow, Exception, EGR Exception, NFL Sampled Data, RPF Failed
class-map match-any system-cpp-police-punt-webauth
  description Punt Webauth
class-map match-any system-cpp-police-l2lvx-control
  description L2 LVX control packets
class-map match-any system-cpp-police-forus
  description Forus Address resolution and Forus traffic
class-map match-any system-cpp-police-multicast-end-station
  description MCAST END STATION
class-map match-any system-cpp-police-high-rate-app
  description High Rate Applications
class-map match-any system-cpp-police-multicast
  description MCAST Data
class-map match-any system-cpp-police-l2-control
  description L2 control
```

```
class-map match-any system-cpp-police-dot1x-auth
  description DOT1X Auth
class-map match-any system-cpp-police-data
  description ICMP redirect, ICMP_GEN and BROADCAST
class-map match-any system-cpp-police-stackwise-virt-control
  description Stackwise Virtual OOB
...
```

The following example shows that the teletype (tty) line 2 is reserved for communicating with the second core:

```
Device# show running

Building configuration...

Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname device
!
enable password lab
!
no ip subnet-zero
!
!
!
interface Ethernet0
 ip address 10.25.213.150 255.255.255.128
 no ip directed-broadcast
 no logging event link-status
!
interface Serial0
 no ip address
 no ip directed-broadcast
 no ip mroute-cache
 shutdown
 no fair-queue
!
interface Serial1
 no ip address
 no ip directed-broadcast
 shutdown
!
ip default-gateway 10.25.213.129
ip classless
ip route 0.0.0.0 0.0.0.0 10.25.213.129
!
!
line con 0
 transport input none
line 1 6
 no exec
 transport input all
line 7
 no exec
 exec-timeout 300 0
 transport input all
line 8 9
 no exec
 transport input all
```

```
line 10
 no exec
 transport input all
 stopbits 1
line 11 12
 no exec
 transport input all
line 13
 no exec
 transport input all
 speed 115200
line 14 16
 no exec
 transport input all
line aux 0
line vty 0 4
 password cisco
 login
!
end
```

Related Commands

Command	Description
copy running-config startup-config	Copies the running configuration to the startup configuration. (Command alias for the **copy system:running-config nvram:startup-config** command.)
show startup-config	Displays the contents of NVRAM (if present and valid) or displays the configuration file pointed to by the CONFIG_FILE environment variable. (Command alias for the **more:nvram startup-config** command.)

show sdm prefer

To display information about the templates that can be used to maximize system resources for a particular feature, use the **show sdm prefer** command in privileged EXEC mode. To display the current template, use the command without a keyword.

show sdm prefer [**advanced**]

Syntax Description

advanced	(Optional) Displays information on the advanced template.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

If you did not reload the device after entering the **sdm prefer** global configuration command, the **show sdm prefer** privileged EXEC command displays the template currently in use and not the newly configured template.

The numbers displayed for each template represent an approximate maximum number for each feature resource. The actual number might vary, depending on the actual number of other features configured. For example, in the default template if your device had more than 16 routed interfaces (subnet VLANs), the number of possible unicast MAC addresses might be less than 6000.

Example

The following is sample output from the **show sdm prefer** command:

```
Device# show sdm prefer

Showing SDM Template Info

This is the Advanced template.
  Number of VLANs:                                      4094
  Unicast MAC addresses:                                16384
  Overflow Unicast MAC addresses:                       256
  L2 Multicast entries:                                 1024
  L3 Multicast entries:                                 1024
  Overflow L3 Multicast entries:                        256
  Directly connected routes:                            10240
  Indirect routes:                                      4096
  Security Access Control Entries:                      1664
  QoS Access Control Entries:                           1024
  Policy Based Routing ACEs:                            512
  Netflow Input ACEs:                                   128
  Netflow Output ACEs:                                  128
  Flow SPAN ACEs:                                       256
  Tunnels:                                              128
  LISP Instance Mapping Entries:                       256
  Control Plane Entries:                               512
  Input Netflow flows:                                 8192
  Output Netflow flows:                                8192
  SGT/DGT (or) MPLS VPN entries:                       2048
  SGT/DGT (or) MPLS VPN Overflow entries:              256
  Wired clients:                                       2048
  MACSec SPD Entries:                                  128

These numbers are typical for L2 and IPv4 features.
Some features such as IPv6, use up double the entry size;
so only half as many entries can be created.
```

show tech-support confidential

To hide confidential information from the **show tech-support** output, use the **show tech-support confidential** command in privileged EXEC mode.

show tech-support confidential output *file-name*

Syntax Description

output *file-name*	Specifies the output file where the tech-support data is to be saved.

Command Default

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.3.1	This command was introduced.

Usage Guidelines

The **show tech-support confidential** command will hide sensitive data like MAC addresses, IP addresses, and passwords. The output will be the same as that of the **show tech-support** command with all the customer-specific data masked.

The output from the **show tech-support confidential** command is very long. To better manage this output, you can redirect the output to a file in the local writable storage file system or the remote file system by using the **show tech-support confidential output** *location:filename*) . Redirecting the output to a file also makes sending the output to your Cisco Technical Assistance Center (TAC) representative easier.

```
Device# show tech-support confidential output flash:tech_confidential
Collecting tech-support without confidential info, it will take few min..
```

To view the output of the redirected file, use the command **more** *location:filename*.

show tech-support monitor

To display the SPAN monitor information, use the **show tech-support monitor** command in privileged EXEC mode.

show tech-support monitor [{**switch** *switch-number* | **active** | **standby**}]

Syntax Description

switch-number	Specifies the switch.
active	Specifies the active instance of the switch.
standby	Specifies the standby instance of the switch.

Command Default

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.3.1	This command was introduced.

Usage Guidelines

The output from the **show tech-support monitor** command is very long. To better manage this output, you can redirect the output to a file (for example, **show tech-support monitor** [**switch** *switch-number* | **active** | **standby**] | **redirect location:***filename*) in the local writable storage file system or the remote file system. Redirecting the output to a file also makes sending the output to your Cisco Technical Assistance Center (TAC) representative easier.

To view the output of the redirected file, use the command **more location:***filename*.

show tech-support platform

To display detailed information about a platform for use by technical support, use the **show tech-support platform** command in privileged EXEC mode.

show tech-support platform

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Usage Guidelines

This command is used for platform-specific debugging. The output provides detailed information about a platform, such as CPU usage, Ternary Content Addressable Memory (TCAM) usage, capacity, and memory usage.

The output of the **show tech-support platform** command is very long. To better manage this output, you can redirect the output to an external file (for example, **show tech-support platform | redirect flash:***filename*) in the local writable storage file system or remote file system.

The output of the **show tech-support platform** command displays a list commands and their output. These commands may differ based on the platform.

Examples

The following is sample output from the **show tech-support platform** command:

```
Device# show tech-support platform

.
.
.
------------------ show platform hardware capacity ------------------


Load Average
 Slot  Status  1-Min  5-Min 15-Min
1-RP0 Healthy   0.25   0.17   0.12

Memory (kB)
 Slot  Status    Total     Used (Pct)     Free (Pct) Committed (Pct)
1-RP0 Healthy  3964428  2212476 (56%)  1751952 (44%)   3420472 (86%)

CPU Utilization
 Slot  CPU   User System   Nice   Idle    IRQ   SIRQ IOwait
1-RP0    0   1.40   0.90   0.00  97.60   0.00   0.10   0.00
         1   2.00   0.20   0.00  97.79   0.00   0.00   0.00
         2   0.20   0.00   0.00  99.80   0.00   0.00   0.00
         3   0.79   0.19   0.00  99.00   0.00   0.00   0.00
         4   5.61   0.50   0.00  93.88   0.00   0.00   0.00
         5   2.90   0.40   0.00  96.70   0.00   0.00   0.00


 *: 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
------------------------------------------------------------------------------------------

  Vlan1                         0         0         0         0         0         0
  0         0         0
* GigabitEthernet0/0            0     10179         0         0      2000         4
  0         0         0
  GigabitEthernet1/0/1          0         0         0         0         0         0
  0         0         0
  GigabitEthernet1/0/2          0         0         0         0         0         0
  0         0         0
  GigabitEthernet1/0/3          0         0         0         0         0         0
  0         0         0
  GigabitEthernet1/0/4          0         0         0         0         0         0
  0         0         0
  GigabitEthernet1/0/5          0         0         0         0         0         0
  0         0         0
  GigabitEthernet1/0/6          0         0         0         0         0         0
  0         0         0
  GigabitEthernet1/0/7          0         0         0         0         0         0
  0         0         0
  GigabitEthernet1/0/8          0         0         0         0         0         0
  0         0         0
  GigabitEthernet1/0/9          0         0         0         0         0         0
  0         0         0
  GigabitEthernet1/0/10         0         0         0         0         0         0
  0         0         0
  GigabitEthernet1/0/11         0         0         0         0         0         0
  0         0         0
  GigabitEthernet1/0/12         0         0         0         0         0         0
  0         0         0
  GigabitEthernet1/0/13         0         0         0         0         0         0
  0         0         0
  GigabitEthernet1/0/14         0         0         0         0         0         0
  0         0         0
  GigabitEthernet1/0/15         0         0         0         0         0         0
  0         0         0
  GigabitEthernet1/0/16         0         0         0         0         0         0
  0         0         0
  GigabitEthernet1/0/17         0         0         0         0         0         0
  0         0         0
  GigabitEthernet1/0/18         0         0         0         0         0         0
  0         0         0
  GigabitEthernet1/0/19         0         0         0         0         0         0
  0         0         0
  GigabitEthernet1/0/20         0         0         0         0         0         0
  0         0         0
  GigabitEthernet1/0/21         0         0         0         0         0         0
  0         0         0
  GigabitEthernet1/0/22         0         0         0         0         0         0
  0         0         0
  GigabitEthernet1/0/23         0         0         0         0         0         0
  0         0         0
  GigabitEthernet1/0/24         0         0         0         0         0         0
  0         0         0
  GigabitEthernet1/0/25         0         0         0         0         0         0
  0         0         0
  GigabitEthernet1/0/26         0         0         0         0         0         0
  0         0         0
  GigabitEthernet1/0/27         0         0         0         0         0         0
  0         0         0
  GigabitEthernet1/0/28         0         0         0         0         0         0
  0         0         0
  GigabitEthernet1/0/29         0         0         0         0         0         0
  0         0         0
  GigabitEthernet1/0/30         0         0         0         0         0         0
  0         0         0
  GigabitEthernet1/0/31         0         0         0         0         0         0
  0         0         0
  GigabitEthernet1/0/32         0         0         0         0         0         0
  0         0         0
  GigabitEthernet1/0/33         0         0         0         0         0         0
  0         0         0
  GigabitEthernet1/0/34         0         0         0         0         0         0
  0         0         0
  GigabitEthernet1/0/35         0         0         0         0         0         0
  0         0         0
  GigabitEthernet1/0/36         0         0         0         0         0         0
  0         0         0
  Te1/0/37                      0         0         0         0         0         0
  0         0         0
  Te1/0/38                      0         0         0         0         0         0
  0         0         0
  Te1/0/39                      0         0         0         0         0         0
  0         0         0
  Te1/0/40                      0         0         0         0         0         0
  0         0         0
  Te1/0/41                      0         0         0         0         0         0
  0         0         0
  Te1/0/42                      0         0         0         0         0         0
  0         0         0
  Te1/0/43                      0         0         0         0         0         0
  0         0         0
  Te1/0/44                      0         0         0         0         0         0
  0         0         0
  Te1/0/45                      0         0         0         0         0         0
  0         0         0
  Te1/0/46                      0         0         0         0         0         0
  0         0         0
  Te1/0/47                      0         0         0         0         0         0
  0         0         0
  Te1/0/48                      0         0         0         0         0         0
  0         0         0
  Te1/1/1                       0         0         0         0         0         0
  0         0         0
  Te1/1/2                       0         0         0         0         0         0
  0         0         0
  Te1/1/3                       0         0         0         0         0         0
  0         0         0
  Te1/1/4                       0         0         0         0         0         0
  0         0         0
ASIC 0 Info
------------
ASIC 0 HASH Table 0 Software info:  FSE 0
 MAB 0: Unicast MAC addresses srip 0 1
 MAB 1: Unicast MAC addresses srip 0 1
 MAB 2: Unicast MAC addresses srip 0 1
 MAB 3: Unicast MAC addresses srip 0 1
 MAB 4: Unicast MAC addresses srip 0 1
 MAB 5: Unicast MAC addresses srip 0 1
 MAB 6: Unicast MAC addresses srip 0 1
 MAB 7: Unicast MAC addresses srip 0 1
ASIC 0 HASH Table 1 Software info:  FSE 0
 MAB 0: Unicast MAC addresses srip 0 1
 MAB 1: Unicast MAC addresses srip 0 1
 MAB 2: Unicast MAC addresses srip 0 1
 MAB 3: Unicast MAC addresses srip 0 1
 MAB 4: Unicast MAC addresses srip 0 1
 MAB 5: Unicast MAC addresses srip 0 1
 MAB 6: Unicast MAC addresses srip 0 1
 MAB 7: Unicast MAC addresses srip 0 1
ASIC 0 HASH Table 2 Software info:  FSE 1
 MAB 0: L3 Multicast entries srip 2 3
 MAB 1: L3 Multicast entries srip 2 3
 MAB 2: SGT_DGT         srip 0 1
 MAB 3: SGT_DGT         srip 0 1
 MAB 4: (null)          srip
 MAB 5: (null)          srip
 MAB 6: (null)          srip
 MAB 7: (null)          srip
.
.
.
```

Output fields are self-explanatory.

Related Commands

Command	Description
show tech-support platform evpn_vxlan	Displays EVPN-VXLAN-related platform information.
show tech-support platform fabric	Displays detailed information about the switch fabic.
show tech-support platform igmp_snooping	Displays IGMP snooping information about a group.
show tech-support platform layer3	Displays Layer 3 platform forwarding information.
show tech-support platform mld_snooping	Displays MLD snooping information about a group.

show tech-support platform evpn_vxlan

To display Ethernet VPN (EVPN)-Virtual eXtensible LAN (VXLAN)-related platform information for use by technical support, use the **show tech-support platform evpn_vxlan** command in privileged EXEC mode.

show tech-support platform evpn_vxlan switch *switch-number*

Syntax Description

switch *switch-number*	Displays information for the specified switch. Valid values are from 1 to 9.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Usage Guidelines

The output of this command is very long. To better manage this output, you can redirect the output to an external file (for example, **show tech-support platform evpn_vxlan switch 1 | redirect flash:***filename*) in the local writable storage file system or remote file system.

Examples

The following is sample output from the **show tech-support platform evpn_vxlan** command:

```
Device# show tech-support platform evpn_vxlan switch 1
.
.
.
    "show clock"
    "show version"
    "show running-config"switch no: 1


----- sh sdm prefer -----

Showing SDM Template Info

This is the Advanced template.
  Number of VLANs:                                    4094
  Unicast MAC addresses:                              32768
  Overflow Unicast MAC addresses:                     512
  L2 Multicast entries:                               4096
  Overflow L2 Multicast entries:                      512
  L3 Multicast entries:                               4096
  Overflow L3 Multicast entries:                      512
  Directly connected routes:                          16384
  Indirect routes:                                    7168
  STP Instances:                                      4096
  Security Access Control Entries:                    3072
  QoS Access Control Entries:                         2560
  Policy Based Routing ACEs:                          1024
  Netflow ACEs:                                       768
  Flow SPAN ACEs:                                     512
  Tunnels:                                            256
  LISP Instance Mapping Entries:                      256
  Control Plane Entries:                              512
  Input Netflow flows:                                 8192
  Output Netflow flows:                                16384
  SGT/DGT (or) MPLS VPN entries:                       4096
  SGT/DGT (or) MPLS VPN Overflow entries:              512
  Wired clients:                                       2048
  MACSec SPD Entries:                                  256
  MPLS L3 VPN VRF:                                     127
  MPLS Labels:                                         2048
  MPLS L3 VPN Routes VRF Mode:                         7168
  MPLS L3 VPN Routes Prefix Mode:                      3072
  MVPN MDT Tunnels:                                    256
  L2 VPN EOMPLS Attachment Circuit:                    256
  MAX VPLS Bridge Domains :                            64
  MAX VPLS Peers Per Bridge Domain:                    8
  MAX VPLS/VPWS Pseudowires :                          256
These numbers are typical for L2 and IPv4 features.
Some features such as IPv6, use up double the entry size;
so only half as many entries can be created.
* values can be modified by sdm cli.



----- show platform software fed switch 1 ifm interfaces nve -----



----- show platform software fed switch 1 ifm interfaces efp -----



----- show platform software fed switch 1 matm macTable -----


Total Mac number of addresses:: 0
*a_time=aging_time(secs)  *e_time=total_elapsed_time(secs)
Type:
MAT_DYNAMIC_ADDR           0x1  MAT_STATIC_ADDR            0x2  MAT_CPU_ADDR
 0x4  MAT_DISCARD_ADDR           0x8
MAT_ALL_VLANS             0x10  MAT_NO_FORWARD            0x20  MAT_IPMULT_ADDR
0x40  MAT_RESYNC                0x80
MAT_DO_NOT_AGE           0x100  MAT_SECURE_ADDR          0x200  MAT_NO_PORT
0x400  MAT_DROP_ADDR            0x800
MAT_DUP_ADDR            0x1000  MAT_NULL_DESTINATION    0x2000  MAT_DOT1X_ADDR
0x4000  MAT_ROUTER_ADDR         0x8000
MAT_WIRELESS_ADDR      0x10000  MAT_SECURE_CFG_ADDR    0x20000  MAT_OPQ_DATA_PRESENT
0x40000  MAT_WIRED_TUNNEL_ADDR  0x80000
MAT_DLR_ADDR          0x100000  MAT_MRP_ADDR          0x200000  MAT_MSRP_ADDR
0x400000  MAT_LISP_LOCAL_ADDR   0x800000
MAT_LISP_REMOTE_ADDR 0x1000000  MAT_VPLS_ADDR        0x2000000
Device#
```

Output fields are self-explanatory.

Related Commands

Command	Description
show tech-support platform	Displays detailed information about a platform for use by technical support.

show tech-support platform fabric

To display information about the switch fabric, use the **show tech-support platform fabric** command in privileged EXEC mode.

show tech-support platform fabric [{**display-cli** | **vrf** *vrf-name* {**ipv4 display-cli** | **ipv6 display-cli** | **source instance-id** *instance-id* {**ipv4** *ip-address/ip-prefix* | **ipv6** *ipv6-address/ipv6-prefix* | **mac** *mac-address*} {**dest instance-id** *instance-id*} {**ipv4** *ip-address/ip-prefix* | **ipv6** *ipv6-address/ipv6-prefix* | **mac** *mac-address*} [{**display-cli**}]}}]

Syntax Description

display-cli	(Optional) Displays the list of show commands available in the output of this command.
vrf *vrf-name*	(Optional) Displays fabric-related information for the specified virtual routing and forwarding (VRF) instance.
ipv4 *ip-address/ip-prefix*	(Optional) Displays fabric-related information for the source or destination IP VRF.
ipv6 *ipv6-address/ipv6-prefix*	(Optional) Displays fabric-related information for the source or destination IPv6 VRF.
source	(Optional) Displays fabric-related information for the source VRF.
instance-id *instance-id*	(Optional) Displays information about the endpoint identifier (EID) of the source.
mac *mac-address*	(Optional) Displays fabric-related information for the source and destination MAC VRF for Layer 2 extension deployments.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Usage Guidelines

The output of this command is very long. To better manage this output, you can redirect the output to an external file (for example, **show tech-support platform fabric | redirect flash:***filename*) in the local writable storage file system or remote file system.

The output of this command displays a list commands and their output. These commands may differ based on the platform.

Examples

The following is sample output from the **show tech-support platform fabric vrf source instance-id ipv4 dest instance-id ipv4** command:

```
Device# show tech-support platform fabric vrf DEFAULT_VN source instance-id
4098 ipv4 10.1.1.1/32 dest instance-id 4098 ipv4 10.12.12.12/32

.
.
.
-----show ip lisp eid-table vrf DEFAULT_VN forwarding  eid remote 10.12.12.12-----


Prefix                 Fwd action  Locator status bits   encap_iid
10.12.12.12/32         encap       0x00000001            N/A
  packets/bytes       1/576
  path list 7F44EEC2C188, 4 locks, per-destination, flags 0x49 [shble, rif, hwcn]
    ifnums:
      LISP0.4098(78): 192.0.2.2
    1 path
      path 7F44F8B5AFF0, share 10/10, type attached nexthop, for IPv4
        nexthop 192.0.2.2 LISP0.4098, IP midchain out of LISP0.4098, addr 192.0.2.2
7F44F8E86CE8
    1 output chain
      chain[0]: IP midchain out of LISP0.4098, addr 192.0.2.2 7F44F8E86CE8
                IP adj out of GigabitEthernet1/0/1, addr 10.0.2.1 7F44F8E87378


-----show lisp instance-id 4098 ipv4 map-cache-----


LISP IPv4 Mapping Cache for EID-table vrf DEFAULT_VN (IID 4098), 3 entries

0.0.0.0/0, uptime: 02:46:01, expires: never, via static-send-map-request
  Encapsulating to proxy ETR
10.1.1.0/24, uptime: 02:46:01, expires: never, via dynamic-EID, send-map-request
  Encapsulating to proxy ETR
10.12.12.12/32, uptime: 02:45:54, expires: 21:14:06, via map-reply, complete
  Locator  Uptime    State      Pri/Wgt     Encap-IID
  192.0.2.2  02:45:54  up          10/10        -


-----show lisp instance-id 4098 ipv4  map-cache detail-----


LISP IPv4 Mapping Cache for EID-table vrf DEFAULT_VN (IID 4098), 3 entries

0.0.0.0/0, uptime: 02:46:01, expires: never, via static-send-map-request
  Sources: static-send-map-request
  State: send-map-request, last modified: 02:46:01, map-source: local
  Exempt, Packets out: 2(676 bytes) (~ 02:45:38 ago)
  Configured as EID address space
  Encapsulating to proxy ETR
101.1.0/24, uptime: 02:46:01, expires: never, via dynamic-EID, send-map-request
  Sources: NONE
  State: send-map-request, last modified: 02:46:01, map-source: local
  Exempt, Packets out: 0(0 bytes)
  Configured as EID address space
  Configured as dynamic-EID address space
  Encapsulating dynamic-EID traffic
  Encapsulating to proxy ETR
```

```
10.12.12.12/32, uptime: 02:45:54, expires: 21:14:06, via map-reply, complete
  Sources: map-reply
  State: complete, last modified: 02:45:54, map-source: 10.0.1.2
  Idle, Packets out: 1(576 bytes) (~ 02:45:38 ago)
  Locator  Uptime    State      Pri/Wgt     Encap-IID
  192.0.2.2  02:45:54  up          10/10        -
    Last up-down state change:         02:45:54, state change count: 1
    Last route reachability change:    02:45:54, state change count: 1
    Last priority / weight change:     never/never
    RLOC-probing loc-status algorithm:
      Last RLOC-probe sent:            02:45:54 (rtt 1ms)


-----show lisp instance-id 4098 ipv4 map-cache  10.12.12.12/32-----


LISP IPv4 Mapping Cache for EID-table vrf DEFAULT_VN (IID 4098), 3 entries

10.12.12.12/32, uptime: 02:45:54, expires: 21:14:06, via map-reply, complete
  Sources: map-reply
  State: complete, last modified: 02:45:54, map-source: 10.0.1.2
  Idle, Packets out: 1(576 bytes) (~ 02:45:38 ago)
  Locator  Uptime    State      Pri/Wgt     Encap-IID
  192.0.2.2  02:45:54  up          10/10        -
    Last up-down state change:         02:45:54, state change count: 1
    Last route reachability change:    02:45:54, state change count: 1
    Last priority / weight change:     never/never
    RLOC-probing loc-status algorithm:
      Last RLOC-probe sent:            02:45:54 (rtt 1ms)


-----show ip cef vrf DEFAULT_VN 10.12.12.12/32 internal-----


10.12.12.12/32, epoch 1, flags [sc, lisp elig], refcnt 6, per-destination sharing
  sources: LISP, IPL
  feature space:
    Broker: linked, distributed at 1st priority
  subblocks:
    SC owned,sourced: LISP remote EID - locator status bits 0x00000001
    LISP remote EID: 1 packets 576 bytes fwd action encap, cfg as EID space
    LISP source path list
      path list 7F44EEC2C188, 4 locks, per-destination, flags 0x49 [shble, rif, hwcn]
        ifnums:
          LISP0.4098(78): 192.0.2.2
        1 path
          path 7F44F8B5AFF0, share 10/10, type attached nexthop, for IPv4
            nexthop 192.0.2.2 LISP0.4098, IP midchain out of LISP0.4098, addr 192.0.2.2
7F44F8E86CE8
        1 output chain
          chain[0]: IP midchain out of LISP0.4098, addr 192.0.2.2 7F44F8E86CE8
                    IP adj out of GigabitEthernet1/0/1, addr 10.0.2.1 7F44F8E87378
      Dependent covered prefix type LISP, cover 0.0.0.0/0
    2 IPL sources [no flags]
  ifnums:
    LISP0.4098(78): 192.0.2.2
  path list 7F44EEC2C188, 3 locks, per-destination, flags 0x49 [shble, rif, hwcn]
    path 7F44F8B5AFF0, share 10/10, type attached nexthop, for IPv4
     nexthop 192.0.2.2 LISP0.4098, IP midchain out of LISP0.4098, addr 192.0.2.2 7F44F8E86CE8

  output chain:
    PushCounter(LISP:10.12.12.12/32) 7F44F3C8B8D8
    IP midchain out of LISP0.4098, addr 192.0.2.2 7F44F8E86CE8
    IP adj out of GigabitEthernet1/0/1, addr 10.0.2.1 7F44F8E87378
```

```
switch no: 1
.
.
.

Device# show tech-support platform fabric vrf Campus_VN source instance-id 8189
mac 00b7.7128.00a1 dest instance-id 8189 mac 00b7.7128.00a0   | i show

------------------ show clock ------------------
------------------ show version ------------------
------------------ show running-config ------------------
------------------ show device-tracking database ------------------
------------------ show lisp site ------------------
-------------------- show mac address-table address 00B7.7128.00A0-----
-------------------- show ip arp vrf Campus_VN-----
Device#
```

Output fields are self-explanatory.

Related Commands

Command	Description
show tech-support platform	Displays detailed information about a platform for use by technical support.

show tech-support platform igmp_snooping

To display Internet Group Management Protocol (IGMP) snooping information about a group, use the **show tech-support platform igmp_snooping** command in privileged EXEC mode.

show tech-support platform igmp_snooping [{**Group_ipAddr** *ipv4-address* | [{**vlan** *vlan-ID*}]}]

Syntax Description

Group_ipAddr	(Optional) Displays snooping information about the specified group address.
ipv4-address	(Optional) IPv4 address of the group.
vlan *vlan-ID*	(Optional) Displays IGMP snooping VLAN information. Valid values are from 1 to 4094.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

The output of this command is very long. To better manage this output, you can redirect the output to a file (for example, **show tech-support platform igmp_snooping | redirect flash:***filename*) in the local writable storage file system or remote file system.

Examples

The following is sample output from the **show tech-support platform igmp_snooping** command:

```
Device# show tech-support platform igmp_snooping GroupIPAddr 226.6.6.6 vlan

.
.
.
----- show ip igmp snooping groups | i 226.6.6.6 -----

5         226.6.6.6                user                    Gi1/0/8, Gi1/0/27, Gi1/0/28,



----- show ip igmp snooping groups count -----

Total number of groups:   2



----- show ip igmp snooping mrouter -----


Vlan    ports
----    -----
  23    Router
  24    Router
  25    Router


----- show ip igmp snooping querier -----


Vlan      IP Address               IGMP Version   Port
-------------------------------------------------------------
23        10.1.1.1                v2             Router
24        10.1.2.1                v2             Router
25        10.1.3.1                v2             Router



----- show ip igmp snooping vlan 5 -----


Global IGMP Snooping configuration:
-------------------------------------------
IGMP snooping                : Enabled
Global PIM Snooping          : Disabled
IGMPv3 snooping              : Enabled
Report suppression           : Enabled
TCN solicit query            : Disabled
TCN flood query count        : 2
Robustness variable          : 2
Last member query count      : 2
Last member query interval   : 1000

Vlan 5:
--------
IGMP snooping                       : Enabled
Pim Snooping                        : Disabled
IGMPv2 immediate leave              : Disabled
Explicit host tracking              : Enabled
Multicast router learning mode      : pim-dvmrp
CGMP interoperability mode          : IGMP_ONLY
Robustness variable                 : 2
Last member query count             : 2
Last member query interval          : 1000


----- show ip igmp snooping groups vlan 5 -----

Vlan      Group                     Type        Version     Port List
-----------------------------------------------------------------------
5         226.6.6.6                 user                   Gi1/0/8, Gi1/0/27, Gi1/0/28,
                                                           Gi2/0/7, Gi2/0/8, Gi2/0/27,
                                                           Gi2/0/28
5         238.192.0.1               user                   Gi2/0/28



----- show platform software fed active ip igmp snooping vlan 5 -----


Vlan 5
---------
 IGMPSN Enabled  : On
 PIMSN Enabled   : Off
 Flood Mode      : On
 I-Mrouter       : Off
 Oper State      : Up
 STP TCN Flood   : Off
 Routing Enabled : Off
 PIM Enabled     : Off
 PVLAN           : No
 In Retry        : 0x0
 L3mcast Adj      :
 Mrouter PortQ   :
 Flood PortQ     :


----- show platform software fed active ip igmp snooping groups | begin 226.6.6.6 -----

Vlan:5 Group:226.6.6.6
---------------------------------
Member ports   :
CAPWAP ports   :
Host Type Flags: 0
Failure Flags  : 0
DI handle      : 0x7f11151cbad8
REP RI handle  : 0x7f11151cc018
SI handle      : 0x7f11151cd198
HTM handle     : 0x7f11151cd518

si hdl : 0x7f11151cd198 rep ri hdl : 0x7f11151cc018 di hdl :  0x7f11151cbad8 htm hdl :
0x7f11151cd518
.
.
.
Device#
```

Output fields are self-explanatory.

Related Commands

Command	Description
ip igmp snooping	Enables IGMP snooping globally or on an interface.
show ip igmp snooping	Displays the IGMP snooping configuration of a device.
show tech-support platform	Displays detailed information about a platform for use by technical support.

show tech-support platform layer3

To display Layer 3 platform forwarding information, use the **show tech-support platform layer3** command in privileged EXEC mode.

show tech-support platform layer3 {**multicast Group_ipAddr** *ipv4-address* **switch** *switch-number* **srcIP** *ipv4-address* | **unicast** {**dstIP** *ipv4-address* **srcIP** *ipv4-address* | **vrf** *vrf-name* **destIP** *ipv4-address* **srcIP** *ipv4-address*}}

Syntax Description

multicast	Displays multicast information.
Group_ipv6Addr *ipv4-address*	Displays information about the specified multicast group address.
switch *switch-number*	Displays information about the specified switch. Valid values are from 1 to 9.
srcIP *ipv4-address*	Displays information about the specified source address.
unicast	Displays unicast-related information.
dstIP *ipv4-address*	Displays information about the specified destination address.
vrf *vrf-name*	Displays unicast-related virtual routing and forwarding (VRF) information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Usage Guidelines

The output of this command is very long. To better manage this output, you can redirect the output to an external file (for example, **show tech-support platform layer3 multicast group 224.1.1.1 switch 1 srcIP 10.10.0.2 | redirect flash:***filename*) in the local writable storage file system or remote file system.

Examples

The following is sample output from the **show tech-support platform layer3 multicast group** command:

```
Device# show tech-support platform layer3 multicast group_ipAddr 224.1.1.1
switch 1 srcIp 10.10.0.2

.
.
.
destination IP: 224.1.1.1
source IP: 10.10.0.2
```

```
switch no: 1


----- show ip mroute 224.1.1.1 10.10.0.2 -----


IP Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected,
       L - Local, P - Pruned, R - RP-bit set, F - Register flag,
       T - SPT-bit set, J - Join SPT, M - MSDP created entry, E - Extranet,
       X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement,
       U - URD, I - Received Source Specific Host Report,
       Z - Multicast Tunnel, z - MDT-data group sender,
       Y - Joined MDT-data group, y - Sending to MDT-data group,
       G - Received BGP C-Mroute, g - Sent BGP C-Mroute,
       N - Received BGP Shared-Tree Prune, n - BGP C-Mroute suppressed,
       Q - Received BGP S-A Route, q - Sent BGP S-A Route,
       V - RD & Vector, v - Vector, p - PIM Joins on route,
       x - VxLAN group, c - PFP-SA cache created entry
Outgoing interface flags: H - Hardware switched, A - Assert winner, p - PIM Join
 Timers: Uptime/Expires
 Interface state: Interface, Next-Hop or VCD, State/Mode

(10.10.0.2, 224.1.1.1), 00:00:22/00:02:37, flags: LFT
  Incoming interface: GigabitEthernet1/0/10, RPF nbr 0.0.0.0, Registering
  Outgoing interface list:
    Vlan20, Forward/Sparse, 00:00:22/00:02:37, A



----- show ip mfib 224.1.1.1 10.10.0.2 -----


Entry Flags:    C - Directly Connected, S - Signal, IA - Inherit A flag,
                ET - Data Rate Exceeds Threshold, K - Keepalive
                DDE - Data Driven Event, HW - Hardware Installed
                ME - MoFRR ECMP entry, MNE - MoFRR Non-ECMP entry, MP - MFIB
                MoFRR Primary, RP - MRIB MoFRR Primary, P - MoFRR Primary
                MS  - MoFRR  Entry in Sync, MC - MoFRR entry in MoFRR Client.
I/O Item Flags: IC - Internal Copy, NP - Not platform switched,
                NS - Negate Signalling, SP - Signal Present,
                A - Accept, F - Forward, RA - MRIB Accept, RF - MRIB Forward,
                MA - MFIB Accept, A2 - Accept backup,
                RA2 - MRIB Accept backup, MA2 - MFIB Accept backup

Forwarding Counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts:      Total/RPF failed/Other drops
I/O Item Counts:   FS Pkt Count/PS Pkt Count
Default
 (10.10.0.2,224.1.1.1) Flags: HW
   SW Forwarding: 0/0/0/0, Other: 1/1/0
   HW Forwarding:   NA/NA/NA/NA, Other: NA/NA/NA
   GigabitEthernet1/0/10 Flags: A
   Vlan20 Flags: F IC
     Pkts: 0/0
   Tunnel0 Flags: F
     Pkts: 0/0



----- show platform software fed switch 1 ip multicast interface summary -----

Multicast Interface database
```

```
VRF  Interface                 IF ID              PIM Status  State              RI Handle
           SVI
------------------------------------------------------------------------------------------
0    GigabitEthernet1/0/10     0x000000000000005f  enabled     0x0000000000000010
0x00007fb414b1f108  false
0    Vlan20                    0x0000000000000060  enabled     0x0000000000000010
0x00007fb414b31a98  true



----- show platform software fed switch 1 ip multicast groups summary -----

Multicast Groups database

Mvrf_id: 0  Mroute: (*, 224.0.1.40/32)  Flags:  C IC
  Htm: 0x00007fb414b23ce8  Si: 0x00007fb414b23a08  Di: 0x00007fb414b240e8  Rep_ri:
  0x00007fb414b245f8

Mvrf_id: 0  Mroute: (*, 224.0.0.0/4)  Flags:  C
  Htm: 0x00007fb4143549e8  Si: 0x00007fb414b20a48  Di: 0x00007fb414b1fe78  Rep_ri:
  0x00007fb414b20428

Mvrf_id: 0  Mroute: (*, 224.1.1.1/32)  Flags:  C IC
  Htm: 0x00007fb414b2cc98  Si: 0x00007fb414b2b678  Di: 0x00007fb414b2ab98  Rep_ri:
  0x00007fb414b2b0c8

Mvrf_id: 0  Mroute: (10.10.0.2, 224.1.1.1/32)  Flags:  IC
  Htm: 0x00007fb414b2f348  Si: 0x00007fb414b321d8  Di: 0x00007fb414b2dba8  Rep_ri:
  0x00007fb414b30ed8




----- show platform software fed switch 1 ip multicast groups count -----


Total Number of entries:4



----- show platform software fed switch 1 ip multicast groups 224.1.1.1/32
source 10.10.0.2 detail -----


MROUTE ENTRY vrf 0 (10.10.0.2, 224.1.1.1/32)
  HW Handle: 140411418055080 Flags:  IC
RPF interface: GigabitEthernet1/0/10(95)):
  HW Handle:140411418055080 Flags:A
Number of OIF: 3
Flags: 0x4   Pkts : 0
OIF Details:
     Tunnel0      Adj: 0xf8000636    F
     Vlan20      Adj: 0xf8000601  F IC
     GigabitEthernet1/0/10        A
Htm: 0x7fb414b2f348  Si: 0x7fb414b321d8  Di: 0x7fb414b2dba8  Rep_ri: 0x7fb414b30ed8


DI details
----------
Handle:0x7fb414b2dba8 Res-Type:ASIC_RSC_DI Res-Switch-Num:255 Asic-Num:255
Feature-ID:AL_FID_L3_
MULTICAST_IPV4 Lkp-ftr-id:LKP_FEAT_INVALID ref_count:1
priv_ri/priv_si Handle:(nil) Hardware Indices/Handles: index0:0x538e
mtu_index/l3u_ri_index0:0x0  index1:0x538e  mtu_index/l3u_ri_index1:0x0
```

```
Cookie length: 56
00 00 00 00 00 00 00 00 00 00 00 00 02 00 0a 0a 01 01 01 e0 00 00 00 00 00 00 00 00 00 00
00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Detailed Resource Information (ASIC# 0)
----------------------------------------

Destination Index (DI) [0x538e]
portMap = 0x00000000                0
cmi1 = 0x385
rcpPortMap = 0

al_rsc_cmi
CPU Map Index (CMI) [0x385]
ctiLo0 = 0x9
ctiLo1 = 0
ctiLo2 = 0
cpuQNum0 = 0x9e
cpuQNum1 = 0
cpuQNum2 = 0
npuIndex = 0
strip_seg = 0x0
copy_seg = 0x0
Detailed Resource Information (ASIC# 1)
----------------------------------------

Destination Index (DI) [0x538e]
portMap = 0x00000000                0
cmi1 = 0x385
rcpPortMap = 0

al_rsc_cmi
CPU Map Index (CMI) [0x385]
ctiLo0 = 0x9
ctiLo1 = 0
ctiLo2 = 0
cpuQNum0 = 0x9e
cpuQNum1 = 0
cpuQNum2 = 0
npuIndex = 0
strip_seg = 0x0
copy_seg = 0x0

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

RI details
----------
Handle:0x7fb414b30ed8 Res-Type:ASIC_RSC_RI_REP Res-Switch-Num:255 Asic-Num:255 Feature-ID:
AL_FID_L3_MULTICAST_IPV4 Lkp-ftr-id:LKP_FEAT_INVALID ref_count:1
priv_ri/priv_si Handle:(nil) Hardware Indices/Handles: index0:0x5  mtu_index/l3u_ri_index0:0x0

index1:0x5  mtu_index/l3u_ri_index1:0x0
Cookie length: 56
00 00 00 00 00 00 00 00 00 00 00 00 02 00 0a 0a 01 01 01 e0 00 00 00 00 00 00 00 00 00 00
00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Detailed Resource Information (ASIC# 0)
----------------------------------------

Detailed Resource Information (ASIC# 1)
----------------------------------------


==============================================================
SI details
----------
Handle:0x7fb414b321d8 Res-Type:ASIC_RSC_SI_STATS Res-Switch-Num:255 Asic-Num:255 Feature-ID:
AL_FID_L3_MULTICAST_IPV4 Lkp-ftr-id:LKP_FEAT_INVALID ref_count:1
priv_ri/priv_si Handle:(nil) Hardware Indices/Handles: index0:0x4004  mtu_index/l3u_ri_index0:
0x0  sm handle 0:0x7fb414b2df98  index1:0x4004  mtu_index/l3u_ri_index1:0x0
Cookie length: 56
00 00 00 00 00 00 00 00 00 00 00 00 02 00 0a 0a 01 01 01 e0 00 00 00 00 00 00 00 00 00
00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
Detailed Resource Information (ASIC# 0)
----------------------------------------
Detailed Resource Information (ASIC# 1)
----------------------------------------

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

HTM details
-----------
Handle:0x7fb414b2f348 Res-Type:ASIC_RSC_HASH_TCAM Res-Switch-Num:0 Asic-Num:255 Feature-ID:
AL_FID_L3_MULTICAST_IPV4 Lkp-ftr-id:LKP_FEAT_IPV4_MCAST_SG ref_count:1
priv_ri/priv_si Handle:(nil) Hardware Indices/Handles: handle0:0x7fb414b2f558
Detailed Resource Information (ASIC# 0)
----------------------------------------
Number of HTM Entries: 1

Entry #0: (handle 0x7fb414b2f558)

KEY - src_addr:10.10.0.2 starg_station_index: 16387
MASK - src_addr:0.0.0.0 starg_station_index: 0
AD: use_starg_match: 0 mcast_bridge_frame: 0 mcast_rep_frame: 0 rpf_valid: 1 rpf_le_ptr: 0

afd_client_flag: 0 dest_mod_bridge: 0 dest_mod_route: 1 cpp_type: 0 dest_mod_index: 0
rp_index:
0 priority: 5 rpf_le: 36 station_index: 16388 capwap_mgid_present: 0 mgid 0

==============================================================
```

The following is sample output from the **show tech-support platform layer3 unicast vrf** command:

```
Device# show tech-support platform layer3 unicast vrf vr1 dstIP 10.0.0.20
srcIP 10.0.0.10

.
.
.
destination IP: 10.0.0.20
source IP: 10.0.0.10
vrf name :

Switch/Stack Mac Address : 5006.ab89.0280 - Local Mac Address
Mac persistency wait time: Indefinite
                                             H/W   Current
Switch#   Role    Mac Address     Priority Version  State
-------------------------------------------------------------------------------------
*1       Active   5006.ab89.0280     1      V02     Ready




----- show switch -------
```

```
10.0.0.10 -> 10.0.0.20 =>IP adj out of GigabitEthernet1/0/7, addr 10.0.0.20


----- show ip cef    exact-route platform  10.0.0.10 10.0.0.20 -----



nexthop is 10.0.0.20


Protocol Interface                 Address
IP       GigabitEthernet1/0/7      10.0.0.20(8)
                                   0 packets, 0 bytes
                                   epoch 0
                                   sourced in sev-epoch 0
                                   Encap length 14
                                   00211BFDE6495006AB8902C00800
                                   L2 destination address byte offset 0
                                   L2 destination address byte length 6
                                   Link-type after encap: ip
                                   ARP


----- show adjacency 10.0.0.20 detail -----



Routing entry for 10.0.0.0/24
  Known via "connected", distance 0, metric 0 (connected, via interface)
  Routing Descriptor Blocks:
  * directly connected, via GigabitEthernet1/0/7
      Route metric is 0, traffic share count is 1


----- show ip route   10.0.0.20 -----



10.0.0.20/32, epoch 3, flags [attached]
  Adj source: IP adj out of GigabitEthernet1/0/7, addr 10.0.0.20 FF90E67820
    Dependent covered prefix type adjfib, cover 10.0.0.0/24
  attached to GigabitEthernet1/0/7


----- show ip cef   10.0.0.20 detail -----



ip prefix: 10.0.0.20/32


Forwarding Table

10.0.0.20/32 -> OBJ_ADJACENCY (29), urpf: 30
Connected Interface: 31
Prefix Flags: Directly L2 attached
OM handle: 0x10205416d8



----- show platform software ip switch 1 R0 cef prefix  10.0.0.20/32 detail -----
```

```
OBJ_ADJACENCY found: 29


Number of adjacency objects: 5

Adjacency id: 0x1d (29)
  Interface: GigabitEthernet1/0/7, IF index: 31, Link Type: MCP_LINK_IP
  Encap: 0:21:1b:fd:e6:49:50:6:ab:89:2:c0:8:0
  Encap Length: 14, Encap Type: MCP_ET_ARPA, MTU: 1500
  Flags: no-l3-inject
  Incomplete behavior type: None
  Fixup: unknown
  Fixup_Flags_2: unknown
  Nexthop addr: 10.0.0.20
  IP FRR MCP_ADJ_IPFRR_NONE 0
  OM handle: 0x1020541348




----- show platform software adjacency switch 1 R0 index 29 -----



Forwarding Table

10.0.0.20/32 -> OBJ_ADJACENCY (29), urpf: 30
Connected Interface: 31
Prefix Flags: Directly L2 attached
aom id: 393, HW handle: (nil) (created)



----- show platform software ip switch 1 F0 cef prefix  10.0.0.20/32 detail -----



OBJ_ADJACENCY found: 29


Number of adjacency objects: 5

Adjacency id: 0x1d (29)
  Interface: GigabitEthernet1/0/7, IF index: 31, Link Type: MCP_LINK_IP
  Encap: 0:21:1b:fd:e6:49:50:6:ab:89:2:c0:8:0
  Encap Length: 14, Encap Type: MCP_ET_ARPA, MTU: 1500
  Flags: no-l3-inject
  Incomplete behavior type: None
  Fixup: unknown
  Fixup_Flags_2: unknown
  Nexthop addr: 10.0.0.20
  IP FRR MCP_ADJ_IPFRR_NONE 0
  aom id: 391, HW handle: (nil) (created)




----- show platform software adjacency switch 1 F0 index 29 -----



found aom id: 391
```

```
Object identifier: 391
  Description: adj 0x1d, Flags None
  Status: Done, Epoch: 0, Client data: 0xc6a747a8



----- show platform software object-manager switch 1 F0 object 391 -----


Object identifier: 66
  Description: intf GigabitEthernet1/0/7, handle 31, hw handle 31, HW dirty: NONE AOM dirty
 NONE
  Status: Done



----- show platform software object-manager switch 1 F0 object 391  parents -----


Object identifier: 393
  Description: PREFIX 10.0.0.20/32 (Table id 0)
  Status: Done
.
.
.
```

Output fields are self-explanatory.

Related Commands

Command	Description
show tech-support platform	Displays detailed information about a platform for use by technical support.

show tech-support platform mld_snooping

To display Multicast Listener Discovery (MLD) snooping information about a group, use the **show tech-support platform mld_snooping** command in privileged EXEC mode.

show tech-support platform mld_snooping [{**Group_ipv6Addr** *ipv6-address* }][{**vlan** *vlan-ID*}]

Syntax Description

Group_ipv6Addr	(Optional) Displays snooping information about the specified group address.
ipv6-address	(Optional) IPv6 address of the group.
vlan *vlan-ID*	(Optional) Displays MLD snooping VLAN information. Valid values are from 1 to 4094.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Usage Guidelines

The output of this command is very long. To better manage this output, you can redirect the output to an external file (for example, **show tech-support platform mld_snooping | redirect flash:***filename*) in the local writable storage file system or remote file system.

Examples

The following is sample output from the **show tech-support platform mld_snooping** command:

```
Device# show tech-support platform mld_snooping GroupIPv6Addr FF02::5:1

.
.
.
------------------ show running-config ------------------


Building configuration...

Current configuration : 11419 bytes
!
! Last configuration change at 09:17:04 UTC Thu Sep 6 2018
!
version 16.10
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service call-home
no platform punt-keepalive disable-kernel-core
!
hostname Switch
!
!
vrf definition Mgmt-vrf
```

```
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
!
no aaa new-model
switch 1 provision ws-c3650-12x48uq
!
!
!
!
call-home
 ! If contact email address in call-home is configured as sch-smart-licensing@cisco.com
 ! the email address configured in Cisco Smart License Portal will be used as contact email
 address to send SCH notifications.
 contact-email-addr sch-smart-licensing@cisco.com
 profile "profile-1"
  active
  destination transport-method http
  no destination transport-method email
!
!
!
!
!
ip admission watch-list expiry-time 0
!
!
!
login on-success log
!
!
!
!
!
no device-tracking logging theft
!
crypto pki trustpoint TP-self-signed-559433368
 enrollment selfsigned
 subject-name cn=IOS-Self-Signed-Certificate-559433368
 revocation-check none
 rsakeypair TP-self-signed-559433368
!
crypto pki trustpoint SLA-TrustPoint
 enrollment pkcs12
 revocation-check crl
!
!
crypto pki certificate chain TP-self-signed-559433368
 certificate self-signed 01
  30820229 30820192 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
  30312E30 2C060355 04031325 494F532D 53656C66 2D536967 6E65642D 43657274
  69666963 6174652D 35353934 33333336 38301E17 0D313531 32303331 32353432
  325A170D 32303031 30313030 30303030 5A303031 2E302C06 03550403 1325494F
  532D5365 6C662D53 69676E65 642D4365 72746966 69636174 652D3535 39343333
  33363830 819F300D 06092A86 4886F70D 01010105 0003818D 00308189 02818100
  AD8C9C3B FEE7FFC8 986837D2 4C126172 446C3C53 E040F798 4BA61C97 7506FDCE
  46365D0A E47E3F4F C774CA5B 73E2A8DD B72A2E98 C66DB196 94E8150F 0B669CF6
  AA5BC4CD FC2E02F6 FE08B17F 0164FC19 7DC84ABB C99D91D6 398233FF 814EF6DA
  6DC8FC20 CA12C0D6 1CB28EDA 6ADD6DFA 7E3E8281 4A189A9A AA44FCC0 BA9BD8A5
  02030100 01A35330 51300F06 03551D13 0101FF04 05300301 01FF301F 0603551D
  23041830 16801448 668D668E C92914BB 69E9BA64 F61228DE 132E2030 1D060355
  1D0E0416 04144866 8D668EC9 2914BB69 E9BA64F6 1228DE13 2E20300D 06092A86
  4886F70D 01010505 00038181 0000F1D3 3DD1E5F1 EB714A95 D5819933 CAD0C943
  59927D55 9D70CAD0 D64830EB D54380AD D2B5B613 F8AF7A5B 1F801134 246F760D
  5E5515DB D098304F 5086F6CE 88E8B576 F6B93A88 F458FDCF 91A42D7E FA741908
  5C892D78 600FB655 E6C5A4D0 6C1F1B9A 3AECA550 E3DC0881 01C4D004 7AB65BC3
  88CF24DE DAA19474 51B535A5 0C
   quit
crypto pki certificate chain SLA-TrustPoint
 certificate ca 01
  30820321 30820209 A0030201 02020101 300D0609 2A864886 F70D0101 0B050030
  32310E30 0C060355 040A1305 43697363 6F312030 1E060355 04031317 43697363
  6F204C69 63656E73 696E6720 526F6F74 20434130 1E170D31 33303533 30313934
  3834375A 170D3338 30353330 31393438 34375A30 32310E30 0C060355 040A1305
  43697363 6F312030 1E060355 04031317 43697363 6F204C69 63656E73 696E6720
  526F6F74 20434130 82012230 0D06092A 864886F7 0D010101 05000382 010F0030
  82010A02 82010100 A6BCBD96 131E05F7 145EA72C 2CD686E6 17222EA1 F1EFF64D
  CBB4C798 212AA147 C655D8D7 9471380D 8711441E 1AAF071A 9CAE6388 8A38E520
  1C394D78 462EF239 C659F715 B98C0A59 5BBB5CBD 0CFEBEA3 700A8BF7 D8F256EE
  4AA4E80D DB6FD1C9 60B1FD18 FFC69C96 6FA68957 A2617DE7 104FDC5F EA2956AC
  7390A3EB 2B5436AD C847A2C5 DAB553EB 69A9A535 58E9F3E3 C0BD23CF 58BD7188
  68E69491 20F320E7 948E71D7 AE3BCC84 F10684C7 4BC8E00F 539BA42B 42C68BB7
  C7479096 B4CB2D62 EA2F505D C7B062A4 6811D95B E8250FC4 5D5D5FB8 8F27D191
  C55F0D76 61F9A4CD 3D992327 A8BB03BD 4E6D7069 7CBADF8B DF5F4368 95135E44
  DFC7C6CF 04DD7FD1 02030100 01A34230 40300E06 03551D0F 0101FF04 04030201
  06300F06 03551D13 0101FF04 05300301 01FF301D 0603551D 0E041604 1449DC85
  4B3D31E5 1B3E6A17 606AF333 3D3B4C73 E8300D06 092A8648 86F70D01 010B0500
  03820101 00507F24 D3932A66 86025D9F E838AE5C 6D4DF6B0 49631C78 240DA905
  604EDCDE FF4FED2B 77FC460E CD636FDB DD44681E 3A5673AB 9093D3B1 6C9E3D8B
  D98987BF E40CBD9E 1AECA0C2 2189BB5C 8FA85686 CD98B646 5575B146 8DFC66A8
  467A3DF4 4D565700 6ADF0F0D CF835015 3C04FF7C 21E878AC 11BA9CD2 55A9232C
  7CA7B7E6 C1AF74F6 152E99B7 B1FCF9BB E973DE7F 5BDDEB86 C71E3B49 1765308B
  5FB0DA06 B92AFE7F 494E8A9E 07B85737 F3A58BE1 1A48A229 C37C1E69 39F08678
  80DDCD16 D6BACECA EEBC7CF9 8428787B 35202CDC 60E4616A B623CDBD 230E3AFB
  418616A9 4093E049 4D10AB75 27E86F73 932E35B5 8862FDAE 0275156F 719BB2F0
  D697DF7F 28
   quit
!
!
!
diagnostic bootup level minimal
diagnostic monitor syslog
!
spanning-tree mode rapid-pvst
spanning-tree extend system-id
!
!
!
redundancy
 mode sso
!
!
!
!
!
!
class-map match-any system-cpp-police-topology-control
  description Topology control
class-map match-any system-cpp-police-sw-forward
  description Sw forwarding, L2 LVX data, LOGGING
class-map match-any system-cpp-default
  description EWLC control, EWLC data, Inter FED
class-map match-any system-cpp-police-sys-data
  description Learning cache ovfl, High Rate App, Exception, EGR Exception, NFL SAMPLED
```

```
DATA, RPF Failed
class-map match-any AutoQos-4.0-RT1-Class
 match dscp ef
 match dscp cs6
class-map match-any system-cpp-police-punt-webauth
  description Punt Webauth
class-map match-any AutoQos-4.0-RT2-Class
 match dscp cs4
 match dscp cs3
 match dscp af41
class-map match-any system-cpp-police-l2lvx-control
  description L2 LVX control packets
class-map match-any system-cpp-police-forus
  description Forus Address resolution and Forus traffic
class-map match-any system-cpp-police-multicast-end-station
  description MCAST END STATION
class-map match-any system-cpp-police-multicast
  description Transit Traffic and MCAST Data
class-map match-any system-cpp-police-l2-control
  description L2 control
class-map match-any system-cpp-police-dot1x-auth
  description DOT1X Auth
class-map match-any system-cpp-police-data
  description ICMP redirect, ICMP_GEN and BROADCAST
class-map match-any system-cpp-police-stackwise-virt-control
  description Stackwise Virtual
class-map match-any system-cpp-police-control-low-priority
  description ICMP redirect and general punt
class-map match-any system-cpp-police-wireless-priority1
  description Wireless priority 1
class-map match-any system-cpp-police-wireless-priority2
  description Wireless priority 2
class-map match-any system-cpp-police-wireless-priority3-4-5
  description Wireless priority 3,4 and 5
class-map match-any non-client-nrt-class
class-map match-any system-cpp-police-routing-control
  description Routing control and Low Latency
class-map match-any system-cpp-police-protocol-snooping
  description Protocol snooping
class-map match-any system-cpp-police-dhcp-snooping
  description DHCP snooping
class-map match-any system-cpp-police-system-critical
  description System Critical and Gold Pkt
!
policy-map system-cpp-policy
 class system-cpp-police-data
  police rate 200 pps
 class system-cpp-police-routing-control
  police rate 500 pps
 class system-cpp-police-control-low-priority
 class system-cpp-police-wireless-priority1
 class system-cpp-police-wireless-priority2
 class system-cpp-police-wireless-priority3-4-5
policy-map port_child_policy
 class non-client-nrt-class
  bandwidth remaining ratio 10
!
!
!
!
!
!
!
!
```

```
!
!
interface GigabitEthernet0/0
 vrf forwarding Mgmt-vrf
 no ip address
 speed 1000
 negotiation auto
!
interface GigabitEthernet1/0/1
 switchport mode access
 macsec network-link
!
interface GigabitEthernet1/0/2
!
interface GigabitEthernet1/0/3
!
interface TenGigabitEthernet1/1/1
!
interface TenGigabitEthernet1/1/2
!
interface TenGigabitEthernet1/1/3
!
interface TenGigabitEthernet1/1/4
!
interface Vlan1
 no ip address
 shutdown
!
ip forward-protocol nd
ip http server
ip http authentication local
ip http secure-server
!
ip access-list extended AutoQos-4.0-wlan-Acl-Bulk-Data
 permit tcp any any eq 22
 permit tcp any any eq 465
 permit tcp any any eq 143
 permit tcp any any eq 993
 permit tcp any any eq 995
 permit tcp any any eq 1914
 permit tcp any any eq ftp
 permit tcp any any eq ftp-data
 permit tcp any any eq smtp
 permit tcp any any eq pop3
ip access-list extended AutoQos-4.0-wlan-Acl-MultiEnhanced-Conf
 permit udp any any range 16384 32767
 permit tcp any any range 50000 59999
ip access-list extended AutoQos-4.0-wlan-Acl-Scavanger
 permit tcp any any range 2300 2400
 permit udp any any range 2300 2400
 permit tcp any any range 6881 6999
 permit tcp any any range 28800 29100
 permit tcp any any eq 1214
 permit udp any any eq 1214
 permit tcp any any eq 3689
 permit udp any any eq 3689
 permit tcp any any eq 11999
ip access-list extended AutoQos-4.0-wlan-Acl-Signaling
 permit tcp any any range 2000 2002
 permit tcp any any range 5060 5061
 permit udp any any range 5060 5061
ip access-list extended AutoQos-4.0-wlan-Acl-Transactional-Data
 permit tcp any any eq 443
 permit tcp any any eq 1521
 permit udp any any eq 1521
 permit tcp any any eq 1526
 permit udp any any eq 1526
 permit tcp any any eq 1575
 permit udp any any eq 1575
 permit tcp any any eq 1630
 permit udp any any eq 1630
 permit tcp any any eq 1527
 permit tcp any any eq 6200
 permit tcp any any eq 3389
 permit tcp any any eq 5985
 permit tcp any any eq 8080
!
!
!
ipv6 access-list preauth_ipv6_acl
 permit udp any any eq domain
 permit tcp any any eq domain
 permit icmp any any nd-ns
 permit icmp any any nd-na
 permit icmp any any router-solicitation
 permit icmp any any router-advertisement
 permit icmp any any redirect
 permit udp any eq 547 any eq 546
 permit udp any eq 546 any eq 547
 deny ipv6 any any
!
control-plane
 service-policy input system-cpp-policy
!
!
line con 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login
line vty 5 15
 login
!
!
mac address-table notification mac-move
!
!
!
!
!
end


-----show switch | Include Ready-----

*1       Active   188b.9dfc.eb00     1      V00     Ready


----- show ipv6 mld snooping address | i FF02::5:1 -----

Vlan      Group                    Type        Version     Port List
-----------------------------------------------------------------------
123       FF02::5:1                mld         v2          Gi2/0/1

Device#
```

Output fields are self-explanatory.

Related Commands

Command	Description
ipv6 mld snooping	Enables MLDv2 protocol snooping globally.
show ipv6 mld snooping	Displays MLDv2 snooping information.
show tech-support platform	Displays detailed information about a platform for use by technical support.

show tech-support port

To display port-related information for use by technical support, use the **show tech-support port** command in privileged EXEC mode.

show tech-support port

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Gibraltar 16.10.1	This command was introduced.

Usage Guidelines

The output of the **show tech-support port** command is very long. To better manage this output, you can redirect the output to an external file (for example, **show tech-support port | redirect flash:***filename*) in the local writable storage file system or remote file system.

The output of this command displays the following commands:

- **show clock**
- **show version**
- **show module**
- **show inventory**
- **show interface status**
- **show interface counters**
- **show interface counters errors**
- **show interfaces**
- **show interfaces capabilities**
- **show controllers**
- **show controllers utilization**
- **show idprom interface**
- **show controller ethernet-controller phy detail**
- **show switch**
- **show platform software fed switch active port summary**
- **show platform software fed switch ifm interfaces ethernet**
- **show platform software fed switch ifm mappings**
- **show platform software fed switch ifm mappings lpn**

- **show platform software fed switch ifm mappings gpn**
- **show platform software fed switch ifm mappings port-le**
- **show platform software fed switch ifm if-id**
- **show platform software fed switch active port if_id**

Examples

The following is sample output from the **show tech-support port** command:

```
Device# show tech-support port
.
.
.
  ----- show controllers utilization -----

Port       Receive Utilization  Transmit Utilization
Gi1/0/1       0   0
Gi1/0/2       0   0
Gi1/0/3       0   0
Gi1/0/4       0   0
Gi1/0/5       0   0
Gi1/0/6       0   0
Gi1/0/7       0   0
Gi1/0/8       0   0
Gi1/0/9       0   0
Gi1/0/10       0   0
Gi1/0/11       0   0
Gi1/0/12       0   0
Gi1/0/13       0   0
Gi1/0/14       0   0
Gi1/0/15       0   0
Gi1/0/16       0   0
Gi1/0/17       0   0
Gi1/0/18       0   0
Gi1/0/19       0   0
Gi1/0/20       0   0
Gi1/0/21       0   0
Gi1/0/22       0   0
Gi1/0/23       0   0
Gi1/0/24       0   0
Gi1/0/25       0   0
Gi1/0/26       0   0
Gi1/0/27       0   0
Gi1/0/28       0   0
Gi1/0/29       0   0
Gi1/0/30       0   0
Gi1/0/31       0   0
Gi1/0/32       0   0
Gi1/0/33       0   0
Gi1/0/34       0   0
Gi1/0/35       0   0
Gi1/0/36       0   0
Te1/0/37       0   0
Te1/0/38       0   0
Te1/0/39       0   0
Te1/0/40       0   0
Te1/0/41       0   0
Te1/0/42       0   0
Te1/0/43       0   0
Te1/0/44       0   0
```

```
Te1/0/45       0   0
Te1/0/46       0   0
Te1/0/47       0   0
Te1/0/48       0   0
Te1/1/1       0   0
Te1/1/2       0   0
Te1/1/3       0   0
Te1/1/4       0   0

Total Ports : 52
Total Ports Receive Bandwidth Percentage Utilization  : 0
Total Ports Transmit Bandwidth Percentage Utilization : 0

Average Switch  Percentage Utilization : 0


----- show idprom interface Gi1/0/1 -----


*Sep  7 08:57:24.249:  No module is present
.
.
.
```

The output fields are self-explanatory.

show tech-support pvlan

To display the private VLAN related information, use the **show tech-support pvlan** command in privileged EXEC mode.

show tech-support pvlan [{**pvlan_id** *pvlan-id*}]

Syntax Description

pvlan_id *pvlan-id*	Specifies the private VLAN ID.

Command Default

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Amsterdam 17.3.1	This command was introduced.

Usage Guidelines

The output from the **show tech-support pvlan** command is very long. To better manage this output, you can redirect the output to a file in the local writable storage file system or the remote file system by using the **show tech-support pvlan** [**pvlan_id** *pvlan-id*] | **redirect** *location:filename*) . Redirecting the output to a file also makes sending the output to your Cisco Technical Assistance Center (TAC) representative easier.

To view the output of the redirected file, use the command **more** *location:filename*.

show version

To display information about the currently loaded software along with hardware and device information, use the **show version** command in user EXEC or privileged EXEC mode.

show version [{**switch** *node*}][{**installed** | **provisioned** | **running**}]

Syntax Description

switch *node*	(optional) Only a single switch may be specified. Default is all switches in a stacked system.
running	(optional) Specifies information on the files currently running.
provisioned	(optional)Specifies information on the software files that are provisioned.
installed	Specifies information on the software installed on the RP
user-interface	Specifies information on the files related to the user-interface.

Command Default

No default behavior or values.

Command Modes

User EXEC (>)

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

This command displays information about the Cisco IOS software version currently running on a device, the ROM Monitor and Bootflash software versions, and information about the hardware configuration, including the amount of system memory. Because this command displays both software and hardware information, the output of this command is the same as the output of the **show hardware** command. (The **show hardware** command is a command alias for the **show version** command.)

Specifically, the **show version** command provides the following information:

- Software information
  - Main Cisco IOS image version
  - Main Cisco IOS image capabilities (feature set)
  - Location and name of bootfile in ROM
  - Bootflash image version (depending on platform)
- Device-specific information
  - Device name
  - System uptime
  - System reload reason
  - Config-register setting
  - Config-register settings for after the next reload (depending on platform)

- Hardware information
    - Platform type
    - Processor type
    - Processor hardware revision
    - Amount of main (processor) memory installed
    - Amount I/O memory installed
    - Amount of Flash memory installed on different types (depending on platform)
    - Processor board ID

The output of this command uses the following format:

```
Cisco IOS Software, <platform> Software (<image-id>), Version <software-version>,
  <software-type

Technical Support: http://www.cisco.com/techsupport
Copyright (c) <date-range> by Cisco Systems, Inc.
Compiled <day> <date> <time> by <compiler-id>

ROM: System Bootstrap, Version <software-version>,  <software-type>
BOOTLDR: <platform> Software (image-id), Version <software-version>,  <software-type>

<router-name> uptime is <w> weeks, <d> days, <h> hours,
<m> minutes
System returned to ROM by reload at <time> <day> <date>
System image file is "<filesystem-location>/<software-image-name>"
Last reload reason: <reload-reason>Cisco <platform-processor-type>
processor (revision <processor-revision-id>) with <free-DRAM-memory>
K/<packet-memory>K bytes of memory.
Processor board ID <ID-number

<CPU-type> CPU at <clock-speed>Mhz, Implementation <number>, Rev <
Revision-number>, <kilobytes-Processor-Cache-Memory>KB <cache-Level> Cache
```

See the Examples section for descriptions of the fields in this output.

Entering **show version** displays the IOS XE software version and the IOS XE software bundle which includes a set of individual packages that comprise the complete set of software that runs on the switch.

The **show version running** command displays the list of individual packages that are currently running on the switch. When booted in installed mode, this is typically the set of packages listed in the booted provisioning file. When booted in bundle mode, this is typically the set of packages contained in the bundle.

The **show version provisioned** command displays information about the provisioned package set.

The following is sample output from the **show version** command on a Cisco Catalyst 9300 Series Switch:

```
Device# show version
Cisco IOS XE Software, Version BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2
Cisco IOS Software [Fuji], Catalyst L3 Switch Software (CAT9K_IOSXE), Experimental Version
 16.10.20180903:072347
[v1610_throttle-/nobackup/mcpre/BLD-BLD_V1610_THROTTLE_LATEST_20180903_070602 183]
Copyright (c) 1986-2018 by Cisco Systems, Inc.
Compiled Mon 03-Sep-18 11:53 by mcpre


Cisco IOS-XE software, Copyright (c) 2005-2018 by cisco Systems, Inc.
```

```
All rights reserved.  Certain components of Cisco IOS-XE software are
licensed under the GNU General Public License ("GPL") Version 2.0.  The
software code licensed under GPL Version 2.0 is free software that comes
with ABSOLUTELY NO WARRANTY.  You can redistribute and/or modify such
GPL code under the terms of GPL Version 2.0.  For more details, see the
documentation or "License Notice" file accompanying the IOS-XE software,
or the applicable URL provided on the flyer accompanying the IOS-XE
software.


ROM: IOS-XE ROMMON
BOOTLDR: System Bootstrap, Version 16.10.1r, RELEASE SOFTWARE (P)

C9300 uptime is 20 hours, 7 minutes
Uptime for this control processor is 20 hours, 8 minutes
System returned to ROM by Image Install
System image file is "flash:packages.conf"
Last reload reason: Image Install



This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to
export@cisco.com.


Technology Package License Information:

------------------------------------------------------------------------------
Technology-package                                     Technology-package
Current                        Type                       Next reboot
------------------------------------------------------------------------------
network-advantage       Smart License                     network-advantage
dna-advantage           Subscription Smart License        dna-advantage


Smart Licensing Status: UNREGISTERED/EVAL MODE

cisco C9300-24U (X86) processor with 1415813K/6147K bytes of memory.
Processor board ID FCW2125L0BH
8 Virtual Ethernet interfaces
56 Gigabit Ethernet interfaces
16 Ten Gigabit Ethernet interfaces
4 TwentyFive Gigabit Ethernet interfaces
4 Forty Gigabit Ethernet interfaces
2048K bytes of non-volatile configuration memory.
8388608K bytes of physical memory.
1638400K bytes of Crash Files at crashinfo:.
1638400K bytes of Crash Files at crashinfo-2:.
11264000K bytes of Flash at flash:.
11264000K bytes of Flash at flash-2:.
0K bytes of WebUI ODM Files at webui:.
```

```
Base Ethernet MAC Address          : 70:d3:79:be:6c:80
Motherboard Assembly Number        : 73-17954-06
Motherboard Serial Number          : FOC21230KPX
Model Revision Number              : A0
Motherboard Revision Number        : A0
Model Number                       : C9300-24U
System Serial Number               : FCW2125L0BH


Switch Ports Model              SW Version        SW Image              Mode
------ ----- -----              ----------        ----------            ----
*    1 40    C9300-24U          16.10.1           CAT9K_IOSXE           INSTALL
     2 40    C9300-24U          16.10.1           CAT9K_IOSXE           INSTALL


Switch 02
---------
Switch uptime                      : 20 hours, 8 minutes

Base Ethernet MAC Address          : 70:d3:79:84:85:80
Motherboard Assembly Number        : 73-17954-06
Motherboard Serial Number          : FOC21230KPK
Model Revision Number              : A0
Motherboard Revision Number        : A0
Model Number                       : C9300-24U
System Serial Number               : FCW2125L03W
Last reload reason                 : Image Install

Configuration register is 0x102
```

In the following example, the **show version running** command is entered on a Cisco Catalyst 9300 Series Switch to view information about the packages currently running on both switches in a 2-member stack:

```
Device# show version running
Package: Provisioning File, version: n/a, status: active
  Role: provisioning file
  File: /flash/packages.conf, on: RP0
  Built: n/a, by: n/a
  File SHA1 checksum: 6a43991bae5b94de0df8083550f827a3c01756c5

Package: rpbase, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2, status:
 active
  Role: rp_base
  File: /flash/cat9k-rpbase.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg,
 on: RP0
  Built: 2018-09-03_13.11, by: mcpre
  File SHA1 checksum: 78331327788b2cd00624043d71a15094bd19d885

Package: rpboot, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2, status:
 active
  Role: rp_boot
  File: /flash/cat9k-rpboot.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg,
 on: RP0
  Built: 2018-09-03_13.11, by: mcpre
  File SHA1 checksum: n/a

Package: guestshell, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2,
status: active
  Role: guestshell
  File:
/flash/cat9k-guestshell.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg,
on: RP0/0
```

```
  Built: 2018-09-03_13.11, by: mcpre
  File SHA1 checksum: 10827f9f9db3b016d19a926acc6be0541440b8d7

Package: rpbase, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2, status:
 active
  Role: rp_daemons
  File: /flash/cat9k-rpbase.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg,
 on: RP0/0
  Built: 2018-09-03_13.11, by: mcpre
  File SHA1 checksum: 78331327788b2cd00624043d71a15094bd19d885

Package: rpbase, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2, status:
 active
  Role: rp_iosd
  File: /flash/cat9k-rpbase.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg,
 on: RP0/0
  Built: 2018-09-03_13.11, by: mcpre
  File SHA1 checksum: 78331327788b2cd00624043d71a15094bd19d885

Package: rpbase, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2, status:
 active
  Role: rp_security
  File: /flash/cat9k-rpbase.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg,
 on: RP0/0
  Built: 2018-09-03_13.11, by: mcpre
  File SHA1 checksum: 78331327788b2cd00624043d71a15094bd19d885

Package: webui, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2, status:
 active
  Role: rp_webui
  File: /flash/cat9k-webui.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg,
 on: RP0/0
  Built: 2018-09-03_13.11, by: mcpre
  File SHA1 checksum: 5112d7749b38fa1e122ce6ee1bfb266ad7eb553a

Package: srdriver, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2, status:
 active
  Role: srdriver
  File:
/flash/cat9k-srdriver.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg, on:
 RP0/0
  Built: 2018-09-03_13.11, by: mcpre
  File SHA1 checksum: aff411e981a8dfc8de14005cc33462dc69f8bfaf

Package: cc_srdriver, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2,
status: active
  Role: cc_srdriver
  File:
/flash/cat9k-cc_srdriver.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg,
 on: SIP0
  Built: 2018-09-03_13.11, by: mcpre
  File SHA1 checksum: e3da784f3e61ef1e153028e53d9dc94b2c9b1bf7
```

In the following example, the **show version provisioned** command is entered on a Cisco Catalyst 9300 Series Switch that is the active switch in a 2-member stack. The **show version provisioned** command displays information about the packages in the provisioned package set.

```
Device# show version provisioned
Package: Provisioning File, version: n/a, status: active
  Role: provisioning file
  File: /flash/packages.conf, on: RP0
  Built: n/a, by: n/a
  File SHA1 checksum: 6a43991bae5b94de0df8083550f827a3c01756c5
```

```
Package: rpbase, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2, status:
 n/a
  Role: rp_base
  File: /flash/cat9k-rpbase.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg,
 on: RP0
  Built: 2018-09-03_13.11, by: mcpre
  File SHA1 checksum: 78331327788b2cd00624043d71a15094bd19d885

Package: guestshell, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2,
status: n/a
  Role: guestshell
  File:
/flash/cat9k-guestshell.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg,
on: RP0
  Built: 2018-09-03_13.11, by: mcpre
  File SHA1 checksum: 10827f9f9db3b016d19a926acc6be0541440b8d7

Package: rpboot, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2, status:
 n/a
  Role: rp_boot
  File: /flash/cat9k-rpboot.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg,
 on: RP0
  Built: 2018-09-03_13.11, by: mcpre
  File SHA1 checksum: n/a

Package: rpbase, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2, status:
 n/a
  Role: rp_daemons
  File: /flash/cat9k-rpbase.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg,
 on: RP0
  Built: 2018-09-03_13.11, by: mcpre
  File SHA1 checksum: 78331327788b2cd00624043d71a15094bd19d885

Package: rpbase, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2, status:
 n/a
  Role: rp_iosd
  File: /flash/cat9k-rpbase.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg,
 on: RP0
  Built: 2018-09-03_13.11, by: mcpre
  File SHA1 checksum: 78331327788b2cd00624043d71a15094bd19d885

Package: rpbase, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2, status:
 n/a
  Role: rp_security
  File: /flash/cat9k-rpbase.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg,
 on: RP0
  Built: 2018-09-03_13.11, by: mcpre
  File SHA1 checksum: 78331327788b2cd00624043d71a15094bd19d885

Package: webui, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2, status:
 n/a
  Role: rp_webui
  File: /flash/cat9k-webui.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg,
 on: RP0
  Built: 2018-09-03_13.11, by: mcpre
  File SHA1 checksum: 5112d7749b38fa1e122ce6ee1bfb266ad7eb553a

Package: wlc, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2, status:
n/a
  Role: rp_wlc
  File: /flash/cat9k-wlc.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg,
 on: RP0
  Built: 2018-09-03_13.11, by: mcpre
  File SHA1 checksum: ada21bb3d57e1b03e5af2329503ed6caa7236d6e

Package: srdriver, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2, status:
 n/a
  Role: srdriver
  File:
/flash/cat9k-srdriver.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg, on:
 RP0
  Built: 2018-09-03_13.11, by: mcpre
  File SHA1 checksum: aff411e981a8dfc8de14005cc33462dc69f8bfaf

Package: espbase, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2, status:
 n/a
  Role: fp
  File: /flash/cat9k-espbase.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg,
 on: ESP0
  Built: 2018-09-03_13.11, by: mcpre
  File SHA1 checksum: 1a2317485f285a3945b31ae57aa64c56ed30a8c0

Package: sipbase, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2, status:
 n/a
  Role: cc
  File: /flash/cat9k-sipbase.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg,
 on: SIP0
  Built: 2018-09-03_13.11, by: mcpre
  File SHA1 checksum: ce821195f0c0bd5e44f21e32fca76cf9b2eed02b

Package: sipspa, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2, status:
 n/a
  Role: cc_spa
  File: /flash/cat9k-sipspa.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg,
 on: SIP0
  Built: 2018-09-03_13.11, by: mcpre
  File SHA1 checksum: 54645404860b662d72f8ff7fa5e6e88cb0960e20

Package: cc_srdriver, version: BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2,
status: n/a
  Role: cc_srdriver
  File:
/flash/cat9k-cc_srdriver.BLD_V1610_THROTTLE_LATEST_20180903_070602_V16_10_0_101_2.SSA.pkg,
 on: SIP0
  Built: 2018-09-03_13.11, by: mcpre
  File SHA1 checksum: e3da784f3e61ef1e153028e53d9dc94b2c9b1bf7
```

Table 11: Table 5, show version running Field Descriptions

Field	Description
Package:	The individual sub-package name.
version:	The individual sub-package version.
status:	Reveals if the package is active or inactive for the specific Supervisor module.
File:	The filename of the individual package file.
on:	The slot number of the Active or Standby Supervisor that this package is running on.
Built:	The date the individual package was built.

system env temperature threshold yellow

To configure the difference between the yellow and red temperature thresholds that determines the value of yellow threshold, use the **system env temperature threshold yellow** command in global configuration mode. To return to the default value, use the **no** form of this command.

system env temperature threshold yellow *value*
no system env temperature threshold yellow *value*

Syntax Description

value	Specifies the difference between the yellow and red threshold values (in Celsius). The range is 10 to 25.

Command Default

These are the default values

Table 12: Default Values for the Temperature Thresholds

Device	Difference between Yellow and Red	Red[1]
	14°C	60°C

[1] You cannot configure the red temperature threshold.

Command Modes

Global configuration

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

You cannot configure the green and red thresholds but can configure the yellow threshold. Use the **system env temperature threshold yellow** *value* global configuration command to specify the difference between the yellow and red thresholds and to configure the yellow threshold. For example, if the red threshold is 66 degrees C and you want to configure the yellow threshold as 51 degrees C, set the difference between the thresholds as 15 by using the **system env temperature threshold yellow 15** command. For example, if the red threshold is 60 degrees C and you want to configure the yellow threshold as 51 degrees C, set the difference between the thresholds as 15 by using the **system env temperature threshold yellow 9** command.

Note The internal temperature sensor in the device measures the internal system temperature and might vary ±5 degrees C.

Examples

This example sets 15 as the difference between the yellow and red thresholds:

```
Device(config)# system env temperature threshold yellow 15
Device(config)#
```

traceroute mac

To display the Layer 2 path taken by the packets from the specified source MAC address to the specified destination MAC address, use the **traceroute mac** command in privileged EXEC mode.

traceroute mac [**interface** *interface-id*] *source-mac-address* [**interface** *interface-id*] *destination-mac-address* [**vlan** *vlan-id*] [**detail**]

Syntax Description

interface *interface-id*	(Optional) Specifies an interface on the source or destination device.
source-mac-address	The MAC address of the source device in hexadecimal format.
destination-mac-address	The MAC address of the destination device in hexadecimal format.
vlan *vlan-id*	(Optional) Specifies the VLAN on which to trace the Layer 2 path that the packets take from the source device to the destination device. Valid VLAN IDs are 1 to 4094.
detail	(Optional) Specifies that detailed information appears.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.
Cisco IOS XE Bengaluru 17.5.1	**aborted** was replaced with **terminated** in the output error message for the **traceroute mac** command.

Usage Guidelines

For Layer 2 traceroute to function properly, Cisco Discovery Protocol (CDP) must be enabled on all of the devices in the network. Do not disable CDP.

When the device detects a device in the Layer 2 path that does not support Layer 2 traceroute, the device continues to send Layer 2 trace queries and lets them time out.

The maximum number of hops identified in the path is ten.

Layer 2 traceroute supports only unicast traffic. If you specify a multicast source or destination MAC address, the physical path is not identified, and an error message appears.

The **traceroute mac** command output shows the Layer 2 path when the specified source and destination addresses belong to the same VLAN.

If you specify source and destination addresses that belong to different VLANs, the Layer 2 path is not identified, and an error message appears.

If the source or destination MAC address belongs to multiple VLANs, you must specify the VLAN to which both the source and destination MAC addresses belong.

If the VLAN is not specified, the path is not identified, and an error message appears.

The Layer 2 traceroute feature is not supported when multiple devices are attached to one port through hubs (for example, multiple CDP neighbors are detected on a port).

When more than one CDP neighbor is detected on a port, the Layer 2 path is not identified, and an error message appears.

This feature is not supported in Token Ring VLANs.

Examples

This example shows how to display the Layer 2 path by specifying the source and destination MAC addresses:

```
Device# traceroute mac 0000.0201.0601 0000.0201.0201
  Source 0000.0201.0601 found on con6[WS-C3750E-24PD] (2.2.6.6)
  con6 (2.2.6.6) :Gi0/0/1 => Gi0/0/3
  con5                 (2.2.5.5        )  :    Gi0/0/3 => Gi0/0/1
  con1                 (2.2.1.1        )  :    Gi0/0/1 => Gi0/0/2
  con2                 (2.2.2.2        )  :    Gi0/0/2 => Gi0/0/1
  Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
  Layer 2 trace completed
```

This example shows how to display the Layer 2 path by using the **detail** keyword:

```
Device# traceroute mac 0000.0201.0601 0000.0201.0201 detail
  Source 0000.0201.0601 found on con6[WS-C3750E-24PD] (2.2.6.6)
  con6 / WS-C3750E-24PD / 2.2.6.6 :
          Gi0/0/2 [auto, auto] => Gi0/0/3 [auto, auto]
  con5 / WS-C2950G-24-EI / 2.2.5.5 :
          Fa0/3 [auto, auto] => Gi0/1 [auto, auto]
  con1 / WS-C3550-12G / 2.2.1.1 :
          Gi0/1 [auto, auto] => Gi0/2 [auto, auto]
  con2 / WS-C3550-24 / 2.2.2.2 :
          Gi0/2 [auto, auto] => Fa0/1 [auto, auto]
  Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
  Layer 2 trace completed.
```

This example shows how to display the Layer 2 path by specifying the interfaces on the source and destination devices:

```
Device# traceroute mac interface fastethernet0/1 0000.0201.0601 interface fastethernet0/3
0000.0201.0201
  Source 0000.0201.0601 found on con6[WS-C3750E-24PD] (2.2.6.6)
  con6 (2.2.6.6) :Gi0/0/1 => Gi0/0/3
  con5                 (2.2.5.5        )  :    Gi0/0/3 => Gi0/0/1
  con1                 (2.2.1.1        )  :    Gi0/0/1 => Gi0/0/2
  con2                 (2.2.2.2        )  :    Gi0/0/2 => Gi0/0/1
  Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
  Layer 2 trace completed
```

This example shows the Layer 2 path when the device is not connected to the source device:

```
Device# traceroute mac 0000.0201.0501 0000.0201.0201 detail
  Source not directly connected, tracing source .....
  Source 0000.0201.0501 found on con5[WS-C3750E-24TD] (2.2.5.5)
  con5 / WS-C3750E-24TD / 2.2.5.5 :
          Gi0/0/1 [auto, auto] => Gi0/0/3 [auto, auto]
  con1 / WS-C3550-12G / 2.2.1.1 :
          Gi0/1 [auto, auto] => Gi0/2 [auto, auto]
  con2 / WS-C3550-24 / 2.2.2.2 :
          Gi0/2 [auto, auto] => Fa0/1 [auto, auto]
  Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
  Layer 2 trace completed.
```

This example shows the Layer 2 path when the device cannot find the destination port for the source MAC address:

```
Device# traceroute mac 0000.0011.1111 0000.0201.0201
  Error:Source Mac address not found.
  Layer2 trace terminated.
```

This example shows the Layer 2 path when the source and destination devices are in different VLANs:

```
Device# traceroute mac 0000.0201.0601 0000.0301.0201
  Error:Source and destination macs are on different vlans.
  Layer2 trace terminated.
```

This example shows the Layer 2 path when the destination MAC address is a multicast address:

```
Device# traceroute mac 0000.0201.0601 0100.0201.0201
  Invalid destination mac address
```

This example shows the Layer 2 path when source and destination devices belong to multiple VLANs:

```
Device# traceroute mac 0000.0201.0601 0000.0201.0201
  Error:Mac found on multiple vlans.
  Layer2 trace terminated.
```

traceroute mac ip

To display the Layer 2 path taken by the packets from the specified source IP address or hostname to the specified destination IP address or hostname, use the **traceroute mac ip** command in privileged EXEC mode.

traceroute mac ip { *source-ip-address source-hostname* } { *destination-ip-address destination-hostname* } [**detail**]

Syntax Description

source-ip-address	The IP address of the source device as a 32-bit quantity in dotted-decimal format.
source-hostname	The IP hostname of the source device.
destination-ip-address	The IP address of the destination device as a 32-bit quantity in dotted-decimal format.
destination-hostname	The IP hostname of the destination device.
detail	(Optional) Specifies that detailed information appears.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.
Cisco IOS XE Bengaluru 17.5.1	**aborted** was replaced with **terminated** in the output error message for the **traceroute mac ip** command.

Usage Guidelines

For Layer 2 traceroute to function properly, Cisco Discovery Protocol (CDP) must be enabled on each device in the network. Do not disable CDP.

When the device detects a device in the Layer 2 path that does not support Layer 2 traceroute, the device continues to send Layer 2 trace queries and lets them time out.

The maximum number of hops identified in the path is ten.

The **traceroute mac ip** command output shows the Layer 2 path when the specified source and destination IP addresses are in the same subnet.

When you specify the IP addresses, the device uses Address Resolution Protocol (ARP) to associate the IP addresses with the corresponding MAC addresses and the VLAN IDs.

- If an ARP entry exists for the specified IP address, the device uses the associated MAC address and identifies the physical path.
- If an ARP entry does not exist, the device sends an ARP query and tries to resolve the IP address. The IP addresses must be in the same subnet. If the IP address is not resolved, the path is not identified, and an error message appears.

The Layer 2 traceroute feature is not supported when multiple devices are attached to one port through hubs (for example, multiple CDP neighbors are detected on a port).

When more than one CDP neighbor is detected on a port, the Layer 2 path is not identified, and an error message appears.

This feature is not supported in Token Ring VLANs.

Examples

This example shows how to display the Layer 2 path by specifying the source and destination IP addresses and by using the **detail** keyword:

```
Device# traceroute mac ip 2.2.66.66 2.2.22.22 detail
Translating IP to mac .....
2.2.66.66 => 0000.0201.0601
2.2.22.22 => 0000.0201.0201

Source 0000.0201.0601 found on con6[WS-C2950G-24-EI] (2.2.6.6)
con6 / WS-C3750E-24TD / 2.2.6.6 :
        Gi0/0/1 [auto, auto] => Gi0/0/3 [auto, auto]
con5 / WS-C2950G-24-EI / 2.2.5.5 :
        Fa0/3 [auto, auto] => Gi0/1 [auto, auto]
con1 / WS-C3550-12G / 2.2.1.1 :
        Gi0/1 [auto, auto] => Gi0/2 [auto, auto]
con2 / WS-C3550-24 / 2.2.2.2 :
        Gi0/2 [auto, auto] => Fa0/1 [auto, auto]
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed.
```

This example shows how to display the Layer 2 path by specifying the source and destination hostnames:

```
Device# traceroute mac ip con6 con2
Translating IP to mac .....
2.2.66.66 => 0000.0201.0601
2.2.22.22 => 0000.0201.0201

Source 0000.0201.0601 found on con6
con6 (2.2.6.6) :Gi0/0/1 => Gi0/0/3
con5                 (2.2.5.5        )  :    Gi0/0/3 => Gi0/1
con1                 (2.2.1.1        )  :    Gi0/0/1 => Gi0/2
con2                 (2.2.2.2        )  :    Gi0/0/2 => Fa0/1
Destination 0000.0201.0201 found on con2
Layer 2 trace completed
```

This example shows the Layer 2 path when ARP cannot associate the source IP address with the corresponding MAC address:

```
Device# traceroute mac ip 2.2.66.66 2.2.77.77
Arp failed for destination 2.2.77.77.
Layer2 trace terminated.
```

type

To display the contents of one or more files, use the **type** command in boot loader mode.

type *filesystem:/file-url...*

Syntax Description

filesystem:	Alias for a file system. Use **flash:** for the system board flash device; use **usbflash0:** for USB memory sticks.
/file-url...	Path (directory) and name of the files to display. Separate each filename with a space.

Command Default

No default behavior or values.

Command Modes

Boot loader

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Filenames and directory names are case sensitive.

If you specify a list of files, the contents of each file appear sequentially.

Examples

This example shows how to display the contents of a file:

```
Device: type flash:image_file_name
version_suffix: universal-122-xx.SEx
version_directory: image_file_name
image_system_type_id: 0x00000002
image_name: image_file_name.bin
ios_image_file_size: 8919552
total_image_file_size: 11592192
image_feature: IP|LAYER_3|PLUS|MIN_DRAM_MEG=128
image_family: family
stacking_number: 1.34
board_ids: 0x00000068 0x00000069 0x0000006a 0x0000006b
info_end:
```

unset

To reset one or more environment variables, use the **unset** command in boot loader mode.

unset *variable...*

Syntax Description

variable	Use one of these keywords for *variable*: **MANUAL_BOOT**—Specifies whether the device automatically or manually boots.
	BOOT—Resets the list of executable files to try to load and execute when automatically booting. If the BOOT environment variable is not set, the system attempts to load and execute the first executable image it can find by using a recursive, depth-first search through the flash: file system. If the BOOT variable is set but the specified images cannot be loaded, the system attempts to boot the first bootable file that it can find in the flash: file system.
	ENABLE_BREAK—Specifies whether the automatic boot process can be interrupted by using the **Break** key on the console after the flash: file system has been initialized.
	HELPER—Identifies the semicolon-separated list of loadable files to dynamically load during the boot loader initialization. Helper files extend or patch the functionality of the boot loader.
	PS1—Specifies the string that is used as the command-line prompt in boot loader mode.
	CONFIG_FILE—Resets the filename that Cisco IOS uses to read and write a nonvolatile copy of the system configuration.
	BAUD—Resets the rate in bits per second (b/s) used for the console. The Cisco IOS software inherits the baud rate setting from the boot loader and continues to use this value unless the configuration file specifies another setting.

Command Default

No default behavior or values.

Command Modes

Boot loader

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Usage Guidelines

Under typical circumstances, it is not necessary to alter the setting of the environment variables.

The MANUAL_BOOT environment variable can also be reset by using the **no boot manual** global configuration command.

The BOOT environment variable can also be reset by using the **no boot system** global configuration command.

The ENABLE_BREAK environment variable can also be reset by using the **no boot enable-break** global configuration command.

The HELPER environment variable can also be reset by using the **no boot helper** global configuration command.

The CONFIG_FILE environment variable can also be reset by using the **no boot config-file** global configuration command.

Example

This example shows how to unset the SWITCH_PRIORITY environment variable:

```
Device: unset SWITCH_PRIORITY
```

version

To display the boot loader version, use the **version** command in boot loader mode.

version [*-v*]

Syntax Description

-v	Displays Hardware Anchor, Microloader, Firmware-DDR and ROMMON Revision versions.

Command Default

No default behavior or values.

Command Modes

Boot loader

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.2	This command was introduced.

Examples

This example shows how to display the boot loader version on a device:

```
Device: version -v
System Bootstrap, Version 16.10.1r, RELEASE SOFTWARE (P)
Compiled Tue 09/04/2018 22:58:10 by rel

Current ROMMON image : Primary
C9200-48P-4X platform with 2097152 Kbytes of main memory

HARDWARE ANCHOR : v027.0  crayprod_20160517 20160517-2135
MICROLOADER     : v061.0  rel_16_10_1r 20180904-2252
FIRMWARE-DDR    : v011.0  rel_16_10_1r 20180904-2254
ROMMON REVISION : v010.003
```