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 3.3SECisco IOS XE 3.3SE	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 [**-post** | **-n** | **-p** | *flag*] *filesystem:/file-url...*

Syntax Description		
	-post	(Optional) Run the loaded image with an extended or comprehensive power-on self-test (POST). Using this keyword causes POST to take longer to complete.
	-n	(Optional) Pause for the Cisco IOS Debugger immediately after launching.
	-p	(Optional) Pause for the JTAG Debugger right after loading the image.
	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 3.3SECisco IOS XE 3.3SE	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.

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 3.3SECisco IOS XE 3.3SE	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:
```

clear location

To clear a specific radio frequency identification (RFID) tag or all of the RFID tags information in the entire database, use the **clear location** command in EXEC mode.

clear location [mac-address *mac-address* | **rfid]**

Syntax Description

mac-address *mac-address*	MAC address of a specific RFID tag.
rfid	Specifies all of the RFID tags in the database.

Command Default No default behavior or values.

Command Modes User EXEC

Privileged EXEC

Command History	Release	Modification
	Cisco IOS XE 3.3SECisco IOS XE 3.3SE	This command was introduced.

This example shows how to clear information about all of the RFID tags in the database:

```
Device> clear location rfid
```

clear location statistics

To clear radio-frequency identification (RFID) statistics, use the **clear location statistics** command in EXEC mode.

clear location statistics

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	Modification
	Cisco IOS XE 3.3SECisco IOS XE 3.3SE	This command was introduced.

The following is sample output from the **clear location rfid** command and shows how to clear RFID statistics:

```
Device> clear location statistics
```

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 3.3SECisco IOS XE 3.3SE	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 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 16.11.1	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 16.11.1	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 16.11.1	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 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 3.3SECisco IOS XE 3.3SE	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
```

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 3.3SECisco IOS XE 3.3SE	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 3.3SECisco IOS XE 3.3SE	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
1644045	Size of the file.
<date>	Last modification date.
env_vars	Filename.

emergency-install

To perform an emergency installation on your system, use the **emergency-install** command in boot loader mode.

emergency-install *url://<url>*

Syntax Description   *<url>*   URL and name of the file containing the emergency installation bundle image.

Command Default   No default behavior or values.

Command Modes   Boot loader

Command History	Release	Modification
	Cisco IOS XE 3.3SECisco IOS XE 3.3SE	This command was introduced.

Usage Guidelines The boot flash is erased during the installation operation.

Example

This example shows how to perform the emergency install operation using the contents of an image file:

```
Device: emergency-install tftp:<url>
The bootflash will be erased during install operation, continue (y/n)?y
Starting emergency recovery (tftp:<url> ...
Reading full image into memory......................done
Nova Bundle Image
--------------------------------------
Kernel Address    : 0x6042d5c8
Kernel Size       : 0x317ccc/3243212
Initramfs Address : 0x60745294
Initramfs Size    : 0xdc6774/14444404
Compression Format: .mzip

Bootable image at @ ram:0x6042d5c8
Bootable image segment 0 address range [0x81100000, 0x81b80000] is in range        \
[0x80180000, 0x90000000].
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
File "sda9:c3850-recovery.bin" uncompressed and installed, entry point: 0x811060f0
Loading Linux kernel with entry point 0x811060f0 ...
Bootloader: Done loading app on core_mask: 0xf

### Launching Linux Kernel (flags = 0x5)


Initiating Emergency Installation of bundle                                        \
tftp:<url>


Downloading bundle tftp:<url>...

Validating bundle tftp:<url>...
Installing bundle tftp:<url>...
Verifying bundle tftp:<url>...
Package cat3k_caa-base.SPA.03.02.00SE.pkg is Digitally Signed
Package cat3k_caa-drivers.SPA.03.02.00.SE.pkg is Digitally Signed
Package cat3k_caa-infra.SPA.03.02.00SE.pkg is Digitally Signed
Package cat3k_caa-iosd-universalk9.SPA.150-1.EX.pkg is Digitally Signed
Package cat3k_caa-platform.SPA.03.02.00.SE.pkg is Digitally Signed
Package cat3k_caa-wcm.SPA.10.0.100.0.pkg is Digitally Signed
Preparing flash...
Syncing device...
Emergency Install successful... Rebooting
Restarting system.\ufffd


Booting...(use DDR clock 667 MHz)Initializing and Testing RAM                       \
+++@@@@####...++@@++@@++@@++@@++@@++@@++@@++@@done.
Memory Test Pass!
```

```
Base ethernet MAC Address: 20:37:06:ce:25:80
Initializing Flash...

flashfs[7]: 0 files, 1 directories
flashfs[7]: 0 orphaned files, 0 orphaned directories
flashfs[7]: Total bytes: 6784000
flashfs[7]: Bytes used: 1024
flashfs[7]: Bytes available: 6782976
flashfs[7]: flashfs fsck took 1 seconds....done Initializing Flash.

The system is not configured to boot automatically. The
following command will finish loading the operating system
software:

    boot
```

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 3.3SECisco IOS XE 3.3SE	This command was introduced.

This example shows how to exit the configuration mode:

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

factory-reset

To remove all the customer specific data that has been added on the device since the time of shipping from the factory, use the **factory-reset** command in the Privileged EXEC mode.

factory-reset {**all** | **config** | **boot-vars**}

Syntax Description	**all**	Removes all the data from the device, including configuration data, crash information, log files, boot variables, core files, IOS images including the current boot image.
	config	Removes all the configuration data, including user data, startup, and running configuration.
	boot-vars	Resets boot variables.

Command Default   There are no defaults for this command.

Command Modes   Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 16.6.1	This command was introduced.

Usage Guidelines   No system configuration is required to use the **factory-reset** command. Use the command with all options enabled.

The **factory-reset** command erases IOS images, boot variables, configuration data and all user data. Data can be in the form of configuration, log files, boot variables, and core files.

The system reloads to perform the factory reset and boots into ROMMON mode.

After the **factory reset** command is executed, you can load the IOS image from ROMMON using USB or TFTP.

✎

Note   Do not unplug the power or interrupt the factory reset operation.

This command is used in the following two scenarios:

- Return Material Authorization (RMA) for a device: If you have to return a device to Cisco for RMA, remove all customer-specific data before obtaining a RMA certificate for the device.

- Recovering the compromised device: If the key material or credentials stored on a device is compromised, reset the device to factory configuration and then reconfigure the device.

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 3.3SECisco IOS XE 3.3SE	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 3.3SECisco IOS XE 3.3SE	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
```

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: | pram: | 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, it triggers post-install scripts to restart the necessary processes, or triggers a reload for non-restartable 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 automatic timer to terminate the installation.
	prompt-level {**all**	**none**}	(Optional) Prompts the 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 will prompt users as to whether they want to continue.
		The **all** keyword allows you to enable prompts. The **none** keyword disables prompts.
	add	Copies files from a remote location (via FTP, TFTP) to a device and performs Software Maintenance Upgrade (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. It also adds an entry in the package file, so that the status can be monitored and maintained.
	{ **bootflash:**	**flash:** |**ftp:** |**harddisk:** |**http:** |**https:**	**pram:** |**rcp:**	**scp:**	**tftp:** |**webui:**}	Specifies the package to be added.

commit	Makes SMU changes persistent over reloads.
	You can do 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 automatic timer for installation.
deactivate	Deactivates an installed package.
	Deactivating a package also updates the package status and triggers a process restart or a reload.
label *id*	Specifies the id of the install point to label.
description	Adds a description to specified install point.
label-name *name*	Adds a description to specified install point.
remove	Remove installed packages.
	The package file is removed from the file system. The **remove** keyword can only be used on packages that are currently inactive.
inactive	Removes all inactive packages from the device.
rollback	Rollbacks the data model interface (DMI) package (DMP) 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 Everest 16.6.1	This command was introduced.

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 contain a minimal set of files for patching the release along with some metadata that describes the contents of the package.

Packages must be added prior to activating the SMU.

A package must be deactivated, before it is removed from the bootflash. A removed packaged must be added again.

Example

The following example shows how to add an install package on a device:

```
Device# install add file tftp://172.16.0.1//tftpboot/folder1/cat3k-
universalk9.2017-01-10_13.15.1.CSCxxxxxxx.SSA.dmp.bin

install_add: START Sun Feb 26 05:57:04 UTC 2017
Downloading file tftp://172.16.0.1//tftpboot/folder1/cat3k-universalk9.2017-01-10_13.15.1.
CSCvb12345.SSA.dmp.bin
Finished downloading file
tftp://172.16.0.1//tftpboot/folder1/cat3k-universalk9.2017-01-10_13.15.1.
CSCxxxxxxx.SSA.dmp.bin to
bootflash:cat3k-universalk9.2017-01-10_13.15.1.CSCxxxxxxx.SSA.dmp.bin
SUCCESS: install_add /bootflash/cat3k-universalk9.2017-01-10_13.15.1.CSCxxxxxxx.SSA.dmp.bin

Sun Feb 26 05:57:22 UTC 2017
```

The following example shows how to activate an install package:

```
Device# install activate file bootflash:cat3k-universalk9.2017-01-10_13.15.1.
CSCxxxxxxx.SSA.dmp.bin

install_activate: START Sun Feb 26 05:58:41 UTC 2017
DMP package.
Netconf processes stopped
SUCCESS: install_activate
/bootflash/cat3k-universalk9.2017-01-10_13.15.1.CSCxxxxxxx.SSA.dmp.bin
Sun Feb 26 05:58:58 UTC 2017
*Feb 26 05:58:47.655: %DMI-4-CONTROL_SOCKET_CLOSED:  SIP0: nesd:
Confd control socket closed Lost connection to ConfD (45): EOF on socket to ConfD.
*Feb 26 05:58:47.661: %DMI-4-SUB_READ_FAIL:  SIP0: vtyserverutild:
Confd subscription socket read failed Lost connection to ConfD (45):
EOF on socket to ConfD.
*Feb 26 05:58:47.667: %DMI-4-CONTROL_SOCKET_CLOSED:  SIP0: syncfd:
Confd control socket closed Lost connection to ConfD (45): EOF on socket to ConfD.
*Feb 26 05:59:43.269: %DMI-5-SYNC_START:  SIP0: syncfd:
External change to running configuration detected.
The running configuration will be synchronized to the NETCONF running data store.
*Feb 26 05:59:44.624: %DMI-5-SYNC_COMPLETE:  SIP0: syncfd:
The running configuration has been synchronized to the NETCONF running data store.
```

The following example shows how to commit an installed package:

```
Device# install commit

install_commit: START Sun Feb 26 06:46:48 UTC 2017
SUCCESS: install_commit  Sun Feb 26 06:46:52 UTC 2017
```

The following example shows how to rollback to the base SMU package:

```
Device# install rollback to base

install_rollback: START Sun Feb 26 06:50:29 UTC 2017
7 install_rollback: Restarting impacted processes to take effect
7 install_rollback: restarting confd

*Feb 26 06:50:34.957: %DMI-4-CONTROL_SOCKET_CLOSED:  SIP0: syncfd:
```

```
Confd control socket closed Lost connection to ConfD (45): EOF on socket to ConfD.
*Feb 26 06:50:34.962: %DMI-4-CONTROL_SOCKET_CLOSED:  SIP0: nesd:
Confd control socket closed Lost connection to ConfD (45): EOF on socket to ConfD.
*Feb 26 06:50:34.963: %DMI-4-SUB_READ_FAIL:  SIP0: vtyserverutild:
Confd subscription socket read failed Lost connection to ConfD (45):
EOF on socket to ConfD.Netconf processes stopped
7 install_rollback: DMP activate complete
SUCCESS: install_rollback  Sun Feb 26 06:50:41 UTC 2017
*Feb 26 06:51:28.901: %DMI-5-SYNC_START:  SIP0: syncfd:
External change to running configuration detected.
The running configuration will be synchronized to the NETCONF running data store.
*Feb 26 06:51:30.339: %DMI-5-SYNC_COMPLETE:  SIP0: syncfd:
The running configuration has been synchronized to the NETCONF running data store.
```

Related Commands	Command	Description
	show install	Displays information about install packages.

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 3.3SE	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 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 *base-license-level* **addon** *addon-license-level*
no license boot level

Syntax Description	*base-license-level*	Level at which the switch is booted, for example, **ipservice**
		Base licenses that are available are:
		• LAN Base
		• IP Base
		• IP Service
	addon-license-level	Additional licenses that can be subscribed for a fixed term of three, five, or seven years.
		Add-on licenses that are available are:
		• Digital Networking Architecture (DNA) Essentials
		• DNA Advantage (includes DNA Essentials)

Command Default The switch boots the configured image.

Command Modes Global configuration (config)

Command History

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

Usage Guidelines 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.

Examples The following example shows how to activate the *ipbase* license on a switch at the next reload:

```
Device(config)# license boot level ipbase
```

license smart conversion start

To migrate all the installed traditional licenses from the device to Cisco Smart Software Manager (CSSM), use the **license smart conversion start** command in privileged EXEC mode.

license smart conversion   start

Syntax Description   This command has no arguments or keywords.

Command Default   Privileged EXEC (#)

Command History

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

Usage Guidelines   On executing the **license smart conversion start** command, the device converts the traditional license and sends the migration data to CSSM. CSSM creates license entitlements, which is deposited in the user account.

> **Note**   License conversion takes an hour or more to complete.

Examples   The following shows how to start license conversion:

```
Device# license smart conversion start
```

Related Commands

Command	Description
license smart conversion stop	Cancels license conversion
show license status	Displays compliance status of a license.
show license usage	Displays license usage information

license smart conversion stop

To cancel license conversion if network failure occurs, use the **license smart conversion stop** command in privileged EXEC mode.

license smart conversion   stop

Syntax Description   This command has no arguments or keywords.

Command Default   Privileged EXEC (#)

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

Example

This example shows how to stop license conversion:

```
Device# license smart conversion stop
Some Smart Licensing Conversion jobs stopped successfully.
```

Related Commands	Command	Description
	license smart conversion start	Starts license conversion
	show license status	Displays compliance status of a license.
	show license usage	Displays license usage information

license smart deregister

To cancel device registration from Cisco Smart Software Manager (CSSM), use the **license smart deregister** command in privileged EXEC mode.

license smart deregister

Syntax Description   This command has no arguments or keywords.

Command Default   Privileged EXEC (#)

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

Usage Guidelines   Use the **license smart deregister** command for these purposes:

- When your device is taken off the inventory

- When your device is shipped elsewhere for redeployment

- When your device is returned to Cisco for replacement using the return merchandise authorization (RMA) process

Example

This example shows how to deregister a device from CSSM:

```
Device# license smart deregister
*Jun 25 00:20:13.291 PDT: %SMART_LIC-6-AGENT_DEREG_SUCCESS: Smart Agent for Licensing
De-registration with the Cisco Smart Software Manager or satellite was successful
*Jun 25 00:20:13.291 PDT: %SMART_LIC-5-EVAL_START: Entering evaluation period
```

```
*Jun 25 00:20:13.291 PDT: %SMART_LIC-6-EXPORT_CONTROLLED: Usage of export controlled features
 is Not Allowed for udi PID:ISR4461/K9,SN:FDO2213A0GL
```

Related Commands

Command	Description
license smart register idtoken	Registers a device in CSSM.
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 usage	Displays license usage information

license smart register idtoken

To register a device with the token generated from Cisco Smart Software Manager (CSSM), use the **license smart register idtoken** command in privileged EXEC mode.

license smart register idtoken *token_ID* {**force**}

Syntax Description

token_ID	Device with the token generated from CSSM.
force	Forcefully registers your device irrespective of whether the device is registered or not.

Command Modes   Privileged EXEC (#)

Command History

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

Example

This example shows how to register a device on CSSM:

```
Device# license smart register idtoken
$Tl4UytrNXBzbEs1ck8veUtWaG5abnZJOFdDa1FwbVRa%0AblRMbz0%3D%0A
Registration process is in progress. Use the 'show license status' command to check the
progress and result
Device#% Generating 2048 bit RSA keys, keys will be exportable...
[OK] (elapsed time was 0 seconds)
```

Related Commands

Command	Description
license smart deregister	Cancels the device registration from CSSM.
show license all	Displays entitlements information.

Command	Description
show license status	Displays compliance status of a license.
show license summary	Displays summary of all active licenses.
show license usage	Displays license usage information

license smart renew

To manually renew your device's ID or authorization with Cisco Smart Software Manager (CSSM), use the **license smart renew** command in privileged EXEC mode.

license smart renew {**auth** | **id**}

Syntax Description

auth	Renews your authorization.
id	Renews your ID.

Command Default Privileged EXEC (#)

Command History

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

Usage Guidelines Authorization periods are renewed by the smart licensing system every 30 days. As long as the license is in an *Authorized* or *Out of compliance* state, the authorization period is renewed. The grace period starts when an authorization period expires. During the grace period or when the license is in the *Expired* state, the system continues to try and renew the authorization period. If a retry is successful, a new authorization period starts.

Example

This example shows how to renew a device license:

```
Device# license smart renew auth
```

Related Commands

Command	Description
show license all	Displays entitlements information.
show license status	Displays compliance status of a license.
show license usage	Displays license usage information

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 3.3SE	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 3.3SECisco IOS XE 3.3SE	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
```

mac address-table move update

To enable the MAC address table move update feature, use the **mac address-table move update** command in global configuration mode on the switch stack or on a standalone switch. To return to the default setting, use the **no** form of this command.

mac address-table move update {**receive | transmit**}
no mac address-table move update {**receive | transmit**}

Syntax Description

receive	Specifies that the switch processes MAC address-table move update messages.
transmit	Specifies that the switch sends MAC address-table move update messages to other switches in the network if the primary link goes down and the standby link comes up.

Command Default   By default, the MAC address-table move update feature is disabled.

Command Modes   Global configuration

Command History

Command History

Release	Modification
Cisco IOS XE 3.3SECisco IOS XE 3.3SE	This command was introduced.

Usage Guidelines	The MAC address-table move update feature allows the switch to provide rapid bidirectional convergence if a primary (forwarding) link goes down and the standby link begins forwarding traffic.
	You can configure the access switch to send the MAC address-table move update messages if the primary link goes down and the standby link comes up. You can configure the uplink switches to receive and process the MAC address-table move update messages.

Examples

This example shows how to configure an access switch to send MAC address-table move update messages:

```
Device# configure terminal
Device(config)# mac address-table move update transmit
Device(config)# end
```

This example shows how to configure an uplink switch to get and process MAC address-table move update messages:

```
Device# configure terminal
Device(config)# mac address-table move update receive
Device(config)# end
```

You can verify your setting by entering the **show mac address-table move update** privileged EXEC command.

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 3.3SECisco IOS XE 3.3SE	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 3.3SECisco IOS XE 3.3SE	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 3.3SECisco IOS XE 3.3SE	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 3.3SECisco IOS XE 3.3SE	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
YnM0Vk13TTJBakFzTmjBZS9pd2JQTWRjOWpHOnBYNThuS0RZZkxhUTRVRmpwRVY2cUhPNGw3YWVHelJJekk9YXg0VkZwK3FmYlRFSkNQaVkyMVBYUz
% 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
zSSd4YYXQEBAQYYYBRg4FAYYYYXVMCHB6csUmD10BAQFcd7CxcRUeD7B4wWQJ4BAYYAG8GAYrDVEFTRFUEiwGAENQV9FRU1PXNUQV9T5dOSU5HtFWQAC0M5DAxIUMfU5CQAOMjQEVESE5iRkE=
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 Denali 16.1.1	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#
```

request platform software package clean

To remove media files that are not required, use the **request platform software package clean** command in privileged EXEC mode.

```
request platform software package clean [{file URL | pattern URL | switch
switch-ID {file URL | pattern URL}}]
```

Syntax Description	**file** *URL*	(Optional) Specifies the URL to the file. The URL contains the file system, directories, and the filename.
	pattern *URL*	(Optional) Specifies the pattern to clean one or more matching paths.
	switch *switch-ID*	(Optional) Specifies the switch for provisioning.

Command Default No default behavior or values

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Denali 16.1.1	This command was introduced.

Usage Guidelines

Example

The following example shows how to clean unused media files from the device:

```
Device# request platform software package clean

This operation may take several minutes...
Running command on switch 1
Cleaning up unnecessary package files
No path specified, will use booted path consolidated:packages.conf
Cleaning sw/isos
  Scanning boot directory for packages ... done.
  Preparing packages list to delete ...
    cat3k_caa-guestshell.BLD_V168_THROTTLE_LATEST_20180925_154546_V16_8_1_191_2.SSA.pkg
      File is in use, will not delete.
    cat3k_caa-rpbase.BLD_V168_THROTTLE_LATEST_20180925_154546_V16_8_1_191_2.SSA.pkg
      File is in use, will not delete.
    cat3k_caa-rpcore.BLD_V168_THROTTLE_LATEST_20180925_154546_V16_8_1_191_2.SSA.pkg
      File is in use, will not delete.
    cat3k_caa-srdriver.BLD_V168_THROTTLE_LATEST_20180925_154546_V16_8_1_191_2.SSA.pkg
      File is in use, will not delete.
    cat3k_caa-webui.BLD_V168_THROTTLE_LATEST_20180925_154546_V16_8_1_191_2.SSA.pkg
      File is in use, will not delete.
  packages.conf
      File is in use, will not delete.
  done.

SUCCESS: No extra package or provisioning files found on media. Nothing to clean.
```

Related Commands

Command	Description
request platform software package install file	Upgrades a consolidated package or sub-package.
request platform software package install rollback	Rolls back a previous software upgrade.

request platform software package copy

To copy a Cisco IOS XE image file, use the **request platform software package copy** command in privileged EXEC mode.

request platform software package copy switch *switch-ID* **file** *file-URL* **to** *file-URL*

Syntax Description

switch *switch-ID*	Specifies the switch for provisioning.
file *file-URL*	URL to the consolidated package or sub-package.
to	Specifies the destination URL to where the files are to be copied.

Command Default No default behavior or values.

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Denali 16.1.1	This command was introduced.

Usage Guidelines

Example

The following example shows how to copy an image file to a destination directory:

```
Device# request platform software package copy switch all file
tftp://10.10.11.250/cat3k_caa-universalk9.16.08.05.SPA.bin to
ftp:cat3k_caa-universalk9.16.08.05.SPA.bin
```

Command	Description
request platform software package install file	Upgrades a consolidated package or sub-package.
request platform software package install rollback	Rolls back a previous software upgrade.

request platform software package describe file

To gather descriptive information about an individual module or a Cisco IOS-XE image file, use the **request platform software package describe file**command in privileged EXEC or diagnostic mode.

request platform software package describe file *URL* [**detail**] [**verbose**]

Syntax Description

URL	Specifies the URL to the file. The *URL* contains the file system, directories, and the filename.
detail	(Optional) Specifies detailed output.

verbose	(Optional) Displays verbose information, meaning that all information about the file is displayed on the console.

Command Default   No default behavior or values.

Command Modes   Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Denali 16.1.1	This command was introduced.

Usage Guidelines   This command can only be used to gather information on individual module and Cisco IOS-XE image files. Using this command to collect information on any other file will generate output, but the generated output is useless.

The output of this command can be used for the following functions:

- To confirm the individual module files that are part of a Cisco IOS-XE image.

- To confirm whether or not a file is bootable.

- To confirm the contexts in which a file must be reloaded or booted.

- To confirm whether or not a file is corrupted.

- To confirm file and header sizes, build dates, and various other general information.

Examples   In the following example, this command is entered to gather information about an individual SIP Base module file on the bootflash: file system.

```
Device# request platform software package describe file
bootflash:cat3k_caa-universalk9_universalk9.16.09.02.SPA.bin

Package: cat3k_caa-universalk9_universalk9.16.09.02.SPA.bin
  Size: 36954316
  Timestamp: 2018-11-07 15:36:27 UTC
  Canonical path: /bootflash/cat3k_caa-universalk9_universalk9.16.09.02.SPA.bin

  Raw disk-file SHA1sum:
    3ee37cdbe276316968866b16df7d8a5733a1502e

  Computed SHA1sum:
    f2db80416a1245a5b1abf2988088860b38ce7898
  Contained SHA1sum:
    f2db80416a1245a5b1abf2988088860b38ce7898
  Hashes match. Package is valid.

  Header size:     204 bytes
  Package type:    10000
  Package flags:   0
  Header version:  0

  Internal package information:
    Name: cc
    BuildTime: 2018-11-07_05.24
    ReleaseDate: Wed 07-Nov-18 01:00
```

```
          RouteProcessor: rp1
          Platform: Cat3XXX
          User: mcpre
          PackageName: ipbasek9
          Build: cat3k_caa-universalk9_universalk9.16.09.02.SPA.bin


      Package is bootable on SIP when specified
      by packages provisioning file.
```

In the following example, this command is used to gather information about a Cisco IOS-XE image on the bootflash: file system.

```
Device# request platform software package describe file
bootflash:cat3k_caa-universalk9_universalk9.16.09.02.SPA.bin

Package: cat3k_caa-universalk9_universalk9.16.09.02.SPA.bin
  Size: 218783948
  Timestamp: 2018-11-07 17:14:09 UTC
  Canonical path: /bootflash/cat3k_caa-universalk9_universalk9.16.09.02.SPA.bin

  Raw disk-file SHA1sum:
    d2999fc7e27e01344903a42ffacd62c156eba4cc

  Computed SHA1sum:
    5f8cda8518d01d8282d80ecd34f7715783f4a813
  Contained SHA1sum:
    5f8cda8518d01d8282d80ecd34f7715783f4a813
  Hashes match. Package is valid.

  Header size:     204 bytes
  Package type:    30000
  Package flags:   0
  Header version:  0

  Internal package information:
    Name: rp_super
    BuildTime: 2018-11-07_05.24
    ReleaseDate: Wed 07-Nov-18 01:00
    RouteProcessor: rp1
    Platform: Cat3XXX
    User: mcpre
    PackageName: ipbasek9
    Build: cat3k_caa-universalk9_universalk9.16.09.02


  Package is bootable from media and tftp.
  Package contents:

  Package: cat3k_caa-universalk9_universalk9.16.09.02.SPA.bin
    Size: 52072652
    Timestamp: 2018-11-07 13:33:13 UTC

    Raw disk-file SHA1sum:
      f1aad6d687256aa327a4efa84deab949fbed12b8

    Computed SHA1sum:
      15502fd1b8f9ffd4af4014ad4d8026c837929fe6
    Contained SHA1sum:
      15502fd1b8f9ffd4af4014ad4d8026c837929fe6
    Hashes match. Package is valid.

    Header size:     204 bytes
```

```
     Package type:    20000
     Package flags:   0
     Header version:  0

     Internal package information:
       Name: fp
       BuildTime: 2018-11-07_05.24
       ReleaseDate: Wed 07-Nov-18 01:00
       RouteProcessor: rp1
       Platform: Cat3XXX
       User: mcpre
       PackageName: ipbasek9
       Build: cat3k_caa-universalk9_universalk9.16.09.02.SPA.bin


     Package is bootable on ESP when specified
     by packages provisioning file.

   Package: cat3k_caa-universalk9_universalk9.16.09.02.SPA.bin
     Size: 21844172
     Timestamp: 2018-11-07 13:33:01 UTC

     Raw disk-file SHA1sum:
       025e6159dd91cef9d254ca9fff2602d8ce065939

     Computed SHA1sum:
       ea1b358324ba5815b9ea623b453a98800eae1c78
     Contained SHA1sum:
       ea1b358324ba5815b9ea623b453a98800eae1c78
     Hashes match. Package is valid.

     Header size:     204 bytes
     Package type:    30004
     Package flags:   0
     Header version:  0

     Internal package information:
       Name: ipbasek9
       BuildTime: 2018-11-07_05.24
       ReleaseDate: Wed 07-Nov-07 01:00
       RouteProcessor: rp1
       Platform: Cat3XXXX
       User: mcpre
       PackageName: ipbasek9
       Build: 16.9.20180925:160127


     Package is not bootable.

   Package: cat3k_caa-universalk9.16.09.02.SPA.bin
     Size: 21520588
     Timestamp: 2007-12-04 13:33:06 UTC

     Raw disk-file SHA1sum:
       432dfa61736d8a51baefbb2d70199d712618dcd2

     Computed SHA1sum:
       83c0335a3adcea574bff237a6c8640a110a045d4
     Contained SHA1sum:
       83c0335a3adcea574bff237a6c8640a110a045d4
     Hashes match. Package is valid.

     Header size:     204 bytes
     Package type:    30001
```

```
Package flags:   0
Header version:  0

Internal package information:
  Name: rp_base
  BuildTime: 2007-12-04_05.24
  ReleaseDate: Tue 04-Dec-07 01:00
  RouteProcessor: rp1
  Platform: Cat3XXX
  User: mcpre
  PackageName: ipbasek9
  Build: v_16.9.20180925:160127


Package is bootable on RP when specified
by packages provisioning file.

Package: cat3k_caa-universalk9_universalk9.16.09.02.SPA.bin
  Size: 24965324
  Timestamp: 2018-11-07 13:33:08 UTC

  Raw disk-file SHA1sum:
    eb964b33d4959c21b605d0989e7151cd73488a8f

  Computed SHA1sum:
    19b58886f97c79f885ab76c1695d1a6f4348674e
  Contained SHA1sum:
    19b58886f97c79f885ab76c1695d1a6f4348674e
  Hashes match. Package is valid.

  Header size:      204 bytes
  Package type:     30002
  Package flags:    0
  Header version:   0

  Internal package information:
    Name: rp_daemons
    BuildTime: 2018-11-07_05.24
    ReleaseDate: Wed 07-Nov-07 01:00
    RouteProcessor: rp1
    Platform: Cat3XXX
    User: mcpre
    PackageName: ipbasek9
    Build: v_16.9.20180925:160127


  Package is not bootable.

Package: cat3k_caa-universalk9.16.09.02.SPA.bin
  Size: 48515276
  Timestamp: 2007-12-04 13:33:13 UTC

  Raw disk-file SHA1sum:
    bc13462d6a4af7a817a7346a44a0ef7270e3a81b

  Computed SHA1sum:
    f1235d703cc422e53bce850c032ff3363b587d70
  Contained SHA1sum:
    f1235d703cc422e53bce850c032ff3363b587d70
  Hashes match. Package is valid.

  Header size:      204 bytes
  Package type:     30003
  Package flags:    0
```

```
       Header version:  0

     Internal package information:
       Name: rp_iosd
       BuildTime: 2007-12-04_05.24
       ReleaseDate: Tue 04-Dec-07 01:00
       RouteProcessor: rp1
       Platform: Cat3XXX
       User: mcpre
       PackageName: ipbasek9
       Build: v_16.9.20180925:160127


     Package is not bootable.

   Package: cat3k_caa-universalk9.16.09.02.SPA.bin
     Size: 36954316
     Timestamp: 2007-12-04 13:33:11 UTC

     Raw disk-file SHA1sum:
       3ee37cdbe276316968866b16df7d8a5733a1502e

     Computed SHA1sum:
       f2db80416a1245a5b1abf2988088860b38ce7898
     Contained SHA1sum:
       f2db80416a1245a5b1abf2988088860b38ce7898
     Hashes match. Package is valid.

     Header size:     204 bytes
     Package type:    10000
     Package flags:   0
     Header version:  0

     Internal package information:
       Name: cc
       BuildTime: 2007-12-04_05.24
       ReleaseDate: Tue 04-Dec-07 01:00
       RouteProcessor: rp1
       Platform: Cat3XXX
       User: mcpre
       PackageName: ipbasek9
       Build: v_16.9.20180925:160127


     Package is bootable on SIP when specified
     by packages provisioning file.

   Package: cat3k_caa-universalk9.16.09.02.SPA.bin
     Size: 19933388
     Timestamp: 2007-12-04 13:33:06 UTC

     Raw disk-file SHA1sum:
       44b6d15cba31fb0e9b27464665ee8a24b92adfd2

     Computed SHA1sum:
       b1d5faf093b183e196c7c8e1023fe1f7aafdd36d
     Contained SHA1sum:
       b1d5faf093b183e196c7c8e1023fe1f7aafdd36d
     Hashes match. Package is valid.

     Header size:     204 bytes
     Package type:    10001
     Package flags:   0
     Header version:  0
```

```
Internal package information:
  Name: cc_spa
  BuildTime: 2007-12-04_05.24
  ReleaseDate: Tue 04-Dec-07 01:00
  RouteProcessor: rp1
  Platform: Cat3XXX
  User: mcpre
  PackageName: ipbasek9
  Build: v_16.9.20180925:160127


Package is not bootable.
```

Related Commands

Command	Description
request platform software package install file	Upgrades an individual package or a superpackage file.

request platform software package expand

To extract the individual modules from a Cisco IOS-XE image, use the **request platform software package expand** command in privileged EXEC mode.

request platform software package expand {**file** *source-URL* | **switch** *switch-ID* **file** *source-URL*}[**to** *destination-URL*] [**auto-copy**] [**force**] [**overwrite**] [**retain-source-file**] [**verbose**] [**wipe**]

Syntax Description

source-URL	Specifies the URL to the Cisco IOS-XE file that stores the contents that will be extracted.
switch *switch-ID*	Specifies the switch ID.
to *destination-URL*	(Optional) Specifies the destination URL where the files that were extracted from the Cisco IOS-XE file are left after the operation is complete. If this option is not entered, the Cisco IOS-XE image file contents are extracted onto the same directory where the Cisco IOS-XE image file is currently stored.
auto-copy	(Optional) Copies packages to provisioning directory.
force	(Optional) Specifies that the operation will be forced, meaning that the upgrade will proceed despite any warning messages.
over-write	(Optional) Overwrites non-identical packages and unused provisioning files.
retain-to-source	(Optional) Retains the source file after expansion.
verbose	(Optional) Displays verbose information, meaning all output that can be displayed on the console during the process will be displayed.
wipe	(Optional) Erases all content on the destination snapshot directory before extracting the files and placing them on the snapshot directory.

Command Default   No default behavior or values

Command Modes   Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Denali 16.1.1	This command was introduced.

Usage Guidelines   This command only extracts individual module files and a provisioning file from the Cisco IOS-XE image. Additional configuration is needed to configure the router to boot using the provisioning files and run using the individual modules.

When this command is used, copies of each module and the provisioning file within the Cisco IOS-XE image are copied and placed on the destination directory. The Cisco IOS-XE image file is unchanged after the operation is complete.

If the **to** destination-URL option is not entered, the Cisco IOS-XE image contents will be extracted onto the same directory where the Cisco IOS-XE image is currently stored.

If this command is used to extract individual module files onto a directory that already contains individual module files, the files are extracted to an automatically created directory on the destination device.

Examples   The following example shows how to extract individual modules and the provisioning file from a Cisco IOS-XE image that has already been placed in the directory where the user wants to store the individual modules and the provisioning file.

Output of the directory before and after the extraction is given to confirm that files were extracted.

```
Device# dir bootflash:

Directory of bootflash:/
   11  drwx       16384   Dec 4 2018 11:26:07 +00:00  lost+found
14401  drwx        4096   Dec 4 2018 11:27:41 +00:00  .installer
   12  -rw-   218783948   Dec 4 2018 12:12:16 +00:00 cat3k_caa-universalk9.16.09.02.SPA.bin

Device# request platform software package expand file
bootflash:cat3k_caa-universalk9.16.09.02.SPA.bin

Verifying parameters
Validating package type
Copying package files

Device# dir bootflash:

Directory of bootflash:/
   11  drwx       16384   Dec 4 2018 11:26:07 +00:00  lost+found
14401  drwx        4096   Dec 4 2018 11:27:41 +00:00  .installer
   12  -rw-   218783948   Dec 4 2018 12:12:16 +00:00  cat3k_caa-universalk9.16.09.02.SPA.bin
28802  -rw-        7145   Dec 4 2018 12:14:22 +00:00  packages.conf
928833536 bytes total (483700736 bytes free)
```

Related Commands

Command	Description
request platform software package install file	Upgrades an individual module or a Cisco IOS-XE file.

request platform software package install auto-upgrade

To initiate automatic upgrade of software on all incompatible switches, use the **request platform software package install auto-upgrade** command in privileged EXEC mode.

request platform software package install auto-upgrade

Syntax Description
This command has no arguments or keywords.

Command Default
No default behavior or values.

Command Modes
Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Denali 16.1.1	This command was introduced.

Examples
The following example shows how to automatically upgrade the software:

```
Device# request platform software package install auto-upgrade
```

Related Commands

Command	Description
request platform software package install file	Upgrades a consolidated package or sub-package.
request platform software package install rollback	Rolls back a previous software upgrade.

request platform software package install commit

To cancel the rollback timer and commit a software upgrade, use the **request platform software package install commit** command in privileged EXEC mode.

request platform software package install switch *switch-ID***commit** [**verbose**]

Syntax Description

switch *switch-ID*	Specifies the switch ID.
verbose	(Optional) Displays verbose information, meaning all information that can be displayed on the console during the process will be displayed.

Command Default
No default behavior or values.

Command Modes
Privileged EXEC (#)

Release	Modification
Cisco IOS XE Denali 16.1.1	This command was introduced.

Usage Guidelines   This command is entered after the **request platform software package install switch** *switch-ID* **file auto-rollback** command is used to begin an individual sub-package or a consolidated package upgrade. When the **auto-rollback** *minutes* option is used, a rollback timer that cancels the upgrade after the number of specified *minutes*cancels the upgrade if the **request platform software package install switch** *switch-ID* **commit** command is not entered to commit the upgrade.

The rollback timer expires and the upgrade does not complete; and the device continues running the previous sub-package or consolidated package.

Examples   The following example shows how to commit an upgrade:

```
Device# request platform software package install switch all commit
```

Related Commands

Command	Description
request platform software package install file	Upgrades a consolidated package or sub-package.
request platform software package install rollback	Rolls back a previous software upgrade.

request platform software package install file

To upgrade a consolidated package or an individual sub-package, use the **request platform software package install file** command in privileged EXEC mode.

request platform software package install switch *switch-ID* **file** *file-URL* [**auto-rollback** *minutes*] [**interface-module-delay** *seconds*] [**provisioning-file** *provisioning-file-URL*] [**slot** *slot-number*] [**bay** *bay-number*] [**auto-copy**] [**force**] [**ignore-compact-check**] [**mdr**] [**new**] [**on-reboot**] [**retain-source-file**] [**verbose**]

Syntax Description

switch *switch-ID*	Specifies the switch for provisioning.
file-URL	URL to the consolidated package or sub-package.
auto-rollback *minutes*	(Optional) Specifies the setting of a rollback timer, and sets the number of minutes on the rollback timer before the rollback timer expires.
interface-module-delay *seconds*	(Optional) Specifies the interface module restart timeout delay.
provisioning-file *provisioning-file-URL*	(Optional) Specifies the URL to the provisioning file. A provisioning file is used for booting only when a device is booted using individual sub-packages.
slot *slot-number*	(Optional) Specifies the device slot number where a shared port adapter interface processor (SIP) can be installed.

bay *bay-number*	(Optional) Specifies the shared port adapter (SPA) bay number within a SIP.
auto-copy	(Optional) Specifies that the device will automatically copy packages to provisioning directory.
force	(Optional) Specifies that the operation will be forced, meaning that the upgrade will proceed despite any warning messages.
ignore-compact-check	(Optional) Specifies that the compatibility check is ignored.
mdr	(Optional) Specifies that minimal disruptive restart is used.
new	(Optional) Creates a new package provisioning file.
on-reboot	(Optional) Specifies that the installation will not be completed until the next RP reboot.
retain-source-file	(Optional) Retains the source file after installation.
verbose	(Optional) Displays verbose information, meaning all output that can be displayed on the console during the process will be displayed.

Command Default If you do not enter the **request platform software package install file** command, the consolidated or sub package upgrades are not initiated on the device.

Command Modes Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Denali 16.1.1	This command was introduced.

Usage Guidelines This command is used to upgrade consolidated packages and individual sub-packages.

When the **auto-rollback** *minutes* option is used, the **request platform software package install switch** *switch-ID* **commit** command must be entered before the rollback timer expires to complete the upgrade. If this command is not entered, the device rolls back to the previous software version. The rollback timer expires after the number of specified *minutes*. If the **auto-rollback** *minutes* option is not used, the upgrade automatically happens.

In the following example, the **request platform software package install** command is used to upgrade a consolidated package. The **force** option, which forces the upgrade past any prompt (such as, already having the same consolidated package installed), is used in this example.

```
Device# request platform software package install rp 0 file
bootflash:cat3k_caa-universalk9.16.03.05.SPA.bin force

--- Starting installation state synchronization ---
Finished installation state synchronization
--- Starting file path checking ---
Finished file path checking
--- Starting image file verification ---
Checking image file names
Verifying image file locations
```

```
Locating image files and validating name syntax
Inspecting image file types
Processing image file constraints
Extracting super package content
Verifying parameters
Validating package type
Copying package files
Checking and verifying packages contained in super package
Creating candidate provisioning file

  WARNING:
  WARNING: Candidate software will be installed upon reboot
  WARNING:

Finished image file verification
--- Starting candidate package set construction ---
Verifying existing software set
Processing candidate provisioning file
Constructing working set for candidate package set
Constructing working set for running package set
Checking command output
Constructing merge of running and candidate packages
Finished candidate package set construction
--- Starting compatibility testing ---
Determining whether candidate package set is compatible
WARNING:
WARNING: Candidate software combination not found in compatibility database
WARNING:
Determining whether installation is valid
Determining whether installation is valid ... skipped
Checking IPC compatibility with running software
Checking IPC compatibility with running software ... skipped
Checking candidate package set infrastructure compatibility
Checking infrastructure compatibility with running software
Checking infrastructure compatibility with running software ... skipped
Finished compatibility testing
--- Starting commit of software changes ---
Updating provisioning rollback files
Creating pending provisioning file
Committing provisioning file
Finished commit of software changes
SUCCESS: Software provisioned.  New software will load on reboot.

Device# reload
```

Note A reload must be performed to finish this procedure.

Related Commands

Command	Description
request platform software package install commit	Cancels the rollback timer and commits a software upgrade.
request platform software package install rollback	Rolls back a previous software upgrade.
request platform software package install snapshot	Creates a snapshot directory that will contain all the files extracted from a consolidated package.

request platform software package install rollback

To roll back a previous software upgrade, use the **request platform software package install rollback** command in privileged EXEC mode.

request platform software package install switch *switch-ID* **rollback** [{**as-booted** | **provisioning-file** *provisioning-file-URL*}] [**auto-copy**] [**force**] [**ignore-compact-check**] [**new**] [**on-reboot**] [**retain-source-file**] [**verbose**]

Syntax Description		
	switch *switch-ID*	Specifies the switch for provisioning.
	as-booted	(Optional) Specifies that the software update will not occur, and that the device will instead boot using the same procedure that it used during the last reboot.
	provisioning-file *provisioning-file-URL*	(Optional) Specifies that the software update will not occur, and that the device will instead boot using the specified provisioning file.
	auto-copy	(Optional) Specifies that the device will automatically copy packages to provisioning directory.
	force	(Optional) Specifies that the operation will be forced, meaning that the upgrade will proceed despite any warning messages.
	ignore-compact-check	(Optional) Specifies that the compatibility check is ignored.
	new	(Optional) Creates a new package provisioning file.
	on-reboot	(Optional) Specifies that the installation will not be completed until the next reboot.
	retain-source-file	(Optional) Retains the source file after installation,
	verbose	(Optional) Displays verbose information, meaning all output that can be displayed on the console during the process will be displayed.

Command Default No default behavior or values

Command Modes Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Everest 16.1.1	This command was introduced.

Usage Guidelines This command rolls back a configuration that has an active rollback timer. Active rollback timers are used when the **auto-rollback** option is entered when software is being upgraded using the **request platform software package install file** command.

Examples

The following example shows that an upgrade using a rollback timer is rolled back to the previous configuration:

```
Device# request platform software package install switch all rollback
```

Related Commands

Command	Description
request platform software package install commit	Cancel the rollback timer and commits a software upgrade.
request platform software package install file	Upgrades a consolidated package or an individual sub-package.

request platform software package install snapshot

To create a snapshot directory that contains all the files extracted from a consolidated package, use the **request platform software package install snapshot** command in privileged EXEC mode.

request platform software package install switch *switch-ID* **snapshot to** *URL* [**as** *snapshot-provisioning-filename*] [**force**] [**verbose**] [**wipe**]

Syntax Description

switch *switch-ID*	Specifies the switch for provisioning.
snapshot to *URL*	Creates a directory and extracts all files from the consolidated package into that directory. The directory is named in the command-line as part of the *URL_FS*. If the *URL_FS* is specified as a file system, the files in the consolidated package will be extracted onto the file system and not a directory on the file system.
as *snapshot-provisioning-filename*	(Optional) Renames the provisioning file in the snapshot directory. If this option is not used, the existing provisioning filename of the provisioning file in the consolidated package is used.
wipe	(Optional) Erases all content on the destination snapshot directory before extracting files and placing them on the snapshot directory.
force	(Optional) Specifies that the operation will be forced; meaning that the upgrade will proceed despite any warning messages.
verbose	(Optional) Displays verbose information, meaning all output is displayed on the console during the provisioning process.

Command Default   No default behavior or values

Command Modes   Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Everest 16.1.1	This command was introduced.

Usage Guidelines

This command is used to create a directory at the destination device and extract the individual sub-packages in a consolidated package to that directory.

The **request platform software package expand** command is the only other command that can be used to extract individual sub-packages from a consolidated package.

Examples

In the following example, a snapshot directory named snapdir1_snap is created in the bootflash: file system, and the individual sub-package files from the consolidated package are extracted into the snapshot directory.

The second portion of the example first sets up the router to reboot using the files in the snapshot directory (deletes all previous boot system commands, configures the configuration register, then enters a boot system command to boot using the extracted provisioning file), saves the new configuration, then reboots so the device will boot using the extracted provisioning file, which allows the router to run using the extracted individual sub-package files.

```
Device# request platform software package install switch all snapshot to
bootflash:snapdir1_snap

--- Starting active image file snapshot --- Validating snapshot parameters Creating
destination directory
Copying files to destination media
   Copied provisioning file as packages.conf
Moving files into final location Finished active image file snapshot
Device(config)# no boot system
Device(config)# config-register 0x1
Device(config)# boot system harddisk:snapdir1_snap/packages.conf
Device(config)# exit
*May 11 01:31:04.815: %SYS-5-CONFIG_I: Configured from console by con
Device# write memory

Building configuration...
[OK]

Device# reload
```

Related Commands	Command	Description
	request platform software package install file	Upgrades a consolidated package or an individual sub-package.

request platform software package verify

To verify the In-Service Software Upgrade (ISSU) software package compatibility, use the **requestplatform software package verify** command in privileged EXEC mode.

request platform software package verify switch *switch-ID* **file** *file-URL* [**bay** *bay-number*] [**slot** *slot-number*] [**auto-copy**] [**force**] [**mdr**]

Syntax Description	**switch** *switch-ID*	Specifies the switch for provisioning.
	file-URL	URL to the consolidated package or sub-package.
	bay *bay-number*	(Optional) Specifies the shared port adapter (SPA) bay number within a SIP.
	slot *slot-number*	(Optional) Specifies the device slot number where a shared port adapter interface processor (SIP) can be installed.
	auto-copy	(Optional) Specifies that the device will automatically copy packages to provisioning directory.
	force	(Optional) Specifies that the operation will be forced, meaning that the upgrade will proceed despite any warning messages.
	mdr	(Optional) Specifies that minimal disruptive restart is used.

Command Default   No default behavior or values.

Command Modes   Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Denali 16.1.1	This command was introduced.

Example

The following example shows how to verify Cisco IOS XE image:

```
Device# request platform software package verify switch all file
bootflash:cat3k_caa-universalk9.16.03.05.SPA.bin
```

Related Commands

Command	Description
request platform software package install commit	Cancels the rollback timer and commits a software upgrade.
request platform software package install rollback	Rolls back a previous software upgrade.
request platform software package install snapshot	Creates a snapshot directory that will contain all the files extracted from a consolidated package.

request platform software package uninstall

To uninstall a software package, use the **request platform software package uninstall** command in privileged EXEC mode.

request platform software package uninstall switch *switch-ID* **file** *file-URL*   [**bay** *bay-number*]
[**slot** *slot-number*]   [**auto-copy**] [**force**] [**mdr**]

Syntax Description		
	switch *switch-ID*	Specifies the switch for provisioning.
	file-URL	URL to the consolidated package or sub-package.
	bay *bay-number*	(Optional) Specifies the shared port adapter (SPA) bay number within a SIP.
	slot *slot-number*	(Optional) Specifies the device slot number where a shared port adapter interface processor (SIP) can be installed.
	auto-copy	(Optional) Specifies that the device will automatically copy packages to provisioning directory.
	force	(Optional) Specifies that the operation will be forced, meaning that the upgrade will proceed despite any warning messages.
	mdr	(Optional) Specifies that minimal disruptive restart is used.

Command Default   No default behavior or values.

Command Modes   Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Denali 16.1.1	This command was introduced.

Example

The following example shows how to uninstall a software package:

```
Device# request platform software package uninstall
```

Related Commands	Command	Description
	request platform software package install commit	Cancels the rollback timer and commits a software upgrade.
	request platform software package install rollback	Rolls back a previous software upgrade.
	request platform software package install snapshot	Creates a snapshot directory that will contain all the files extracted from a consolidated package.

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 3.3SECisco IOS XE 3.3SE	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 3.3SECisco IOS XE 3.3SE	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 3.3SECisco IOS XE 3.3SE	This command was introduced.

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

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

Example

This example shows how to configure the advanced template:

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

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 automatically or manually boots.

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

set

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 3.3SECisco IOS XE 3.3SE	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
Cisco IOS XE 3.3SE	This command was introduced.

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

```
Device# 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 cable-diagnostics tdr

To display the Time Domain Reflector (TDR) results, use the **show cable-diagnostics tdr** command in privileged EXEC mode.

show   cable-diagnostics   tdr   interface *interface-id*

Syntax Description	*interface-id*	Specifies the interface on which TDR is run.

Command Default No default behavior or values.

Command Modes Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.3SECisco IOS XE 3.3SE	This command was introduced.

Usage Guidelines TDR is supported only on 10/100/100 copper Ethernet ports. It is not supported on 10-Gigabit Ethernet ports and small form-factor pluggable (SFP) module ports.

Examples

This example shows the output from the **show cable-diagnostics tdr interface** *interface-id* command on a device:

```
Device# show cable-diagnostics tdr interface gigabitethernet1/0/23
  TDR test last run on: March 01 00:04:08
  Interface  Speed  Local pair  Pair length        Remote pair  Pair status
  ---------  -----  ----------  -----------------  -----------  --------------------
  Gi1/0/23   1000M  Pair A      1    +/- 1 meters  Pair A       Normal
                    Pair B      1    +/- 1 meters  Pair B       Normal
                    Pair C      1    +/- 1 meters  Pair C       Normal
                    Pair D      1    +/- 1 meters  Pair D       Normal
```

Table 2: Field Descriptions for the show cable-diagnostics tdr Command Output

Field	Description
Interface	The interface on which TDR is run.
Speed	The speed of connection.
Local pair	The name of the pair of wires that TDR is testing on the local interface.
Pair length	The location of the problem on the cable, with respect to your device. TDR can only find the location in one of these cases: • The cable is properly connected, the link is up, and the interface speed is 1000 Mb/s. • The cable is open. • The cable has a short.
Remote pair	The name of the pair of wires to which the local pair is connected. TDR can learn about the remote pair only when the cable is properly connected and the link is up.

Field	Description
Pair status	The status of the pair of wires on which TDR is running: • Normal—The pair of wires is properly connected. • Not completed—The test is running and is not completed. • Not supported—The interface does not support TDR. • Open—The pair of wires is open. • Shorted—The pair of wires is shorted. • ImpedanceMis—The impedance is mismatched. • Short/Impedance Mismatched—The impedance mismatched or the cable is short. • InProgress—The diagnostic test is in progress.

This example shows the output from the **show interface** *interface-id* command when TDR is running:

```
Device# show interface gigabitethernet1/0/2
  gigabitethernet1/0/2 is up, line protocol is up (connected: TDR in Progress)
```

This example shows the output from the **show cable-diagnostics tdr interface** *interface-id* command when TDR is not running:

```
Device# show cable-diagnostics tdr interface gigabitethernet1/0/2
  % TDR test was never issued on gigabitethernet1/0/2
```

If an interface does not support TDR, this message appears:

```
% TDR test is not supported on device 1
```

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

To display fan, temperature, and power information for the switch (standalone switch, active switch, or standby switch), use the **show env** command in EXEC modes.

show env { **all** | **fan** | **power** [**all** | **switch** [*switch-number*]] | **stack** [*stack-number*] | **temperature** [**status**] }

Syntax Description	**all**	Displays fan, temperature and power environmental status.
	fan	Displays the switch fan status.
	power	Displays the power supply status.
	all	(Optional) Displays the status for all power supplies.
	switch *switch-number*	(Optional) Displays the power supply status for a specific switch.
	stack *switch-number*	(Optional) Displays all environmental status for each switch in the stack or for a specified switch. The range is 1 to 9, depending on the switch member numbers in the stack.
	temperature	Displays the switch temperature status.
	status	(Optional) Displays the temperature status and threshold values.

Command Default
No default behavior or values.

Command Modes
User EXEC

Privileged EXEC

Command History	Release	Modification
	Cisco IOS XE 3.3SECisco IOS XE 3.3SE	This command was introduced.

Usage Guidelines

Use the **show env stack** [*switch-number*] command to display information about any switch in the stack from any member switch.

Use the **show env temperature status** command to display the switch temperature states and threshold levels.

Examples

This example shows how to display information about member switch 1 from the active switch:

```
Device> show env stack 1
Device 1:
Device Fan 1 is OK
Device Fan 2 is OK
Device Fan 3 is OK
FAN-PS1 is OK
FAN-PS2 is NOT PRESENT
Device 1: SYSTEM TEMPERATURE is OK
Temperature Value: 32 Degree Celsius
Temperature State: GREEN
Yellow Threshold : 41 Degree Celsius
Red Threshold : 56 Degree Celsius

Device>
```

This example shows how to display temperature value, state, and threshold values:

```
Device> show env temperature status
Temperature Value: 32 Degree Celsius
Temperature State: GREEN
Yellow Threshold : 41 Degree Celsius
Red Threshold : 56 Degree Celsius

Device>
```

Table 3: States in the show env temperature status Command Output

State	Description
Green	The switch temperature is in the *normal* operating range.
Yellow	The temperature is in the *warning* range. You should check the external temperature around the switch.
Red	The temperature is in the *critical* range. The switch might not run properly if the temperature is in this range.

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 4: 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 3.3SE	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:

```
Device# 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 5: 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.

Field	Description
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 Everest 16.6.1	This command was introduced.

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

Example

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

```
Device# show install package bootflash:cat3k-universalk9.2017-01-10_13.15.1.
CSCxxx.SSA.dmp.bin
Name:  cat3k-universalk9.2017-01-10_13.15.1.CSCxxx.SS
Version:  16.6.1.0.199.1484082952..Everest
Platform:  Catalyst3k
Package Type:  dmp
Defect ID:  CSCxxx
Package State:  Added
Supersedes List:  {}
Smu ID:  1
```

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

```
Device# show install summary

Active Packages:
    bootflash:cat3k-universalk9.2017-01-10_13.15.1.CSCxxx.SSA.dmp.bin
Inactive Packages:
   No packages
Committed Packages:
    bootflash:cat3k-universalk9.2017-01-10_13.15.1.CSCxxx.SSA.dmp.bin
Uncommitted Packages:
   No packages
Device#
```

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

Table 6: 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 log** command:

```
Device# show install log

[0|install_op_boot]: START Fri Feb 24 19:20:19 Universal 2017
[0|install_op_boot]: END SUCCESS  Fri Feb 24 19:20:23 Universal 2017
[3|install_add]: START Sun Feb 26 05:55:31 UTC 2017
[3|install_add( FATAL)]: File path (scp) is not yet supported for this command
```

```
[4|install_add]: START Sun Feb 26 05:57:04 UTC 2017
[4|install_add]: END SUCCESS
/bootflash/cat3k-universalk9.2017-01-10_13.15.1.CSCvb12345.SSA.dmp.bin
Sun Feb 26 05:57:22 UTC 2017
[5|install_activate]: START Sun Feb 26 05:58:41 UTC 2017
```

Related Commands

Command	Description
install	Installs SMU packages.

show license all

To display the entitlements information, use the **show license all** command in privileged EXEC mode.

show license all

Syntax Description   This command has no arguments or keywords.

Command Default   Licensing information of multiple show license commands is concatenated and displayed.

Command Modes   Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.1	This command was introduced.
Cisco IOS XE Gibraltar 16.12.6	What was EVAL MODE or EVAL EXPIRY prior to Cisco IOS XE Gibraltar 16.12.6, was changed to display IN-USE.
	This change applies only to a device that meets the following conditions:
	• Was using an evaluation or expired evaluation license prior to Cisco IOS XE Gibraltar 16.12.6.
	• Is not connected to CSSM
	• Is running Cisco IOS XE Gibraltar 16.12.6 or later release.
	If a device is connected to CSSM, there is no change.

Usage Guidelines   The command also displays whether smart licensing is enabled, all associated licensing certificates, compliance status, and so on.

Examples

Registered and Authorized Licenses

The following is sample output of the **show license all** command on a device that is using registered and authorized licenses:

```
Device# show license all

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

Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Smart Account: EG-SA
  Virtual Account: EG-VA
  Export-Controlled Functionality: Allowed
  Initial Registration: SUCCEEDED on Jul 09 10:08:19 2018 UTC
  Last Renewal Attempt: None
  Next Renewal Attempt: Jan 05 10:08:19 2019 UTC
  Registration Expires: Jul 09 10:02:35 2019 UTC

License Authorization:
  Status: AUTHORIZED on Jul 09 11:16:10 2018 UTC
  Last Communication Attempt: SUCCEEDED on Jul 09 11:16:10 2018 UTC
  Next Communication Attempt: Aug 08 11:16:09 2018 UTC
  Communication Deadline: Oct 07 11:10:28 2018 UTC

License Conversion:
  Automatic Conversion Enabled: False
  Active: PID:WS-C3850-24P,SN:FOC1842U0FC
  Status: Successful on Jul 09 11:16:06 2018 UTC
  Standby: PID:WS-C3850-24P,SN:FOC1842U0CZ
  Status: Successful on Jul 09 11:16:06 2018 UTC
  Member: PID:WS-C3850-24P,SN:FOC1842X0FD
  Status: Successful on Jul 09 11:16:06 2018 UTC

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

C3850-DNA-E-24 (C3850-24 DNA Essentials):
  Description: C3850-DNA-E
  Count: 3
  Version: 1.0
  Status: AUTHORIZED

C3850_24_Lanbase (C3850-24 LAN Base):
  Description: C3850 24 Port Lanbase
  Count: 3
  Version: 1.0
  Status: AUTHORIZED
```

```
Product Information
===================
UDI: PID:WS-C3850-24P,SN:FOC1842U0FC

HA UDI List:
    Active:PID:WS-C3850-24P,SN:FOC1842U0FC
    Standby:PID:WS-C3850-24P,SN:FOC1842U0CZ
    Member:PID:WS-C3850-24P,SN:FOC1842X0FD

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
```

Evaluation Licenses

The following is sample output of the **show license all** command on a device that *was* using evaluation licenses prior to Cisco IOS XE Gibraltar 16.12.6, is not connected to CSSM, and is now running Cisco IOS XE Gibraltar 16.12.6. In the output, note how the status is no longer displayed as EVAL MODE, but IN-USE. There is no change in the registration status of the device - this continues to be displayed as UNREGISTERED.

```
Device# show license all

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

Smart Licensing is ENABLED

Registration:
  Status: UNREGISTERED
  Export-Controlled Functionality: NOT ALLOWED

License Authorization:
  Status: IN-USE

License Conversion:
  Automatic Conversion Enabled: False
  Active: PID:WS-C3850-48T,SN:FOC2231L38N
  Status: Not started
  Standby: PID:WS-C3850-48P,SN:FOC2250U0P9
  Status: Not started
  Member: PID:WS-C3850-12X48U,SN:FOC2235X0RY
  Status: Not started
  Member: PID:WS-C3850-12S,SN:FCW2232D1DQ
  Status: Not started

Export Authorization Key:
  Features Authorized:
    <none>

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

(C3850-48 LAN Base):
  Description:
  Count: 3
  Version: 1.0
  Status: IN-USE
  Export status: NOT RESTRICTED

(C3850-12XS LAN Base):
  Description:
  Count: 1
  Version: 1.0
  Status: IN-USE
  Export status: NOT RESTRICTED

Product Information
===================
UDI: PID:WS-C3850-48T,SN:FOC2231L38N

HA UDI List:
    Active:PID:WS-C3850-48T,SN:FOC2231L38N
    Standby:PID:WS-C3850-48P,SN:FOC2250U0P9
    Member:PID:WS-C3850-12X48U,SN:FOC2235X0RY
    Member:PID:WS-C3850-12S,SN:FCW2232D1DQ

Agent Version
=============
Smart Agent for Licensing: 4.8.16_rel/80

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

Related Commands

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

To display the compliance status of a license, use the **show license status** command in privileged EXEC mode.

show license status

Syntax Description   This command has no arguments or keywords.

Command Default   Compliance status of all licenses available on the device is displayed.

Command Modes   Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.1	This command was introduced.
Cisco IOS XE Gibraltar 16.12.6	What was EVAL MODE or EVAL EXPIRED prior to Cisco IOS XE Gibraltar 16.12.6, was changed to display IN-USE.
	This change applies only to a device that meets the following conditions:
	• Was using an evaluation or expired evaluation license prior to Cisco IOS XE Gibraltar 16.12.6.
	• Is not connected to CSSM
	• Is now running Cisco IOS XE Gibraltar 16.12.6 or a later release.
	If a device is connected to CSSM, there is no change.

Examples

Registered and Authorized Licenses

The following is sample output of the **show license status** command on a device that is using registered and authorized licenses:

```
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: EG-SA
  Virtual Account: EG-VA
  Export-Controlled Functionality: Allowed
  Initial Registration: SUCCEEDED on Jul 09 10:08:19 2018 UTC
```

```
        Last Renewal Attempt: None
        Next Renewal Attempt: Jan 05 10:08:19 2019 UTC
        Registration Expires: Jul 09 10:02:35 2019 UTC

    License Authorization:
        Status: AUTHORIZED on Jul 09 11:16:10 2018 UTC
        Last Communication Attempt: SUCCEEDED on Jul 09 11:16:10 2018 UTC
        Next Communication Attempt: Aug 08 11:16:09 2018 UTC
        Communication Deadline: Oct 07 11:10:28 2018 UTC

    License Conversion:
        Automatic Conversion Enabled: False
        Active: PID:WS-C3850-24P,SN:FOC1842U0FC
        Status: Successful on Jul 09 11:16:06 2018 UTC
        Standby: PID:WS-C3850-24P,SN:FOC1842U0CZ
        Status: Successful on Jul 09 11:16:06 2018 UTC
        Member: PID:WS-C3850-24P,SN:FOC1842X0FD
        Status: Successful on Jul 09 11:16:06 2018 UTC
```

Evaluation Licenses

The following is sample output of the **show license status** command on a device that *was* using evaluation licenses prior to Cisco IOS XE Gibraltar 16.12.6, is not connected to CSSM, and is now running Cisco IOS XE Gibraltar 16.12.6. In the output, note how the status is no longer displayed as EVAL MODE, but IN-USE. There is no change in the registration status of the device - this continues to be displayed as UNREGISTERED.

```
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: UNREGISTERED
  Export-Controlled Functionality: NOT ALLOWED

License Authorization:
  Status: IN-USE

License Conversion:
  Automatic Conversion Enabled: False
  Active: PID:WS-C3850-48T,SN:FOC2231L38N
  Status: Not started
  Standby: PID:WS-C3850-48P,SN:FOC2250U0P9
  Status: Not started
  Member: PID:WS-C3850-12X48U,SN:FOC2235X0RY
  Status: Not started
  Member: PID:WS-C3850-12S,SN:FCW2232D1DQ
  Status: Not started

Export Authorization Key:
  Features Authorized:
    <none>
```

Related Commands	Command	Description
	show license all	Displays entitlements 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 summary of all active licenses, use the **show license summary** command in privileged EXEC.

show license summary

Syntax Description   This command has no arguments or keywords.

Command Default   All available licenses on the device are displayed.

Command Modes   Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.1	This command was introduced.
Cisco IOS XE Gibraltar 16.12.6	What was EVAL MODE or EVAL EXPIRED prior to Cisco IOS XE Gibraltar 16.12.6, was changed to display IN-USE.
	This change applies only to a device that meets the following conditions:
	• Was using an evaluation or expired evaluation license prior to Cisco IOS XE Gibraltar 16.12.6.
	• Is not connected to CSSM
	• Is now running Cisco IOS XE Gibraltar 16.12.6 or a later release.
	If a device is connected to CSSM, there is no change.

Examples

Registered and Authorized Licenses

The following is sample output of the **show license summary** command on a device that is using registered and authorized licenses:

```
Device# show license summary
Smart Licensing is ENABLED

Registration:
  Status: REGISTERED
  Smart Account: EG-SA
  Virtual Account: EG-VA
  Export-Controlled Functionality: Allowed
  Last Renewal Attempt: None
  Next Renewal Attempt: Jan 05 10:08:20 2019 UTC

License Authorization:
  Status: AUTHORIZED
  Last Communication Attempt: SUCCEEDED
  Next Communication Attempt: Aug 08 11:16:10 2018 UTC

License Usage:
  License               Entitlement tag              Count Status
  --------------------------------------------------------------------------
  C3850-DNA-E-24        (C3850-24 DNA Essentials)        3 AUTHORIZED
  C3850_24_Lanbase      (C3850-24 LAN Base)              3 AUTHORIZED
```

Evaluation Licenses

The following are sample outputs of the **show license summary** command on a device that *was* using evaluation licenses prior to Cisco IOS XE Gibraltar 16.12.6, is not connected to CSSM, and is now running Cisco IOS XE Gibraltar 16.12.6. In the output, note how the status is no longer displayed as EVAL MODE, but IN-USE. The notification relating to the remaining evaluation period is also no longer displayed. There is no change in the registration status of the device - this continues to be displayed as UNREGISTERED.

Sample output of **show license summary**, prior to Cisco IOS XE Gibraltar 16.12.6:

```
Device# show license summary

Smart Licensing is ENABLED
License Reservation is ENABLED

Registration:
  Status: UNREGISTERED
  Export-Controlled Functionality: NOT ALLOWED

License Authorization:
  Status: EVAL MODE
  Evaluation Period Remaining: 89 days, 22 hours, 47 minutes, 10 seconds

License Usage:
  License           Entitlement tag              Count Status
  ----------------------------------------------------------------
  C3850-DNA-E-24    (C3850-24 DNA Essentials)        1 EVAL MODE
  C3850_24_Lanbase  (C3850-24 LAN Base)              1 EVAL MODE
```

Sample output of **show license summary**, in Cisco IOS XE Gibraltar 16.12.6:

```
Device# show license summary
```

```
Smart Licensing is ENABLED
License Reservation is ENABLED

Registration:
  Status: UNREGISTERED
  Export-Controlled Functionality: NOT ALLOWED

License Authorization:
  Status: IN-USE

License Usage:
  License           Entitlement tag              Count Status
  --------------------------------------------------------------
  C3850-DNA-E-24    (C3850-24 DNA Essentials)       1 IN-USE
  C3850_24_Lanbase  (C3850-24 LAN Base)             1 IN-USE
```

Expired Evaluation Licenses

The following are "before" and "after"sample outputs of the **show license summary** command on a device that *was* using expired evaluation licenses prior to Cisco IOS XE Gibraltar 16.12.6, is not connected to CSSM, and is now running Cisco IOS XE Gibraltar 16.12.6. In the output, note how the status is no longer displayed as EVAL EXPIRED, but IN-USE. There is no change in the registration status of the device - this continues to be displayed as UNREGISTERED.

Sample output of **show license summary**, prior to Cisco IOS XE Gibraltar 16.12.6:

```
Device# show license summary

Smart Licensing is ENABLED

Registration:
  Status: UNREGISTERED
  Export-Controlled Functionality: NOT ALLOWED

License Authorization:
  Status: EVAL EXPIRED

License Usage:
  License                Entitlement tag              Count Status
  --------------------------------------------------------------------------
                         (C3850-24XS IP Services)        1 EVAL EXPIRED
                         (C3850-12XS DNA Advantage)      1 EVAL EXPIRED
```

Sample output of **show license summary**, in Cisco IOS XE Gibraltar 16.12.6:

```
Device# show license summary

Smart Licensing is ENABLED
License Reservation is ENABLED

Registration:
  Status: UNREGISTERED
  Export-Controlled Functionality: NOT ALLOWED

License Authorization:
  Status: IN-USE
```

```
License Usage:
  License                    Entitlement tag               Count Status
  ----------------------------------------------------------------------
                             (C3850-24 IP Services)            1 IN-USE
                             (C3850-24 DNA Advantage)          1 IN-USE
```

Related Commands

Command	Description
show license all	Displays entitlements information.
show license status	Displays compliance status of a license.
show license udi	Displays UDI.
show license usage	Displays license usage information
show tech-support license	Displays the debug output.

show license tech support

To display detailed licensing information, which the technical support team can use for troubleshooting, use the **show license tech support** command in privileged EXEC mode.

show license tech support

Syntax Description   This command has no arguments or keywords.

Command Default   Detailed licensing information for all available licenses is displayed.

Command Modes   Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS XE Fuji 16.9.1	This command was introduced.
Cisco IOS XE Gibraltar 16.12.6	What was EVAL MODE or EVAL EXPIRED prior to Cisco IOS XE Gibraltar 16.12.6, was changed to display IN-USE.
	This change applies only to a device that meets the following conditions:
	• Was using an evaluation or expired evaluation license prior to Cisco IOS XE Gibraltar 16.12.6.
	• Is not connected to CSSM
	• Is now running Cisco IOS XE Gibraltar 16.12.6 or a later release.
	If a device is connected to CSSM, there is no change.

Examples   The following is sample output of the **show license tech support** command on a device that *was* using evaluation licenses prior to Cisco IOS XE Gibraltar 16.12.6, is not connected to CSSM, and is now running Cisco IOS XE Gibraltar 16.12.6. In the output, note how the status is no longer

displayed as EVAL MODE, but IN-USE. There is no change in the registration status of the device
- this continues to be displayed as UNREGISTERED.

```
Device# show license tech support
Smart Licensing Tech Support info

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

Smart Licensing is ENABLED

Registration:
  Status: UNREGISTERED
  Export-Controlled Functionality: NOT ALLOWED

License Authorization:
  Status: IN-USE

License Conversion:
  Automatic Conversion Enabled: False
  Active: PID:WS-C3850-48T,SN:FOC2231L38N
  Status: Not started
  Standby: PID:WS-C3850-48P,SN:FOC2250U0P9
  Status: Not started
  Member: PID:WS-C3850-12X48U,SN:FOC2235X0RY
  Status: Not started
  Member: PID:WS-C3850-12S,SN:FCW2232D1DQ
  Status: Not started

Export Authorization Key:
  Features Authorized:
    <none>

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
=============
Handle: 1
  License: <empty>
  Entitlement tag:
regid.2018-02.com.cisco.C3850_48_Lanbase,1.0_055ff5a5-e741-4c01-892b-345e342308cd
  Description: <empty>
  Count: 3
  Version: 1.0
  Status: IN-USE(6)
  Status time: Jun 22 07:52:45 2021 UTC
  Request Time: Jun 22 07:52:45 2021 UTC
  Export status: NOT RESTRICTED
  Soft Enforced: True

Handle: 4
  License: <empty>
  Entitlement tag:
regid.2018-02.com.cisco.C3850_XS_12_Lanbase,1.0_269e0b71-86b5-433e-a179-16d428bc95c1
```

```
   Description: <empty>
   Count: 1
   Version: 1.0
   Status: IN-USE(6)
   Status time: Jun 22 07:52:45 2021 UTC
   Request Time: Jun 22 07:52:45 2021 UTC
   Export status: NOT RESTRICTED
   Soft Enforced: True

Product Information
===================
UDI: PID:WS-C3850-48T,SN:FOC2231L38N

HA UDI List:
    Active:PID:WS-C3850-48T,SN:FOC2231L38N
    Standby:PID:WS-C3850-48P,SN:FOC2250U0P9
    Member:PID:WS-C3850-12X48U,SN:FOC2235X0RY
    Member:PID:WS-C3850-12S,SN:FCW2232D1DQ

Agent Version
=============
Smart Agent for Licensing: 4.8.16_rel/80

Upcoming Scheduled Jobs
=======================
Current time: Jun 22 10:45:21 2021 UTC
Daily: Jun 23 07:52:02 2021 UTC (21 hours, 6 minutes, 41 seconds remaining)
Init Flag Check: Not Available
Evaluation Expiration Check: Sep 18 13:36:22 2021 UTC (88 days, 2 hours, 51 minutes, 1
seconds remaining)
In Use Countdown: Jul 20 13:36:22 2021 UTC (28 days, 2 hours, 51 minutes, 1 seconds remaining)
Reservation configuration mismatch between nodes in HA mode: Jan 01 00:00:00 1970 UTC
(1158031640 days, 20 hours, 14 minutes, 55 seconds remaining)

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: DISABLED

Other Info
==========
Software ID: regid.2014-07.com.cisco.Prd_Catalyst3850,1.0_b5b32167-3385-487e-8ba5-7eea7250ec81
Agent State: unidentified
TS enable: True
Transport: Callhome
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: True
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
SmartAgentClientWaitForServer: 2000
SmartAgentCmReTrySend: True
SmartAgentClientIsUnified: True
SmartAgentCmClient: True
SmartAgentClientName: UnifiedClient
builtInEncryption: True
enableOnInit: True
routingReadyByEvent: True
systemInitByEvent: True
evDisplayInUse: True
SmartAgentFederalLicense: True
SmartAgent_Crypto_Exit_CB: 0xAAB8A9EF80
SmartAgent_Crypto_Start_CB: 0xAAB8A9EF78
SmartAgentMultiTenant: False
attr365DayEvalSyslog: True
checkPointWriteOnly: False
SmartAgentDelayCertValidation: False
enableByDefault: False
conversionAutomatic: False
conversionAllowed: True
storageEncryptDisable: False
storageLoadUnencryptedDisable: False
TSPluginDisable: False
bypassUDICheck: False
loggingAddTStamp: False
loggingAddTid: True
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: 250 KB

Platform Provided Mapping Table
===============================
<empty>
```

show license udi

To display the Unique Device Identifier (UDI), use the **show license udi** command in privileged EXEC mode.

show license udi

Syntax Description
This command has no arguments or keywords.

Command Default
Privileged EXEC (#)

Command History

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

Example

This example shows a sample output from the **show license udi** command:

```
Device# show license udi
UDI: PID:WS-C3850-24P,SN:FOC1842U0FC

HA UDI List:
    Active:PID:WS-C3850-24P,SN:FOC1842U0FC
    Standby:PID:WS-C3850-24P,SN:FOC1842U0CZ
    Member:PID:WS-C3850-24P,SN:FOC1842X0FD
```

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 usage	Displays license usage information
show tech-support license	Displays the debug output.

show license usage

To display license usage information, use the **show license usage** command in privileged EXEC mode.

show license usage

Syntax Description
This command has no arguments or keywords.

Command Default
License usage information is displayed.

Command Modes
Privileged EXEC (#)

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

This example shows a sample output from the **show license usage** command:

```
Device# show license usage
License Authorization:
  Status: AUTHORIZED on Jul 09 11:16:10 2018 UTC

C3850-DNA-E-24 (C3850-24 DNA Essentials):
  Description: C3850-DNA-E
  Count: 3
  Version: 1.0
  Status: AUTHORIZED

C3850_24_Lanbase (C3850-24 LAN Base):
  Description: C3850 24 Port Lanbase
  Count: 3
  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, use the **show location** command in privileged EXEC mode.

show location {**detail** *mac-addr* | **plm** | **statistics** | **summary rfid** | **rfid** {**client** | **config** | **detail** *MAC-addr* | **summary**}}

Syntax Description	**detail** *mac-addr*	Displays detailed location information with the RSSI table for a particular client.
	plm	Displays location path loss measurement (CCX S60) configuration.
	statistics	Displays location-based system statistics.
	summary	Displays location-based system summary information.
	rfid	Displays the RFID tag tracking information.
	client	Displays the summary of RFID tags that are clients.

config	Displays the configuration options for RFID tag tracking.
detail *MAC-addr*	Displays the detailed information for one rfid tag.
summary	Displays summary information for all known rfid tags.

Command Default No default behavior or values.

Command Modes Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.3SECisco IOS XE 3.3SE	This command was introduced.

The following is sample output from the **show location plm** command:

```
Device# show location plm
Location Path Loss Configuration

Calbration client        : Disabled, Radio: Multiband
Normal clients           : Disabled
Burst interval           : 60
```

show location ap-detect

To display the location information detected by specified access point, use the **show location ap-detect** command in privileged EXEC mode.

show location ap-detect {**all** | **client** | **rfid** | **rogue-ap** | **rogue-client**} *ap-name*

Syntax Description

all	Displays information of the client, RFID, rogue access point, and rogue client.
client	Displays the client information.
rfid	Displays RFID information.
rogue-ap	Displays rogue access point information.
rogue-client	Displays rogue client information.
ap-name	Specified access point name.

Command Default No default behavior or values.

Command Modes Privileged EXEC

Command History	Release	Modification
	Cisco IOS XE 3.3SECisco IOS XE 3.3SE	This command was introduced.

The following is sample output from the **show location ap-detect client** command:

```
Device# show location ap-detect client AP02
Clients

MAC Address       Status          Slot  Antenna    RSSI
----------------------------------------------------------
2477.0389.96ac    Associated        1        0      -60
2477.0389.96ac    Associated        1        1      -61
2477.0389.96ac    Associated        0        0      -46
2477.0389.96ac    Associated        0        1      -41


RFID Tags



Rogue AP's



Rogue Clients

MAC Address       State           Slot    Rssi
---------------------------------------------------------
0040.96b3.bce6    Alert             1      -58
586d.8ff0.891a    Alert             1      -72
```

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 Denali 16.1.1	This command was introduced.
Cisco IOS XE Gibraltar 16.11.1	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 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 3.3SECisco IOS XE 3.3SE	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 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
Cisco IOS XE Denali 16.3.2	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 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 16.11.1	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 16.11.1	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 7: *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.
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 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
Cisco IOS XE Denali 16.3.2	This command was introduced.

Examples

This example shows how to view the checksum record for a specific SUDI :

```
Device# 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/2bPPu8Xs1gYJQk0XuPL1hS27PKSSb3TkL4Eq1ZKR4OCXPDJoBYVL0fdX41Id
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
BQcBAQREMEIwQAYIKwYBBQUHMAKGNGh0dHA6Ly93d3cuY2lzY28uY29tL3N1Y3Vy
aXR5L3BraS9jZXJ0cy9jcmNhMjA0OC5jZXIwXAYDVR0gBFUwUzBRBgorBgEEAQkV
AQwAMEMwQQYIKwYBBQUHAgEWNWh0dHA6Ly93d3cuY2lzY28uY29tL3N1bGY3VyaXR5
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
NRMzQ2hpcElEPVVZSk5ORmRRRRlFvN1ZIVmxJRT1qZENNBeU9DDQXhPRG93TlRveE1T
QVg5eWc9MA0GCSqGSIb3DQEBCwUAA4IBAQBKicTRZbVCRjVIR5MQcWXUT086v6Ej
HaHDHTts3YpQoyAVfioNg2x8J6EXcEau4voyVu+eMUuoNL4szPhmmDcULfiCGBcA
/R3EFuoVMIzNT0geziytsCf728KGw1oGuosgVjNGOOahUELu4+F/My7bIJNbH+PD
KjIFmhJpJg0F3q17yClAeXvd13g3W393i35d00Lm5L1WbBfQtyBaOLAbxsHvutrX
u1VZ5sdqSTwTkkO9vKMaQjh7a8J/AmJi93jvzM69pe5711P1zqZfYfpiJ3cyJ0xf
I4brQ1smdczloFD4asF7A+1vor5e4VDBP0ppmeFAJvCQ52JTpj0M0o1D
-----END CERTIFICATE-----

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 3.3SECisco IOS XE 3.3SE	This command was introduced.

Usage Guidelines

If you did not reload the switch 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:                        32768
 Overflow Unicast MAC addresses:               512
 IGMP and Multicast groups:                    8192
 Overflow IGMP and Multicast groups:           512
 Directly connected routes:                    32768
 Indirect routes:                              7680
 Security Access Control Entries:              3072
 QoS Access Control Entries:                   3072
 Policy Based Routing ACEs:                    1024
 Netflow ACEs:                                 1024
 Input Microflow policer ACEs:                 256
 Output Microflow policer ACEs:                256
 Flow SPAN ACEs:                               256
 Tunnels:                                      256
 Control Plane Entries:                        512
 Input Netflow flows:                          8192
 Output Netflow flows:                         16384
 SGT/DGT entries:                              4096
 SGT/DGT Overflow entries:                     512
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.

Device#
```

show tech-support license

To display the debug output, use the **show license tech support** command in privileged EXEC mode.

show tech-support license

Syntax Description

This command has no arguments or keywords.

Command Default

Privileged EXEC (#)

Command History

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

Example

This example shows a sample output from the **show tech-support license** command:

```
Device# show tech-support license
Load for five secs: 5%/0%; one minute: 7%; five minutes: 6%
No time source, 12:36:46.732 EDT Tue Jul 17 2018


------------------ show clock ------------------

Load for five secs: 5%/0%; one minute: 7%; five minutes: 6%
No time source, 12:36:46.733 EDT Tue Jul 17 2018

12:36:46.733 EDT Tue Jul 17 2018
```

```
----------------- show version -----------------

Load for five secs: 5%/0%; one minute: 7%; five minutes: 6%
No time source, 12:36:46.734 EDT Tue Jul 17 2018
Cisco IOS XE Software, Version BLD_V169_THROTTLE_LATEST_20180712_092155_2
Cisco IOS Software [Fuji], Catalyst L3 Switch Software (CAT3K_CAA-UNIVERSALK9-M), Experimental
 Version 16.9.20180712:083903
[v169_throttle-/scratch/mcpre/BLD-BLD_V169_THROTTLE_LATEST_20180712_092155 143]
Copyright (c) 1986-2018 by Cisco Systems, Inc.
Compiled Thu 12-Jul-18 06:52 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.
!
!
!
```

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 license usage	Displays license usage information

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 16.11.1	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 16.11.1	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 16.11.1	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 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 16.11.1	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 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 16.11.1	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 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 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 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
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 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 16.11.1	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 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 16.11.1	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 fabric.
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 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
```

Command Modes   User EXEC (>)

Privileged EXEC (#)

Command History	Release	Modification
	Cisco IOS XE Gibraltar 16.11.1	This command was modified to display the latest reload reason for all switches in a stack in the output.
	Cisco IOS XE 3.3SE	This command was implemented on the Cisco Catalyst 3650 Series Switches

Example:

```
Device# show version

Cisco IOS XE Software, Version BLD_POLARIS_DEV_LATEST_20180713_195337
Cisco IOS Software [Fuji], Catalyst L3 Switch Software (CAT3K_CAA-UNIVERSALK9-M), Experimental
 Version 16.11.20180713:191831
[polaris_dev-/nobackup/mcpre/BLD-BLD_POLARIS_DEV_LATEST_20180713_195337 124]
Copyright (c) 1986-2018 by Cisco Systems, Inc.
Compiled Fri 13-Jul-18 17:11 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: CAT3K_CAA Boot Loader (CAT3K_CAA-HBOOT-M) Version 4.66, engineering software (D)

 --More--          Switch uptime is 14 hours, 23 minutes
Uptime for this control processor is 14 hours, 26 minutes
System returned to ROM by Power Failure or Unknown
System image file is "flash:packages.conf"
Last reload reason: Power Failure or Unknown



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.

 --More--
Technology Package License Information:

-------------------------------------------------------------------------
Technology-package                                       Technology-package
```

```
Current                        Type                        Next reboot
------------------------------------------------------------------------------
ipservicesk9          Smart License                    ipservicesk9
None                  Subscription Smart License       None


cisco WS-C3650-48FQM (MIPS) processor (revision PP) with 829450K/6147K bytes of memory.
Processor board ID FDO2011V00A
1 Virtual Ethernet interface
198 Gigabit Ethernet interfaces
46 Ten Gigabit Ethernet interfaces
2 Forty Gigabit Ethernet interfaces
2048K bytes of non-volatile configuration memory.
4194304K bytes of physical memory.
255037K bytes of Crash Files at crashinfo:.
150009K bytes of Crash Files at crashinfo-2:.
150009K bytes of Crash Files at crashinfo-3:.
 --More--        250456K bytes of Crash Files at crashinfo-5:.
3417161K bytes of Flash at flash:.
3544695K bytes of Flash at flash-2:.
3544695K bytes of Flash at flash-3:.
1609272K bytes of Flash at flash-5:.
0K bytes of WebUI ODM Files at webui:.
250456K bytes of Crash Files at crashinfo-4:.
1609272K bytes of Flash at flash-4:.


Base Ethernet MAC Address       : cc:46:d6:c5:2a:00
Motherboard Assembly Number     : 73-17734-02
Motherboard Serial Number       : FDO200608QX
Model Revision Number           : PP
Motherboard Revision Number     : 05
Model Number                    : WS-C3650-48FQM
System Serial Number            : FDO200608QX


Switch Ports Model              SW Version      SW Image            Mode
------ ----- -----              ----------      ----------          ----
*   1 52    WS-C3650-48FQM      16.11.1         CAT3K_CAA-UNIVERSALK9 INSTALL
    2 58    WS-C3650-12X48UZ    16.11.1         CAT3K_CAA-UNIVERSALK9 INSTALL
    3 56    WS-C3650-12X48UR    16.11.1         CAT3K_CAA-UNIVERSALK9 INSTALL
    4 52    WS-C3650-48PD       16.11.1         CAT3K_CAA-UNIVERSALK9 INSTALL
    5 28    WS-C3650-24PS       16.11.1         CAT3K_CAA-UNIVERSALK9 INSTALL


Switch 02
---------
Switch uptime                   : 14 hours, 26 minutes

Base Ethernet MAC Address       : 58:97:bd:59:58:00
Motherboard Assembly Number     : 73-100820-03
Motherboard Serial Number       : FDO20080L3B
Model Revision Number           : PP
Motherboard Revision Number     : 03
Model Number                    : WS-C3650-12X48UZ
System Serial Number            : FDO20080L3B
Last reload reason              : Power Failure or Unknown

Switch 03
---------
Switch uptime                   : 14 hours, 26 minutes

Base Ethernet MAC Address       : 00:f6:63:8a:45:00
Motherboard Assembly Number     : 73-100818-03
 --More--        Motherboard Serial Number        : FDO20261CMV
Model Revision Number           : A0
```

```
Motherboard Revision Number          : A0
Model Number                         : WS-C3650-12X48UR
System Serial Number                 : FDO20261CMV
Last reload reason                   : Power Failure or Unknown

Switch 04
---------
Switch uptime                        : 13 hours, 42 minutes

Base Ethernet MAC Address            : 70:db:98:01:42:00
Motherboard Assembly Number          : 73-15897-06
Motherboard Serial Number            : FDO210722MV
Model Revision Number                : Q0
Motherboard Revision Number          : A0
Model Number                         : WS-C3650-48PD
System Serial Number                 : FDO210722MV
Last reload reason                   : Power Failure or Unknown

Switch 05
---------
Switch uptime                        : 14 hours, 26 minutes
 --More--
Base Ethernet MAC Address            : f8:72:ea:0d:cc:00
Motherboard Assembly Number          : 73-15128-05
Motherboard Serial Number            : FDO17331P6G
Model Revision Number                : A0
Motherboard Revision Number          : A0
Model Number                         : WS-C3650-24PS
System Serial Number                 : FDO17331P6G
Last reload reason                   : Power Failure or Unknown

Configuration register is 0x102
```

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 8: Default Values for the Temperature Thresholds

Device	Difference between Yellow and Red	Red[1]
Catalyst 3650	14°C	60°C

[1] You cannot configure the red temperature threshold.

Command Modes	Global configuration

Command History

Release	Modification
Cisco IOS XE 3.3SECisco IOS XE 3.3SE	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)#
```

test cable-diagnostics tdr

To run the Time Domain Reflector (TDR) feature on an interface, use the **test cable-diagnostics tdr** command in privileged EXEC mode.

test cable-diagnostics tdr interface *interface-id*

Syntax Description	*interface-id*	The interface on which to run TDR.

Command Default	No default behavior or values.

Command Modes	Privileged EXEC

Command History

Release	Modification
Cisco IOS XE 3.3SECisco IOS XE 3.3SE	This command was introduced.

Usage Guidelines

TDR is supported only on 10/100/100 copper Ethernet ports. It is not supported on 10-Gigabit Ethernet ports or small form-factor pluggable (SFP) module ports.

After you run TDR by using the **test cable-diagnostics tdr interface** *interface-id* command, use the **show cable-diagnostics tdr interface** *interface-id* privileged EXEC command to display the results.

This example shows how to run TDR on an interface:

```
Device# test cable-diagnostics tdr interface gigabitethernet1/0/2
TDR test started on interface Gi1/0/2
A TDR test can take a few seconds to run on an interface
Use 'show cable-diagnostics tdr' to read the TDR results
```

If you enter the **test cable-diagnostics tdr interface** *interface-id* command on an interface that has an link up status and a speed of 10 or 100 Mb/s, these messages appear:

```
Device# test cable-diagnostics tdr interface gigabitethernet1/0/3
TDR test on Gi1/0/9 will affect link state and traffic
TDR test started on interface Gi1/0/3
A TDR test can take a few seconds to run on an interface
Use 'show cable-diagnostics tdr' to read the TDR results.
```

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 3.3SECisco IOS XE 3.3SE	This command was introduced.

Usage Guidelines For Layer 2 traceroute to function properly, Cisco Discovery Protocol (CDP) must be enabled on all of the devicees 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 devicees:

```
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 aborted.
```

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 aborted.
```

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 devicees belong to multiple VLANs:

```
Device# traceroute mac 0000.0201.0601 0000.0201.0201
  Error:Mac found on multiple vlans.
```

```
Layer2 trace aborted.
```

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 3.3SECisco IOS XE 3.3SE	This command was introduced.

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 aborted.
```

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 3.3SECisco IOS XE 3.3SE	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 3.3SECisco IOS XE 3.3SE	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

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 3.3SECisco IOS XE 3.3SE	This command was introduced.

Examples   This example shows how to display the boot loader version on a device:

```
Device: version
CAT3K_CAA Boot Loader (CAT3K_CAA-HBOOT-M) Version 1.2, RELEASE SOFTWARE (P)
Compiled Sun Jul 14 20:22:00 PDT 2013 by rel
```