



System Management Commands

- [arp, page 5](#)
- [boot, page 6](#)
- [cat, page 8](#)
- [clear location, page 9](#)
- [clear location statistics, page 10](#)
- [clear nmsp statistics, page 11](#)
- [clear wireless ccx statistics, page 12](#)
- [clear wireless client tsm dot11, page 13](#)
- [clear wireless location s69 statistics, page 14](#)
- [copy, page 15](#)
- [copy startup-config tftp:, page 16](#)
- [copy tftp: startup-config, page 17](#)
- [debug call-admission wireless all, page 18](#)
- [debug rfid, page 19](#)
- [debug voice diagnostics mac-address, page 20](#)
- [debug wps mfp, page 21](#)
- [delete, page 22](#)
- [dir, page 23](#)
- [emergency-install, page 25](#)
- [exit, page 27](#)
- [flash_init, page 28](#)
- [help, page 29](#)
- [license right-to-use, page 30](#)
- [location, page 32](#)

- [location algorithm, page 36](#)
- [location expiry, page 37](#)
- [location notify-threshold, page 38](#)
- [location plm calibrating, page 39](#)
- [location rfid, page 40](#)
- [location rssi-half-life, page 41](#)
- [mac address-table move update, page 42](#)
- [mgmt_init, page 44](#)
- [mkdir, page 45](#)
- [more, page 46](#)
- [nmsp notification interval, page 47](#)
- [no debug all, page 49](#)
- [readrtc, page 50](#)
- [rename, page 51](#)
- [reset, page 52](#)
- [rmdir, page 53](#)
- [sdm prefer, page 54](#)
- [set, page 55](#)
- [show ap name config general, page 58](#)
- [show avc client, page 60](#)
- [show avc wlan, page 61](#)
- [show cable-diagnostics tdr, page 63](#)
- [show debug, page 66](#)
- [show env, page 67](#)
- [show flow monitor, page 70](#)
- [show license right-to-use, page 75](#)
- [show location, page 77](#)
- [show location ap-detect, page 78](#)
- [show mac address-table move update, page 80](#)
- [show nmsp, page 81](#)
- [show sdm prefer, page 83](#)
- [show tech-support wireless, page 85](#)
- [show wireless ap summary \(MA\), page 87](#)

- [show wireless ap summary, page 88](#)
- [show wireless band-select, page 89](#)
- [show wireless client calls, page 90](#)
- [show wireless client dot11, page 91](#)
- [show wireless client location-calibration, page 92](#)
- [show wireless client probing, page 93](#)
- [show wireless client summary, page 94](#)
- [show wireless client timers, page 95](#)
- [show wireless client voice diagnostics, page 96](#)
- [show wireless country, page 97](#)
- [show wireless detail, page 100](#)
- [show wireless dtls connections, page 101](#)
- [show wireless flow-control, page 102](#)
- [show wireless flow-control statistics, page 103](#)
- [show wireless load-balancing, page 104](#)
- [show wireless mobility summary, page 105](#)
- [show wireless performance, page 106](#)
- [show wireless pmk-cache, page 107](#)
- [show wireless probe, page 108](#)
- [show wireless sip preferred-call-no, page 109](#)
- [show wireless summary, page 110](#)
- [show wireless wlan summary, page 111](#)
- [show wlan name, page 112](#)
- [shutdown, page 115](#)
- [system env temperature threshold yellow, page 116](#)
- [test cable-diagnostics tdr, page 118](#)
- [traceroute mac, page 119](#)
- [traceroute mac ip, page 122](#)
- [trapflags, page 125](#)
- [trapflags client, page 126](#)
- [type, page 127](#)
- [unset, page 128](#)
- [version, page 130](#)

- [wireless client](#), page 131
- [wireless client mac-address deauthenticate](#), page 133
- [wireless client mac-address](#), page 134
- [wireless load-balancing](#), page 139
- [wireless sip preferred-call-no](#), page 140
- [writertc](#), page 141

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

<i>ip_address</i>	(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 3.3SE	Cisco 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:

```
Switch: 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.
<i>filesystem:</i>	Alias for a file system. Use flash: for the system board flash device; use usbflash0: for USB memory sticks.
<i>/file-url</i>	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 3.3SE	Cisco IOS XE 3.3SE
	This command was introduced.

Usage Guidelines

When you enter the **boot** command without any arguments, the switch 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.

Examples

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

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

<i>filesystem:</i>	Specifies a file system.
<i>/file-url</i>	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 3.3SE	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:

```
Switch: 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 <i>mac-address</i>	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 3.3SE	This command was introduced.

Examples

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

```
Switch> 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 3.3SE	Cisco IOS XE 3.3SE
	This command was introduced.

Examples

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

```
Switch> clear location statistics
```

clear nmsp statistics

To clear the Network Mobility Services Protocol (NMSP) statistics, use the **clear nmsp statistics** command in EXEC mode.

clear nmsp 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.

Examples The following is sample output from the **clear nmsp statistics** command and shows how to clear all statistics about NMSP information exchanged between the controller and the connected Cisco Mobility Services Engine (MSE):

```
Switch> clear nmsp statistics
```

clear wireless ccx statistics

To clear CCX statistics, use the **clear wireless ccx statistics** command in EXEC mode.

clear wireless ccx 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.

Examples The following is sample output from the **clear wireless ccx statistics** command and shows how to clear all collected statistics about CCX clients:

```
Switch> clear wireless ccx statistics
```

clear wireless client tsm dot11

To clear the traffic stream metrics (TSM) statistics for a particular access point or all of the access points to which this client is associated, use the **clear wireless client tsm dot11** command in EXEC mode.

clear wireless client tsm dot11 {**24ghz**|**5ghz**} *client-mac-addr* {**all**| **name** *ap-name*}

Syntax Description

24ghz	Specifies the 802.11a network.
5ghz	Specifies the 802.11b network.
<i>client-mac-addr</i>	MAC address of the client.
all	Specifies all access points.
name <i>ap-name</i>	Name of a Cisco lightweight access point.

Command Default

No default behavior or values.

Command Modes

User EXEC
Privileged EXEC

Command History

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

Examples

The following is sample output from the **clear wireless client tsm dot11** command and shows how to clear the TSM for the MAC address 00:40:96:a8:f7:98 on all of the access points 5-GHz radios where this client is known:

```
Switch> clear wireless client tsm dot11 5ghz 00:40:96:a8:f7:98 all
```

clear wireless location s69 statistics

To clear statistics about S69 exchanges with CCXv5 clients, use the **clear wireless location s69 statistics** command in EXEC mode.

clear wireless location s69 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 3.3SE	Cisco IOS XE 3.3SE
	This command was introduced.

Usage Guidelines

S69 messages are exchanged between CCXv5 clients and the wireless infrastructure. The CCXv5 client uses S69 message to request location information, that is then returned by the wireless infrastructure through a S69 response message.

Examples

The following is sample output from the **clear wireless location s69 statistics** command and shows how to clear statistics about S69 exchanges with CCXv5 clients:

```
Switch> clear wireless location s69 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

<i>filesystem:</i>	Alias for a file system. Use usbflash0: for USB memory sticks.
<i>/source-file-url</i>	Path (directory) and filename (source) to be copied.
<i>/destination-file-url</i>	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 3.3SE	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:

```
Switch: 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

<i>remote host {ip-address}/{name}</i>	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:

```
Switch: 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

<i>remote host {ip-address}/{name}</i>	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:

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

debug call-admission wireless all

To enable debugging of the wireless Call Admission Control (CAC) feature, use the **debug call-admission wireless all** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug call-admission wireless all [**switch** *switch*]

no debug call-admission wireless all [**switch** *switch*]

Syntax Description

switch	Configures debugging options for all wireless CAC messages associated to a particular switch.
---------------	---

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

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

Examples

The following is sample output from the **debug call-admission wireless switch** command and shows how to enable debugging options for CAC messages:

```
Switch# debug call-admission wireless switch 1 all
```

debug rfid

To configure radio-frequency identification (RFID) debug options, use the **debug rfid** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug rfid {*debug_leaf_name* | **all** | **detail** | **error** | **nmsp** | **receive**} [**filter** | **switch** *switch*]

no debug rfid {*debug_leaf_name* | **all** | **detail** | **error** | **nmsp** | **receive**} [**filter** | **switch** *switch*]

Syntax Description

<i>debug_leaf_name</i>	Debug leaf name.
all	Configures debugging of all RFID.
detail	Configures debugging of RFID detail.
error	Configures debugging of RFID error messages.
nmsp	Configures debugging of RFID Network Mobility Services Protocol (NMSP) messages.
receive	Configures debugging of incoming RFID tag messages.
<i>filter</i>	Debug flag filter name.
switch <i>switch</i>	Configures RFID debugging for switch.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

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

Examples

The following is sample output from the **debug rfid** command and shows how to enable debugging of RFID error messages:

```
Switch# debug rfid error switch 1
```

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 <i>mac-address1</i> mac-address <i>mac-address2</i>	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 3.3SE	This command was introduced.

Examples

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:

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

debug wps mfp

To enable WPS MFP debugging options, use the **debug wps mfp** command in privileged EXEC mode. To disable debugging, use the no form of this command.

debug wps mfp {**all** | **capwap** | **client** | **detail** | **mm** | **report**} [**switch** *switch*]

Syntax Description

wps mfp	Configures WPS MFP debugging options.
all	Displays all WPS MFP debugging messages.
capwap	Displays MFP messages.
client	Displays client MFP messages.
detail	Displays detailed MFP CAPWAP messages.
mm	Displays MFP mobility (inter-controller) messages.
report	Displays MFP reports.
switch <i>switch</i>	Displays the WPS MFP debugging for the switch.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

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

Examples

This example shows how to enable WPS MFP debugging options for client:

```
Switch# debug wps mfp client switch 1
```

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

<i>filesystem:</i>	Alias for a file system. Use usbflash0: for USB memory sticks.
<i>/file-url...</i>	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 3.3SE	This command was introduced.

Usage Guidelines

Filenames and directory names are case sensitive.

The switch prompts you for confirmation before deleting each file.

Examples

This example shows how to delete two files:

```
Switch: 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

<i>filesystem:</i>	Alias for a file system. Use flash: for the system board flash device; use usbflash0: for USB memory sticks.
<i>/file-url</i>	(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 3.3SE	This command was introduced.

Usage Guidelines

Directory names are case sensitive.

Examples

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

```
Switch: 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.

Field	Description
-rwx	File permission, which can be any or all of the following: <ul style="list-style-type: none"> • d—directory • r—readable • w—writable • x—executable
1644045	Size of the file.
<date>	Last modification date.
env_vars	Filename.

Related Commands

Command	Description
mkdir	Creates one or more directories on the specified file system.
rmdir	Removes one or more empty directories from the specified file system.

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

<i><url></i>	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 3.3SE	This command was introduced.

Usage Guidelines

The boot flash is erased during the installation operation.

Examples

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

```
Switch: 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.

Examples	<p>This example shows how to exit the configuration mode:</p> <pre>Switch(config)# exit Switch#</pre>
-----------------	--

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 3.3SE	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.

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

```
Switch: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
```

license right-to-use

To configure right-to-use access point adder licenses on the switch, use the **license right-to-use** command in privileged EXEC mode.

license right-to-use {**activate** | **deactivate**} **apcount** | **ibase** | **ipservices** | **lanbase**

Syntax Description

activate	Activates permanent or evaluation ap-count licenses.
deactivate	Deactivates permanent or evaluation ap-count licenses.
apcount <i>count</i>	Specifies the number of ap-count licenses added. You can configure the number of adder licenses from 5 to 50.
ibase <i>count</i>	Activates ibase licenses on the switch.
ipservices <i>count</i>	Activates ipservices licenses on the switch.
lanbase <i>count</i>	Activates lanbase licenses on the switch.

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 3.3SE	This command was introduced.

Examples

This example shows how to activate an ap-count evaluation license:

```
Switch# license right-to-use activate apcount evaluation
Switch# end
```

This example shows how to activate an ap-count permanent license:

```
Switch# license right-to-use deactivate apcount evaluation  
Switch# end
```

This example shows how to add a new ap-count license:

```
Switch# license right-to-use activate apcount 500 slot 1  
Switch# end
```

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| algorithm| civic-location identifier {host| id}| civic-location identifier {host| id}| elin-location {string |identifier id}|
expiry {calibrating-clienttimeout-value|clienttimeout-value|rouge-aps timeout-value|tagtimeout-value}|
geo-location identifier {host| id}| notify-threshold {clientdb|rouge-apsdb|tagsdb| plm {calibrating|
{multiband | uniband}| clientburst-interval}| prefer {cdp weightpriority-value|lldp-med
weightpriority-value|static config weightpriority-value}|rfid {status
|timeoutrfid-timeout-value|vendor-namename}| rssi-half-life {
calibrating-clientseconds|clientseconds|rouge-apsseconds|tagsseconds}

no location {admin-tag string| algorithm| civic-location identifier {host| id}| civic-location identifier
{host| id}| elin-location {string |identifier id}|
expiry {calibrating-clienttimeout-value|clienttimeout-value|rouge-aps timeout-value|tagtimeout-value}|
geo-location identifier {host| id}| notify-threshold {clientdb|rouge-apsdb|tagsdb| plm {calibrating|
{multiband | uniband}| clientburst-interval}| prefer {cdp weightpriority-value|lldp-med
weightpriority-value|static config weightpriority-value}|rfid {status
|timeoutrfid-timeout-value|vendor-namename}| rssi-half-life {
calibrating-clientseconds|clientseconds|rouge-apsseconds|tagsseconds}
```

Syntax Description

admin-tag <i>string</i>	Configures administrative tag or site information. Site or location information in alphanumeric format.
algorithm	Configures the algorithm used to average RSSI and SNR values.
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.
<i>id</i>	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).

expiry { calibrating-client client rogue-aps tags } <i>timeout-value</i>	Configures the timeout for RSSI values for calibrating clients, clients, rogue access points, and RFID tags. The valid range for the timeout parameter for calibrating clients is 1 to 3600 seconds, and the default value is 5 seconds. The valid range for the timeout parameter for clients, rogue access points, and RFID tags is 5 to 3600 seconds, and the default value is 5 seconds
geo-location	Configures geo-spatial location information.
notify-threshold { client rogue-aps tags } <i>db</i>	Configures the NMSP notification threshold for RSSI measurements. The valid range for the threshold parameter is 0 to 10 dB, and the default value is 0 dB.
calibrating { multiband uniband } client <i>seconds</i>	Configures path loss measurement (CCX S60) request for calibrating clients and burst interval for clients. The valid range for the burst interval parameter is 0 to 3600 seconds.
prefer	Sets location information source priority.
rfid	Configures RFID tag tracking for a location.
rssi-half-life	Configures the RSSI half life for various devices.

Command Default No default behavior or values.

Command Modes Global configuration

Release	Modification
Cisco IOS XE 3.3SE	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.

Examples

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

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

```
Switch(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:

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

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

location algorithm

To configure the algorithm used to average RSSI and SNR values, use the **location algorithm** command in global configuration mode. To remove the algorithm used to average RSSI and SNR values, use the **no** form of this command.

location algorithm {**rssi-average** | **simple**}

no location algorithm {**rssi-average** | **simple**}

Syntax Description

rssi-average	Specifies a more accurate algorithm but with more CPU overhead.
simple	Specifies faster algorithm with smaller CPU overhead but less accuracy.

Command Default

RSSI average

Command Modes

Global configuration

Command History

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

Examples

This example shows how to configure a more accurate algorithm but with more CPU overhead:

```
Switch# configure terminal
Switch(config)# location algorithm rssi-average
Switch(config)# end
```

location expiry

To configure the timeout for RSSI values, use the **location expiry** command in global configuration mode.

location expiry {**calibrating-client** | **client** | **rogue-aps** | **tags** } *timeout-value*

Syntax Description

calibrating-client	Specifies the RSSI timeout value for calibrating clients.
client	(Optional) Specifies the RSSI timeout value for clients.
rogue-aps	Specifies the RSSI timeout value for rogue access points.
tags	Specifies the RSSI timeout value for RFID tags.
<i>timeout-value</i>	<p>The valid range for the timeout parameter for calibrating clients is 1 to 3600 seconds, and the default value is 5 seconds.</p> <p>The valid range for the timeout parameter for clients, rogue access points, and RFID tags is 5 to 3600 seconds, and the default value is 5 seconds.</p>

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

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

Examples

This example shows how to set the RSSI timeout value for wireless clients:

```
Switch# configure terminal
Switch(config)# location expiry client 1000
Switch(config)# end
```

location notify-threshold

To configure the NMSP notification threshold for RSSI measurements, use the **location notify-threshold** command in global configuration mode. To remove the NMSP notification threshold for RSSI measurements, use the **no** form of this command.

location notify-threshold {**client** | **rogue-aps** | **tags** } *db*

no location notify-threshold {**client** | **rogue-aps** | **tags** }

Syntax Description

client	Specifies the NMSP notification threshold (in dB) for clients and rogue clients. The valid range for the threshold parameter is 0 to 10 dB, and the default value is 0 dB.
rogue-aps	Specifies the NMSP notification threshold (in dB) for rogue access points. The valid range for the threshold parameter is 0 to 10 dB, and the default value is 0 dB.
tags	Specifies the NMSP notification threshold (in dB) for RFID tags. The valid range for the threshold parameter is 0 to 10 dB, and the default value is 0 dB.
<i>db</i>	The valid range for the threshold parameter is 0 to 10 dB, and the default value is 0 dB.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

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

Examples

This example shows how to configure the NMSP notification threshold to 10 dB for clients. A notification NMSP message is sent to MSE as soon as the client RSSI changes by 10 dB:

```
Switch# configure terminal
Switch(config)# location notify-threshold client 10
Switch(config)# end
```

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 3.3SE	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.

Examples

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

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

location rfid

To configure RFID tag tracking for a location, use the **location rfid** command in global configuration mode. To remove a RFID tag tracking for a location, use the **no** form of this command.

location rfid { **status**| **timeout** *seconds*| **vendor-name** *name*}

no location rfid { **status**| **timeout** *seconds*| **vendor-name**}

Syntax Description

status	Enables location tracking for RFID tags. The no location rfid status command disables location tracking for tags.
timeout <i>seconds</i>	Specifies the location RFID timeout value. Determines the amount of time for which a detected RFID location information is considered as valid. Any RSSI change (below the RSSI threshold) in the configured interval do not result in a new location computation and a message is sent to the MSE. The valid timeout range is from 60 through 7200 seconds.
vendor-name <i>name</i>	Specifies the RFID tag vendor name.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

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

Usage Guidelines

The **no location rfid status** command disables location RFID status. The **no location rfid timeout** command returns to the default timeout value. The **no location rfid vendor-name** disables tracking for a particular vendor.

Examples

The example shows how to configure the static RFID tag data timeout:

```
Switch# configure terminal
Switch(config)# location rfid timeout 1000
Switch(config)# end
```


location rssi-half-life

To configure the RSSI half life for various devices, use the **location rssi-half-life** command in global configuration mode. To remove a RSSI half life for various devices, use the **no** form of this command.

location rssi-half-life { **calibrating-client** | **client** | **rogue-aps** | **tags** } *seconds*

no location rssi-half-life { **calibrating-client** | **client** | **rogue-aps** | **tags** }

Syntax Description

calibrating-client	Specifies the RSSI half life for calibrating clients.
client	Specifies the RSSI half life for clients.
rogue-aps	Specifies the RSSI half life for rogue access points.
tags	Specifies the RSSI half life for RFID tags.
<i>seconds</i>	The valid range for the half-life parameter is 0, 1, 2, 5, 10, 20, 30, 60, 90, 120, 180, or 300 seconds, and the default value is 0 seconds.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

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

Examples

This example shows how to configure the half life value for a client RSSI to 100 seconds:

```
Switch# configure terminal
Switch(config)# location rssi-half-life client 100
Switch(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

Release	Modification
Cisco IOS XE 3.3SE	Cisco 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:

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

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

```
Switch# configure terminal
Switch(config)# mac address-table move update receive
Switch(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 3.3SE	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:

Switch: **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

<i>filesystem:</i>	Alias for a file system. Use usbflash0: for USB memory sticks.
<i>/directory-url...</i>	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 3.3SE	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.

Examples

This example shows how to make a directory called Saved_Configs:

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

Related Commands

Command	Description
dir	Displays the list of files and directories on the specified file system.
rmdir	Removes one or more empty directories from the specified file system.

more

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

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

Syntax Description

<i>filesystem:</i>	Alias for a file system. Use flash: for the system board flash device.
<i>/file-url...</i>	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:

```
Switch: 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:
```

nmosp notification interval

To modify the Network Mobility Services Protocol (NMSP) notification interval value on the controller to address latency in the network, use the **nmosp notification interval** command in global configuration mode.

nmosp notification interval { **attachment** | **location** | **rss**i { **clients** | **r**fid | **rogues** { **ap** | **client** } } }

Syntax Description

attachment	Specifies the time used to aggregate attachment information.
location	Specifies the time used to aggregate location information.
rss i	Specifies the time used to aggregate RSSI information.
clients	Specifies the time interval for clients.
r fid	Specifies the time interval for rfid tags.
rogues	Specifies the time interval for rogue APs and rogue clients .
ap	Specifies the time used to aggregate rogue APs .
client	Specifies the time used to aggregate rogue clients.

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

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

Examples

This example shows how to set the NMSP notification interval for the active RFID tags to 25 seconds:

```
Switch# configure terminal
Switch(config)# nmosp notification-interval rfid 25
Switch(config)# end
```

This example shows how to modify NMSP notification intervals for device attachment (connecting to the network or disconnecting from the network) every 10 seconds:

```
Switch# configure terminal
```

```
Switch(config)# nmosp notification-interval attachment 10  
Switch(config)# end
```

This example shows how to configure NMSP notification intervals for location parameters (location change) every 20 seconds:

```
Switch# configure terminal  
Switch(config)# nmosp notification-interval location 20  
Switch(config)# 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.

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

readrtc

To display the current value of the Real Time Clock (RTC) setting, use the **readrtc** command in boot loader mode.

readrtc

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 3.3SE	This command was introduced.

Examples

This example shows how to display the current RTC setting:

```
Switch: readrtc
Wednesday 03-27-13
11:42:38
```

Related Commands

Command	Description
writrtc	Updates the value of the Real Time Clock (RTC) setting.

rename

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

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

Syntax Description

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

Command Default

No default behavior or values.

Command Modes

Boot loader

Command History

Release	Modification
Cisco 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*:

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

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

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 switch; 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 3.3SE	Cisco IOS XE 3.3SE
	This command was introduced.

Examples

This example shows how to reset the system:

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

Related Commands

Command	Description
set	Sets or displays environment variables.
unset	Resets one or more environment variables.

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

<i>filesystem:</i>	Alias for a file system. Use usbflash0: for USB memory sticks.
<i>/directory-url...</i>	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 3.3SE	Cisco 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 switch prompts you for confirmation before deleting each directory.

Examples

This example shows how to remove a directory:

Switch: **rmdir usbflash0:Test**

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

Related Commands

Command	Description
dir	Displays the list of files and directories on the specified file system.
mkdir	Creates one or more directories on the specified file system.

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

Usage Guidelines

In a switch stack, all stack members must use the same SDM template that is stored on the active switch. When a new switch is added to a stack, the SDM configuration that is stored on the active switch overrides the template configured on an individual switch.

Examples

This example shows how to configure the advanced template:

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

Related Commands

Command	Description
show sdm prefer	Displays the SDM template in use.

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 switch.

set *variable value*

Syntax Description

<i>variable</i>	Use one of the following keywords for <i>variable</i> and the appropriate value for <i>value</i> :
<i>value</i>	<p>MANUAL_BOOT—Decides whether the switch automatically or manually boots.</p> <p>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 switch from the boot loader mode.</p>
	<p>BOOT <i>filesystem:/file-url</i>—Identifies a semicolon-separated list of executable files to try to load and execute when automatically booting.</p> <p>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.</p>
	<p>ENABLE_BREAK—Allows the automatic boot process to be interrupted when the user presses the Break key on the console.</p> <p>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.</p>
	<p>HELPER <i>filesystem:/file-url</i>—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.</p>
	<p>PS1 <i>prompt</i>—Specifies a string that is used as the command-line prompt in boot loader mode.</p>
	<p>CONFIG_FILE <i>flash:/file-url</i>—Specifies the filename that Cisco IOS uses to read and write a nonvolatile copy of the system configuration.</p>
	<p>BAUD <i>rate</i>—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.</p> <p>The most commonly used values are 300, 1200, 2400, 9600, 19200, 57600, and 115200.</p>
	<p>SWITCH_NUMBER <i>stack-member-number</i>—Changes the member number of a stack member.</p>
	<p>SWITCH_PRIORITY <i>priority-number</i>—Changes the priority value of a stack member.</p>

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 switch:

CONFIG_FILE: config.text

BAUD: 9600 b/s

SWITCH_NUMBER: 1

SWITCH_PRIORITY: 1

**Note**

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

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

Many environment variables are predefined and have default values.

Command Modes

Boot loader

Command History

Release	Modification
Cisco IOS XE 3.3SE	Cisco 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 switch *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 (=).

Examples

This example shows how to set the SWITCH_PRIORITY environment variable:

```
Switch: set SWITCH_PRIORITY 2
```

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

Related Commands

Command	Description
reset	Performs a hard reset on the system.
unset	Resets one or more environment variables.

show ap name config general

To display detailed information of an MA access point, use the **show ap name config general** command.

show ap name *ap-name ma-ip* config general

Syntax Description

<i>ap-name</i>	Access Point name.
<i>ma-ip</i>	MA IPv4 Address.

Command Default

None

Command History

Release	Modification
Cisco IOS XE 3.7.3E	This command was introduced.

Usage Guidelines

This command works only with MC.

Examples

The following example shows how to display the detailed information of an MA access point:

```
Cisco controller# show ap name AP5 211.0.0.4 config general

Cisco AP Name                : AP5
Cisco AP Identifier           : 0
Country Code                  : US - United States
Regulatory Domain Allowed by Country : 802.11bg:-A      802.11a:-AB
AP Country Code               : US - United States
AP Regulatory Domain
  Slot 0                      : -A
  Slot 1                      : -A
Switch Port Number            : Gi1/0/5
MAC Address                   : 6c20.56e1.4a57
IP Address Configuration      : DHCP
IP Address                    : 211.0.0.170
IP Netmask                    : 255.255.255.0
Gateway IP Address            : 211.0.0.100
CAPWAP Path MTU               : 1485
Telnet State                   : Disabled
SSH State                     : Disabled
Jumbo MTU Status              : Disabled
Cisco AP Location             : default location
Cisco AP Group Name           : default-group
Administrative State          : Enabled
Operation State               : Registered
AP Mode                       : Local
AP Submode                    : Not Configured
Remote AP Debug               : Disabled
Logging Trap Severity Level   : informational
Software Version              : 10.3.123.92
Boot Version                   : 12.4.23.0
```

```
Stats Reporting Period           : 180
LED State                       : Enabled
PoE Pre-Standard Switch         : Disabled
PoE Power Injector MAC Address  : Disabled
Power Type/Mode                 : PoE/Full Power (normal mode)
Number of Slots                 : 2
AP Model                        : AIR-CAP3602I-A-K9
AP Image                        : C3600-K9W8-M
IOS Version                     : 15.3(20151222:165605)$
Reset Button                    : Enabled
AP Serial Number                : FGL1645W0W1
AP Certificate Type             : Manufacture Installed
Management Frame Protection Validation : Disabled
AP User Mode                    : Customized
AP User Name                    : cisco
AP 802.1X User Mode             : Not Configured
AP 802.1X User Name            : Not Configured
Cisco AP System Logging Host    : 255.255.255.255
AP Up Time                      : 23 minutes 53 seconds
AP CAPWAP Up Time              : 21 minutes 53 seconds
Join Date and Time              : 01/18/2016 02:36:09
Join Taken Time                 : 1 minute 59 seconds
Ethernet Port Duplex            : Auto
Ethernet Port Speed             : Auto
AP Link Latency                 : Disabled
Rogue Detection                 : Enabled
AP TCP MSS Adjust               : Disabled
AP TCP MSS Size                 : 0
AP IPv6 TCP MSS Adjust          : Disabled
AP IPv6 TCP MSS Size            : 1220
```

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 <i>client-mac</i>	Specifies the client MAC address.
top <i>n</i> 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.

Examples

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

Switch# **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 avc wlan

To display information about top applications and users using the applications, use the **show avc wlan** command in privileged EXEC mode.

show avc wlan ssid top n application [aggregate | upstream | downstream]

Syntax Description

wlan ssid	Specifies the Service Set Identifier (SSID) for WLAN.
top n application	Specifies the number of top "N" applications.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

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

Examples

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

Switch# **show avc wlan Lobby_WLAN top 10 application aggregate**

Cumulative Stats:

No.	AppName	Packet-Count	Byte-Count	AvgPkt-Size	usage%
1	ssl	10598677	1979525706	997	42
2	vnc	5550900	3764612847	678	14
3	http	3043131	2691327197	884	10
4	unknown	1856297	1140264956	614	4
5	video-over-http	1625019	2063335150	1269	8
6	binary-over-http	1329115	1744190344	1312	6
7	webex-meeting	1146872	540713787	471	2
8	rtp	923900	635650544	688	2
9	unknown	752341	911000213	1210	3
10	youtube	631085	706636186	1119	3

Last Interval (90 seconds) Stats:

No.	AppName	Packet-Count	Byte-Count	AvgPkt-Size	usage%
1	vnc	687093	602731844	877	68
2	video-over-http	213272	279831588	1312	31
3	ssl	6515	5029365	771	1
4	webex-meeting	3649	1722663	472	0
5	http	2634	1334355	506	0
6	unknown	1436	99412	69	0
7	google-services	722	378121	523	0
8	linkedin	655	393263	600	0
9	exchange	432	167390	387	0

show avc wlan

10	gtalk-chat	330	17330	52	0
----	------------	-----	-------	----	---

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

<i>interface-id</i>	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 3.3SE	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 switch:

```
Switch# 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.

Field	Description
Pair length	<p>The location of the problem on the cable, with respect to your switch. TDR can only find the location in one of these cases:</p> <ul style="list-style-type: none"> • 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	<p>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.</p>
Pair status	<p>The status of the pair of wires on which TDR is running:</p> <ul style="list-style-type: none"> • 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:

```
Switch# 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:

```
Switch# 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 switch 1
```

Related Commands

Command	Description
test cable-diagnostics tdr	Runs the Time Domain Reflector (TDR) feature on an interface.

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

<i>Condition identifier</i>	Sets the value of the condition identifier to be used. Range is between 1 and 1000.
<i>All conditions</i>	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:

```
Switch# 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, stack master, or stack member), 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 <i>switch-number</i>	(Optional) Displays the power supply status for a specific switch.
stack <i>switch-number</i>	(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 stack member 1 from the master switch:

```
Switch> show env stack 1
Switch :1
Switch 1 Fan 1 is OK
Switch 1 Fan 2 is OK
Switch 1 Fan 3 is OK
FAN-PS1 is OK
FAN-PS2 is NOT PRESENT
Switch 1: SYSTEM TEMPERATURE is OK
Inlet Temperature Value: 32 Degree Celsius
Temperature State: GREEN
Yellow Threshold : 46 Degree Celsius
Red Threshold : 56 Degree Celsius

Hotspot Temperature Value: 43 Degree Celsius
Temperature State: GREEN
Yellow Threshold : 105 Degree Celsius
Red Threshold : 125 Degree Celsius

Switch>
```

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

```
Switch> show env temperature status
Temperature Value: 26 Degree Celsius
Temperature State: GREEN
Yellow Threshold : 46 Degree Celsius
Red Threshold : 56 Degree Celsius

Hotspot Temperature Value: 43 Degree Celsius
Temperature State: GREEN
Yellow Threshold : 105 Degree Celsius
Red Threshold : 125 Degree Celsius

Switch>
```

Examples

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

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

Switch>
```

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

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

Switch>

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

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

show flow monitor

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

show flow monitor [**broker** [**detail**| **picture**]] [**name** *monitor-name* [**cache** [**format** {**csv**| **record**| **table**}]]| **provisioning**| **statistics**]

Syntax Description

broker	(Optional) Displays information about the state of the broker for the flow monitor
detail	(Optional) Displays detailed information about the flow monitor broker.
picture	(Optional) Displays a picture of the broker state.
name	(Optional) Specifies the name of a flow monitor.
<i>monitor-name</i>	(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.
provisioning	(Optional) Displays the flow monitor provisioning information.
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 Flexible NetFlow 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 Flexible NetFlow collects values as additional data for the cache.

Examples

The following example displays the status for a flow monitor:

```
Switch# 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 4: 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: <ul style="list-style-type: none"> • allocated—The cache is allocated. • being deleted—The cache is being deleted. • not allocated—The cache is not allocated.
Size	Current cache size.
Inactive Timeout	Current value for the inactive timeout in seconds.

Field	Description
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:

```
Switch# show flow monitor FLOW-MONITOR-1 cache
  Cache type:                Normal (Platform cache)
  Cache size:                Unknown
  Current entries:           1

  Flows added:               3
  Flows aged:                2
    - Active timeout        ( 300 secs)  2

DATALINK MAC SOURCE ADDRESS INPUT:  0000.0000.1000
DATALINK MAC DESTINATION ADDRESS INPUT:  6400.F125.59E6
IPV6 SOURCE ADDRESS:                2001:DB8::1
IPV6 DESTINATION ADDRESS:            2001:DB8:1::1
TRNS SOURCE PORT:                   1111
TRNS DESTINATION PORT:               2222
IP VERSION:                         6
IP PROTOCOL:                        6
IP TOS:                              0x05
IP TTL:                              11
tcp flags:                           0x20
counter bytes long:                  132059538
counter packets long:                1158417
```

This table describes the significant fields shown in the display.

Table 5: show flow monitor monitor-name cache Field Descriptions

Field	Description
Cache type	Flow monitor cache type. The value is always normal, as it is the only supported cache type.
Cache Size	Number of entries in the cache.
Current entries	Number of entries in the cache that are in use.
Flows added	Flows added to the cache since the cache was created.
Flows aged	Flows expired from the cache since the cache was created.
Active timeout	Current value for the active timeout in seconds.
Inactive timeout	Current value for the inactive timeout in seconds.
DATALINK MAC SOURCE ADDRESS INPUT	MAC source address of input packets.
DATALINK MAC DESTINATION ADDRESS INPUT	MAC destination address of input packets.
IPV6 SOURCE ADDRESS	IPv6 source address.

Field	Description
IPV6 DESTINATION ADDRESS	IPv6 destination address.
TRNS SOURCE PORT	Source port for the transport protocol.
TRNS DESTINATION PORT	Destination port for the transport protocol.
IP VERSION	IP version.
IP PROTOCOL	Protocol number.
IP TOS	IP type of service (ToS) value.
IP TTL	IP time-to-live (TTL) value.
tcp flags	Value of the TCP flags.
counter bytes	Number of bytes that have been counted.
counter packets	Number of packets that have been counted.

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

```
Switch# show flow monitor FLOW-MONITOR-1 cache format table
Cache type: Normal (Platform cache)
Cache size: Unknown
Current entries: 1

Flows added: 3
Flows aged: 2
- Active timeout ( 300 secs) 2

DATALINK MAC SRC ADDR INPUT DATALINK MAC DST ADDR INPUT IPV6 SRC ADDR IPV6 DST ADDR
TRNS SRC PORT TRNS DST PORT IP VERSION IP PROT IP TOS IP TTL tcp flags bytes long
pkts long
=====
=====
=====
0000.0000.1000 6400.F125.59E6 2001:DB8::1 2001:DB8:1::1
1111 2222 6 6 0x05 11 0x20 132059538
1158417
```

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:

```
Switch# show flow monitor name FLOW-MONITOR-IPv6 cache format record
Cache type: Normal (Platform cache)
Cache size: Unknown
Current entries: 1

Flows added: 3
Flows aged: 2
- Active timeout ( 300 secs) 2

DATALINK MAC SOURCE ADDRESS INPUT: 0000.0000.1000
DATALINK MAC DESTINATION ADDRESS INPUT: 6400.F125.59E6
IPV6 SOURCE ADDRESS: 2001::2
IPV6 DESTINATION ADDRESS: 2002::2
```

```
TRNS SOURCE PORT:          1111
TRNS DESTINATION PORT:     2222
IP VERSION:                6
IP PROTOCOL:               6
IP TOS:                    0x05
IP TTL:                    11
tcp flags:                 0x20
counter bytes long:        132059538
counter packets long:      1158417
```

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

```
Switch# show flow monitor FLOW-MONITOR-1 statistics
Cache type:                Normal (Platform cache)
Cache size:                Unknown
Current entries:           1

Flows added:               3
Flows aged:                2
  - Active timeout        ( 300 secs) 2
```

show license right-to-use

To display detailed information for apcount adder licenses installed on the switch, use the **show license right-to-use** command in EXEC modes.

show license right-to-use {default | detail | eula | mismatch | slot | summary | usage}

Syntax Description

default	Displays the default license information.
detail	Displays details of all the licenses in the stack.
eula	Displays the EULA text.
mismatch	Displays mismatch license information.
slot	Specifies the switch number.
summary	Displays consolidated stack-wide license information.
usage	Displays the usage details of all licenses.

Command Default

No default behavior or values.

Command Modes

User EXEC
Privileged EXEC

Command History

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

Examples

The following is sample output from the **show license right-to-use usage** command and displays all the detailed information:

Switch# **show license right-to-use usage**

Slot#	License Name	Type	usage-duration (y:m:d)	In-Use	EULA
1	ipservices	permanent	0 :0 :1	yes	yes
1	ipbase	permanent	0 :0 :0	no	no
1	ipbase	evaluation	0 :0 :0	no	no
1	lanbase	permanent	0 :0 :7	no	yes
1	apcount	evaluation	0 :0 :0	no	no
1	apcount	base	0 :0 :0	no	no
1	apcount	adder	0 :0 :0	no	yes
1	apcount	adder	0 :0 :0	no	yes

1	apcount	add	0 :0 :0	no	yes
1	apcount	add	0 :0 :0	no	yes
1	apcount	add	0 :0 :0	no	yes

Switch#

The following is sample output from the **show license right-to-use detail** command and displays the detailed information of licenses:

Switch# **show license right-to-use detail**

```

Index 1:  License Name: apcount
          Period left: 16
          License Type: evaluation
          License State: Not Activated
          License Count: 1000
          License Location: Slot 1
Index 2:  License Name: apcount
          Period left: Lifetime
          License Type: adder
          License State: Active, In use
          License Count: 125
          License Location: Slot 1

```

The following is sample output from the **show license right-to-use summary** command when the evaluation license is active:

```

Switch# show license right-to-use summary
  License Name   Type      Count   Period left
-----
  apcount       evaluation  1000    50
-----

Evaluation AP-Count: Enabled
Total AP Count Licenses: 1000
AP Count Licenses In-use: 100
AP Count Licenses Remaining: 900

```

The following is sample output from the **show license right-to-use summary** command when the adder licenses are active:

```

Switch# show license right-to-use summary
  License Name   Type      Count   Period left
-----
  apcount       adder      125     Lifetime
-----

Evaluation AP-Count: Disabled
Total AP Count Licenses: 125
AP Count Licenses In-use: 100
AP Count Licenses Remaining: 25

```

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 <i>mac-addr</i>	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 <i>MAC-addr</i>	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 3.3SE	This command was introduced.

Examples

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

```
Switch# 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.
<i>ap-name</i>	Specified access point name.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

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

Examples

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

```
Switch# 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 mac address-table move update

To display the MAC address-table move update information on the switch, 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	Modification
	Cisco IOS XE 3.3SE	Cisco IOS XE 3.3SE
		This command was introduced.

Examples This example shows the output from the **show mac address-table move update** command:

```
Switch# 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 nmosp

To display the Network Mobility Services Protocol (NMSP) configuration settings, use the **show nmosp** command.

show nmosp {**attachment** | {**suppress interfaces**}| **capability**| **notification interval**| **statistics** {**connection**| **summary**}| **status**| **subscription detail** [*ip-addr*]| **summary**}

Syntax Description

attachment suppress interfaces	Displays attachment suppress interfaces.
capability	Displays NMSP capabilities.
notification interval	Displays the NMSP notification interval.
statistics connection	Displays all connection-specific counters.
statistics summary	Displays the NMSP counters.
status	Displays status of active NMSP connections.
subscription detail <i>ip-addr</i>	The details are only for the NMSP services subscribed to by a specific IP address.
subscription summary	Displays details for all of the NMSP services to which the controller is subscribed. The details are only for the NMSP services subscribed to by a specific IP address.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

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

Examples

The following is sample output from the **show nmosp notification interval** command:

```
Switch# show nmosp notification interval
NMSP Notification Intervals
-----
RSSI Interval:
  Client           : 2 sec
  RFID             : 2 sec
```

show nmsp

```
Rogue AP           : 2 sec
Rogue Client       : 2 sec
Attachment Interval : 30 sec
Location Interval  : 30 sec
```

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 3.3SE	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 switch had more than 16 routed interfaces (subnet VLANs), the number of possible unicast MAC addresses might be less than 6000.

Examples The following is sample output from the **show sdm prefer** command:

```
Switch# 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
```

show sdm prefer

```

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.

```

Switch#

Related Commands

Command	Description
sdm prefer	Specifies the SDM template to be used on the switch.

show tech-support wireless

To display Cisco wireless LAN controller variables frequently requested by Cisco Technical Assistance Center (TAC), use the **show tech-support wireless** command in privileged EXEC mode.

show tech-support wireless

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 3.3SE	This command was introduced.

Examples

The following is sample output from the **show tech-support wireless** command:

```
Switch# show tech-support wireless
*** show ap capwap timers ***
```

```
Cisco AP CAPWAP timers
```

```
AP Discovery timer      : 10
AP Heart Beat timeout   : 30
Primary Discovery timer : 120
Primed Join timeout     : 0
Fast Heartbeat          : Disabled
Fast Heartbeat timeout  : 1
```

```
*** show ap capwap retransmit ***
Global control packet retransmit interval : 3
Global control packet retransmit count : 5
```

AP Name	Retransmit Interval	Retransmit Count
TSIM_AP-2	3	5
TSIM_AP-3	3	5

```
*** show ap dot11 24ghz cleanair air-quality summary ***
```

```
AQ = Air Quality
DFS = Dynamic Frequency Selection
```

```
*** show ap dot11 24ghz cleanair air-quality worst ***
```

```
AQ = Air Quality
DFS = Dynamic Frequency Selection
AP Name      Channel  Avg AQ  Min AQ  Interferers  DFS
-----
              0        0        0        0          No
```

```
*** show ap dot11 24ghz cleanair config ***
```

```
Clean Air Solution..... : Disabled
Air Quality Settings:
```

```

Air Quality Reporting..... : Disabled
Air Quality Reporting Period (min)..... : 15
Air Quality Alarms..... : Enabled
Air Quality Alarm Threshold..... : 10
Interference Device Settings:
  Interference Device Reporting..... : Enabled
  Bluetooth Link..... : Enabled
  Microwave Oven..... : Enabled
  802.11 FH..... : Enabled
  Bluetooth Discovery..... : Enabled
  TDD Transmitter..... : Enabled
  Jammer..... : Enabled
  Continuous Transmitter..... : Enabled
  DECT-like Phone..... : Enabled
  Video Camera..... : Enabled
  802.15.4..... : Enabled
  WiFi Inverted..... : Enabled
  WiFi Invalid Channel..... : Enabled
  SuperAG..... : Enabled
  Canopy..... : Enabled
  Microsoft Device..... : Enabled
  WiMax Mobile..... : Enabled
  WiMax Fixed..... : Enabled
  Interference Device Types Triggering Alarms:
    Bluetooth Link..... : Disabled
    Microwave Oven..... : Disabled
    802.11 FH..... : Disabled
    Bluetooth Discovery..... : Disabled
    TDD Transmitter..... : Disabled
    Jammer..... : Disabled
    Continuous Transmitter..... : Disabled
    DECT-like Phone..... : Disabled
    Video Camera..... : Disabled
  802.15.4..... : Disabled
    WiFi Inverted..... : Enabled
    WiFi Invalid Channel..... : Enabled
    SuperAG..... : Disabled
    Canopy..... : Disabled
    Microsoft Device..... : Disabled
    WiMax Mobile..... : Disabled
    WiMax Fixed..... : Disabled
  Interference Device Alarms..... : Enabled
Additional Clean Air Settings:
  CleanAir Event-driven RRM State..... : Disabled
  CleanAir Driven RRM Sensitivity..... : LOW
  CleanAir Persistent Devices state..... : Disabled

```

show wireless ap summary (MA)

To display the wireless access point mobility agent (MA) summary information, use the **show wireless ap summary** command.

show wireless ap *ma-ip* **summary**

Syntax Description

<i>ma-ip</i>	MA IPv4 Address.
--------------	------------------

Command Default

None

Command History

Release	Modification
Cisco IOS XE 3.7.3E	This command was introduced.

Usage Guidelines

This command works only with MC.

Examples

The following example shows how to display the wireless access point MA summary:

```
Cisco controller# show wireless ap 211.0.0.4 summary
```

Mobility Agent Access Point Summary:

```
Mobility Role           : Mobility Agent
Mobility Agent IP       : 211.0.0.4
Mobility Switch Peer Group Name : SPG1
Multicast Group IP Address : 0.0.0.0
Capwap Multicast Iif-Id  : NA
Link Encryption         : Disabled
Total AP Joined         : 1
IOS Version              : Not Available
AP software version     : 10.3.123.92
```

Codes U - Up, UR - Unregistered, D - Downloading, R - Registered
AP Up Time in hours:minutes:seconds

AP Name	AP Model	Port	IP Address	Radio (Ghz)	State	Radio MAC	AP
AP5	3602I	Gi1/0/5	211.0.0.170	2.4, 5	R	1ce6.c75b.3e70	
UpTime	Clients						
00:21:06	0						

show wireless ap summary

To display the number of access points known to the controller, use the **show wireless ap summary** command.

show wireless ap summary

Syntax Description

This command has no keywords or arguments

Command Default

None

Command History

Release	Modification
Cisco IOS XE 3.7.3E	This command was introduced.

Examples

The following example shows how to display the number of access points known to the controller:

```
Cisco controller# show wireless ap summary
```

```
Sub-Domain Access Point Summary
```

```
Maximum AP Limit: 100
Total AP License Installed: 60
Total AP License Available: 59
Total AP Joined: 1
```

```
AP UpTime in hours:minutes:seconds
```

HostName	Controller IP	AP name	AP Group	AP Model	AP IP
AP UpTime	Clients				
Switch	52.2.2.1	APd48c.b5e1.05bd	default-group	1142N	52.2.2.155
452:37:01	0				

show wireless band-select

To display the status of the band-select configuration, use the **show wireless band-select** command in privileged EXEC mode.

show wireless band-select

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 3.3SE	This command was introduced.

Examples

The following is sample output from the **show wireless band-select** command:

```
Switch# show wireless band-select
Band Select Probe Response    : per WLAN enabling
Cycle Count                   : 2
Cycle Threshold (millisec)    : 200
Age Out Suppression (sec)     : 20
Age Out Dual Band (sec)       : 60
Client RSSI (dBm)             : 80
```

show wireless client calls

To display the total number of active or rejected calls on the switch, use the **show wireless client calls** command in privileged EXEC mode.

show wireless client calls {active | rejected}

Syntax Description

active	Displays active calls.
rejected	Displays rejected calls.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

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

Examples

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

```
switch# show wireless client calls active
```

TSPEC Calls:

```
-----
MAC Address      AP Name          Status           WLAN  Authenticated
-----
0000.1515.000f   AP-2             Associated       1    Yes
```

SIP Calls:

```
-----
Number of Active TSPEC calls on 802.11a and 802.11b/g: 1
Number of Active SIP calls on 802.11a and 802.11b/g: 0
```

show wireless client dot11

To display the total number of active or rejected calls for a specific band (2.4 Ghz or 5 Ghz), use the **show wireless client dot11** command in privileged EXEC mode.

show wireless client dot11 {24ghz | 5ghz} calls {active | rejected}

Syntax Description

24ghz	Displays the 802.11b/g network.
5ghz	Displays the 802.11a network.
calls	Displays the wireless client calls.
active	Displays active calls.
rejected	Displays rejected calls.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

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

Examples

The following is sample output from the **show wireless client dot11** command:

```
Switch# show wireless client dot11 5ghz calls active
```

```
  TSPEC Calls:
  -----
```

```
  SIP Calls:
  -----
```

```
Number of Active TSPEC calls on 802.11a: 0
Number of Active SIP calls on 802.11a: 0
```

show wireless client location-calibration

To display the list of clients currently used to perform location calibration, use the **show wireless client location-calibration** command in privileged EXEC mode.

show wireless client location-calibration

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 3.3SECisco IOS XE 3.3SE	This command was introduced.

Examples The following is sample output from the **show wireless client location-calibration** command:

```
Switch# show wireless client location-calibration
```

show wireless client probing

To display the number of probing clients, use the **show wireless client probing** command in privileged EXEC mode.

show wireless client probing

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 3.3SECisco IOS XE 3.3SE	This command was introduced.

Examples	The following is sample output from the show wireless client probing command:
-----------------	--

```
Switch# show wireless client probing
MAC Address
-----
000b.cd15.0001
000b.cd15.0002
000b.cd15.0003
000b.cd15.0004
000b.cd15.0005
000b.cd15.0006
```

show wireless client summary

To display a summary of active clients associated with the controller, use the **show wireless client summary** command in privileged EXEC mode.

show wireless client summary

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 3.3SE	This command was introduced.

Usage Guidelines The following is sample output from the **show wireless client summary** command:
Use the **show wireless exclusionlist** command to display clients on the exclusion list (blacklisted).

Examples

```
Switch# show wireless client summary
Number of Local Clients : 1
```

MAC Address	AP Name	WLAN State	Protocol
0000.1515.000f	AP-2	1 UP	11a

show wireless client timers

To display 802.11 system timers, use the **show wireless client timers** command in privileged EXEC mode.

show wireless client timers

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 3.3SECisco IOS XE 3.3SE	This command was introduced.

Examples The following is sample output from the **show wireless client timers** command:

```
Switch# show wireless client timers
Authentication Response Timeout (seconds)      : 10
```

show wireless client voice diagnostics

To display wireless client voice diagnostic parameters, use the **show wireless client voice diagnostics** command in privileged EXEC mode.

show wireless client voice diagnostics {**qos-map** | **roam-history** | **rsi** | **status** | **tspec**}

Syntax Description

qos-map	Displays information about the QoS and DSCP mapping and packet statistics in each of the four queues: VO, VI, BE, BK. The different DSCP values are also displayed.
roam-history	Displays information about the last 3 roaming histories for each known client. The output contains the timestamp, access point associated with roaming, roaming reason, and if there is a roaming failure, a reason for the roaming failure.
rsi	Displays the client's RSSI values in the last 5 seconds when voice diagnostics are enabled.
status	Displays status of voice diagnostics for clients.
tspec	Displays voice diagnostics that are enabled for TSPEC clients.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

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

Usage Guidelines

Debug voice diagnostics must be enabled for voice diagnostics to work.

Examples

The following is sample output from the **show wireless client voice diagnostics status** command:

```
Switch# show wireless client voice diagnostics status
Voice Diagnostics Status: FALSE
```


show wireless country

To display the configured country and the radio types supported, use the **show wireless country** command in privileged EXEC mode.

show wireless country {channels| configured| supported [tx-power]}

Syntax Description

channels	Displays the list of possible channels for each band, and the list of channels allowed in the configured countries.
configured	Display configured countries.
supported tx-power	Displays the list of allowed Tx powers in each supported country.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

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

Examples

The following is sample output from the **show wireless country channels** command:

```
Switch# show wireless country channels
Configured Country.....: US - United States
KEY: * = Channel is legal in this country and may be configured manually.
      A = Channel is the Auto-RF default in this country.
      . = Channel is not legal in this country.
      C = Channel has been configured for use by Auto-RF.
      x = Channel is available to be configured for use by Auto-RF.
      (-,-) = (indoor, outdoor) regulatory domain allowed by this country.
-----:+++++-----
      802.11bg      :
      Channels      :           1 1 1 1 1
                     : 1 2 3 4 5 6 7 8 9 0 1 2 3 4
-----:+++++-----
      (-A , -AB )  US : A * * * * A * * * * A . . .
      Auto-RF      : . . . . .
-----:+++++-----
      802.11a      :
      Channels      :           1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
                     : 3 3 3 4 4 4 4 4 5 5 6 6 0 0 0 1 1 2 2 2 3 3 4 4 5 5 6 6
                     : 4 6 8 0 2 4 6 8 2 6 0 4 0 4 8 2 6 0 4 8 2 6 0 9 3 7 1 5
-----:+++++-----
      (-A , -AB )  US : . A . A . A . A A A A * * * * . . . * * A A A *
      Auto-RF      : . . . . .
-----:+++++-----
      4.9GHz 802.11a :
      Channels      :           1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2
                     : 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6
```

show wireless country

```

-----:~::~-----
US (-A , -AB ) : * * * * * A * * * * * A
Auto-RF       : . . . . .
-----:~::~-----

```

The following is sample output from the **show wireless country configured** command:

```

Switch# show wireless country configured
Configured Country.....: US - United States
Configured Country Codes
      US - United States : 802.11a Indoor,Outdoor/ 802.11b / 802.11g

```

The following is sample output from the **show wireless country supported tx-power** command:

```

Switch# show wireless country supported tx-power
KEY: ##      = Tx Power in dBm.
      ##*    = Channel supports radar detection .
      .      = Channel is not legal in this country.
      (-)    = Regulatory Domains allowed by this country.
      (-,-)  = (indoor, outdoor) regulatory Domains allowed by this country.
-----:~::~-----
      802.11bg :
      Channels :
                : 1 1 1 1 1
                : 1 2 3 4 5 6 7 8 9 0 1 2 3 4
-----:~::~-----
(-CE , -CE ) AE : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E , -E ) AL : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-A , -AR ) AR : 27 27 27 27 27 27 27 27 27 27 27 27 . . .
(-E , -E ) AT : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-A , -NA ) AU : 27 27 27 27 27 27 27 27 27 27 27 27 . . .
(-E , - ) BA : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E , -E ) BE : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E , -E ) BG : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E , - ) BH : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-A , -A ) BO : 27 27 27 27 27 27 27 27 27 27 27 27 . . .
(-A , -AR ) BR : 27 27 27 27 27 27 27 27 27 27 27 27 . . .
(-E , - ) BY : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-A , -ABN ) CA : 27 27 27 27 27 27 27 27 27 27 27 27 . . .
(-A , -ABN ) CA2 : 27 27 27 27 27 27 27 27 27 27 27 27 . . .
(-E , -E ) CH : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-AER , -AR ) CL : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E , -E ) CM : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-CE , -CE ) CN : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-A , -AR ) CO : 27 27 27 27 27 27 27 27 27 27 27 27 . . .
(-A , -AB ) CR : 27 27 27 27 27 27 27 27 27 27 27 27 . . .
(-E , -E ) CY : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E , -E ) CZ : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E , -E ) DE : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E , -E ) DK : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-A , -ABN ) DO : 27 27 27 27 27 27 27 27 27 27 27 27 . . .
(-E , - ) DZ : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-A , -AB ) EC : 27 27 27 27 27 27 27 27 27 27 27 27 . . .
(-E , -E ) EE : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E , -E ) EG : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E , -E ) ES : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E , -E ) FI : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E , -E ) FR : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E , -E ) GB : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E , -E ) GI : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E , -E ) GR : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-A , -NA ) HK : 27 27 27 27 27 27 27 27 27 27 27 27 . . .
(-E , - ) HR : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E , -E ) HU : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E , -ER ) ID : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E , -E ) IE : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-EI , -IE ) IL : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-I , -I ) ILO : . . . . 20 20 20 20 20 20 20 20 .
(-A , -AN ) IN : 27 27 27 27 27 27 27 27 27 27 27 27 . . .
(-E , -E ) IQ : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E , -E ) IS : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-E , -E ) IT : 20 20 20 20 20 20 20 20 20 20 20 20 20 20 .
(-JPU , -JPU ) J2 : 23 23 23 23 23 23 23 23 23 23 23 23 23 23

```

```

(-JPU , -JPU ) J3 : 23 23 23 23 23 23 23 23 23 23 23 23 23 23
(-JPQU, -PQ ) J4 : 23 23 23 23 23 23 23 23 23 23 23 23 23 23
(-E , - ) JO : 20 20 20 20 20 20 20 20 20 20 20 20 20 20
(-JPU , -JPU ) JP : 23 23 23 23 23 23 23 23 23 23 23 23 23 23
(-ACE , -ACEK) KE : 20 20 20 20 20 20 20 20 20 20 20 20 20 20
(-E , -E ) KN : 20 20 20 20 20 20 20 20 20 20 20 20 20 20
(-ACE , -ACEK) KR : 20 20 20 20 20 20 20 20 20 20 20 20 20 20
(-E , -E ) KW : 20 20 20 20 20 20 20 20 20 20 20 20 20 20
(-E , -E ) KZ : 20 20 20 20 20 20 20 20 20 20 20 20 20 20
(-E , -E ) LB : 20 20 20 20 20 20 20 20 20 20 20 20 20 20
(-E , -E ) LI : 20 20 20 20 20 20 20 20 20 20 20 20 20 20
(-E , -E ) LK : 20 20 20 20 20 20 20 20 20 20 20 20 20 20
(-E , -E ) LT : 20 20 20 20 20 20 20 20 20 20 20 20 20 20
(-E , -E ) LU : 20 20 20 20 20 20 20 20 20 20 20 20 20 20
(-E , -E ) LV : 20 20 20 20 20 20 20 20 20 20 20 20 20 20
(-E , -E ) MC : 20 20 20 20 20 20 20 20 20 20 20 20 20 20
(-E , -E ) ME : 20 20 20 20 20 20 20 20 20 20 20 20 20 20
(-E , -E ) MK : 20 20 20 20 20 20 20 20 20 20 20 20 20 20
(-E , -E ) MO : 20 20 20 20 20 20 20 20 20 20 20 20 20 20
(-E , -E ) MT : 20 20 20 20 20 20 20 20 20 20 20 20 20 20
(-A , -NA ) MX : 27 27 27 27 27 27 27 27 27 27 27 27 27 27
(-ACE , -AEC ) MY : 20 20 20 20 20 20 20 20 20 20 20 20 20 20
(-E , -E ) NL : 20 20 20 20 20 20 20 20 20 20 20 20 20 20
(-E , -E ) NO : 20 20 20 20 20 20 20 20 20 20 20 20 20 20
(-A , -NA ) NZ : 27 27 27 27 27 27 27 27 27 27 27 27 27 27
(-E , -E ) OM : 20 20 20 20 20 20 20 20 20 20 20 20 20 20
(-A , -AR ) PA : 27 27 27 27 27 27 27 27 27 27 27 27 27 27
(-A , -AR ) PE : 27 27 27 27 27 27 27 27 27 27 27 27 27 27
(-A , -ABN ) PH : 27 27 27 27 27 27 27 27 27 27 27 27 27 27
(-A , -ABN ) PH2 : 27 27 27 27 27 27 27 27 27 27 27 27 27 27
(-E , -E ) PK : 20 20 20 20 20 20 20 20 20 20 20 20 20 20
(-E , -E ) PL : 20 20 20 20 20 20 20 20 20 20 20 20 20 20
(-A , -A ) PR : 27 27 27 27 27 27 27 27 27 27 27 27 27 27
(-E , -E ) PT : 20 20 20 20 20 20 20 20 20 20 20 20 20 20
(-A , -A ) PY : 27 27 27 27 27 27 27 27 27 27 27 27 27 27
(-E , -E ) QA : 20 20 20 20 20 20 20 20 20 20 20 20 20 20
(-E , -E ) RO : 20 20 20 20 20 20 20 20 20 20 20 20 20 20
(-E , -E ) RS : 20 20 20 20 20 20 20 20 20 20 20 20 20 20
(-AER , -ER ) RU : 20 20 20 20 20 20 20 20 20 20 20 20 20 20
(-AE , -AE ) SA : 20 20 20 20 20 20 20 20 20 20 20 20 20 20
(-E , -E ) SE : 20 20 20 20 20 20 20 20 20 20 20 20 20 20
(-E , -SE ) SG : 20 20 20 20 20 20 20 20 20 20 20 20 20 20
(-E , -E ) SI : 20 20 20 20 20 20 20 20 20 20 20 20 20 20
(-E , -E ) SK : 20 20 20 20 20 20 20 20 20 20 20 20 20 20
(-E , -ER ) TH : 20 20 20 20 20 20 20 20 20 20 20 20 20 20
(-E , -E ) TN : 20 20 20 20 20 20 20 20 20 20 20 20 20 20
(-EI , -E ) TR : 20 20 20 20 20 20 20 20 20 20 20 20 20 20
(-A , -ANT ) TW : 27 27 27 27 27 27 27 27 27 27 27 27 27 27
(-E , -E ) UA : 20 20 20 20 20 20 20 20 20 20 20 20 20 20
(-A , -AB ) US : 27 27 27 27 27 27 27 27 27 27 27 27 27 27
(-A , -AB ) US2 : 27 27 27 27 27 27 27 27 27 27 27 27 27 27
(-A , -AB ) USL : 27 27 27 27 27 27 27 27 27 27 27 27 27 27
(-A , - ) USX : 27 27 27 27 27 27 27 27 27 27 27 27 27 27
(-A , -A ) UY : 27 27 27 27 27 27 27 27 27 27 27 27 27 27
(-A , -AR ) VE : 27 27 27 27 27 27 27 27 27 27 27 27 27 27
(-E , -E ) VN : 20 20 20 20 20 20 20 20 20 20 20 20 20 20
(-E , -E ) ZA : 20 20 20 20 20 20 20 20 20 20 20 20 20 20

```

show wireless detail

To display the details of the wireless parameters configured, use the **show wireless detail** command in privileged EXEC mode.

show wireless detail

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 3.3SECisco IOS XE 3.3SE	This command was introduced.

Usage Guidelines	The following parameters are displayed:
	<ul style="list-style-type: none">• The wireless user idle timeout• The controller configured RF group name• Fast SSID change

Examples	The following is sample output from the show wireless detail command:
-----------------	--

```
Switch# show wireless detail
User Timeout           : 300
RF network              : default
Fast SSID              : Disabled
```

show wireless dtls connections

To display the Datagram Transport Layer Security (DTLS) server status, use the **show wireless dtls connections** command in privileged EXEC mode.

show wireless dtls connections

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 3.3SE	This command was introduced.

Examples

The following is sample output from the **show wireless dtls connections** command:

```
Switch# show wireless dtls connections
AP Name      Local Port  Peer IP      Peer Port    Ciphersuite
-----
AP-2         Capwap_Ctrl 10.0.0.16    52346        TLS_RSA_WITH_AES_128_CBC_SHA
AP-3         Capwap_Ctrl 10.0.0.17    52347        TLS_RSA_WITH_AES_128_CBC_SHA
```

show wireless flow-control

To display the information about flow control on a particular channel, use the **show wireless flow-control** command in privileged EXEC mode.

show wireless flow-control *channel-id*

Syntax Description	<div><div><i>channel-id</i></div><div>Identification number for a channel through which flow control is monitored.</div></div>					
Command Default	No default behavior or values.					
Command Modes	Privileged EXEC					
Command History	<table><tr><th>Release</th><th>Modification</th></tr><tr><td>Cisco IOS XE 3.3SE</td><td>This command was introduced.</td></tr></table>		Release	Modification	Cisco IOS XE 3.3SE	This command was introduced.
Release	Modification					
Cisco IOS XE 3.3SE	This command was introduced.					

Examples

The following is sample output from the **show wireless flow-control** *channel-id* command:

```
Switch# show wireless flow-control 3
Channel Name           : CAPWAP
FC State               : Disabled
Remote Server State    : Enabled
Pass-thru Mode         : Disabled
EnQ Disabled           : Disabled
Queue Depth            : 2048
Max Retries            : 5
Min Retry Gap (mSec)   : 3
```

show wireless flow-control statistics

To display the complete information about flow control on a particular channel, use the **show wireless flow-control statistics** command in privileged EXEC mode.

show wireless flow-control *channel-id* **statistics**

Syntax Description	<i>channel-id</i>	Identification number for a channel through which flow control is monitored.
Command Default	No default behavior or values.	
Command Modes	Privileged EXEC	
Command History	Release	Modification
	Cisco IOS XE 3.3SE	This command was introduced.

Examples

The following is sample output from the **show wireless flow-control channel-id statistics** command:

```
Switch# show wireless flow-control 3 statistics
Channel Name                : CAPWAP
# of times channel went into FC      : 0
# of times channel came out of FC    : 0
Total msg count received by the FC Infra : 1
Pass-thru msgs send count          : 0
Pass-thru msgs fail count          : 0
# of msgs successfully queued       : 0
# of msgs for which queuing failed  : 0
# of msgs sent thru after queuing   : 0
# of msgs sent w/o queuing          : 1
# of msgs for which send failed     : 0
# of invalid EAGAINS received       : 0
Highest watermark reached           : 0
# of times Q hit max capacity        : 0
Avg time channel stays in FC (mSec)  : 0
```

show wireless load-balancing

To display the status of the load-balancing feature, use the **show wireless load-balancing** command in privileged EXEC mode.

show wireless load-balancing

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 3.3SECisco IOS XE 3.3SE	This command was introduced.

Examples The following is sample output from the **show wireless load-balancing** command:

```
> show wireless load-balancing
Aggressive Load Balancing.....: per WLAN enabling
Aggressive Load Balancing Window (clients).....: 5
Aggressive Load Balancing Denial Count.....: 3

Statistics
Total Denied Count (clients).....: 0
Total Denial Sent (messages).....: 0
Exceeded Denial Max Limit Count (times).....: 0
None 5G Candidate Count (times).....: 0
None 2.4G Candidate Count (times).....: 0
```


show wireless mobility summary

To display the summary of the mobility management configuration, use the **show wireless mobility summary** command.

show wireless mobility *ma-ip* **summary**

Syntax Description	
<i>ma-ip</i>	MA IPv4 Address.

Command Default	None
-----------------	------

Command History	Release	Modification
	Cisco IOS XE 3.7.3E	This command was introduced.

Usage Guidelines	This command works only with MC.
------------------	----------------------------------

Examples The following example shows how to display the summary of the mobility management configuration:

```
Cisco controller# show wireless mobility 211.0.0.4 summary
```

Mobility Agent Summary:

```

Mobility Role                : Mobility Agent
Wireless Management VLAN    : 211
Wireless Management IP Address : 211.0.0.4
Mobility Switch Peer Group Name : SPG1
Multicast IP Address        : 0.0.0.0
DTLS Mode                   : Enabled
Mobility Keepalive Interval/Count : 10/3
Mobility Control Message DSCP Value : 48
Switch Peer Group Members Configured : 1
Central Management          : Enabled

```

Link Status is Control Link Status : Data Link Status

The status of Mobility Controller:

Host Name	IP	Public IP	Link Status
ct3850-62	211.0.0.8	211.0.0.8	UP : UP

Switch Peer Group members:

Host Name	IP	Public IP	Data Link Status
ct3850-63	211.0.0.4	211.0.0.4	N/A

show wireless performance

To display aggressive load balancing configuration, use the **show wireless performance** command in privileged EXEC mode.

show wireless performance {ap| client} summary

Syntax Description

ap summary	Displays aggressive load balancing configuration of access points configured to the controller.
client summary	Displays aggressive load balancing configuration details of the clients.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

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

Examples

The following is sample output from the **show wireless performance ap summary** command.

```
Switch# show wireless performance ap summary
Number of APs:
```

The following is sample output from the **show wireless performance client summary** command.

```
Switch# show wireless performance client summary
Number of Clients:
```

```
MAC Address          AP Name              Status              WLAN/Guest-Lan Auth Protocol Port Wired
-----
```

show wireless pmk-cache

To display information about the pairwise master key (PMK) cache, use the **show wireless pmk-cache** command in privileged EXEC mode.

show wireless pmk-cache[*mac-address mac-addr*]

Syntax Description

mac-address mac-addr	(Optional) Information about a single entry in the PMK cache.
-----------------------------	---

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

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

Examples

The following is sample output from the **show wireless pmk-cache mac-address** command:

```
Switch# show wireless pmk-cache mac-address H.H.H
Number of PMK caches in total : 0
```

show wireless probe

To display the advanced probe request filtering configuration and the number of probes sent to the WLAN controller per access point per client and the probe interval in milliseconds, use the **show wireless probe** command in privileged EXEC mode.

show wireless probe

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 3.3SE	This command was introduced.

Examples

The following is sample output from the **show wireless probe** command:

```
Switch# show wireless probe
Probe request filtering           : Enabled
Number of probes per client per radio fwd from AP: 2
Probe request rate-limiting interval : 500 msec
Aggregate probe request interval   : 500 msec
```

show wireless sip preferred-call-no

To display SIP preferred call numbers, use the **show wireless sip preferred-call-no** command in privileged EXEC mode.

show wireless sip preferred-call-no

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 3.3SECisco IOS XE 3.3SE	This command was introduced.

Examples The following is sample output from the **show wireless sip preferred-call-no** command:

```
Switch# show wireless sip preferred-call-no
Index Preferred-Number
-----
1      1031
2      1032
4      1034
```

show wireless summary

To display the number of access points, radios and wireless clients known to the controller, use the **show wireless summary** command in privileged EXEC mode.

show wireless summary

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

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

```
Switch# show wireless summary

Access Point Summary

              Total      Up      Down
-----
802.11a/n      2        2        0
802.11b/g/n    2        2        0
All APs        2        2        0

Client Summary

Current Clients : 1
Excluded Clients: 0
Disabled Clients: 0
```

show wireless wlan summary

To display wireless WLAN details, use the **show wireless wlan summary** command.

show wireless wlan summary

Syntax Description

This command has no keywords or arguments.

Command Default

None

Command History

Release	Modification
Cisco IOS XE 3.7.3E	This command was introduced.

Examples

The following example shows how to display wireless WLAN summary:

```
Cisco controller# show wireless WLAN summary
```

```
Total WLAN Configured: 2
```

```
Total Client Count: 0
```

ID	Profile Name Status	SSID	Security	Radio	VLAN	Client
1	benimr3 UP	benimr3	NONE	All	602	0
2	Proton_2 UP	Proton_2	NONE	All	202	0

show wlan name

To display the MA's WLAN configuration by name, use the **show wlan name** command.

show wlan name *name ma-ip*

Syntax Description

<i>name</i>	Access point name.
<i>ma-ip</i>	MA IPv4 address.

Command Default

None

Command History

Release	Modification
Cisco IOS XE 3.7.3E	This command was introduced.

Usage Guidelines

This command works only with MC.

Examples

The following example shows how to display the MA WLAN configuration by name:

```
Cisco controller# show wlan name anu_mcma 211.0.0.4

WLAN Profile Name      : anu_mcma
=====
Identifier              : 1
Network Name (SSID)    : anu_mcma
Status                  : Disabled
Broadcast SSID          : Enabled
Max Associated Clients per WLAN : 0
Max Associated Clients per AP per WLAN : 0
Max Associated Clients per AP Radio per WLAN : 0
AAA Policy Override     : Disabled
Network Admission Control
  NAC-State              : Disabled
Number of Active Clients : 0
Exclusionlist Timeout    : 60
Session Timeout         : 1800 seconds
CHD per WLAN            : Enabled
Webauth DHCP exclusion  : Disabled
Interface               : 211
Interface Status        : Up
Multicast Interface     : Unconfigured
WLAN IPv4 ACL           :
WLAN IPv6 ACL           : unconfigured
DHCP Server             : Default
DHCP Address Assignment Required : Disabled
DHCP Option 82          : Disabled
DHCP Option 82 Format    : ap-mac
DHCP Option 82 Ascii Mode : Disabled
DHCP Option 82 Rid Mode  : Disabled
```



```

Local Profiling -Policy Name           : Disabled
Device Classification                  : Disabled
QoS Service Policy - Input
  Policy Name                         : unknown
  Policy State                        : None
QoS Service Policy - Output
  Policy Name                         : unknown
  Policy State                        : None
QoS Client Service Policy
  Input Policy Name                   : unknown
  Output Policy Name                  : unknown
WMM                                    : Allowed
WifiDirect                            : Disabled
Channel Scan Defer Priority:
  Priority (default)                  : 4
  Priority (default)                  : 5
  Priority (default)                  : 6
Scan Defer Time (msecs)                : 100
Media Stream Multicast-direct          : Disabled
CCX - AironetIe Support                : Enabled
CCX - Gratuitous ProbeResponse (GPR)   : Disabled
CCX - Diagnostics Channel Capability   : Disabled
Dot11-Phone Mode (7920)                : Invalid
Wired Protocol                        : None
Peer-to-Peer Blocking Action           : Disabled
Radio Policy                          : All
DTIM period for 802.11a radio           : 1
DTIM period for 802.11b radio           : 1
Local EAP Authentication                : Disabled
Mac Filter Authorization list name      : MACFILTER
Accounting list name                   : Disabled
802.1x authentication list name         : wcm_dot1x
Security
  802.11 Authentication                : Open System
  Static WEP Keys                      : Disabled
  802.1X                               : Disabled
  Wi-Fi Protected Access (WPA/WPA2)
    WPA (SSN IE)                      : Disabled
    WPA2 (RSN IE)                     : Enabled
    TKIP Cipher                       : Disabled
    AES Cipher                        : Enabled
  Auth Key Management
    802.1x                            : Enabled
    PSK                              : Disabled
    CCKM                             : Disabled
    FT dot1x                          : Disabled
    FT PSK                            : Disabled
    PMF dot1x                         : Disabled
    PMF PSK                           : Disabled
  FT Support
    FT Reassociation Timeout           : 20
    FT Over-The-DS mode                : Enabled
  PMF Support
    PMF Association Comeback Timeout   : 1
    PMF SA Query Time                  : 200
  CKIP                                : Disabled
  IP Security                         : Disabled
  L2TP                                : Disabled
  Web Based Authentication             : Disabled
  Conditional Web Redirect             : Disabled
  Splash-Page Web Redirect             : Disabled
  Auto Anchor                          : Disabled
  Sticky Anchoring                     : Enabled
  Cranite Passthru                     : Disabled
  Fortress Passthru                    : Disabled
  PPTP                                 : Disabled
  Infrastructure MFP protection         : Enabled
  Client MFP                           : Optional
  Webauth On-mac-filter Failure        : Disabled
  Webauth Authentication List Name     : Disabled
  Webauth Parameter Map                : Disabled
  Tkip MIC Countermeasure Hold-down Timer : 60
Call Snooping                          : Disabled

```

```
Passive Client           : Disabled
Non Cisco WGB           : Disabled
Band Select             : Disabled
Load Balancing          : Disabled
IP Source Guard         : Disabled
Local HTTP Profiling Status : Disabled
Radius HTTP Profiling Status : Disabled
Assisted-Roaming
    Neighbor List       : Disabled
    Prediction List     : Disabled
    Dual Band Support   : Disabled
AVC Visibility          : Disabled
Universal Ap Admin      : Disabled
11ac Mu MIMO           : Disabled
```

shutdown

To shut down VLAN switching, use the **shutdown** command in global configuration mode. To disable the configuration set, use the **no** form of this command.

shutdown [**vlan** *vlan-id*]

no shutdown

Syntax Description

vlan <i>vlan-id</i>	VLAN ID of VLAN to shutdown.
----------------------------	------------------------------

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

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

Examples

This example shows how to shutdown a VLAN:

```
Switch(config)# vlan open1  
Switch(config-vlan)# shutdown
```

This example shows that the access point is not shut down:

```
Switch# configure terminal  
Switch(config)# ap name 3602a no shutdown
```

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 6: Default Values for the Temperature Thresholds

Switch	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 3.3SE	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 switch 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:

```
Switch(config)# system env temperature threshold yellow 15  
Switch(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

<i>interface-id</i>	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 3.3SE	Cisco 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.

Examples

This example shows how to run TDR on an interface:

```
Switch# 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:

```
Switch# 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.
```

Related Commands

Command	Description
show cable-diagnostics tdr	Displays 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 <i>interface-id</i>	(Optional) Specifies an interface on the source or destination switch.
<i>source-mac-address</i>	The MAC address of the source switch in hexadecimal format.
<i>destination-mac-address</i>	The MAC address of the destination switch in hexadecimal format.
vlan <i>vlan-id</i>	(Optional) Specifies the VLAN on which to trace the Layer 2 path that the packets take from the source switch to the destination switch. 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 3.3SE	This command was introduced.

Usage Guidelines

For Layer 2 traceroute to function properly, Cisco Discovery Protocol (CDP) must be enabled on all of the switches in the network. Do not disable CDP.

When the switch detects a device in the Layer 2 path that does not support Layer 2 traceroute, the switch 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:

```
Switch# 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:

```
Switch# 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 switches:

```
Switch# 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 switch is not connected to the source switch:

```
Switch# 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 switch cannot find the destination port for the source MAC address:

```
Switch# 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:

```
Switch# 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:

```
Switch# traceroute mac 0000.0201.0601 0100.0201.0201
Invalid destination mac address
```

This example shows the Layer 2 path when source and destination switches belong to multiple VLANs:

```
Switch# traceroute mac 0000.0201.0601 0000.0201.0201
Error:Mac found on multiple vlans.
Layer2 trace aborted.
```

Related Commands

Command	Description
traceroute mac ip	Displays the Layer 2 path taken by the packets from the specified source IP address or hostname to the specified destination IP address or hostname.

tracert 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 **tracert mac ip** command in privileged EXEC mode.

tracert mac ip {*source-ip-address* | *source-hostname*} {*destination-ip-address* | *destination-hostname*} [**detail**]

Syntax Description

<i>source-ip-address</i>	The IP address of the source switch as a 32-bit quantity in dotted-decimal format.
<i>source-hostname</i>	The IP hostname of the source switch.
<i>destination-ip-address</i>	The IP address of the destination switch as a 32-bit quantity in dotted-decimal format.
<i>destination-hostname</i>	The IP hostname of the destination switch.
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 3.3SE	This command was introduced.

Usage Guidelines

For Layer 2 tracert to function properly, Cisco Discovery Protocol (CDP) must be enabled on each switch in the network. Do not disable CDP.

When the switch detects a device in the Layer 2 path that does not support Layer 2 tracert, the switch continues to send Layer 2 trace queries and lets them time out.

The maximum number of hops identified in the path is ten.

The **tracert 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 switch 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 switch uses the associated MAC address and identifies the physical path.

- If an ARP entry does not exist, the switch 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:

```
Switch# 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:

```
Switch# 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:

```
Switch# traceroute mac ip 2.2.66.66 2.2.77.77
Arp failed for destination 2.2.77.77.
Layer2 trace aborted.
```

Related Commands

Command	Description
tracert mac	Displays the Layer 2 path taken by the packets from the specified source MAC address to the specified destination MAC address.

trapflags

To enable sending rogue access point detection traps, use the **trapflags** command in privileged EXEC mode. To disable sending rogue access point detection traps, use the **no** form of this command.

trapflags rogueap

no trapflags rogueap

Syntax Description

rogueap	Enables sending rogue access point detection traps.
----------------	---

Command Default

Enabled.

Command Modes

Privileged EXEC

Command History

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

Examples

This example shows how to disable the sending of rogue access point detection traps:

```
Switch# configure terminal
Switch(config)# no trapflags rogueap
Switch(config)# end
```

trapflags client

To enable the sending of client-related DOT11 traps, use the **trapflags client** command in privileged EXEC mode. To disable the sending of client-related DOT11 traps, use the **no** form of this command.

trapflags client [**dot11** {**assocfail**| **associate**| **authfail**| **deauthenticate**| **disassociate**}| **excluded**]

no trapflags client [**dot11** {**assocfail**| **associate**| **authfail**| **deauthenticate**| **disassociate**}| **excluded**]

Syntax Description

dot11	Client-related DOT11 traps.
assocfail	Enables the sending of Dot11 association fail traps to clients.
associate	Enables the sending of Dot11 association traps to clients.
authfail	Enables the sending of Dot11 authentication fail traps to clients.
deauthenticate	Enables the sending of Dot11 deauthentication traps to clients.
disassociate	Enables the sending of Dot11 disassociation traps to clients.
excluded	Enables the sending of excluded trap to clients.

Command Default

No default behavior or values.

Command Modes

Privileged EXEC

Command History

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

Examples

This example shows how to enable the sending of Dot11 disassociation trap to clients:

```
Switch# configure terminal
Switch(config)# trapflags client dot11 disassociate
Switch(config)# end
```

type

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

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

Syntax Description

<i>filesystem:</i>	Alias for a file system. Use flash: for the system board flash device; use usbflash0: for USB memory sticks.
<i>/file-url...</i>	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 3.3SE	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:

```
Switch: 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

<i>variable</i>	Use one of these keywords for <i>variable</i> : MANUAL_BOOT —Specifies whether the switch 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 3.3SE	Cisco 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.

Examples

This example shows how to unset the SWITCH_PRIORITY environment variable:

```
Switch: unset SWITCH_PRIORITY
```

Related Commands

Command	Description
set	Sets or displays environment variables.
reset	Performs a hard reset on the system.

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 3.3SE	This command was introduced.

Examples

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

```
Switch: 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
```

wireless client

To configure client parameters, use the **wireless client** command in global configuration mode.

wireless client {**association limit** *assoc-number* **interval** *interval*| **band-select** {**client-rssi** *rssi*| **cycle-count** *count*| **cycle-threshold** *threshold*| **expire dual-band** *timeout*| **expire suppression** *timeout*}| **max-user-login** *max-user-login*| **timers** **auth-timeout** *seconds*| **user-timeout** *user-timeout*}

Syntax Description

association limit <i>assoc-number</i> interval <i>interval</i>	Enables association request limit per access point slot at a given interval and configures the association request limit interval. You can configure number of association request per access point slot at a given interval from one through 100. You can configure client association request limit interval from 100 through 10000 milliseconds.
band-select	Configures band select options for the client.
client-rssi <i>rssi</i>	Sets the client received signal strength indicator (RSSI) threshold for band select. Minimum dBm of a client RSSI to respond to probe between -90 and -20.
cycle-count <i>count</i>	Sets the band select probe cycle count. You can configure the cycle count from one through 10.
cycle-threshold <i>threshold</i>	Sets the time threshold for a new scanning cycle. You can configure the cycle threshold from one through 1000 milliseconds.
expire dual-band <i>timeout</i>	Sets the timeout before stopping to try to push a given client to the 5-GHz band. You can configure the timeout from 10 through 300 seconds, and the default value is 60 seconds.
expire suppression <i>timeout</i>	Sets the expiration time for pruning previously known dual-band clients. You can configure the suppression from 10 through 200 seconds, and the default timeout value is 20 seconds.
max-user-login <i>max-user-login</i>	Configures the maximum number of login sessions for a user.
timers auth-timeout <i>seconds</i>	Configures client timers.
user-timeout <i>user-timeout</i>	Configures the idle client timeout.

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.

Examples This example shows how to set the probe cycle count for band select to 8:

```
Switch# configure terminal
Switch(config)# wireless client band-select cycle-count 8
Switch(config)# end
```

This example shows how to set the time threshold for a new scanning cycle with threshold value of 700 milliseconds:

```
Switch# configure terminal
Switch(config)# wireless client band-select cycle-threshold 700
Switch(config)# end
```

This example shows how to suppress dual-band clients from the dual-band database after 70 seconds:

```
Switch# configure terminal
Switch(config)# wireless client band-select expire suppression 70
Switch(config)# end
```

wireless client mac-address deauthenticate

To disconnect a wireless client, use the **wireless client mac-address deauthenticate** command in global configuration mode.

wirelessclientmac-address *mac-addr***deauthenticate**

Syntax Description

mac-address <i>mac-addr</i>	Wireless client MAC address.
------------------------------------	------------------------------

Command Default

No default behavior or values.

Command Modes

Global configuration

Command History

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

Examples

This example shows how to disconnect a wireless client:

```
Switch# configure terminal
Switch(config)# wireless client mac-address 00:1f:ca:cf:b6:60 deauthenticate
Switch(config)# end
```

wireless client mac-address

To configure the wireless client settings, use the **wireless client mac-address** command in global configuration mode.

```
wireless client mac-address mac-addr ccx {clear-reports|clear-results|default-gw-ping|dhcp-test|  
dns-ping|dns-resolve hostname host-name|get-client-capability|get-manufacturer-info|  
get-operating-parameters|get-profiles|log-request {roam|rsna|syslog}|send-message message-id|  
stats-request measurement-duration {dot11|security}|test-abort|test-association ssid bssid dot11 channel|  
test-dot1x [ profile-id ] bssid dot11 channel|test-profile {any|profile-id}}
```

Syntax Description

<i>mac-addr</i>	MAC address of the client.
ccx	Cisco client extension (CCX).
clear-reports	Clears the client reporting information.
clear-results	Clears the test results on the controller.
default-gw-ping	Sends a request to the client to perform the default gateway ping test.
dhcp-test	Sends a request to the client to perform the DHCP test.
dns-ping	Sends a request to the client to perform the Domain Name System (DNS) server IP address ping test.
dns-resolve <i>hostname</i> <i>host-name</i>	Sends a request to the client to perform the Domain Name System (DNS) resolution test to the specified hostname.
get-client-capability	Sends a request to the client to send its capability information.
get-manufacturer-info	Sends a request to the client to send the manufacturer's information.
get-operating-parameters	Sends a request to the client to send its current operating parameters.
get-profiles	Sends a request to the client to send its profiles.
log-request	Configures a CCX log request for a specified client device.
roam	(Optional) Specifies the request to specify the client CCX roaming log
rsna	(Optional) Specifies the request to specify the client CCX RSNA log.
syslog	(Optional) Specifies the request to specify the client CCX system log.

send-message *message-id*

Sends a message to the client.

Message type that involves one of the following:

- 1—The SSID is invalid
- 2—The network settings are invalid.
- 3—There is a WLAN credibility mismatch.
- 4—The user credentials are incorrect.
- 5—Please call support.
- 6—The problem is resolved.
- 7—The problem has not been resolved.
- 8—Please try again later.
- 9—Please correct the indicated problem.
- 10—Troubleshooting is refused by the network.
- 11—Retrieving client reports.
- 12—Retrieving client logs.
- 13—Retrieval complete.
- 14—Beginning association test.
- 15—Beginning DHCP test.
- 16—Beginning network connectivity test.
- 17—Beginning DNS ping test.
- 18—Beginning name resolution test.
- 19—Beginning 802.1X authentication test.
- 20—Redirecting client to a specific profile.
- 21—Test complete.
- 22—Test passed.
- 23—Test failed.
- 24—Cancel diagnostic channel operation or select a WLAN profile to resume normal operation.
- 25—Log retrieval refused by the client.
- 26—Client report retrieval refused by the client.
- 27—Test request refused by the client.
- 28—Invalid network (IP) setting.
- 29—There is a known outage or problem with the network.
- 30—Scheduled maintenance period.

- 31—The WLAN security method is not correct.
- 32—The WLAN encryption method is not correct.
- 33—The WLAN authentication method is not correct.

stats-request <i>measurement-duration</i>	Sends a request for statistics.
dot11	Optional) Specifies dot11 counters.
security	(Optional) Specifies security counters.
test-abort	Sends a request to the client to abort the current test.
test-association <i>ssid bssid</i> <i>dot11 channel</i>	Sends a request to the client to perform the association test.
test-dot1x	Sends a request to the client to perform the 802.1x test.
<i>profile-id</i>	(Optional) Test profile name.
<i>bssid</i>	Basic SSID.
<i>dot11</i>	Specifies the 802.11a, 802.11b, or 802.11g network.
<i>channel</i>	Channel number.
test-profile	Sends a request to the client to perform the profile redirect test.
any	Sends a request to the client to perform the profile redirect test.
<i>profile-id</i>	Test profile name. Note The profile ID should be from one of the client profiles for which client reporting is enabled.

Command Default No default behavior or values.

Command Modes Global configuration

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

Usage Guidelines The **default-gw-ping** test does not require the client to use the diagnostic channel.

Examples

This example shows how to clear the reporting information of the client MAC address 00:1f:ca:cf:b6:60:

```
Switch# configure terminal  
Switch(config)# wireless client mac-address 00:1f:ca:cf:b6:60 ccx clear-reports  
Switch(config)# end
```

wireless load-balancing

To globally configure aggressive load balancing on the controller, use the **wireless load-balancing** command in global configuration mode.

wireless load-balancing {**denial** *denial-count*|**window** *client-count*}

Syntax Description

denial <i>denial-count</i>	Specifies the number of association denials during load balancing. Maximum number of association denials during load balancing is from 1 to 10 and the default value is 3.
window <i>client-count</i>	Specifies the aggressive load balancing client window, with the number of clients needed to trigger aggressive load balancing on a given access point. Aggressive load balancing client window with the number of clients is from 0 to 20 and the default value is 5.

Command Default

Disabled.

Command Modes

Global configuration

Command History

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

Usage Guidelines

Load-balancing-enabled WLANs do not support time-sensitive applications like voice and video because of roaming delays.

When you use Cisco 7921 and 7920 Wireless IP Phones with controllers, make sure that aggressive load balancing is disabled on the voice WLANs for each controller. Otherwise, the initial roam attempt by the phone might fail, causing a disruption in the audio path.

Examples

This example shows how to configure association denials during load balancing:

```
Switch# configure terminal
Switch(config)# wireless load-balancing denial 5
Switch(config)# end
```

wireless sip preferred-call-no

To add a new preferred call or configure voice prioritization, use the **wireless sip preferred-call-no** command in global configuration mode. To remove a preferred call, use the **no** form of this command.

wireless sip preferred-call-no *callIndex* *call-no*

no wireless sip preferred-call-no *callIndex*

Syntax Description

<i>callIndex</i>	Call index with valid values between 1 and 6.
<i>call-no</i>	Preferred call number that can contain up to 27 characters.

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

Before you configure voice prioritization, you must complete the following prerequisites:

- Set WLAN QoS to allow voice calls to pass through.
- Enable ACM for the radio.
- Enable SIP call snooping on the WLAN.

Examples

This example shows how to add a new preferred call or configure voice prioritization:

```
Switch# configure terminal
Switch(config)# wireless sip preferred-call-no 2 0123456789
Switch(config)# end
```

writertc

To update the value of the Real Time Clock (RTC) setting, use the **writertc** command in boot loader mode.

writertc { *year(0-99)* | *month(1-12)* | *date(1-31)* | *hour (0-23)* | *min(0-59)* | *sec(0-59)* | *dayofweek(1-7)* }

Syntax Description

<i>year(0-99)</i>	0 to 99. Century value is not used.
<i>month(1-12)</i>	1 to 12. 1 is January.
<i>date(1-31)</i>	1 to 31.
<i>hour(0-23)</i>	0 to 23.
<i>min(0-59)</i>	0 to 59.
<i>sec(0-59)</i>	0 to 59.
<i>dayofweek(1-7)</i>	1 to 7. 1 is Monday.

Command Default

No default behavior or values.

Command Modes

Boot loader

Command History

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

Examples

This example shows how to set the current RTC setting as Wednesday 27th August 2013 at 11:45:10:

```
Switch: writertc 13 8 27 11 45 10 3
Switch:
Switch: readrtc
Wednesday 08-27-13
11:45:11
```

Related Commands

Command	Description
readrtc	Displays the current value of the Real Time Clock (RTC) setting.

