# System Management Commands

# ap hyperlocation

To configure Hyperlocation and related parameters, use the **ap hyperlocation** command. To disable Hyperlocation and related parameter configuration, use the **no** form of the commands.

**[no] ap hyperlocation** [**threshold** {**detection** *value-in-dBm*} | {**reset** *value-btwn-0-99*} | {**trigger** *value-btwn-1-100*}]

## Syntax Description

| | |
|---|---|
| **[no] ap hyperlocation** | Enables or disables Hyperlocation. |
| **threshold detection** *value-in-dBm* | Sets threshold to filter out packets with low RSSI. |
| **threshold reset** *value-btwn-0-99* | Resets value in scan cycles after trigger. |

| | |
|---|---|
| **threshold trigger** *value-btwn-1-100* | Sets the number of scan cycles before sending a BAR to clients. |

**Note** Ensure that the Hyperlocation threshold reset value is less than the threshold trigger value.

**Command History**

| Release | Modification |
|---|---|
| Cisco IOS XE Denali 16.2.1 | This command was introduced. |

**Related Topics**

show ap hyperlocation, on page 65

# ap name hyperlocation

To configure hyperlocation and related parameters for an access point (AP), use the **ap name hyperlocation** command. To disable hyperlocation and related parameters, use the **no** form of this command.

**ap name** *ap-name* **hyperlocation ble-beacon** *beacon-id* { **major** *major-value* | **minor** *minor-value* | **txpwr** *att-value* }

**Syntax Description**

| | |
|---|---|
| *ap-name* | Access point name. |
| **ble-beacon** | Configures BLE beacon parameters. |
| *beacon-id* | BLE beacon ID. |
| **major** | Configures BLE beacon major parameter. |
| *major-value* | BLE beacon major value. The range is from 0 to 65535. The default is 0. |
| **minor** | Configures BLE beacon minor parameter. |
| *minor-value* | BLE beacon minor value. The range is from 0 to 65535. The default is 0. |
| **txpwr** | Configures BLE beacon attenuation level. |
| *att-value* | BLE beacon attenuation value, in dBm. The range is from 0 to 52. The default is 0. |

**Command Default**

BLE beacon details are not configured.

**Command Modes**

Privileged EXEC (#)

**Command History**

| Release | Modification |
|---|---|
| Cisco IOS XE Denali 16.3.1 | This command was introduced. |

**Example**

This example shows how to configure hyperlocation and related parameters for an AP:

```
Controller# ap name test-ap hyperlocation ble-beacon 3 txpwr 50
```

# hyperlocation

To configure Hyperlocation and related parameters for an AP group, use the **hyperlocation** command in the WLAN AP Group configuration (`Device(config-apgroup)#`) mode. To disable Hyperlocation and related parameter configuration for the AP group, use the **no** form of the command.

**[no] hyperlocation** [**threshold** {**detection** *value-in-dBm* | **reset** *value-btwn-0-99* | **trigger** *value-btwn-1-100*}]

## Syntax Description

| | |
|---|---|
| **[no] hyperlocation** | Enables or disables Hyperlocation for an AP group. |
| **threshold detection** *value-in-dBm* | Sets threshold to filter out packets with low RSSI. The **[no]** form of the command resets the threshold to its default value. |
| **threshold reset** *value-btwn-0-99* | Resets value in scan cycles after trigger. The **[no]** form of the command resets the threshold to its default value. |
| **threshold trigger** *value-btwn-1-100* | Sets the number of scan cycles before sending a BAR to clients. The **[no]** form of the command resets the threshold to its default value.<br>**Note** Ensure that the Hyperlocation threshold reset value is less than the threshold trigger value. |

## Command Modes

WLAN AP Group configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Denali 16.3.1 | This command was introduced. |

- This example shows how to set threshold to filter out packets with low RSSI:

```
Device(config-apgroup)# [no] hyperlocation threshold detection -100
```

- This example shows how to reset value in scan cycles after trigger:

```
Device(config-apgroup)# [no] hyperlocation threshold reset 8
```

- This example shows how to set the number of scan cycles before sending a BAR to clients:

```
Device(config-apgroup)# [no] hyperlocation threshold trigger 10
```

# ap ntp ip

To configure the IPv4 address of the NTP server, directly reachable by the access points, use the **ap ntp ip** command. To remove the IPv4 address that is configured for the NTP server, use the **no** form of the command.

- NTP is mandatory for Hyperlocation to work. If NTP is not defined, Hyperlocation will not be operational.

- NTP server must be reachable from the AP VLAN.
- If **ap ntp** command is not present, globally configured NTP is used.

**[no] ap ntp ip** *ipv4-addr*

**Syntax Description**

| | |
|---|---|
| *ipv4-addr* | IPv4 address of the NTP server |

**Command History**

| Release | Modification |
|---|---|
| Cisco IOS XE Denali 16.2.1 | This command was introduced. |

**Related Topics**

show ap hyperlocation, on page 65

# ntp ip

To set the IPv4 address of the NTP server, directly reachable by the APs of an AP group, use the **ntp ip** command in the WLAN AP Group configuration (`Device(config-apgroup)#`) mode. To remove the IPv4 address that is configured for the NTP server, use the **no** form of the command.

- NTP is mandatory for Hyperlocation to work. If NTP is not defined, Hyperlocation will not be operational.
- NTP server must be reachable from the AP VLAN.
- If the IPv4 address of the NTP server is not configured, the IP address of the globally configured NTP server is used.

**Note** The **show** commands display the details of the NTP server that is effectively used. For example, if the AP NTP server (configured via the **ntp ip** *ip-addr* command) is set to 0.0.0.0, the **show ap group hyperlocation** {**summary** | **detail**} command shows the details of one of the NTP servers from the system-wide IOS NTP configuration.

**[no] ntp ip** *ipv4-addr*

**Syntax Description**

| | |
|---|---|
| *ipv4-addr* | IPv4 address of the NTP server. The **[no]** form of the command resets the NTP value to 0.0.0.0. |

**Command Modes**

WLAN AP Group configuration

**Command History**

| Release | Modification |
|---|---|
| Cisco IOS XE Denali 16.3.1 | This command was introduced. |

# arp

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

**arp** [*ip_address*]

**Syntax Description**

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

**Command Default**

No default behavior or values.

**Command Modes**

Boot loader

**Command History**

| Release | Modification |
|---|---|
| Cisco IOS XE 3.2SE | This command was introduced. |

**Usage Guidelines**

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

**Examples**

This example shows how to display the ARP table:

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

**Related Topics**

set, on page 60

# boot

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

**boot** [**-post** | **-n** | **-p** | *flag*] *filesystem:/file-url...*

**Syntax Description**

| | |
|---|---|
| **-post** | (Optional) Run the loaded image with an extended or comprehensive power-on self-test (POST). Using this keyword causes POST to take longer to complete. |
| **-n** | (Optional) Pause for the Cisco IOS Debugger immediately after launching. |
| **-p** | (Optional) Pause for the JTAG Debugger right after loading the image. |
| *filesystem:* | Alias for a file system. Use **flash:** for the system board flash device; use **usbflash0:** for USB memory sticks. |

| | |
|---|---|
| */file-url* | Path (directory) and name of a bootable image. Separate image names with a semicolon. |

**Command Default** No default behavior or values.

**Command Modes** Boot loader

**Command History**

| Release | Modification |
|---|---|
| Cisco IOS XE 3.2SE | This command was introduced. |

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

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

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

These settings are not saved for the next boot operation.

Filenames and directory names are case sensitive.

### Example

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

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

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

# cat

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

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

**Syntax Description**

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

**Command Default** No default behavior or values.

**Command Modes** Boot loader

**Command History**

| Release | Modification |
|---|---|
| Cisco IOS XE 3.2SE | This command was introduced. |

**Usage Guidelines**

Filenames and directory names are case sensitive.

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

**Examples**

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

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

# clear location

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

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

**Syntax Description**

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

**Command Default**

No default behavior or values.

**Command Modes**

User EXEC

Privileged EXEC

**Command History**

| Release | Modification |
|---|---|
| Cisco IOS XE 3.2SE | This command was introduced. |

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

```
Device> clear location rfid
```

# clear location statistics

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

**clear location statistics**

**Syntax Description** This command has no arguments or keywords.

**Command Default** No default behavior or values.

**Command Modes** User EXEC

Privileged EXEC

**Command History**

| Release | Modification |
|---|---|
| Cisco IOS XE 3.2SE | This command was introduced. |

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

```
Device> clear location statistics
```

# 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 3.2SE | This command was introduced. |

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):

```
Device> 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 3.2SE | This command was introduced. |

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

```
Device> 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. |
| *client-mac-addr* | MAC address of the client. |
| **all** | Specifies all access points. |

| | |
|---|---|
| **name** *ap-name* | 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 3.2SE | This command was introduced. |

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:

```
Device> 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 3.2SE | 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.

### Example

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:

```
Device> 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**

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

**Command Default**

No default behavior or values.

**Command Modes**

Boot loader

**Command History**

| Release | Modification |
|---|---|
| Cisco IOS XE 3.2SE | This command was introduced. |

**Usage Guidelines**

Filenames and directory names are case sensitive.

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

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

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

**Examples**

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

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

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

# config-ble

To configure a BLE beacon value, use the **config-ble** command.

**config-ble** { **default** {**enable** | **txpwr** | **uuid** } | **enable** | **exit** | **no** {**enable** | **txpwr** | **uuid** *uuid-name* } | **txpwr***att-value* | **uuid**}

**Syntax Description**

| | |
|---|---|
| **default** | Sets a command to its default value. |
| **enable** | Enables a BLE beacon. |
| **txpwr** | Configures the BLE beacon attenuation level. |
| **uuid** | Configures universally unique identifier (UUID). |
| *uuid-string* | UUID hexadecimal string. As defined by RFC standards (RFC4122), the GUI accepts user input in both upper and lowercase characters, but the input is stored in lowercase. |
| **exit** | Exits the config-ble submode. |
| **no** | Negate a command or sets it to default values. |
| *att-value* | BLE beacon attenuation value, in dBm. The range is from 0 to 52. The default is 0. |

**Command Default**

BLE beacon values are not configured.

**Command Modes**

config-ble

**Command History**

| Release | Modification |
|---|---|
| Cisco IOS XE Denali 16.3.1 | This command was introduced. |

**Usage Guidelines**

Use this command to configure BLE beacon parameters.

**Example**

The following example shows how to enable BLE beacon:

```
Controller(config-ble)# enable
```

# copy startup-config tftp:

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

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

**Syntax Description**

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

**Command Default**

No default behavior or values.

**Command Modes**

Privileged EXEC

**Command History**

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

**Usage Guidelines**

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

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

**Examples**

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

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

# copy tftp: startup-config

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

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

**Syntax Description**

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

**Command Default**

No default behavior or values.

**Command Modes**

Privileged EXEC

**Command History**

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

**Usage Guidelines**

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

**Examples**

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

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

# debug 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 3.2SE | This command was introduced. |

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

```
Device# 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**

| | |
|---|---|
| *debug_leaf_name* | 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. |
| *filter* | Debug flag filter name. |
| **switch** *switch* | Configures RFID debugging for device. |

**Command Default** No default behavior or values.

**Command Modes** Privileged EXEC

**Command History**

| Release | Modification |
|---|---|
| Cisco IOS XE 3.2SE | This command was introduced. |

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

```
Device# 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** *mac-address1* **mac-address** *mac-address2* | Specifies MAC addresses of the voice clients. |
| **verbose** | Enables verbose mode for voice diagnostics. |

**Command Default**

No default behavior or values.

**Command Modes**

Privileged EXEC

**Command History**

| Release | Modification |
|---|---|
| Cisco IOS XE 3.2SE | This command was introduced. |

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

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

# debug 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** *switch* | Displays the WPS MFP debugging for the device. |

**Command Default** No default behavior or values.

**Command Modes** Privileged EXEC

**Command History**

| Release | Modification |
|---|---|
| Cisco IOS XE 3.2SE | This command was introduced. |

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

```
Device# 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**

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

**Command Default** No default behavior or values.

**Command Modes** Boot loader

**Command History**

| Release | Modification |
|---|---|
| Cisco IOS XE 3.2SE | This command was introduced. |

**Usage Guidelines** Filenames and directory names are case sensitive.

The device prompts you for confirmation before deleting each file.

**Examples** This example shows how to delete two files:

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

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

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

# dir

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

**dir** *filesystem:/file-url*

## Syntax Description

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

## Command Default

No default behavior or values.

## Command Modes

Boot Loader

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE 3.2SE | This command was introduced. |

## Usage Guidelines

Directory names are case sensitive.

## Examples

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

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

   96453632 bytes available (25732096 bytes used)
```

***Table 1: dir Field Descriptions***

| Field | Description |
|---|---|
| 2 | Index number of the file. |

| Field | Description |
|---|---|
| -rwx | File permission, which can be any or all of the following:<br>• d—directory<br>• r—readable<br>• w—writable<br>• x—executable |
| 1644045 | Size of the file. |
| <date> | Last modification date. |
| env_vars | Filename. |

**Related Topics**

mkdir, on page 35
rmdir, on page 58

# emergency-install

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

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

**Syntax Description**

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

**Command Default**

No default behavior or values.

**Command Modes**

Boot loader

**Command History**

| Release | Modification |
|---|---|
| Cisco IOS XE 3.2SE | This command was introduced. |

**Usage Guidelines**

The boot flash is erased during the installation operation.

**Example**

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

```
Device: emergency-install tftp:<url>
The bootflash will be erased during install operation, continue (y/n)?y
Starting emergency recovery (tftp:<url> ...
Reading full image into memory.....................done
Nova Bundle Image
```

```
--------------------------------------
Kernel Address    : 0x6042d5c8
Kernel Size       : 0x317ccc/3243212
Initramfs Address : 0x60745294
Initramfs Size    : 0xdc6774/14444404
Compression Format: .mzip

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

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



Initiating Emergency Installation of bundle                                      \
tftp:<url>


Downloading bundle tftp:<url>...

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


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

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

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

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

    boot
```

# exit

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

**exit**

**Syntax Description** This command has no arguments or keywords.

**Command Default** No default behavior or values.

**Command Modes** Privileged EXEC

Global configuration

**Command History**

| Release | Modification |
|---|---|
| Cisco IOS XE 3.2SE | This command was introduced. |

This example shows how to exit the configuration mode:

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

# flash_init

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

**flash_init**

**Syntax Description** This command has no arguments or keywords.

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

**Command Modes** Boot loader

**Command History**

| Release | Modification |
|---|---|
| Cisco IOS XE 3.2SE | 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 3.2SE | This command was introduced. |

### Example

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

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

# l2 traceroute

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

**l2 traceroute**
**no l2 traceroute**

**Syntax Description** This command has no arguments or keywords.

**Command Modes** Global configuration (config#)

**Command History**

| Release | Modification |
|---|---|
| Cisco IOS XE 3.2SE | The command was introduced. |

**Usage Guidelines**

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

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

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

# license right-to-use

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

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

**Syntax Description**

| | |
|---|---|
| **activate** | Activates permanent or evaluation ap-count licenses. |
| **deactivate** | Deactivates permanent or evaluation ap-count licenses. |
| **apcount** *count* | Specifies the number of ap-count licenses added.<br>You can configure the number of adder licenses from 5 to 50. |
| **ipbase** *count* | Activates ipbase licenses on the switch. |
| **ipservices** *count* | Activates ipservices licenses on the switch. |
| **lanbase** *count* | 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 3.2SE | This command was introduced. |

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

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

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

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

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

```
Device# license right-to-use activate apcount 500 slot 1
Device# 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-client***timeout-value* | **client***timeout-value* | **rouge-aps***timeout-value* | **tags***timeout-value*} | **geo-location identifier** {**host***id*} | **notify-threshold**{**client***db* | **rouge-aps***db* | **tags***db* | **plm**{**calibrating** | {**multiband** | **uniband**} | **client***burst-interval*} | **prefer**{**cdp weight***priority-value* | **lldp-med weight***priority-value* | **static config weight***priority-value*} | **rfid**{**status** | **timeout***rfid-timeout-value* | **vendor-name***name*} | **rssi-half-life** { **calibrating-client***seconds* | **client***seconds* | **rogue-aps***seconds* | **tags***seconds*}
**no location** {**admin-tag** *string* | **algorithm** | **civic-location identifier** {**host***id*} | **civic-location identifier** {**host***id*} | **elin-location** {*string* | **identifier** *id*} | **expiry**{**calibrating-client***timeout-value* | **client***timeout-value* | **rouge-aps***timeout-value* | **tags***timeout-value*} | **geo-location identifier** {**host***id*} | **notify-threshold**{**client***db* | **rouge-aps***db* | **tags***db* | **plm**{**calibrating** | {**multiband** | **uniband**} | **client***burst-interval*} | **prefer**{**cdp weight***priority-value* | **lldp-med weight***priority-value* | **static config weight***priority-value*} | **rfid**{**status** | **timeout***rfid-timeout-value* | **vendor-name***name*} | **rssi-half-life** { **calibrating-client***seconds* | **client***seconds* | **rogue-aps***seconds* | **tags***seconds*}

## Syntax Description

| | |
|---|---|
| **admin-tag***string* | 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. |
| *id* | Name of the civic, emergency, or geographical location.<br>**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}** *timeout-value* | Configures the timeout for RSSI values for calibrating clients, clients, rouge access points, and RFID tags.<br>The valid range for the timeout parameter for calibrating clients is 1 to 3600 seconds, and the default value is 5 seconds.<br>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}** *db* | Configures the NMSP notification threshold for RSSI measurements.<br>The valid range for the threshold parameter is 0 to 10 dB, and the default value is 0 dB. |
| **calibrating {multiband \| uniband} \| client** *seconds* | Configures path loss measurement (CCX S60) request for calibrating clients and burst interval for clients.<br>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

**Command History**

| Release | Modification |
|---|---|
| Cisco IOS XE 3.2SE | This command was introduced. |

## Usage Guidelines

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

The civic-location identifier must not exceed 250 bytes.

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

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

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

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

- **altitude**—Sets altitude information in units of floor, meters, or feet.
- **latitude**—Sets latitude information in degrees, minutes, and seconds. The range is from -90 degrees to 90 degrees. Positive numbers indicate locations north of the equator.
- **longitude**—Sets longitude information in degrees, minutes, and seconds. The range is from -180 degrees to 180 degrees. Positive numbers indicate locations east of the prime meridian.
- **resolution**—Sets the resolution for latitude and longitude. If the resolution value is not specified, default value of 10 meters is applied to latitude and longitude resolution parameters. For latitude and longitude, the resolution unit is measured in meters. The resolution value can also be a fraction.
- **default**—Sets the geographical location to its default attribute.
- **exit**—Exits from geographical location configuration mode.
- **no**—Negates the specified geographical parameters and sets the default value.

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

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

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

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

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

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

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

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

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

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

# location 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 3.2SE | This command was introduced. |

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

```
Device# configure terminal
Device(config)# location algorithm rssi-average
Device(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. |
| *timeout-value* | The valid range for the timeout parameter for calibrating clients is 1 to 3600 seconds, and the default value is 5 seconds.<br>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. |

**Command Default** No default behavior or values.

**Command Modes** Global configuration

**Command History**

| Release | Modification |
|---|---|
| Cisco IOS XE 3.2SE | This command was introduced. |

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

```
Device# configure terminal
Device(config)# location expiry client 1000
Device(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.<br>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.<br>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.<br>The valid range for the threshold parameter is 0 to 10 dB, and the default value is 0 dB. |
| *db* | 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 3.2SE | This command was introduced. |

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:

```
Device# configure terminal
Device(config)# location notify-threshold client 10
Device(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 3.2SE | This command was introduced. |

**Usage Guidelines**

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

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

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

# 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.<br>The **no location rfid status** command disables location tracking for tags. |
| **timeout** *seconds* | Specifies the location RFID timeout value.<br>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.<br>The valid timeout range is from 60 through 7200 seconds. |
| **vendor-name** *name* | Specifies the RFID tag vendor name. |

**Command Default**

No default behavior or values.

**Command Modes**

Global configuration

**Command History**

| Release | Modification |
|---|---|
| Cisco IOS XE 3.2SE | 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.

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

```
Device# configure terminal
Device(config)# location rfid timeout 1000
Device(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. |

| | |
|---|---|
| *seconds* | 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 3.2SE | This command was introduced. |

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

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

# mac address-table move update

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

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

**Syntax Description**

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

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

**Command Modes** Global configuration

**Command History**

**Command History**

| Release | Modification |
|---|---|
| Cisco IOS XE 3.2SE | This command was introduced. |

**Usage Guidelines** The MAC address-table move update feature allows the switch to provide rapid bidirectional convergence if a primary (forwarding) link goes down and the standby link begins forwarding traffic.

You can configure the access switch to send the MAC address-table move update messages if the primary link goes down and the standby link comes up. You can configure the uplink switches to receive and process the MAC address-table move update messages.

### Examples

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

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

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

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

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

# mgmt_init

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

**mgmt_init**

### Syntax Description

This command has no arguments or keywords.

### Command Default

No default behavior or values.

### Command Modes

Boot loader

### Command History

| Release | Modification |
|---|---|
| Cisco IOS XE 3.2SE | This command was introduced. |

### Usage Guidelines

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

### Examples

This example shows how to initialize the Ethernet management port:

```
Device: mgmt_init
```

# mkdir

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

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

**Syntax Description**

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

**Command Default**

No default behavior or values.

**Command Modes**

Boot loader

**Command History**

| Release | Modification |
|---|---|
| Cisco IOS XE 3.2SE | This command was introduced. |

**Usage Guidelines**

Directory names are case sensitive.

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

### Example

This example shows how to make a directory called Saved_Configs:

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

### Related Topics

dir, on page 19
rmdir, on page 58

# more

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

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

**Syntax Description**

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

**Command Default**

No default behavior or values.

**Command Modes** Boot loader

**Command History**

| Release | Modification |
|---|---|
| Cisco IOS XE 3.2SE | This command was introduced. |

**Usage Guidelines** Filenames and directory names are case sensitive.

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

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

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

# nmsp notification interval

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

**nmsp notification interval** { **attachment** | **location** | **rssi** {**clients** | **rfid** | **rogues** {**ap** | **client** } } }

**Syntax Description**

| | |
|---|---|
| **attachment** | Specifies the time used to aggregate attachment information. |
| **location** | Specifies the time used to aggregate location information. |
| **rssi** | Specifies the time used to aggregate RSSI information. |
| **clients** | Specifies the time interval for clients. |
| **rfid** | 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 3.2SE | This command was introduced. |

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

```
Device# configure terminal
Device(config)# nmsp notification-interval rfid 25
Device(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:

```
Device# configure terminal
Device(config)# nmsp notification-interval attachment 10
Device(config)# end
```

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

```
Device# configure terminal
Device(config)# nmsp notification-interval location 20
Device(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.

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

# rename

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

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

**Syntax Description**

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

**Command Default** No default behavior or values.

**Command Modes** Boot loader

**Command History**

| Release | Modification |
|---|---|
| Cisco IOS XE 3.2SE | This command was introduced. |

**Usage Guidelines**

Filenames and directory names are case sensitive.

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

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

**Examples**

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

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

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

# request platform software console attach switch

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

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

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

**Syntax Description**

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

**Command Default**

By default, all switches in the stack are active.

**Command Modes**

Privileged EXEC (#)

**Command History**

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

**Usage Guidelines**

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

**Examples**

This example shows how to session to the standby switch:

```
Device# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Device(config)# redundancy
Device(config-red)# main-cpu
Device(config-r-mc)# standby console enable
Device(config-r-mc)# end
Device# request platform software console attach switch standby R0
#
# Connecting to the IOS console on the route-processor in slot 0.
# Enter Control-C to exit.
#
Device-stby> enable
Device-stby#
```

# request platform software package clean

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

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

## Syntax Description

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

## Command Default

No default behavior or values

## Command Modes

Privileged EXEC (#)

## Command History

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

## Usage Guidelines

### Example

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

```
Device# request platform software package clean

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

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

## Related Commands

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

# request platform software package copy

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

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

**Syntax Description**

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

**Command Default**

No default behavior or values.

**Command Modes**

Privileged EXEC (#)

**Command History**

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

**Usage Guidelines**

**Example**

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

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

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

# request platform software package describe file

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

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

**Syntax Description**

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

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

## Command Default

No default behavior or values.

## Command Modes

Privileged EXEC (#)

## Command History

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

## Usage Guidelines

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

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

- To confirm the individual module files that are part of a Cisco IOS-XE image.
- To confirm whether or not a file is bootable.
- To confirm the contexts in which a file must be reloaded or booted.
- To confirm whether or not a file is corrupted.
- To confirm file and header sizes, build dates, and various other general information.

## Examples

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

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

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

  Raw disk-file SHA1sum:
    3ee37cdbe276316968866b16df7d8a5733a1502e

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

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

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

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


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

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

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

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

  Raw disk-file SHA1sum:
    d2999fc7e27e01344903a42ffacd62c156eba4cc

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

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

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


  Package is bootable from media and tftp.
  Package contents:

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

    Raw disk-file SHA1sum:
      f1aad6d687256aa327a4efa84deab949fbed12b8

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

    Header size:     204 bytes
```

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

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


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

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

  Raw disk-file SHA1sum:
    025e6159dd91cef9d254ca9fff2602d8ce065939

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

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

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


  Package is not bootable.

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

  Raw disk-file SHA1sum:
    432dfa61736d8a51baefbb2d70199d712618dcd2

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

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

```
  Package flags:   0
  Header version:  0

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


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

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

  Raw disk-file SHA1sum:
    eb964b33d4959c21b605d0989e7151cd73488a8f

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

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

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


  Package is not bootable.

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

  Raw disk-file SHA1sum:
    bc13462d6a4af7a817a7346a44a0ef7270e3a81b

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

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

```
  Header version:  0

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


  Package is not bootable.

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

  Raw disk-file SHA1sum:
    3ee37cdbe276316968866b16df7d8a5733a1502e

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

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

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


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

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

  Raw disk-file SHA1sum:
    44b6d15cba31fb0e9b27464665ee8a24b92adfd2

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

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

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


Package is not bootable.
```

**Related Commands**

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

# request platform software package expand

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

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

**Syntax Description**

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

**Command Default**

No default behavior or values

**Command Modes**

Privileged EXEC (#)

**Command History**

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

**Usage Guidelines**

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

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

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

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

**Examples**

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

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

```
Device# dir bootflash:

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

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

Verifying parameters
Validating package type
Copying package files

Device# dir bootflash:

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

**Related Commands**

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

# request platform software package install auto-upgrade

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

**request platform software package install auto-upgrade**

**Syntax Description** This command has no arguments or keywords.

**Command Default** No default behavior or values.

**Command Modes** Privileged EXEC (#)

**Command History**

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

**Examples**

The following example shows how to automatically upgrade the software:

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

**Related Commands**

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

# request platform software package install commit

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

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

**Syntax Description**

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

**Command Default** No default behavior or values.

**Command Modes** Privileged EXEC (#)

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

## Usage Guidelines

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

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

## Examples

The following example shows how to commit an upgrade:

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

## Related Commands

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

# request platform software package install file

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

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

## Syntax Description

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

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

## Command Default

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

## Command Modes

Privileged EXEC (#)

## Command History

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

## Usage Guidelines

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

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

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

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

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

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

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

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

Device# reload
```

**Note** A reload must be performed to finish this procedure.

## Related Commands

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

# request platform software package install rollback

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

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

## Syntax Description

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

## Command Default

No default behavior or values

## Command Modes

Privileged EXEC (#)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE Everest 16.1.1 | This command was introduced. |

## Usage Guidelines

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

**Examples**

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

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

**Related Commands**

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

# request platform software package install snapshot

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

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

**Syntax Description**

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

**Command Default**

No default behavior or values

**Command Modes**

Privileged EXEC (#)

**Command History**

| Release | Modification |
|---|---|
| Cisco IOS XE Everest 16.1.1 | This command was introduced. |

**Usage Guidelines**

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

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

**Examples**

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

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

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

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

Building configuration...
[OK]

Device# reload
```

**Related Commands**

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

# request platform software package verify

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

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

**Syntax Description**

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

**Command Default**

No default behavior or values.

**Command Modes**

Privileged EXEC (#)

**Command History**

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

### Example

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

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

**Related Commands**

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

# request platform software package uninstall

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

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

**Syntax Description**

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

**Command Default**

No default behavior or values.

**Command Modes**

Privileged EXEC (#)

**Command History**

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

### Example

The following example shows how to uninstall a software package:

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

**Related Commands**

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

# reset

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

**reset**

**Syntax Description** This command has no arguments or keywords.

**Command Default** No default behavior or values.

**Command Modes** Boot loader

**Command History**

| Release | Modification |
|---|---|
| Cisco IOS XE 3.2SE | This command was introduced. |

**Examples** This example shows how to reset the system:

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

**Related Topics**

reset, on page 57
test cable-diagnostics tdr, on page 103

# rmdir

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

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

**Syntax Description**

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

**Command Default** No default behavior or values.

**Command Modes** Boot loader

**Command History**

| Release | Modification |
|---|---|
| Cisco IOS XE 3.2SE | This command was introduced. |

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

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

The device prompts you for confirmation before deleting each directory.

### Example

This example shows how to remove a directory:

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

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

### Related Topics

dir, on page 19

# 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 3.2SE | This command was introduced. |

## Usage Guidelines

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

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

### Example

This example shows how to configure the advanced template:

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

### Related Topics

show sdm prefer, on page 84

# set

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

**set** *variable value*

## Syntax Description

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

## Command Default

The environment variables have these default values:

MANUAL_BOOT: No (0)

BOOT: Null string

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

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

PS1 device:

CONFIG_FILE: config.text

BAUD: 9600 b/s

SWITCH_NUMBER: 1

SWITCH_PRIORITY: 1

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

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

Many environment variables are predefined and have default values.

## Command Modes

Boot loader

## Command History

| Release | Modification |
|---|---|
| Cisco IOS XE 3.2SE | This command was introduced. |

## Usage Guidelines

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

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

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

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

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

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

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

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

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

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

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

### Example

This example shows how to set the SWITCH_PRIORITY environment variable:

```
Device: set SWITCH_PRIORITY 2
```

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

### Related Topics

reset, on page 57
unset, on page 111

# show avc client

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

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

### Syntax Description

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

### Command Default

No default behavior or values.

### Command Modes

Privileged EXEC

### Command History

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

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

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

Cumulative Stats:

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

```
Last Interval(90 seconds) Stats:

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

# show 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. |

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

```
Device# 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
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**

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

**Command Default**

No default behavior or values.

**Command Modes**

Privileged EXEC

**Command History**

| Release | Modification |
|---|---|
| Cisco IOS XE 3.2SE | This command was introduced. |

**Usage Guidelines**

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

### Examples

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

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

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

| Field | Description |
|---|---|
| Interface | The interface on which TDR is run. |
| Speed | The speed of connection. |

| Field | Description |
|---|---|
| Local pair | The name of the pair of wires that TDR is testing on the local interface. |
| Pair length | The location of the problem on the cable, with respect to your device. TDR can only find the location in one of these cases:<br>• The cable is properly connected, the link is up, and the interface speed is 1000 Mb/s.<br>• The cable is open.<br>• The cable has a short. |
| Remote pair | The name of the pair of wires to which the local pair is connected. TDR can learn about the remote pair only when the cable is properly connected and the link is up. |
| Pair status | The status of the pair of wires on which TDR is running:<br>• Normal—The pair of wires is properly connected.<br>• Not completed—The test is running and is not completed.<br>• Not supported—The interface does not support TDR.<br>• Open—The pair of wires is open.<br>• Shorted—The pair of wires is shorted.<br>• ImpedanceMis—The impedance is mismatched.<br>• Short/Impedance Mismatched—The impedance mismatched or the cable is short.<br>• InProgress—The diagnostic test is in progress. |

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

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

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

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

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

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

### Related Topics

test cable-diagnostics tdr, on page 103

# show ap hyperlocation

To view a summary or detailed information of Hyperlocation configuration, use the **show ap hyperlocation** command.

**show ap hyperlocation** {**summary** | **detail**}

**Syntax Description**

| | |
|---|---|
| **summary** | Shows the overall configuration values and operational values |
| **detail** | Shows the overall configuration and operation values as well as detailed information of each AP |

**Command History**

| Release | Modification |
|---|---|
| Cisco IOS XE Denali 16.2.1 | This command was introduced. |

This example shows how to view a summary of Hyperlocation configuration:

```
Device# show ap hyperlocation summary

Hyperlocation operational status: Up
Hyperlocation NTP server currently used: 209.165.200.224
Hyperlocation admin status: Enabled
Hyperlocation detection threshold: -100 dBm
Hyperlocation trigger threshold: 10
Hyperlocation reset threshold: 8
```

**Note** For Hyperlocation to be operational, the following conditions must be met:

- At least one Cisco CMX with Hyperlocation enabled
- Hyperlocation admin state operational
- Either AP NTP or IOS NTP configured

This example shows how to view detailed information about Hyperlocation configuration:

```
Device# show ap hyperlocation detail

Hyperlocation operational status: Up
Hyperlocation NTP server currently used: 209.165.200.224
Hyperlocation admin status: Enabled
Hyperlocation detection threshold: -100 dBm
Hyperlocation trigger threshold: 10
Hyperlocation reset threshold: 8

AP Name                 Radio MAC        Method    Hyperlocation
-----------------------------------------------------------------
AP84b8.0252.b930        84b8.0216.c721   HALO      Enabled
AP84b8.0265.5540        84b8.0243.8796   WSM       Enabled
APf07f.0635.2d40        f07f.0676.3b89   WSM       Enabled
APf4cf.e272.4ed0        f4cf.e223.ba31   HALO      Enabled
```

# show ap name hyperlocation

To view a summary or detailed information about the hyperlocation configuration for an access point (AP), use the **show ap name hyperlocation** command.

**show ap name** *ap-name* **hyperlocation ble-beacon**

**Syntax Description**

| | |
|---|---|
| *ap-name* | Access point name. |
| **hyperlocation** | Displays AP hyperlocation information. |
| **ble-beacon** | Displays BLE beacon configuration of an AP. |

**Command Modes**

Privileged EXEC (#)

**Command History**

| Release | Modification |
|---|---|
| Cisco IOS XE Denali 16.3.1 | This command was introduced. |

### Example

This example shows how to view the BLE beacon configuration of an AP:

```
Device# show ap name test-ap hyperlocation ble-beacon

ID  Major  Minor  TX Power(dBm)
------------------------------
0   0      0      0
1   0      0      0
2   0      0      0
3   0      0      0
```

# show ap group hyperlocation

To view a summary or detailed information of Hyperlocation configuration for an AP group, use the **show ap group** *ap-group-name* **hyperlocation** command.

**show ap group hyperlocation** {**summary** | **detail**}

**Syntax Description**

| | |
|---|---|
| **summary** | Shows the overall configuration values (AP group specific) and operational status and parameters for the AP group. |
| **detail** | Shows both overall (AP group specific) and per-AP configuration values and operational status for the AP group. The APs listed are only those that belong to the AP group. |

**Command Modes**

User EXEC

Privileged EXEC

**Command History**

| Release | Modification |
|---|---|
| Cisco IOS XE Denali 16.3.1 | This command was introduced. |

This example shows how to view a summary of Hyperlocation configuration for an AP group:

```
Device# show ap group my-ap-group hyperlocation summary

Site Name: my-ap-group
Site Description: This is an AP group
Hyperlocation operational status: Up
Reason: N/A
Hyperlocation NTP server: 9.0.0.4
Hyperlocation admin status: Enabled
Hyperlocation detection threshold: -100 dBm
Hyperlocation trigger threshold: 11
Hyperlocation reset threshold: 9
```

**Note** For Hyperlocation to be operational, the following conditions must be met:

- At least one Cisco CMX with Hyperlocation enabled
- Hyperlocation admin state operational
- Either AP NTP or IOS NTP configured

This example shows how to view detailed information about Hyperlocation configuration for an AP group:

```
Device# show ap group my-ap-group hyperlocation detail

Site Name: my-ap-group
Site Description: This is an AP group
Hyperlocation operational status: Up
Reason: N/A
Hyperlocation NTP server: 9.0.0.4
Hyperlocation admin status: Enabled
Hyperlocation detection threshold: -100 dBm
Hyperlocation trigger threshold: 11
Hyperlocation reset threshold: 9

Values for APs in all AP Groups:

AP Name                 Radio MAC        Method    Hyperlocation
-----------------------------------------------------------------
APf07f.0635.2d40        f07f.0676.3b89   WSM       Enabled
APf4cf.e272.4ed0        f4cf.e223.ba31   Local     Enabled
```

# show debug

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

**show debug**

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

**Syntax Description**

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

**Command Default**

No default behavior or values.

**Command Modes**

Privileged EXEC

**Command History**

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

**Usage Guidelines**

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

**Examples**

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

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

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

# show env

To display fan, temperature, and power information for the switch (standalone switch, 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** *switch-number* | (Optional) Displays the power supply status for a specific switch. |

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

**Command Default**

No default behavior or values.

**Command Modes**

User EXEC

Privileged EXEC

**Command History**

| Release | Modification |
|---|---|
| Cisco IOS XE 3.2SE | 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:

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

Device>
```

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

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

Device>
```

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

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

# show env xps

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

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

## Syntax Description

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

## Command Modes

Privileged EXEC

## Command History

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

## Usage Guidelines

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

## Examples

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

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



XPS 0101.0100.0000 :
=========================================================
Data                  Current    Power     Power Port  Switch #  PS A  PS B  Role-State
Committed
Budget
----  --------  ----  ----  ---------- ---------  ------ 1     -        -    715  SP-PS
   223
    1543
2     -        -    -    SP-PS      223       223
3     -        -    -    -          -         -
4     -        -    -    -          -         -
5     -        -    -    -          -         -
6     -        -    -    -          -         -
7     -        -    -    -          -         -
8     -        -    -    -          -         -
9     1        1100 -    RPS-NB     223        070
XPS  -        -    1100  -          -
```

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

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

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

```
Switch#
XPS 010



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

```
Mode               : Enabled (On)
Priority           : 3
Data stack switch # : - Configured role    : Auto-SP Run mode            : -
Cable faults
<output truncated>
```

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

```
================================================================================
XPS 0101.0100.0000 :
================================================================================
Port-Supply SW PID                 Serial#     Status          Mode Watts
----------- -- ------------------  ----------- --------------  ----  -----
XPS-A           Not present
XPS-B           NG3K-PWR-1100WAC   LIT13320NTV OK              SP   1100
1-A         -  -                   -           -
1-B         -  -                   -           -               SP    715
2-A         -  -                   -           -
2-B         -  -                   -           -
9-A                       100WAC    LIT141307RK OK               RPS  1100
9-B                    esent
```

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

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


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

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

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

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


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

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

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

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

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

SW Status Prog
-- ----------- ----
1 Waiting 0%
Switch#
*Mar 22 03:12:46.723: %PLATFORM_XPS-6-UPGRADE_START: XPS 0022.bdd7.9b14 upgrade has
started through the Service Port.
Switch# show env xps upgrade
XPS Upgrade Xfer
SW Status Prog
-- ----------- ----
1 Receiving 1%
Switch# show env xps upgrade
XPS Upgrade Xfer
SW Status Prog
-- ----------- ----
1 Receiving 5%
Switch# show env xps upgrade
XPS Upgrade Xfer
SW Status Prog
-- ----------- ----
1 Reloading 100%
Switch#
*Mar 22 03:16:01.733: %PLATFORM_XPS-6-UPGRADE_DONE: XPS 0022.bdd7.9b14 upgrade has
completed and the XPS is reloading.
```

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

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

***Table 4: Related Commands***

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

# show flow monitor

To display the status and statistics for a 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. |
| *monitor-name* | (Optional) Name of a flow monitor that was previously configured. |
| **cache** | (Optional) Displays the contents of the cache for the flow monitor. |
| **format** | (Optional) Specifies the use of one of the format options for formatting the display output. |
| **csv** | (Optional) Displays the flow monitor cache contents in comma-separated variables (CSV) format. |
| **record** | (Optional) Displays the flow monitor cache contents in record format. |
| **table** | (Optional) Displays the flow monitor cache contents in table format. |
| **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 3.2SE | 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:

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

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

This table describes the significant fields shown in the display.

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

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

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

```
Device# 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 6: 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. |
| 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:

```
Device# 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:

```
Device# 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:

```
Device# 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 device, 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 3.2SE | This command was introduced. |

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

```
Device# 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        adder        0 :0 :0                no    yes
 1      apcount        adder        0 :0 :0                no    yes
 1      apcount        adder        0 :0 :0                no    yes


Device#
```

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

```
Device# 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:

```
Device# 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:

```
Device# 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** *mac-addr* | Displays detailed location information with the RSSI table for a particular client. |
| **plm** | Displays location path loss measurement (CCX S60) configuration. |
| **statistics** | Displays location-based system statistics. |
| **summary** | Displays location-based system summary information. |

| | |
|---|---|
| **rfid** | Displays the RFID tag tracking information. |
| **client** | Displays the summary of RFID tags that are clients. |
| **config** | Displays the configuration options for RFID tag tracking. |
| **detail** *MAC-addr* | Displays the detailed information for one rfid tag. |
| **summary** | Displays summary information for all known rfid tags. |

**Command Default** No default behavior or values.

**Command Modes** Privileged EXEC

**Command History**

| Release | Modification |
|---|---|
| Cisco IOS XE 3.2SE | This command was introduced. |

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

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

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

# show location ap-detect

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

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

**Syntax Description**

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

**Command Default** No default behavior or values.

**Command Modes** Privileged EXEC

**Command History**

| Release | Modification |
|---|---|
| Cisco IOS XE 3.2SE | This command was introduced. |

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

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

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


RFID Tags



Rogue AP's



Rogue Clients

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

# show mac address-table move update

To display the MAC address-table move update information on the device, use the **show mac address-table move update** command in EXEC mode.

**show mac address-table move update**

**Syntax Description** This command has no arguments or keywords.

**Command Default** No default behavior or values.

**Command Modes** User EXEC

Privileged EXEC

**Command History**

| Release | Modification |
|---|---|
| Cisco IOS XE 3.2SE | This command was introduced. |

### Example

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

```
Device# show mac address-table move update

Switch-ID : 010b.4630.1780
Dst mac-address : 0180.c200.0010
Vlans/Macs supported : 1023/8320
Default/Current settings: Rcv Off/On, Xmt Off/On
Max packets per min : Rcv 40, Xmt 60
Rcv packet count : 10
Rcv conforming packet count : 5
Rcv invalid packet count : 0
Rcv packet count this min : 0
Rcv threshold exceed count : 0
Rcv last sequence# this min : 0
Rcv last interface : Po2
Rcv last src-mac-address : 0003.fd6a.8701
Rcv last switch-ID : 0303.fd63.7600
Xmt packet count : 0
Xmt packet count this min : 0
Xmt threshold exceed count : 0
Xmt pak buf unavail cnt : 0
Xmt last interface : None
```

# show nmsp

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

**show nmsp** {**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** *ip-addr* | 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 3.2SE | This command was introduced. |

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

```
Device#  show nmsp notification interval
NMSP Notification Intervals
---------------------------

RSSI Interval:
 Client               : 2 sec
 RFID                 : 2 sec
 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 3.2SE | This command was introduced. |

**Usage Guidelines** If you did not reload the switch after entering the **sdm prefer** global configuration command, the **show sdm prefer** privileged EXEC command displays the template currently in use and not the newly configured template.

The numbers displayed for each template represent an approximate maximum number for each feature resource. The actual number might vary, depending on the actual number of other features configured. For example,

in the default template if your device had more than 16 routed interfaces (subnet VLANs), the number of possible unicast MAC addresses might be less than 6000.

### Example

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

```
Device# show sdm prefer

Showing SDM Template Info

This is the Advanced template.
 Number of VLANs:                                4094
 Unicast MAC addresses:                          32768
 Overflow Unicast MAC addresses:                 512
 IGMP and Multicast groups:                      8192
 Overflow IGMP and Multicast groups:             512
 Directly connected routes:                      32768
 Indirect routes:                                7680
 Security Access Control Entries:                3072
 QoS Access Control Entries:                     3072
 Policy Based Routing ACEs:                      1024
 Netflow ACEs:                                   1024
 Input Microflow policer ACEs:                   256
 Output Microflow policer ACEs:                  256
 Flow SPAN ACEs:                                 256
 Tunnels:                                        256
 Control Plane Entries:                          512
 Input Netflow flows:                            8192
 Output Netflow flows:                          16384
 SGT/DGT entries:                                4096
 SGT/DGT Overflow entries:                       512
These numbers are typical for L2 and IPv4 features.
Some features such as IPv6, use up double the entry size;
so only half as many entries can be created.

Device#
```

### Related Topics

sdm prefer, on page 59

# 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 3.2SE | This command was introduced. |

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

```
Device# 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 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 3.2SE | This command was introduced. |

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

```
Device# 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 device, 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 3.2SE | This command was introduced. |

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

```
device# 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 3.2SE | This command was introduced. |

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

```
Device# 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 3.2SE | This command was introduced. |

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

```
Device# 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 3.2SE | This command was introduced. |

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

```
Device# 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 3.2SE | 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).

```
Device# 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 3.2SE | This command was introduced. |

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

```
Device# 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** | **rssi** | **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. |
| **rssi** | 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 3.2SE | This command was introduced. |

**Usage Guidelines**

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

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

```
Device# 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 3.2SE | This command was introduced. |

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

```
Device# 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         :                           1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
 Channels        : 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 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 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
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
 US (-A   ,-AB  ): * * * * * * * * * * * * * * * * * * * * A * * * * * A
 Auto-RF         : . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
```

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

```
Device# 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:

```
Device# 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  .
 (-E   ,-E   )  AL  :  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  .  .  .
(-E   ,-E   )  AT  :  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  .  .  .
(-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  .  .  .
(-A   ,-AR  )  BR  :  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  .  .  .
(-A   ,-ABN )  CA2 :  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  .
(-AER ,-AR  )  CL  :  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  .
(-CE  ,-CE  )  CN  :  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  .  .  .
(-A   ,-AB  )  CR  :  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  .
(-E   ,-E   )  CZ  :  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  .
(-E   ,-E   )  DK  :  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  .  .  .
(-E   ,-    )  DZ  :  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  .  .  .
(-E   ,-E   )  EE  :  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  .
(-E   ,-E   )  ES  :  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  .
(-E   ,-E   )  FR  :  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  .
(-E   ,-E   )  GI  :  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  .
(-A   ,-NA  )  HK  :  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  .
(-E   ,-E   )  HU  :  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  .
(-E   ,-E   )  IE  :  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  .
(-I   ,-I   )  ILO :   .  .  .  . 20 20 20 20 20 20 20 20 20  .
(-A   ,-AN  )  IN  :  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  .
(-E   ,-E   )  IS  :  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  .
(-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  .
(-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  .
(-E   ,-E   )  KN  :  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  .
(-E   ,-E   )  KW  :  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  .
(-E   ,-E   )  LB  :  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  .
(-E   ,     )  LK  :  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  .
(-E   ,-E   )  LU  :  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  .
(-E   ,-E   )  MC  :  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  .
(-E   ,-E   )  MK  :  20 20 20 20 20 20 20 20 20 20 20 20 20  .
(-E   ,     )  MO  :  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  .
(-A   ,-NA  )  MX  :  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  .
(-E   ,-E   )  NL  :  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  .
(-A   ,-NA  )  NZ  :  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  .
(-A   ,-AR  )  PA  :  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  .  .  .
(-A   ,-ABN )  PH  :  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  .  .  .
(-E   ,-E   )  PK  :  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  .
(-A   ,-A   )  PR  :  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  .
(-A   ,-A   )  PY  :  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  .
(-E   ,-E   )  RO  :  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  .
(-AER ,-ER  )  RU  :  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  .
(-E   ,-E   )  SE  :  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  .
(-E   ,-E   )  SK  :  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  .
(-E   ,-E   )  TN  :  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  .
(-A   ,-ANT )  TW  :  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  .
(-A   ,-AB  )  US  :  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  .  .  .
(-A   ,-AB  )  USL :  27 27 27 27 27 27 27 27 27 27 27  .  .  .
(-A   ,-    )  USX :  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  .  .  .
(-A   ,-AR  )  VE  :  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  .
(-E   ,-E   )  ZA  :  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 3.2SE | This command was introduced. |

**Usage Guidelines**

The following parameters are displayed:

- The wireless user idle timeout
- The controller configured RF group name
- Fast SSID change

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

```
Device# 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 3.2SE | This command was introduced. |

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

```
Device# 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**

| | |
|---|---|
| *channel-id* | 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. |

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

```
Device# 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**

| | |
|---|---|
| *channel-id* | 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. |

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

```
Device# 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 3.2SE | This command was introduced. |

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 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 3.2SE | This command was introduced. |

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

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

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

```
Device# 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 3.2SE | This command was introduced. |

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

```
Device# 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 3.2SE | This command was introduced. |

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

```
Device# 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 3.2SE | This command was introduced. |

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

```
Device# 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 3.2SE | This command was introduced. |

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

```
Device# 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
```

# 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** *vlan-id* | VLAN ID of VLAN to shutdown. |

**Command Default**

No default behavior or values.

**Command Modes**

Global configuration

**Command History**

| Release | Modification |
|---|---|
| Cisco IOS XE 3.2SE | This command was introduced. |

### Examples

This example shows how to shutdown a VLAN:

```
Device(config)# vlan open1
Device(config-wlan)# shutdown
```

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

```
Device# configure terminal
Device(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 7: Default Values for the Temperature Thresholds*

| Device | Difference between Yellow and Red | Red[1] |
|---|---|---|
| Catalyst 3850 | 14°C | 60°C |

[1] You cannot configure the red temperature threshold.

**Command Modes**

Global configuration

**Command History**

| Release | Modification |
|---|---|
| Cisco IOS XE 3.2SE | This command was introduced. |

**Usage Guidelines**

You cannot configure the green and red thresholds but can configure the yellow threshold. Use the **system env temperature threshold yellow** *value* global configuration command to specify the difference between the yellow and red thresholds and to configure the yellow threshold. For example, if the red threshold is 66 degrees C and you want to configure the yellow threshold as 51 degrees C, set the difference between the thresholds as 15 by using the **system env temperature threshold yellow 15** command. For example, if the red threshold is 60 degrees C and you want to configure the yellow threshold as 51 degrees C, set the difference between the thresholds as 15 by using the **system env temperature threshold yellow 9** command.

**Note** The internal temperature sensor in the device measures the internal system temperature and might vary ±5 degrees C.

**Examples**

This example sets 15 as the difference between the yellow and red thresholds:

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

# test cable-diagnostics tdr

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

**test cable-diagnostics tdr interface** *interface-id*

**Syntax Description**

| | |
|---|---|
| *interface-id* | The interface on which to run TDR. |

**Command Default**

No default behavior or values.

**Command Modes**

Privileged EXEC

**Command History**

| Release | Modification |
|---|---|
| Cisco IOS XE 3.2SE | This command was introduced. |

**Usage Guidelines**

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

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

This example shows how to run TDR on an interface:

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

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

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

**Related Topics**

show cable-diagnostics tdr, on page 64

# traceroute mac

To display the Layer 2 path taken by the packets from the specified source MAC address to the specified destination MAC address, use the **traceroute mac** command in privileged EXEC mode.

**traceroute mac** [**interface** *interface-id*] *source-mac-address* [**interface** *interface-id*] *destination-mac-address* [**vlan** *vlan-id*] [**detail**]

**Syntax Description**

| | |
|---|---|
| **interface** *interface-id* | (Optional) Specifies an interface on the source or destination device. |
| *source-mac-address* | The MAC address of the source device in hexadecimal format. |
| *destination-mac-address* | The MAC address of the destination device in hexadecimal format. |
| **vlan** *vlan-id* | (Optional) Specifies the VLAN on which to trace the Layer 2 path that the packets take from the source device to the destination device. Valid VLAN IDs are 1 to 4094. |
| **detail** | (Optional) Specifies that detailed information appears. |

**Command Default** No default behavior or values.

**Command Modes** Privileged EXEC

**Command History**

| Release | Modification |
|---|---|
| Cisco IOS XE 3.2SE | This command was introduced. |

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

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

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

Layer 2 traceroute supports only unicast traffic. If you specify a multicast source or destination MAC address, the physical path is not identified, and an error message appears.

The **traceroute mac** command output shows the Layer 2 path when the specified source and destination addresses belong to the same VLAN.

If you specify source and destination addresses that belong to different VLANs, the Layer 2 path is not identified, and an error message appears.

If the source or destination MAC address belongs to multiple VLANs, you must specify the VLAN to which both the source and destination MAC addresses belong.

If the VLAN is not specified, the path is not identified, and an error message appears.

The Layer 2 traceroute feature is not supported when multiple devices are attached to one port through hubs (for example, multiple CDP neighbors are detected on a port).

When more than one CDP neighbor is detected on a port, the Layer 2 path is not identified, and an error message appears.

This feature is not supported in Token Ring VLANs.

### Examples

This example shows how to display the Layer 2 path by specifying the source and destination MAC addresses:

```
Device# traceroute mac 0000.0201.0601 0000.0201.0201
  Source 0000.0201.0601 found on con6[WS-C3750E-24PD] (2.2.6.6)
  con6 (2.2.6.6) :Gi0/0/1 => Gi0/0/3
  con5                (2.2.5.5        )  :    Gi0/0/3 => Gi0/0/1
  con1                (2.2.1.1        )  :    Gi0/0/1 => Gi0/0/2
  con2                (2.2.2.2        )  :    Gi0/0/2 => Gi0/0/1
  Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
  Layer 2 trace completed
```

This example shows how to display the Layer 2 path by using the **detail** keyword:

```
Device# traceroute mac 0000.0201.0601 0000.0201.0201 detail
```

```
  Source 0000.0201.0601 found on con6[WS-C3750E-24PD] (2.2.6.6)
  con6 / WS-C3750E-24PD / 2.2.6.6 :
         Gi0/0/2 [auto, auto] => Gi0/0/3 [auto, auto]
  con5 / WS-C2950G-24-EI / 2.2.5.5 :
         Fa0/3 [auto, auto] => Gi0/1 [auto, auto]
  con1 / WS-C3550-12G / 2.2.1.1 :
         Gi0/1 [auto, auto] => Gi0/2 [auto, auto]
  con2 / WS-C3550-24 / 2.2.2.2 :
         Gi0/2 [auto, auto] => Fa0/1 [auto, auto]
  Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
  Layer 2 trace completed.
```

This example shows how to display the Layer 2 path by specifying the interfaces on the source and destination devicees:

```
Device# traceroute mac interface fastethernet0/1 0000.0201.0601 interface fastethernet0/3
0000.0201.0201
  Source 0000.0201.0601 found on con6[WS-C3750E-24PD] (2.2.6.6)
  con6 (2.2.6.6) :Gi0/0/1 => Gi0/0/3
  con5                 (2.2.5.5        )  :    Gi0/0/3 => Gi0/0/1
  con1                 (2.2.1.1        )  :    Gi0/0/1 => Gi0/0/2
  con2                 (2.2.2.2        )  :    Gi0/0/2 => Gi0/0/1
  Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
  Layer 2 trace completed
```

This example shows the Layer 2 path when the device is not connected to the source device:

```
Device# traceroute mac 0000.0201.0501 0000.0201.0201 detail
  Source not directly connected, tracing source .....
  Source 0000.0201.0501 found on con5[WS-C3750E-24TD] (2.2.5.5)
  con5 / WS-C3750E-24TD / 2.2.5.5 :
         Gi0/0/1 [auto, auto] => Gi0/0/3 [auto, auto]
  con1 / WS-C3550-12G / 2.2.1.1 :
         Gi0/1 [auto, auto] => Gi0/2 [auto, auto]
  con2 / WS-C3550-24 / 2.2.2.2 :
         Gi0/2 [auto, auto] => Fa0/1 [auto, auto]
  Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
  Layer 2 trace completed.
```

This example shows the Layer 2 path when the device cannot find the destination port for the source MAC address:

```
Device# traceroute mac 0000.0011.1111 0000.0201.0201
  Error:Source Mac address not found.
  Layer2 trace aborted.
```

This example shows the Layer 2 path when the source and destination devices are in different VLANs:

```
Device# traceroute mac 0000.0201.0601 0000.0301.0201
  Error:Source and destination macs are on different vlans.
  Layer2 trace aborted.
```

This example shows the Layer 2 path when the destination MAC address is a multicast address:

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

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

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

### Related Topics

traceroute mac ip, on page 107

# traceroute mac ip

To display the Layer 2 path taken by the packets from the specified source IP address or hostname to the specified destination IP address or hostname, use the **traceroute mac ip** command in privileged EXEC mode.

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

### Syntax Description

| | |
|---|---|
| *source-ip-address* | The IP address of the source device as a 32-bit quantity in dotted-decimal format. |
| *source-hostname* | The IP hostname of the source device. |
| *destination-ip-address* | The IP address of the destination device as a 32-bit quantity in dotted-decimal format. |
| *destination-hostname* | The IP hostname of the destination device. |
| **detail** | (Optional) Specifies that detailed information appears. |

### Command Default

No default behavior or values.

### Command Modes

Privileged EXEC

### Command History

| Release | Modification |
|---|---|
| Cisco IOS XE 3.2SE | This command was introduced. |

### Usage Guidelines

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

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

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

The **traceroute mac ip** command output shows the Layer 2 path when the specified source and destination IP addresses are in the same subnet.

When you specify the IP addresses, the device uses Address Resolution Protocol (ARP) to associate the IP addresses with the corresponding MAC addresses and the VLAN IDs.

- If an ARP entry exists for the specified IP address, the device uses the associated MAC address and identifies the physical path.
- If an ARP entry does not exist, the device sends an ARP query and tries to resolve the IP address. The IP addresses must be in the same subnet. If the IP address is not resolved, the path is not identified, and an error message appears.

The Layer 2 traceroute feature is not supported when multiple devices are attached to one port through hubs (for example, multiple CDP neighbors are detected on a port).

When more than one CDP neighbor is detected on a port, the Layer 2 path is not identified, and an error message appears.

This feature is not supported in Token Ring VLANs.

## Examples

This example shows how to display the Layer 2 path by specifying the source and destination IP addresses and by using the **detail** keyword:

```
Device# traceroute mac ip 2.2.66.66 2.2.22.22 detail
Translating IP to mac .....
2.2.66.66 => 0000.0201.0601
2.2.22.22 => 0000.0201.0201

Source 0000.0201.0601 found on con6[WS-C2950G-24-EI] (2.2.6.6)
con6 / WS-C3750E-24TD / 2.2.6.6 :
        Gi0/0/1 [auto, auto] => Gi0/0/3 [auto, auto]
con5 / WS-C2950G-24-EI / 2.2.5.5 :
        Fa0/3 [auto, auto] => Gi0/1 [auto, auto]
con1 / WS-C3550-12G / 2.2.1.1 :
        Gi0/1 [auto, auto] => Gi0/2 [auto, auto]
con2 / WS-C3550-24 / 2.2.2.2 :
        Gi0/2 [auto, auto] => Fa0/1 [auto, auto]
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed.
```

This example shows how to display the Layer 2 path by specifying the source and destination hostnames:

```
Device# traceroute mac ip con6 con2
Translating IP to mac .....
2.2.66.66 => 0000.0201.0601
2.2.22.22 => 0000.0201.0201

Source 0000.0201.0601 found on con6
con6 (2.2.6.6) :Gi0/0/1 => Gi0/0/3
con5                 (2.2.5.5        )  :    Gi0/0/3 => Gi0/1
con1                 (2.2.1.1        )  :    Gi0/0/1 => Gi0/2
con2                 (2.2.2.2        )  :    Gi0/0/2 => Fa0/1
Destination 0000.0201.0201 found on con2
```

```
Layer 2 trace completed
```

This example shows the Layer 2 path when ARP cannot associate the source IP address with the corresponding MAC address:

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

### Related Topics

traceroute mac, on page 104

# 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 3.2SE | This command was introduced. |

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

```
Device# configure terminal
Device(config)# no trapflags rogueap
Device(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 3.2SE | This command was introduced. |

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

```
Device# configure terminal
Device(config)# trapflags client dot11 disassociate
Device(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**

| | |
|---|---|
| *filesystem:* | Alias for a file system. Use **flash:** for the system board flash device; use **usbflash0:** for USB memory sticks. |
| */file-url...* | Path (directory) and name of the files to display. Separate each filename with a space. |

**Command Default**

No default behavior or values.

**Command Modes**

Boot loader

**Command History**

| Release | Modification |
|---|---|
| Cisco IOS XE 3.2SE | This command was introduced. |

**Usage Guidelines**

Filenames and directory names are case sensitive.

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

**Examples**

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

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

# unset

To reset one or more environment variables, use the **unset** command in boot loader mode.

**unset** *variable...*

**Syntax Description**

| | |
|---|---|
| *variable* | Use one of these keywords for *variable*:<br>**MANUAL_BOOT**—Specifies whether the device automatically or manually boots. |
| | **BOOT**—Resets the list of executable files to try to load and execute when automatically booting. If the BOOT environment variable is not set, the system attempts to load and execute the first executable image it can find by using a recursive, depth-first search through the flash: file system. If the BOOT variable is set but the specified images cannot be loaded, the system attempts to boot the first bootable file that it can find in the flash: file system. |
| | **ENABLE_BREAK**—Specifies whether the automatic boot process can be interrupted by using the **Break** key on the console after the flash: file system has been initialized. |
| | **HELPER**—Identifies the semicolon-separated list of loadable files to dynamically load during the boot loader initialization. Helper files extend or patch the functionality of the boot loader. |
| | **PS1**—Specifies the string that is used as the command-line prompt in boot loader mode. |
| | **CONFIG_FILE**—Resets the filename that Cisco IOS uses to read and write a nonvolatile copy of the system configuration. |

**BAUD**—Resets the rate in bits per second (b/s) used for the console. The Cisco IOS software inherits the baud rate setting from the boot loader and continues to use this value unless the configuration file specifies another setting.

**Command Default**

No default behavior or values.

**Command Modes**

Boot loader

**Command History**

| Release | Modification |
|---|---|
| Cisco IOS XE 3.2SE | This command was introduced. |

**Usage Guidelines**

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

The MANUAL_BOOT environment variable can also be reset by using the **no boot manual** global configuration command.

The BOOT environment variable can also be reset by using the **no boot system** global configuration command.

The ENABLE_BREAK environment variable can also be reset by using the **no boot enable-break** global configuration command.

The HELPER environment variable can also be reset by using the **no boot helper** global configuration command.

The CONFIG_FILE environment variable can also be reset by using the **no boot config-file** global configuration command.

### Example

This example shows how to unset the SWITCH_PRIORITY environment variable:

```
Device: unset SWITCH_PRIORITY
```

### Related Topics

set, on page 60
reset, on page 57

# 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 3.2SE | This command was introduced. |

**Examples**

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

```
Device: version
CAT3K_CAA Boot Loader (CAT3K_CAA-HBOOT-M) Version 1.3, RELEASE SOFTWARE (P)
Compiled Sun Jun 16 18:31:15 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** *assoc-number* **interval** *interval* | Enables association request limit per access point slot at a given interval and configures the association request limit interval.<br>You can configure number of association request per access point slot at a given interval from one through 100.<br>You can configure client association request limit interval from 100 through 10000 milliseconds. |
| **band-select** | Configures band select options for the client. |
| **client-rssi** *rssi* | Sets the client received signal strength indicator (RSSI) threshold for band select.<br>Minimum dBm of a client RSSI to respond to probe between -90 and -20. |
| **cycle-count** *count* | Sets the band select probe cycle count.<br>You can configure the cycle count from one through 10. |
| **cycle-threshold** *threshold* | Sets the time threshold for a new scanning cycle.<br>You can configure the cycle threshold from one through 1000 milliseconds. |
| **expire dual-band** *timeout* | Sets the timeout before stopping to try to push a given client to the 5-GHz band.<br>You can configure the timeout from 10 through 300 seconds, and the default value is 60 seconds. |

| | |
|---|---|
| **expire suppression** *timeout* | Sets the expiration time for pruning previously known dual-band clients.<br>You can configure the suppression from 10 through 200 seconds, and the default timeout value is 20 seconds. |
| **max-user-login** *max-user-login* | Configures the maximum number of login sessions for a user. |
| **timers auth-timeout** *seconds* | Configures client timers. |
| **user-timeout** *user-timeout* | Configures the idle client timeout. |

**Command Default** No default behavior or values.

**Command Modes** Global configuration

**Command History**

| Release | Modification |
|---|---|
| Cisco IOS XE 3.2SE | This command was introduced. |

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

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

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

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

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

```
Device# configure terminal
Device(config)# wireless client band-select expire suppression 70
Device(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** *mac-addr* | Wireless client MAC address. |

**Command Default** No default behavior or values.

**Command Modes** Global configuration

| Command History | Release | Modification |
|---|---|---|
| | Cisco IOS XE 3.2SE | This command was introduced. |

This example shows how to disconnect a wireless client:

```
Device# configure terminal
Device(config)# wireless client mac-address 00:1f:ca:cf:b6:60 deauthenticate
Device(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 | | |
|---|---|---|
| | *mac-addr* | 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 hostname** *host-name* | 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** *measurement-duration* | Senda 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** *ssid bssid dot11 channel* | 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. |
| *profile-id* | (Optional) Test profile name. |
| *bssid* | Basic SSID. |
| *dot11* | Specifies the 802.11a, 802.11b, or 802.11g network. |
| *channel* | 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. |
| *profile-id* | Test profile name.<br>**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 3.2SE | This command was introduced. |

**Usage Guidelines**

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

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

```
Device# configure terminal
```

```
Device(config)# wireless client mac-address 00:1f:ca:cf:b6:60 ccx clear-reports
Device(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** *denial-count* | Specifies the number of association denials during load balancing.<br>Maximum number of association denials during load balancing is from 1 to 10 and the default value is 3. |
| **window** *client-count* | Specifies the aggressive load balancing client window, with the number of clients needed to trigger aggressive load balancing on a given access point.<br>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 3.2SE | 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.

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

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

| | |
|---|---|
| *callIndex* | Call index with valid values between 1 and 6. |
| *call-no* | 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 3.2SE | 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.

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

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