# System Management Commands

# archive download-sw

To download a new image from a TFTP server to the switch or switch stack and to overwrite or keep the existing image, use the **archive download-sw** command in privileged EXEC mode.

**archive download-sw** {**/directory** | **/force-reload** | **/imageonly** | **/leave-old-sw** | **/no-set-boot** | **/no-version-check** | **/overwrite** | **/reload** | **/safe**} *source-url*

## Syntax Description

| | |
|---|---|
| **/directory** | Specifies a directory for the images. |
| **/force-reload** | Unconditionally forces a system reload after successfully downloading the software image. |
| **/imageonly** | Downloads only the software image but not the HTML files associated with embedded Device Manager. The HTML files for the existing version are deleted only if the existing version is being overwritten or removed. |
| **/leave-old-sw** | Keeps the old software version after a successful download. |
| **/no-set-boot** | Stops the setting of the BOOT environment variable from being altered to point to the new software image after it is successfully downloaded. |
| **/no-version-check** | Downloads the software image without verifying its version compatibility with the image that is running on the switch. On a switch stack, downloads the software image without checking the compatibility of the stack protocol version on the image and on the stack.<br>This feature is supported only on the LAN Base image. |
| **/overwrite** | Overwrites the software image in flash memory with the downloaded image. |
| **/reload** | Reloads the system after successfully downloading the image, unless the configuration has been changed and has not saved. |
| **/safe** | Keeps the current software image. Does not delete it to make room for the new software image before the new image is downloaded. The current image is deleted after the download. |

*source-url* Specifies the source URL alias for a local or network file system. These options are supported:

- The secondary boot loader (BS1):

  **bsl:**

- The local flash: file system on the standalone switch or the active switch:

  **flash:**

- The local flash: file system on a member:

  **flash** *member number:*

- FTP:

  **ftp:** [[*//username*[**:***password*]@*location*]*/directory*]*/image-name***.tar**

- An HTTP server:

  **http:** //[[*username:password*]@]{*hostname* | *host-ip*}[*/directory*]*/image-name***.tar**

- A secure HTTP server:

  **https:** //[[*username:password*]@]{*hostname* | *host-ip*}[*/directory*]*/image-name***.tar**

- Remote Copy Protocol (RCP):

  **rcp:** [[*//username*@*location*]*/directory*]*/image-name***.tar**

- TFTP:

  **tftp:** [[*//location*]*/directory*]*/image-name***.tar**

*image-name***.tar** is the software image to download and install on the switch.

## Command Default

The current software image is not overwritten with the downloaded image. Both the software image and HTML files are downloaded. The new image is downloaded to the flash: file system.

The BOOT environment variable is changed to point to the new software image on the flash: file system. Image files are case-sensitive; the image file is provided in TAR format.

Compatibility of the stack protocol version of the image to be downloaded is checked with the version on the stack.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E | This command was introduced. |

## Usage Guidelines

The **/imageonly** option removes the HTML files for the existing image if the existing image is being removed or replaced.

Only the Cisco IOS image (without the HTML files) is downloaded.

Using the **/safe** or **/leave-old-sw** option can cause the new image download to fail if there is insufficient flash memory.

If you leave the software in place, the new image does not have enough flash memory due to space constraints, and an error message is displayed.

If you used the **/leave-old-sw** option and did not overwrite the old image when you downloaded the new one, you can remove the old image by using the **delete** privileged EXEC command.

For more information, see delete, on page 43.

If you want to download an image that has a different stack protocol version than the one existing on the stack, use the **/no-version-check** option.

**Note** This feature is supported only on the LAN Base image.

**Note** Use the **/no-version-check** option carefully. All members, including the active switch, must have the same stack protocol version to be in the same stack.

This option allows an image to be downloaded without first confirming the compatibility of its stack protocol version with the version of the stack.

Use the **/overwrite** option to overwrite the image on the flash device with the downloaded one.

If you specify the command *without* the **/overwrite** option, the download algorithm determines whether or not the new image is the same as the one on the switch flash device or is running on any stack members.

If the images are the same, the download does not occur. If the images are different, the old image is deleted, and the new one is downloaded.

After downloading a new image, enter the **/reload** privileged EXEC command to begin using the new image, or specify the **/reload** or **/force-reload** option in the **archive download-sw** command.

### Examples

This example shows how to download a new image from a TFTP server at 172.20.129.10 and to overwrite the image on the switch:

```
Device# archive download-sw /overwrite tftp://172.20.129.10/test-image.tar
```

This example shows how to download only the software image from a TFTP server at 172.20.129.10 to the switch:

```
Device# archive download-sw /imageonly tftp://172.20.129.10/test-image.tar
```

This example shows how to keep the old software version after a successful download:

```
Device# archive download-sw /leave-old-sw tftp://172.20.129.10/test-image.tar
```

```
Device# archive download-sw /imageonly /destination-system 6 /destination-system 8
tftp://172.20.129.10/test-image.tar
```

# archive tar

To create a TAR file, list files in a TAR file, or extract the files from a TAR file, use the **archive tar** command in privileged EXEC mode.

**archive tar** {**/create** *destination-url* **flash:***/file-url*} | **/table** *source-url* | {**/xtract** *source-url* **flash:***/file-url* [*dir/file...*]}

## Syntax Description

**/create** *destination-url* **flash:***/file-url*

Creates a new TAR file on the local or network file system.

*destination-url*—Specifies the destination URL alias for the local or network file system and the name of the tar file to create. These options are supported:

- The local flash file system:

  **flash:**

- FTP:

  **ftp:** [[*//username*[**:***password*]@*location*]*/directory*]*/itar-filename***.tar**

- An HTTP server:

  **http:** //[[*username:password*]@]{*hostname* | *host-ip*}[*/directory*]*/image-name***.tar**

- A secure HTTP server:

  **https:** //[[*username:password*]@]{*hostname* | *host-ip*}[*/directory*]*/image-name***.tar**

- Remote Copy Protocol (RCP):

  **rcp:** [[*//username*@*location*]*/directory*]*/tar-filename***.tar**

- TFTP:

  **tftp:** [[*//location*]*/directory*]*/image-name***.tar**

*tar-filename***.tar** is the TAR file to be created.

**flash***:/file-url*—Specifies the location on the local flash: file system from which the new tar file is created.

Optionally, you can specify the list of files list of files or directories within the source directory that you want to be written to the new TAR file. If none are specified, all files and directories at this level are written to the newly created TAR file.

**table** *source-url* Displays the contents of an existing TAR file to the screen.

*source-url*—Specifies the source URL alias for the local or network file system. These options are supported:

- The local flash: file system:

  **flash:**

- FTP:

  **ftp:** [[*//username* [ **:** *password*] @*location*] */directory*] */itar-filename***.tar**

- An HTTP server:

  **http:** //[[*username:password*] @] {*hostname* | *host-ip*} [*/directory*] */image-name***.tar**

- A secure HTTP server:

  **https:** //[[*username:password*] @] {*hostname* | *host-ip*} [*/directory*] */image-name***.tar**

- Remote Copy Protocol (RCP):

  **rcp:** [[*//username*@*location*] */directory*] */tar-filename***.tar**

- TFTP:

  **tftp:** [[*//location*] */directory*] */image-name***.tar**

*tar-filename***.tar** is the TAR file to be displayed.

| | |
|---|---|
| **/xtract** *source-url* **flash:***/file-url* [ *dir/file* **. . .** ] | Extracts files from a TAR file to the local file system.<br>*source-url*—Specifies the source URL alias for the local file system. These options are supported:<br>• The local flash: file system:<br>**flash:**<br>• FTP:<br>**ftp:** [[*//username* [ **:** *password* ] @ *location* ] */directory* ] */itar-filename***.tar**<br>• An HTTP server:<br>**http:** //[[*username:password* ] @ ] { *hostname* \| *host-ip* } [ */directory* ] */image-name***.tar**<br>• A secure HTTP server:<br>**https:** //[[*username:password* ] @ ] { *hostname* \| *host-ip* } [ */directory* ] */image-name***.tar**<br>• Remote Copy Protocol (RCP):<br>**rcp:** [[*//username@location* ] */directory* ] */tar-filename***.tar**<br>• TFTP:<br>**tftp:** [[*//location* ] */directory* ] */image-name***.tar**<br>*tar-filename***.tar** is the TAR file from which to extract.<br>**flash***:/file-url* [ *dir/file* **. . .** ]—Specifies the location on the local flash: file system from which the new TAR file is extracted. Use the *dir/file...* option to specify an optional list of files or directories within the TAR file to be extracted. If none are specified, all files and directories are extracted. |

**Command Modes**

Privileged EXEC

**Command History**

| Release | Modification |
|---|---|
| Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E | This command was introduced. |

**Usage Guidelines**

Filenames and directory names are case sensitive.

Image names are case sensitive.

### Examples

This example shows how to create a TAR file. The command writes the contents of the *new-configs* directory on the local flash: file device to a file named *saved.tar* on the TFTP server at 172.20.10.30:

```
Device# archive tar /create tftp:172.20.10.30/saved.tar flash:/new_configs
```

This example shows how to display the contents of the file that is in flash memory. The contents of the TAR file appear on the screen:

```
Device# archive tar /table flash:c2960-lanbase-tar.12-25.FX.tar
info (219 bytes)
(directory)
(610856 bytes)
 info (219 bytes)
info.ver (219 bytes)
```

This example shows how to display only the /html directory and its contents:

```
flash:2960-lanbase-mz.12-25.FX.tar 2960-lanbase-mz.12-25.FX/html
 (directory)
 (556 bytes)
 (9373 bytes)
 (1654 bytes)
<output truncated>
```

This example shows how to extract the contents of a TAR file on the TFTP server at 172.20.10.30. This command extracts just the new-configs directory into the root directory on the local flash: file system. The remaining files in the saved.tar file are not extracted.

```
Device# archive tar /xtract tftp://172.20.10.30/saved.tar flash:/new-configs
```

# archive upload-sw

To upload an existing image to the server, use the **archive upload-sw** privileged EXEC command.

**archive upload-sw** [**/version** *version_string* ] *destination-url*

## Syntax Description

| | |
|---|---|
| **/version** *version_string* | (Optional) Specifies the specific version string of the image to be uploaded. |
| *destination-url* | The destination URL alias for a local or network file system. These options are supported:<br>• The local flash: file system on the standalone switch or the active switch:<br>**flash:**<br>• The local flash: file system on a member:<br>**flash** *member number:*<br>• FTP:<br>**ftp:** [[*//username* [ **:** *password* ] **@** *location* ] */directory* ] */image-name***.tar**<br>• An HTTP server:<br>**http:** //[[*username:password* ] **@** ] { *hostname* \| *host-ip* } [ */directory* ] */image-name***.tar**<br>• A secure HTTP server:<br>**https:** //[[*username:password* ] **@** ] { *hostname* \| *host-ip* } [ */directory* ] */image-name***.tar**<br>• Secure Copy Protocol (SCP):<br>**scp:** [[*//username***@***location* ] */directory* ] */image-name***.tar**<br>• Remote Copy Protocol (RCP):<br>**rcp:** [[*//username***@***location* ] */directory* ] */image-name***.tar**<br>• TFTP:<br>**tftp:** [[*//location* ] */directory* ] */image-name***.tar**<br>*image-name***.tar** is the name of the software image to be stored on the server. |

## Command Default

Uploads the currently running image from the flash: file system.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E | This command was introduced. |

## Usage Guidelines

Use the upload feature only if the HTML files associated with embedded Device Manager have been installed with the existing image.

The files are uploaded in this sequence: the Cisco IOS image, the HTML files, and info. After these files are uploaded, the software creates the TAR file.

Image names are case sensitive.

### Examples

This example shows how to upload the currently running image on member switch 3 to a TFTP server at 172.20.140.2:

```
Switch# archive upload-sw /source-system-num 3tftp://172.20.140.2/test-image.tar
```

# avc dns-as client

To enable Application Visibility Control (AVC) with Domain Name System as an Authoritative Source (DNS-AS) feature (AVC with DNS-AS) on the switch (DNS-AS client) and maintain a list of trusted domains, enter the **avc dns-as client** in global configuration mode

**avc dns-as client** [**enable** | **trusted-domains** [**domain***domain-name*] ]
**no avc dns-as client** [**enable** | **trusted-domains** [**domain***domain-name*] ] ]

## Syntax Description

| | |
|---|---|
| **enable** | Enables AVC with DNS-AS on the DNS-AS client. |
| **trusted-domains** [**domain***domain-name*] | Enter the domain name you would like to add to the list of trusted domains for the DNS-AS client. All remaining domains are ignored and will follow default forwarding behavior.<br>You can enter up to 50 domains.<br>You can use regular expressions to match the domain name. |

## Command Default

AVC with DNS-AS is disabled.

## Command Modes

Global configuration mode

Trusted domain configuration mode

## Command History

| Release | Modification |
|---|---|
| Cisco IOS Release 15.2(5)E1 | This command was introduced. |

## Usage Guidelines

When you use regular expressions to match a domain name, for example, to represent all the domains for an organization, if you enter:

```
Device(config-trusted-domains)# domain *.example.*
```

The DNS-AS client matches www.example.com, ftp.example.org and any other domain that pertains to the organization “example”. Use such an entry in the trusted domain list carefully, because it increases the size of the binding table considerably. Entries in the trusted domain list affect the binding table, because the table serves as a database of parsed DNS server responses, which (among other things) contains the domain name and IP address information.

### Example

The following example shows how to enable AVC with DNS-AS:

```
Device# configure terminal
Device(config)# avc dns-as client enable
```

The following example shows how to make entries in the trusted domain list:

```
Device# configure terminal
Device(config)# trusted-domains
```

```
Device(config-trusted-domains)#  domain www.example.com
Device(config-trusted-domains)#  domain example.com
Device(config-trusted-domains)#  domain www.example.net
Device(config-trusted-domains)#  domain example.net
Device(config-trusted-domains)#  domain www.example.org
Device(config-trusted-domains)#  domain example.org
```

## Related Commands

| Command | Description |
|---|---|
| show avc dns-as client, on page 79 | Displays the various AVC with DNS-AS settings you have configured. |

# show logging smartlog

To display smart logging information, use the **show logging smartlog** command in privileged EXEC mode.

**show logging smartlog** [**event-ids | events | statistics** {**interface** *interface-id* **| summary**}]

## Syntax Description

| | |
|---|---|
| **event-ids** | (Optional) Displays the IDs and names of smart log events. The NetFlow collector uses the event IDs to identify each event. |
| **events** | (Optional) Displays descriptions of smart log events. The display shows the last 10 smart logging events. |
| **statistics** | (Optional) Displays smart log statistics. |
| **interface** *interface-id* | (Optional) Displays smart log statistics for the specified interface. |
| **summary** | (Optional) Displays a summary of the smart log event statistics. |

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E | This command was introduced. |

## Usage Guidelines

You can configure smart logging of packets dropped because of DHCP snooping violations, Dynamic ARP inspection violations, IP source guard denied traffic, or ACL permitted or denied traffic. The packet contents are sent to the identified Cisco IOS NetFlow collector.

The statistics counters reflect the number of packets that have been sent to the collector by smart logging.

### Examples

This example shows output from the **show logging smartlog event-ids** command:

```
Switch# show logging smartlog event-ids
EventID: 1   Description: DHCPSNP
Extended Events:
-----------------------------------
 ID |  Description
-----------------------------------
 1  |  DHCPSNP_DENY_INVALID_MSGTYPE
 2  |  DHCPSNP_DENY_INVALID_PKTLEN
 3  |  DHCPSNP_DENY_INVALID_BIND
 4  |  DHCPSNP_DENY_INVALID_OPT
 5  |  DHCPSNP_DENY_OPT82_DISALLOW
 6  |  DHCPSNP_DENY_SRCMAC_MSMTCH

EventID: 2 Description: DAI
Extended Events:
-----------------------------------
```

```
 ID |  Description
------------------------------------
 1  |  DAI_DENY_INVALID_BIND
 2  |  DAI_DENY_INVALID_SRCMAC
 3  |  DAI_DENY_INVALID_IP
 4  |  DAI_DENY_ACL
 5  |  DAI_DENY_INVALID_PKT
 6  |  DAI_DENY_INVALID_DSTMAC

EventID: 3 Description: IPSG
Extended Events:
------------------------------------
 ID |  Description
------------------------------------
 1  |  IPSG_DENY

EventID: 4 Description: ACL
Extended Events:
------------------------------------
 ID |  Description
------------------------------------
 1  |  PACL_PERMIT
 2  |  PACL_DENY
```

This example shows output from the **show logging smartlog statistics interface** command:

```
Switch# show logging smartlog statistics interface gigabitethernet1/0

Total number of DHCP Snooping logged packets: 0
 DHCPSNP_DENY_INVALID_MSGTYPE: 0

 DHCPSNP_DENY_INVALID_PKTLEN: 0

 DHCPSNP_DENY_INVALID_BIND: 0

 DHCPSNP_DENY_INVALID_OPT: 0

 DHCPSNP_DENY_OPT82_DISALLOW: 0

 DHCPSNP_DENY_SRCMAC_MSMTCH: 0

Total number of Dynamic ARP Inspection logged packets: 0
 DAI_DENY_INVALID_BIND: 0

 DAI_DENY_INVALID_SRCMAC: 0

 DAI_DENY_INVALID_IP: 0

 DAI_DENY_ACL: 0

 DAI_DENY_INVALID_PKT: 0

 DAI_DENY_INVALID_DSTMAC: 0

Total number of IP Source Guard logged packets: 793
 IPSG_DENY: 793

Total number of ACL logged packets: 10135

 PACL_PERMIT: 10135

 PACL_DENY: 0
```

# boot

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

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

## Syntax Description

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

## Command Default

No default behavior or values.

## Command Modes

Boot loader

## Command History

| Release | Modification |
|---|---|
| Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E | This command was introduced. |

## Usage Guidelines

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

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

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

These settings are not saved for the next boot operation.

Filenames and directory names are case sensitive.

### Example

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

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

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

# boot buffersize

To configure the NVRAM buffer size, use the **boot buffersize** global configuration command.

**boot buffersize** *size*

**Syntax Description**

| | |
|---|---|
| *size* | The NVRAM buffer size in KB. The valid range is from 4096 to 1048576. |

**Command Default**

The default NVRAM buffer size is 512 KB.

**Command Modes**

Global configuration

**Command History**

| Release | Modification |
|---|---|
| Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E | This command was introduced. |

**Usage Guidelines**

After you configure the NVRAM buffer size, reload the switch or switch stack.

When you add a switch to a stack and the NVRAM size differs, the new switch synchronizes with the stack and reloads automatically.

### Example

The following example sets the buffer size to 524288 KB:

```
Switch(config)# boot buffersize 524288
```

# boot enable-break

To enable the interruption of the automatic boot process on a standalone switch, use the **boot enable-break** global configuration command. Use the **no** form of this command to return to the default setting.

**boot enable-break**
**no boot enable-break**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Disabled. The automatic boot process cannot be interrupted by pressing the **Break** key on the console.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E | This command was introduced. |

## Usage Guidelines

This command works properly only from a standalone switch. When you enter this command, you can interrupt the automatic boot process by pressing the **Break** key on the console after the flash: file system is initialized.

**Note** Despite setting this command, you can interrupt the automatic boot process at any time by pressing the MODE button on the switch front panel.

This command changes the setting of the ENABLE_BREAK environment variable.

# boot host dhcp

To configure the switch to download files from a DHCP server, use the **boot host dhcp** global configuration command.

**boot host dhcp**

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

**Command Default** None

**Command Modes** Global configuration

**Command History**

| Release | Modification |
|---|---|
| Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E | This command was introduced. |

### Example

This example uses the **boot host dhcp** command to enable auto-configuration with a saved configuration.

```
Switch(config)# boot host dhcp
```

# boot host retry timeout

To set the amount of time for which the system tries to download a configuration file, use the **boot host retry timeout** global configuration command.

**boot host retry timeout** *timeout-value*

## Syntax Description

| | |
|---|---|
| *timeout-value* | The length of time before the system times out, after trying to download a configuration file. |

## Command Default

There is no default. If you do not set a timeout, the system indefinitely tries to obtain an IP address from the DHCP server.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E | This command was introduced. |

### Example

This example sets the timeout to 300 seconds:

```
Switch(config)# boot host retry timeout 300
```

# boot manual

To enable the ability to manually boot a standalone switch during the next boot cycle, use the **boot manual** global configuration command. Use the **no** form of this command to return to the default setting.

**boot manual**
**no boot manual**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Manual booting is disabled.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E | This command was introduced. |

## Usage Guidelines

This command works properly only from a standalone switch.

The next time you reboot the system, the switch is in boot loader mode, which is shown by the *switch:* prompt. To boot up the system, use the **boot** boot loader command, and specify the name of the bootable image.

This command changes the setting of the MANUAL_BOOT environment variable.

# boot system

To specify the name of the configuration file that is used as a boot image, use the **boot system** global configuration command.

**boot system** *filename* [**switch** {*switch number* | **all**}]

## Syntax Description

| | |
|---|---|
| *filename* | The name of the boot image configuration file. |
| **switch** | (Optional) Sets the system image for switches in the stack. |
| *switch number* | The switch number. |
| **all** | Sets the system image for all switches in the stack. |

## Command Default

None

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E | This command was introduced. |

### Example

The following example specifies the name of the boot image configuration file as *config-boot.text*:

```
Switch(config)# boot system config-boot.text
```

# 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 Release 15.0(2)EXCisco IOS Release 15.2(5)E | 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 logging onboard

To clear all of the on-board failure logging (OBFL) data, use the **clear logging onboard** privileged EXEC command on the switch stack or on a standalone switch. The command clears all of the OBFL data except for the uptime and CLI-command information stored in the flash memory.

**clear logging onboard** [ **module** {*switch-number* | **all**} ]

**Note** This command is supported only on the LAN Base image.

## Syntax Description

| | |
|---|---|
| **module** | (Optional) Clears OBFL data on specified switches in the stack. |
| *switch-number* | The identity of the specified switch. The range is from 1 to 4. |
| **all** | (Optional) Clears OBFL data on all switches in the stack. |

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E | This command was introduced. |

## Usage Guidelines

We recommend that you keep OBFL enabled and do not erase the data stored in the flash memory.

### Example

This example shows how to clear all the OBFL information except for the uptime and CLI-command information:

```
Switch# clear logging onboard
Clear logging onboard buffer [confirm]
```

You can verify that the information is deleted by entering the **show logging onboard** privileged EXEC command.

# clear mac address-table

To delete a specific dynamic address, all dynamic addresses on a particular interface, all dynamic addresses on stack members,

or all dynamic addresses on a particular VLAN from the MAC address table, use the **clear mac address-table** privileged EXEC command.

This command also clears the MAC address notification global counters.

**clear mac address-table** {**dynamic** [**address** *mac-addr* | **interface** *interface-id* | **vlan** *vlan-id* ] | **notification**}

**Note** This command is supported only on the LAN Base image.

## Syntax Description

| | |
|---|---|
| **dynamic** | Deletes all dynamic MAC addresses. |
| **address** *mac-addr* | (Optional) Deletes the specified dynamic MAC address. |
| **interface** *interface-id* | (Optional) Deletes all dynamic MAC addresses on the specified physical port or port channel. |
| **vlan** *vlan-id* | (Optional) Deletes all dynamic MAC addresses for the specified VLAN. The range is 1 to 4094. |
| **notification** | Clears the notifications in the history table and reset the counters. |

## Command Default

No default is defined.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E | This command was introduced. |

This example shows how to remove a specific MAC address from the dynamic address table:

```
Switch# clear mac address-table dynamic address 0008.0070.0007
```

You can verify that the information is deleted by entering the **show mac address-table** privileged EXEC command.

# clear mac address-table move update

To clear the mac address-table-move update-related counters, use the **clear mac address-table move update** privileged EXEC command.

**clear mac address-table move update**

## Syntax Description

This command has no arguments or keywords.

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E | This command was introduced. |

### Example

This example shows how to clear the **mac address-table move** update-related counters.

```
Switch# clear mac address-table move update
```

You can verify that the information is cleared by entering the **show mac address-table move update** privileged EXEC command.

# 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 Release 15.0(2)EXCisco IOS Release 15.2(5)E | 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
```

# cluster commander-address

To specify the cluster command MAC address on a cluster member switch when the member has lost communication with the cluster command switch, use the

**cluster commander-address** global configuration command. Use the **no** form of this global configuration command from the

cluster member switch console port to remove the switch from a cluster only during debugging or recovery procedures.

**cluster commander-address** *mac-address* [**member** *number* | **name** *name*]
**no cluster commander-address**

## Syntax Description

| | |
|---|---|
| *mac-address* | The MAC address of the cluster command switch. |
| **member** *number* | (Optional) Specifies the number of a configured cluster member switch. The range is 0 to 15. |
| **name** *name* | (Optional) Specifies the name of the configured cluster up to 31 characters. |

## Command Default

The switch is not a member of any cluster.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E | This command was introduced. |

## Usage Guidelines

This command is available only on the cluster command switch. The cluster command switch automatically provides its MAC address to cluster member switches when these switches join the

cluster. The cluster member switch adds this information and other cluster information to its running configuration file.

A cluster member can have only one cluster command switch.

The cluster member switch retains the identity of the cluster command switch during a system reload by using the *mac-address* parameter.

You can enter the **no** form on a cluster member switch to remove it from the cluster during debugging or recovery procedures. You usually use this command from

the cluster member switch console port only when the member has lost communication with the cluster command switch. With a typical switch configuration, we recommend that you remove

cluster member switches only by entering the **no cluster member** *n* global configuration command on the cluster command switch.

When a standby cluster command switch becomes active (becomes the cluster command switch), it removes the cluster commander address line from its configuration.

### Example

The following example shows partial output from the running configuration of a cluster member:

```
Switch(config)# show running-configuration
<output truncated>
cluster commander-address 00e0.9bc0.a500 member 4 name my_cluster
<output truncated>
```

This example shows how to remove a member from the cluster by using the cluster member console:

```
Switch # configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# no cluster commander-address
```

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

# cluster discovery hop-count

To set the hop-count limit for extended discovery of candidate switches, use the **cluster discovery hop-count** global configuration command on the cluster command switch. Use the **no** form of this command to return to the default setting.

**cluster discovery hop-count** *number*
**no cluster discovery hop-count**

## Syntax Description

| | |
|---|---|
| *number* | The number of hops from the cluster edge that the cluster command switch limits the discovery of candidates. The range is 1 to 7. |

## Command Default

The default hop count is 3.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E | This command was introduced. |

## Usage Guidelines

This command is available only on the cluster command switch. This command does not operate on cluster member switches.

If the hop count is set to 1, extended discovery is disabled. The cluster command switch discovers only candidates that are one hop from the edge of the cluster. The edge of the cluster is the point between the last discovered cluster member switch and the first discovered candidate switch.

### Example

This example shows how to set hop count limit to 4. This command is executed on the cluster command switch:

```
Switch(config)# cluster discovery hop-count 4
```

You can verify your setting by entering the **show cluster** privileged EXEC command.

# cluster enable

To enable a command-capable switch as the cluster command switch, assign a cluster name, and optionally assign a member number to it, use the

**cluster enable** global configuration command. Use the **no** form of the command to remove all members and to

make the cluster command switch a candidate switch.

**cluster enable** *name* [*command-switch-member-number*]
**no cluster enable**

## Syntax Description

| | |
|---|---|
| *name* | The name of the cluster up to 31 characters. Valid characters include only alphanumerics, dashes, and underscores. |
| *command-switch-member-number* | (Optional) A member number that is assigned to the cluster command switch of the cluster. The range is 0 to 15. |

## Command Default

The switch is not a cluster command switch.

No cluster name is defined.

The member number is 0 when the switch is the cluster command switch.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E | This command was introduced. |

## Usage Guidelines

Enter this command on any command-capable switch that is not part of any cluster. This command fails if a device is already configured as a member of the cluster.

You must name the cluster when you enable the cluster command switch. If the switch is already configured as the cluster command switch, this command changes the

cluster name if it is different from the previous cluster name.

### Example

This example shows how to enable the cluster command switch, name the cluster, and set the cluster command switch member number to 4:

```
Switch(config)# cluster enable Engineering-IDF4 4
```

You can verify your setting by entering the **show cluster** privileged EXEC command on the cluster command switch.

# cluster holdtime

To set the duration in seconds before a switch (either the command or cluster member switch) declares the other switch down after not receiving heartbeat messages,

use the **cluster holdtime** global configuration command on the cluster command switch. Use the **no** form of this command

to set the duration to the default value.

**cluster holdtime** *holdtime-in-secs*
**no cluster holdtime**

## Syntax Description

| | |
|---|---|
| *holdtime-in-secs* | Duration in seconds before a switch (either a command or cluster member switch) declares the other switch down. The range is 1 to 300 seconds. |

## Command Default

The default holdtime is 80 seconds.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E | This command was introduced. |

## Usage Guidelines

Enter this command with the **cluster timer** global configuration command only on the cluster command switch. The cluster command switch propagates the

values to all its cluster members so that the setting is consistent among all switches in the cluster.

The holdtime is typically set as a multiple of the interval timer (cluster timer). For example, it takes (holdtime-in-secs divided by the interval-in-secs) number of

heartbeat messages to be missed in a row to declare a switch down.

### Example

This example shows how to change the interval timer and the duration on the cluster command switch:

```
Switch(config)# cluster timer 3
Switch(config)# cluster holdtime 30
```

You can verify your settings by entering the show cluster privileged EXEC command.

# cluster member

To add candidates to a cluster, use the **cluster member** global configuration command on the cluster command switch.

Use the **no** form of the command to remove members from the cluster.

**cluster member** [*n*] **mac-address** *H.H.H* [**password** *enable-password*] [**vlan** *vlan-id*]
**no cluster member** *n*

## Syntax Description

| | |
|---|---|
| *n* | (Optional) The number that identifies a cluster member. The range is 0 to 15. |
| **mac-address** *H.H.H* | Specifies the MAC address of the cluster member switch in hexadecimal format. |
| **password** *enable-password* | (Optional) Enables the password of the candidate switch. The password is not required if there is no password on the candidate switch. |
| **vlan** *vlan-id* | (Optional) Specifies the ID of the VLAN through which the candidate is added to the cluster by the cluster command switch. The range is 1 to 4094. |

## Command Default

A newly enabled cluster command switch has no associated cluster members.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E | This command was introduced. |

## Usage Guidelines

Enter this command only on the cluster command switch to add a candidate to or remove a member from the cluster.

If you enter this command on a switch other than the cluster command switch, the switch rejects the command and displays an error message.

You must enter a member number to remove a switch from the cluster. However, you do not need to enter a member number to add a switch to the cluster.

The cluster command switch selects the next available member number and assigns it to the switch that is joining the cluster.

You must enter the enabled password of the candidate switch for authentication when it joins the cluster. The password is not saved in the running or startup configuration.

After a candidate switch becomes a member of the cluster, its password becomes the same as the cluster command-switch password.

If a switch does not have a configured hostname, the cluster command switch appends a member number to the cluster command-switch hostname and assigns it to the

cluster member switch.

If you do not specify a VLAN ID, the cluster command switch automatically chooses a VLAN and adds the candidate to the cluster.

### Example

This example shows how to add a switch as member 2 with MAC address 00E0.1E00.2222 and the password **key** to a cluster. The cluster command switch

adds the candidate to the cluster through VLAN 3:

```
Switch(config)# cluster member 2 mac-address 00E0.1E00.2222 password key vlan 3
```

This example shows how to add a switch with MAC address 00E0.1E00.3333 to the cluster. This switch does not have a password. The cluster command switch selects the next

available member number and assigns it to the switch that is joining the cluster:

```
Switch(config)# cluster member mac-address 00E0.1E00.3333
```

You can verify your settings by entering the **show cluster members** privileged EXEC command on the cluster command switch.

# cluster outside-interface

To configure the outside interface for cluster Network Address Translation (NAT), use the **cluster outside-interface** global configuration

command on the cluster command switch, so that a member without an IP address can communicate with devices outside the cluster. Use the **no** form

of this command to return to the default setting.

**cluster outside-interface** *interface-id*
**no cluster outside-interface**

## Syntax Description

| | |
|---|---|
| *interface-id* | Interface to serve as the outside interface. Valid interfaces include physical interfaces, port channels, or VLANs. The port channel range is 1 to 6. The VLAN range is 1 to 4094. |

## Command Default

The default outside interface is automatically selected by the cluster command switch.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E | This command was introduced. |

## Usage Guidelines

Enter this command only on the cluster command switch. If you enter this command on a cluster member switch, an error message appears.

### Example

This example shows how to set the outside interface to VLAN 1:

```
Switch(config)# cluster outside-interface vlan 1
```

You can verify your setting by entering the **show running-config** privileged EXEC command.

# cluster run

To enable clustering on a switch, use the **cluster run** global configuration command. Use the **no** form of this command to disable clustering on a switch.

**cluster run**
**no cluster run**

## Syntax Description

This command has no arguments or keywords.

## Command Default

Clustering is enabled on all switches.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E | This command was introduced. |

## Usage Guidelines

When you enter the **no cluster run** command on a cluster command switch, the cluster command switch is disabled. Clustering is disabled, and the switch cannot become a candidate switch.

When you enter the **no cluster run** command on a cluster member switch, it is removed from the cluster. Clustering is disabled, and the switch cannot become a candidate switch.

When you enter the **no cluster run** command on a switch that is not part of a cluster, clustering is disabled on this switch. This switch cannot then become a candidate switch.

### Example

This example shows how to disable clustering on the cluster command switch:

```
Switch(config)# no cluster run
```

# cluster timer

To set the number of seconds between heartbeat messages, use the **cluster timer** global configuration command on the cluster command switch. To set the interval to the default value, use the **no** form of the command

**cluster timer** *interval-in-secs*
**no cluster timer**

## Syntax Description

| | |
|---|---|
| *interval-in-secs* | Interval in seconds between heartbeat messages. The range is 1 to 300 seconds. |

## Command Default

The default interval is 8 seconds.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E | This command was introduced. |

## Usage Guidelines

Enter this command with the **cluster holdtime** global configuration command only on the cluster command switch.

The cluster command switch propagates the values to all its cluster members so that the setting is consistent among all switches in the cluster.

The holdtime is typically set as a multiple of the heartbeat interval timer (**cluster timer**).

For example, the number of heartbeat messages that are missed in a row before a switch is declared down is calculated by dividing the number of seconds of holdtime by the

number of seconds in the interval.

### Example

This example shows how to change the heartbeat interval timer and the duration on the cluster command switch:

```
Switch(config)# cluster timer 3
Switch(config)# cluster holdtime 30
```

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

# 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 Release 15.0(2)EXCisco IOS Release 15.2(5)E | 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.

# debug cluster

Use the **debug cluster** privileged EXEC command to enable debugging of cluster-specific events. Use the **no** form of this command to disable debugging.

**debug cluster** {**discovery** | **events** | **extended** | **hrsp** | **http** | **ip** [**packet**] | **members** | **nat** | **neighbors** | **platform** | **snmp** | **vqpxy**}
**no debug cluster** {**discovery** | **events** | **extended** | **hrsp** | **http** | **ip** [**packet**] | **members** | **nat** | **neighbors** | **platform** | **snmp** | **vqpxy**}

## Syntax Description

| | |
|---|---|
| **discovery** | Displays cluster discovery debug messages. |
| **events** | Displays cluster event debug messages. |
| **extended** | Displays extended discovery debug messages. |
| **hrsp** | Displays the Hot Standby Router Protocol (HSRP) debug messages. |
| **http** | Displays Hypertext Transfer Protocol (HTTP) debug messages. |
| **ip** [**packet**] | Displays IP or transport packet debug messages. |
| **members** | Displays cluster member debug messages. |
| **nat** | Displays Network Address Translation (NAT) debug messages. |
| **neighbors** | Displays cluster neighbor debug messages. |
| **platform** | Displays platform-specific cluster debug messages. |
| **snmp** | Displays Simple Network Management Protocol (SNMP) debug messages. |
| **vqpxy** | Displays VLAN Query Protocol (VQP) proxy debug messages. |

## Command Default

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E | This command was introduced. |

## Usage Guidelines

This command is available only on the cluster command switch stack or cluster command switch.

The **undebug cluster** command works the same as the **no debug cluster** command.

When you enable debugging, it is enabled only on the active switch. To enable debugging on a member switch, you can start a session from the active switch by using the **session** *switch-number* privileged EXEC command.

Then enter the **debug** command at the command-line prompt of the member switch.

You also can use the **remote command** *stack-member-number* LINE privileged EXEC command on the active switch to enable debugging on a member switch without first starting a session.

# debug matm move update

To enable debugging of MAC address-table move update message processing, use the **debug matm move update** privileged EXEC command. Use the **no** form of this command to return to the default setting.

**debug matm move update**
**no debug matm move update**

**Command Default**

Debugging is disabled.

**Command Modes**

Privileged EXEC

**Command History**

| Release | Modification |
|---|---|
| Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E | This command was introduced. |

**Usage Guidelines**

The **undebug matm move update** command works the same as the **no debug matm move update** command.

**Note** This command is supported only on the LAN Base image.

When you enable debugging, it is enabled only on the active switch. To enable debugging on a member switch, you can start a session from the active switch by using the **session** *switch-number* privileged EXEC command.

Then enter the **debug** command at the command-line prompt of the member switch.

You can also use the **remote command** *stack-member-number LINE* privileged EXEC command on the active switch to enable debugging on a member switch without first starting a session.

# 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 Release 15.0(2)EXCisco IOS Release 15.2(5)E | 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 Release 15.0(2)EXCisco IOS Release 15.2(5)E | This command was introduced. |

## Usage Guidelines

Directory names are case sensitive.

## Examples

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

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

  96453632 bytes available (25732096 bytes used)
```

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

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

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

# 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 Release 15.0(2)EXCisco IOS Release 15.2(5)E | 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
```

# hw-module

To enable on-board failure logging (OBFL), use the **hw-module** global configuration command on the switch stack or on a standalone switch. Use the **no** form of this command to disable this feature.

**hw-module module** [ *switch-number*] **logging onboard** [**message level** *level*]
**no hw-module module** [ *switch-number*] **logging onboard** [**message level** *level*]

**Note** This command is supported only on the LAN Base image.

## Syntax Description

| | |
|---|---|
| **module** | Specifies the module number. |
| *switch-number* | (Optional) The switch number, which is the member switch number. If the switch is a standalone switch, the switch number is 1. If the switch is in a stack, the range is 1 to 4, depending on the switch member numbers in the stack. |
| **logging-onboard** | Specifies on-board failure logging. |
| **message level** *level* | (Optional) Specifies the severity of the hardware-related messages that are stored in the flash memory. The range is from 1 to 7. |

## Command Default

OBFL is enabled, and all messages appear.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E | This command was introduced. |

## Usage Guidelines

We recommend that you keep OBFL enabled and do not erase the data stored in the flash memory.

To ensure that the time stamps in the OBFL data logs are accurate, you should manually set the system clock or configure it by using Network Time Protocol (NTP).

If you do not enter the **message level** *level* parameter, all the hardware-related messages generated by the switch are stored in the flash memory.

On a standalone switch, entering the **hw-module module** [*switch-number*] **logging onboard** [**message level** *level*] command is the same as entering the **hw-module module logging onboard** [**message level** *level*] command.

Entering the **hw-module module logging onboard** [**message level** *level*] command on an active switch enables OBFL on all the member switches that support OBFL.

### Example

This example shows how to enable OBFL on a switch stack and to specify that all the hardware-related messages on member switch 4 are stored in the flash memory when this command is entered on the active switch:

```
Switch(config)# hw-module module 4 logging onboard
```

This example shows how to enable OBFL on a standalone switch and to specify that only severity 1 hardware-related messages are stored in the flash memory of the switch:

```
Switch(config)# hw-module module 1 logging onboard message level 1
```

You can verify your settings by entering the **show logging onboard** privileged EXEC command.

# ip name-server

To configure the IP address of the domain name server (DNS), use the **ip name-server** command. To delete the name server use the **no** form of this command.

**ip name-server** [*ip-server-address* | *ipv6-server-address* | *vrf*]
**no ip name-server** [*ip-server-address* | *ipv6-server-address* | *vrf*]

## Syntax Description

| | |
|---|---|
| *ip-server-address* | IPv4 addresses of a name server to use for name and address resolution. |
| *ipv6-server-address* | IPv4 addresses of a name server to use for name and address resolution. |
| *vrf* | VRF name |

## Command Default

No name server addresses are specified.

## Command Modes

Global configuration mode

## Command History

| Release | Modification |
|---|---|
| Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E | This command was introduced. |

## Usage Guidelines

You can configure up to six name servers (including IPv4 and IPv6 name servers).

Separate each server address with a space.

The first server specified is the primary server. The switch sends DNS queries to the primary server first. If that query fails, the backup servers are queried.

Enter the**show ip name-server** command to display all the name server IP addresses that have been maintained.

Specifics for Application Visibility Control (AVC) with Domain Name System as an Authoritative Source (DNS-AS):

Only IPv4 server addresses are supported. Ensure that at least the first two IP addresses in the sequence are IPv4 addresses, because the AVC with DNS-AS feature will use only these. In the example below, the first two addresses are IPv4 (192.0.2.1 and 192.0.2.2), the third one (2001:DB8::1) is an IPv6 address. AVC with DNS-AS uses the first two:

```
Device(config)# ip name-server 192.0.2.1 192.0.2.2 2001:DB8::1
```

### Example

The following example shows how to specify IPv4 hosts 192.0.2.1 and 192.0.2.2 as the name servers:

```
Device# configure terminal
Device(config)# ip name-server 192.0.2.1 192.0.2.2 2001:DB8::1
```

The following example shows how to specify IPv6 hosts 3FFE:C00::250:8BFF:FEE8:F800 and 2001:0DB8::3 as the name servers

```
Device# configure terminal
Device(config)# ip name-server 3FFE:C00::250:8BFF:FEE8:F800 2001:0DB8::3
```

## Related Commands

| Command | Description |
|---|---|
| show ip name-server | Displays all the name server IP addresses that have been maintained |

# license boot level

To boot a new software license on the device, use the license boot level command in global configuration mode. To return to the previously configured license level, use the no form of this command.

**license** {**accept end user agreement force** | **boot level addon** *addon-license-level* {*dna-essentials* | *dna-advantage*}}
**no license** {**accept end user agreement force** | **boot level addon** *addon-license-level* {*dna-essentials* | *dna-advantage*}}

## Syntax Description

| | |
|---|---|
| **accept end user agreement force** | Enables acceptance of the end-user license agreement (EULA). |
| **boot level addon** *addon-license-level* | Enter the add-on license level you want to enable on the switch.<br>• dna-essentials<br>• dna-advantage |

## Command Default

The switch boots the configured image.

## Command Modes

Global configuration (config)

## Command History

| Release | Modification |
|---|---|
| Cisco IOS Release 15.2(6)E1 | This command was introduced. |

## Usage Guidelines

You do not have to reboot the switch for the configure (add-on license) to take effect.

### Example

The following example shows how to activate the dna-essentials license on the switch:

```
Device(config)# license boot level addon dna-essentials
```

# logging

To log messages to a UNIX syslog server host, use the **logging** global configuration command.

**logging** *host*

## Syntax Description

| | |
|---|---|
| *host* | The name or IP address of the host to be used as the syslog server. |

## Command Default

None

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E | This command was introduced. |

## Usage Guidelines

To build a list of syslog servers that receive logging messages, enter this command more than once.

### Example

The following example specifies the logging host IP as 125.1.1.100:

```
Switch(config)# logging 125.1.1.100
```

# logging buffered

To log messages to an internal buffer, use the **logging buffered** global configuration command. Use it on the switch or on a standalone switch or, in the case of a switch stack, on the active switch.

**logging buffered** [*size*]

## Syntax Description

| | |
|---|---|
| *size* | (Optional) The size of the buffer created, in bytes. The range is 4096 to 2147483647 bytes. The default buffer size is 4096 bytes. |

## Command Default

The default buffer size is 4096 bytes.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E | This command was introduced. |

## Usage Guidelines

If a standalone switch or the active switch fails, the log file is lost unless you previously saved it to flash memory using the **logging file flash** global configuration command.

Do not make the buffer size too large because the switch could run out of memory for other tasks.

Use the **show memory** privileged EXEC command to view the free processor memory on the switch.

However, this value is the maximum number of bytes available, and the buffer size should not be set to this amount.

### Example

The following example sets the logging buffer to 8192 bytes:

```
Switch(config)# logging buffered 8192
```

# logging console

To limit messages logged to the console according to severity, use the **logging console** command. Use the **no** form of this command to disable message logging.

**logging console** *level*
**no logging console**

## Syntax Description

*level* The severity level of messages logged to the console. The severity levels are:

- Emergencies—System is unusable (severity=0)
- Alerts—Immediate action needed (severity=1)
- Critical—Critical conditions (severity=2)
- Errors—Error conditions (severity=3)
- Warnings—Warning conditions (severity=4)
- Notifications—Normal but significant conditions (severity=5)
- Informational—Informational messages (severity=6)
- Debugging—Debugging messages (severity=7)
- Discriminator—Establish MD-Console association
- Filtered—Enable filtered logging
- Guaranteed—Guarantee console messages
- XML—Enable logging in XML

## Command Default

By default, the console receives debugging messages and numerically lower levels.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E | This command was introduced. |

### Example

The following example sets the level of console messages received to severity 3 (errors) and above:

```
Switch(config)# logging console 3
```

# logging file flash

To store log messages in a file in flash memory, use the **logging file flash** command. Use it on a standalone switch or, in the case of a switch stack, on the active switch.

**logging file flash***:filename* [*max-file-size* [*min-file-size*]] [*severity-level-number* | *type*]

## Syntax Description

| | |
|---|---|
| *:filename* | The log message filename. |
| *max-file-size* | (Optional) The maximum logging file size. The range is 4096 to 2147483647. The default is 4096 bytes. |
| *min-file-size* | (Optional) The minimum logging file size. The range is 1024 to 2147483647. The default is 2048 bytes. |
| *max-file-size* \| *type* | (Optional) Either the logging severity level or the logging type. The severity range is 0 to 7. |

## Command Default

The default maximum file size is 4096 bytes and the default minimum file size is 1024 bytes.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E | This command was introduced. |

### Example

The following example sets the logging flash: filename to log_msg.txt, the maximum file size to 40960, the minimum file size to 4096, and the message severity level to 3:

```
Switch(config)# logging file flash:log_msg.txt 40960 4096 3
```

# logging history

To change the default level of syslog messages stored in the history file and sent to the SNMP server, use the **logging history** command.

**logging history** *level*

**Syntax Description**

| | |
|---|---|
| *level* | Level of syslog messages stored in the history file and sent to the SNMP server. |

**Command Default**

By default, warning, error, critical, alert, and emergency messages are sent.

**Command Modes**

Global configuration

**Command History**

| Release | Modification |
|---|---|
| Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E | This command was introduced. |

### Example

The following example sets the level of syslog messages stored in the history file and sent to the SNMP server to 3:

```
Switch(config)# logging history 3
```

# logging history size

To specify the number of syslog messages that can be stored in the history table, use the **logging history size** global configuration command.

**Note** When the history table contains the maximum number of message entries specified, the oldest message entry is deleted from the table to allow the new message entry to be stored.

**logging history size** *number*

## Syntax Description

| | |
|---|---|
| *number* | The number of syslog messages that can be stored in the history table. |

## Command Default

The default is to store one message. The range is 0 to 500 messages.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E | This command was introduced. |

### Example

The following example sets the number of syslog messages that can be stored in the history table to 200:

```
Switch(config)# logging history size 200
```

# logging monitor

To limit messages logged to the terminal lines according to severity, use the **logging monitor** command.

**logging monitor** *level*

**Syntax Description**

*level* The severity level of messages logged to the terminal lines. The severity levels are:

- Emergencies—System is unusable (severity=0)
- Alerts—Immediate action needed (severity=1)
- Critical—Critical conditions (severity=2)
- Errors—Error conditions (severity=3)
- Warnings—Warning conditions (severity=4)
- Notifications—Normal but significant conditions (severity=5)
- Informational—Informational messages (severity=6)
- Debugging—Debugging messages (severity=7)

**Command Default**

By default, the terminal receives debugging messages and numerically lower levels.

**Command Modes**

Global configuration

**Command History**

| Release | Modification |
|---|---|
| Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E | This command was introduced. |

### Example

The following example sets the level of terminal messages received to severity 3 (errors) and above:

```
Switch(config)# logging monitor 3
```

# logging trap

To limit messages logged to the syslog servers according to severity, use the **logging trap** command.

**logging trap** *level*

**Syntax Description**

*level* The severity level of messages logged to the syslog servers. The severity levels are:

- Emergencies—System is unusable (severity=0)
- Alerts—Immediate action needed (severity=1)
- Critical—Critical conditions (severity=2)
- Errors—Error conditions (severity=3)
- Warnings—Warning conditions (severity=4)
- Notifications—Normal but significant conditions (severity=5)
- Informational—Informational messages (severity=6)
- Debugging—Debugging messages (severity=7)

**Command Default**

By default, the syslog servers receive debugging messages and numerically lower levels.

**Command Modes**

Global configuration

**Command History**

| Release | Modification |
|---|---|
| Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E | This command was introduced. |

### Example

The following example sets the level of syslog server messages received to severity 3 (errors) and above:

```
Switch(config)# logging trap 3
```

# mac address-table aging-time

To set the length of time that a dynamic entry remains in the MAC address table after the entry is used or updated, use the **mac address-table aging-time** global configuration command. Use the **no** form of this command to return to the default setting.

**mac address-table aging-time** {**0** | *10 -1000000*} [**vlan** *vlan-id*]
**no mac address-table aging-time** {**0** | *10 -1000000*} [**vlan** *vlan-id*]

## Syntax Description

| | |
|---|---|
| **0** | This value disables aging. Static address entries are never aged or removed from the table. |
| *10-1000000* | Aging time in seconds. The range is 10 to 1000000 seconds. |
| **vlan** *vlan-id* | (Optional) Specifies the VLAN ID to which to apply the aging time. The range is 1 to 4094. |

## Command Default

The default is 300 seconds.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E | This command was introduced. |

## Usage Guidelines

The aging time applies to all VLANs or a specified VLAN. If you do not specify a specific VLAN, this command sets the aging time for all VLANs. Enter 0 seconds to disable aging.

### Example

This example shows how to set the aging time to 200 seconds for all VLANs:

```
Device(config)# mac address-table aging-time 200
```

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

# mac address-table learning vlan

To enable MAC address learning on a VLAN, use the **mac address-table learning** global configuration command. Use the **no** form of this command to disable MAC address learning on a VLAN to control which VLANs can learn MAC addresses.

**mac address-table learning vlan** *vlan-id*

**no mac address-table learning vlan** *vlan-id*

**Note** This command is supported only on the LAN Base image.

**Syntax Description**

| | |
|---|---|
| *vlan-id* | The VLAN ID or a range of VLAN IDs separated by a hyphen or comma. Valid VLAN IDs are 1 to 4094. |

**Command Default** By default, MAC address learning is enabled on all VLANs.

**Command Modes** Global configuration

**Command History**

| Release | Modification |
|---|---|
| Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E | This command was introduced. |

**Usage Guidelines**

When you control MAC address learning on a VLAN, you can manage the available MAC address table space by controlling which VLANs, and therefore which ports, can learn MAC addresses.

You can disable MAC address learning on a single VLAN ID (for example, **no mac address-table learning vlan 223**) or on a range of VLAN IDs (for example, **no mac address-table learning vlan 1-20, 15**).

Before you disable MAC address learning, be sure that you are familiar with the network topology and the switch system configuration.

Disabling MAC address learning on a VLAN could cause flooding in the network.

For example, if you disable MAC address learning on a VLAN with a configured switch virtual interface (SVI), the switch floods all IP packets in the Layer 2 domain.

If you disable MAC address learning on a VLAN that includes more than two ports, every packet entering the switch is flooded in that VLAN domain.

We recommend that you disable MAC address learning only in VLANs that contain two ports and that you use caution before disabling MAC address learning on a VLAN with an SVI.

You cannot disable MAC address learning on a VLAN that the switch uses internally. If the VLAN ID that you enter in the **no mac address-table learning vlan** *vlan-id* command is an internal VLAN, the switch generates an error message and rejects the command.

To view a list of which internal VLANs are being used, enter the **show vlan internal usage** privileged EXEC command.

If you disable MAC address learning on a VLAN configured as a private VLAN primary or a secondary VLAN, the MAC addresses are still learned on the other VLAN (primary or secondary) that belongs to the private VLAN.

You cannot disable MAC address learning on an RSPAN VLAN. The configuration is not allowed.

If you disable MAC address learning on a VLAN that includes a secure port, MAC address learning is not disabled on the secure port. If you later disable port security on the interface, the disabled MAC address learning state is enabled.

To display the MAC address learning status of all VLANs or a specified VLAN, enter the **show mac-address-table learning** [**vlan** *vlan-id* ] command.

### Example

This example shows how to disable MAC address learning on VLAN 2003:

```
Switch(config)#  no mac address-table learning vlan 2003
```

To display the MAC address learning status of all VLANs or a specified VLAN, enter the **mac address-table learning vlan** [*vlan-id* ] command.

# logging smartlog

To enable smart logging, use the **logging smartlog** command in global configuration mode on the device.

Smart logging sends the contents of specified dropped packets to a Cisco IOS Flexible NetFlow collector.

To disable smart logging or return to the default setting, use the **no** form of this command.

**logging smartlog** [**exporter** *name* | **packet capture size** *bytes*]
**no logging smartlog** [**exporter** *name* | **packet capture size** *bytes*]

## Syntax Description

| | |
|---|---|
| **exporter** *name* | (Optional) Identifies the Cisco IOS NetFlow exporter (collector) to which contents of dropped packets are sent. You must have already configured the exporter using the Flexible NetFlow CLI. If the exporter name does not exist, you receive an error message. By default, the device sends data to the collector every 60 seconds. |
| **packet capture size** *bytes* | (Optional) Specifies the size of the smart log packet sent to the collector in the number of bytes. The range is from 64 to 1024 bytes in 4-byte increments. The default size is 64 bytes. Increasing the packet capture size reduces the number of flow records per packet. |

## Command Default

By default, smart logging is not enabled.

## Command Modes

Global configuration.

## Command History

| Release | Modification |
|---|---|
| Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E | This command was introduced. |

## Usage Guidelines

You must configure a NetFlow collector before you enable smart logging. For information on configuring Cisco Flexible NetFlow, see the *Cisco IOS Flexible NetFlow Configuration Guide*.

You can configure smart logging of packets dropped due to DHCP snooping violations, Dynamic ARP inspection violations, IP source guard denied traffic, or ACL permitted or denied traffic.

You can verify the configuration by entering the **show logging smartlog** privileged EXEC command.

### Examples

This example shows a typical smart logging configuration. It assumes that you have already used the Flexible NetFlow CLI to configure the NetFlow exporter *cisco*, and configures smart logging to capture the first 128 bytes of the packets:

```
Device(config)# logging smartlog
Device(config)# logging smartlog cisco
Device(config)# logging smartlog packet capture size 128
```

# mac address-table notification

To enable the MAC address notification feature on the switch stack, use the **mac address-table notification** global configuration command. Use the **no** form of this command to return to the default setting.

**mac address-table notification** [**mac-move** | **threshold** [ [**limit** *percentage*] **interval** *time*]
**no mac address-table notification** [**mac-move** | **threshold** [ [**limit** *percentage*] **interval** *time*]

## Syntax Description

| | |
|---|---|
| **mac-move** | (Optional) Enables MAC move notification. |
| **threshold** | (Optional) Enables MAC threshold notification. |
| **limit** *percentage* | (Optional) Sets the MAC utilization threshold percentage. The range is 1 to 100 percent. The default is 50 percent. |
| **interval** *time* | (Optional) Sets the time between MAC threshold notifications. The range is 120 to 1000000 seconds. The default is 120 seconds. |

## Command Default

By default, the MAC address notification, MAC move, and MAC threshold monitoring are disabled.

The default MAC utilization threshold is 50 percent.

The default time between MAC threshold notifications is 120 seconds.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E | This command was introduced. |

## Usage Guidelines

You can enable traps whenever a MAC address is moved from one port to another in the same VLAN by entering the **mac address-table notification mac-move** command and the snmp-server enable traps **mac-notification move global configuration** command.

To generate traps whenever the MAC address table threshold limit is reached or exceeded, enter the **mac address-table notification** *threshold* [**limit** *percentage*] | [**interval** *time*] command and the **snmp-server enable traps mac-notification threshold** global configuration command.

### Example

This example shows how to set the threshold limit to 10 and set the interval time to 120 seconds:

```
Device(config)# mac address-table notification threshold limit 10 interval 120
```

You can verify your settings by entering the **show mac address-table notification** privileged EXEC command.

# mac address-table static

To add static addresses to the MAC address table, use the **mac address-table static** global configuration command. Use the **no** form of this command to remove static entries from the table.

**mac address-table static** *mac-addr* **vlan** *vlan-id* **interface** *interface-id*
**no mac address-table static** *mac-addr* **vlan** *vlan-id* **interface** *interface-id*

## Syntax Description

| | |
|---|---|
| *mac-addr* | Destination MAC address (unicast or multicast) to add to the address table. Packets with this destination address received in the specified VLAN are forwarded to the specified interface. |
| **vlan** *vlan-id* | Specifies the VLAN for which the packet with the specified MAC address is received. The range is 1 to 4094. |
| **interface** *interface-id* | Specifies the interface to which the received packet is forwarded. Valid interfaces include physical ports and port channels. |

## Command Default

No static addresses are configured.

## Command Modes

Global configuration

## Command History

## Command History

| Release | Modification |
|---|---|
| Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E | This command was introduced. |

This example shows how to add the static address c2f3.220a.12f4 to the MAC address table. When a packet is received in VLAN 4 with this MAC address as its destination, the packet is forwarded to the specified interface:

```
Device(config)# mac address-table static c2f3.220a.12f4 vlan 4 interface gigabitethernet6/0/1
```

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

# 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 Release 15.0(2)EXCisco IOS Release 15.2(5)E | This command was introduced. |

## Usage Guidelines

Directory names are case sensitive.

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

### Example

This example shows how to make a directory called Saved_Configs:

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

# more

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

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

**Syntax Description**

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

**Command Default**

No default behavior or values.

**Command Modes**

Boot loader

**Command History**

| Release | Modification |
|---|---|
| Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E | 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 Release 15.0(2)EXCisco IOS Release 15.2(5)E | 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
```

# rcommand

To start a Telnet session and to execute commands, use the **rcommand** user EXEC command. Use it on the switch stack, on the cluster command switch, or on a cluster member switch. To end the session, enter the **exit** command.

**rcommand** {*n* | **commander** | **mac-address** *hw-addr*}

## Syntax Description

| | |
|---|---|
| *n* | The number that identifies a cluster member. The range is 0 to 15. |
| **commander** | Provides access to the cluster command switch from a cluster member switch. |
| **mac-address** *hw-addr* | Specifies the MAC address of the cluster member switch. |

## Command Modes

User EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E | This command was introduced. |

## Usage Guidelines

This command is available only on the cluster command switch stack or cluster command switch.

If the switch is the cluster command switch, but the cluster member switch *n* does not exist, an error message appears. To get the switch number, enter the **show cluster members** privileged EXEC command on the cluster command switch.

You can use this command to access a cluster member switch from the cluster command-switch prompt or to access a cluster command switch from the member-switch prompt.

For Catalyst 2900 XL, 3500 XL, 2950, 2960, 2970, 3550, 3560, and 3750 switches, the Telnet session accesses the member-switch command-line interface (CLI) at the same privilege level as on the cluster command switch.

For example, if you execute this command at user level on the cluster command switch, the cluster member switch is accessed at user level. If you use this command on the cluster command switch at the privilege level, the command accesses the remote device at the privilege level.

If you use an intermediate enable-level lower than the privilege, access to the cluster member switch is at the user level.

For Catalyst 1900 and 2820 switches running standard edition software, the Telnet session accesses the menu console (the menu-driven interface) if the cluster command switch is at privilege level 15.

If the cluster command switch is at privilege level 1, you are prompted for the password before being able to access the menu console.

Cluster command switch privilege levels map to the cluster member switches running standard edition software as follows:

- If the cluster command switch privilege level is from 1 to 14, the cluster member switch is accessed at privilege level 1.

- If the cluster command switch privilege level is 15, the cluster member switch is accessed at privilege level 15.

The Catalyst 1900 and 2820 CLI is available only on switches running Enterprise Edition Software.

This command will not work if the vty lines of the cluster command switch have access-class configurations.

You are not prompted for a password because the cluster member switches inherited the password of the cluster command switch when they joined the cluster.

## Example

This example shows how to start a session with member 3. All subsequent commands are directed to member 3 until you enter the **exit** command or close the session:

```
Switch> rcommand 3
Switch-3# show version
Cisco Internet Operating System Software ...
...
Switch-3# exit
Switch>
```

# 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 Release 15.0(2)EXCisco IOS Release 15.2(5)E | 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.

# 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 Release 15.0(2)EXCisco IOS Release 15.2(5)E | This command was introduced. |

## Examples

This example shows how to reset the system:

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

# rmdir

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

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

## Syntax Description

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

## Command Default

No default behavior or values.

## Command Modes

Boot loader

## Command History

| Release | Modification |
|---|---|
| Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E | 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.

# service sequence-numbers

To display messages with sequence numbers when there is more than one log message with the same time stamp, use the **service sequence-numbers** global configuration command.

**service sequence-numbers**

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

**Command Default** By default, sequence numbers in log messages are not displayed.

**Command Modes** Global configuration

**Command History**

| Release | Modification |
|---|---|
| Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E | This command was introduced. |

### Example

This example shows how to display messages with sequence numbers when there is more than one log message with the same time stamp:

```
Switch(config)# service sequence-numbers
```

# 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 Release 15.0(2)EXCisco IOS Release 15.2(5)E | This command was introduced. |

## Usage Guidelines

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

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

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

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

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

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

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

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

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

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

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

### Example

This example shows how to set the SWITCH_PRIORITY environment variable:

```
Device: set SWITCH_PRIORITY 2
```

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

# show avc dns-as client

To display the various AVC with DNS-AS settings you have configured, enter the **show avc dns-as client** command in Privileged EXEC mode

**show avc dns-as client**[{**binding-table** [ | **detail**] | | **name-server brief** | | **rate-limiter-table** | | **statistics** | **status** | **trusted domains**}]

## Syntax Description

| | |
|---|---|
| **binding-table** [**detail**] | Displays AVC with DNS-AS metadata for the list of trusted domains and resolved entries. You can filter the output by application name, domain name, and so on.<br>The optional **detail** keyword displays the same information, in a different format. |
| **name-server brief** | Displays information about the DNS server to which the metadata request was sent. |
| **rate-limiter-table** | — |
| **statistics** | Displays packet logging information—the number of DNS queries sent and the number of responses received. |
| **status** | Displays current status of the DNS-AS client. Use this command to know whether AVC with DNS-AS is enabled or not. |
| **trusted-domains** | Displays list of trusted domains maintined in the binding table. |

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS Release 15.2(5)E1 | This command was introduced. |

### show avc dns-as client binding-table detailed

```
Device# show avc dns-as client binding-table
 Switch# show avc dns-as client binding-table detailed
DNS-AS generated protocols:
Max number of protocols :50
Customization interval [min] :N/A

Age : The amount of time that the entry is active
TTL : Time to live which was learned from DNS-AS server
Time To Expire : Entry expiration time in case device does not see DNS traffic for the entry
 host

Protocol-Name : example
VRF : <default>
Host : www.example.com
Age[min] : 2
TTL[min] : 60
Time To Expire[min] : 58
TXT Record : app-name:example|app-class:VO|business:YES
```

```
Traffic Class : voip-telephony
Business Relevance : business relevant
IP : 192.0.2.121
: 192.0.2.254
: 198.51.100.1
: 198.51.100.254
: 192.51.100.12
: 203.0.113.125
<output truncated>
```

### show avc dns-as client name-server brief

```
Device# show avc dns-as client name-server brief

Server-IP | Vrf-name
-----------------------------------------------------
192.0.2.1 | <default>
192.0.2.2 | <default>
```

### show avc dns-as client statistics

**Note** Two DNS servers are configured in this example.

```
Device# show avc dns-as client statistics
Server details: vrf-id = 0 vrf-name = <default> ip = 192.0.2.1
AAAA Query Error packets 0
AAAA Query TX packets 0
AAAA Response RX packets 0
TXT Query Error packets 0
TXT Query TX packets 8
TXT Response RX packets 0
A Query Error packets 0
A Query TX packets 6
A Response RX packets 0
Server details: vrf-id = 0 vrf-name = <default> ip = 192.0.2.2
AAAA Query Error packets 0
AAAA Query TX packets 0
AAAA Response RX packets 0
TXT Query Error packets 0
TXT Query TX packets 2
TXT Response RX packets 2
A Query Error packets 0
A Query TX packets 4
A Response RX packets 2
Total Drop packets 0

avc_dns_as_pkts_logged = 2
avc_dns_as_q_pkts_processed = 2
```

### show avc dns-as client status

```
Device# show avc dns-as client status
DNS-AS client is enabled
```

### show avc dns-as client trusted-domains

```
Device# show avc dns-as client trusted-domains
Id   | Trusted domain
-----------------------------------------------------
    1| example.com
    2| www.example.com
    3| example.net
    4| www.example.net
    5| example.org
    6| www.example.org
```

## Related Commands

| Command | Description |
|---|---|
| avc dns-as client, on page 14 | Enables AVC with DNS-AS on the switch (DNS-AS client) and maintains a list of trusted domains |

# show boot

To display the settings of the boot environment variables, use the **show boot** privileged EXEC command.

**show boot**

## Syntax Description

This command has no arguments or keywords.

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E | This command was introduced. |

### Example

This example shows the output from the **show boot** command. The table below describes each field in the display:

```
Switch# show boot
BOOT path-list        :flash:/image
Config file           :flash:/config.text
Private Config file   :flash:/private-config.text
Enable Break          :no
Manual Boot           :yes
HELPER path-list      :
Auto upgrade          :yes
------------------
```

For switch stacks, information is shown for each switch in the stack.

This feature is supported only on the LAN Base image.

***Table 2: show boot Field Descriptions***

| Field | Description |
|---|---|
| BOOT path-list | Displays a semicolon-separated list of executable files to try to load and execute when automatically booting up.<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. In a depth-first search of a directory, each encountered subdirectory is completely searched before continuing the search in the original directory.<br>If the BOOT variable is set but the specified images cannot be loaded, the system attempts to boot up with the first bootable file that it can find in the flash: file system. |

| Field | Description |
|---|---|
| Config file | Displays the filename that Cisco IOS uses to read and write a nonvolatile copy of the system configuration. |
| Private config file | Displays the filename that Cisco IOS uses to read and write a private nonvolatile copy of the system configuration. |
| Enable break | Displays whether a break is permitted during booting up is enabled or disabled. If it is set to yes, on, or 1, you can interrupt the automatic bootup process by pressing the **Break** key on the console after the flash: file system is initialized. |
| Manual boot | Displays whether the switch automatically or manually boots up. If it is set to no or 0, the bootloader attempts to automatically boot up the system. If it is set to anything else, you must manually boot up the switch from the bootloader mode. |
| Helper path-list | Displays a semicolon-separated list of loadable files to dynamically load during the bootloader initialization. Helper files extend or patch the functionality of the bootloader. |
| Auto upgrade | Displays whether the switch stack is set to automatically copy its software version to an incompatible switch so that it can join the stack.<br>A switch in version-mismatch mode is a switch that has a different stack protocol version than the version on the stack. Switches in version-mismatch mode cannot join the stack. If the stack has an image that can be copied to a switch in version-mismatch mode, and if the **boot auto-copy-sw** feature is enabled, the stack automatically copies the image from another stack member to the switch in version-mismatch mode. The switch then exits version-mismatch mode, reboots, and joins the stack. |
| NVRAM/Config file buffer size | Displays the buffer size that Cisco IOS uses to hold a copy of the configuration file in memory. The configuration file cannot be larger than the buffer size allocation. |

# show cable-diagnostics prbs

To display the pseudo-random binary sequence (PRBS) test results, use the **show cable-diagnostics prbs** command in privileged EXEC mode.

**show cable-diagnostics prbs interface** *interface-id*

**Syntax Description**

| | |
|---|---|
| *interface-id* | The interface on which PRBS is run. |

**Command Default**

None

**Command Modes**

Privileged EXEC

**Command History**

| Release | Modification |
|---|---|
| Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E | This command was introduced. |

**Usage Guidelines**

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

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

```
Switch# show cable-diagnostics prbs interface gigabitethernet1/0/23
  prbs 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 3: Field Descriptions for the show cable-diagnostics prbs Command Output***

| Field | Description |
|---|---|
| Interface | Interface on which PRBS is run. |
| Speed | Speed of connection. |
| Local pair | The name of the pair of wires that PRBS is testing on the local interface. |
| Pair length | The location of the problem on the cable, with respect to your device. PRBS 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 10-Gps.<br>• The cable is open.<br>• The cable has a short. |

| Field | Description |
|---|---|
| Remote pair | The name of the pair of wires to which the local pair is connected. PRBS 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 PRBS 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 PRBS.<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 PRBS is running:

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

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

```
Switch# show cable-diagnostics PRBS interface gigabitethernet1/0/2
  % PRBS test was never issued on Gi1/0/2
```

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

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

# 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 Release 15.0(2)EXCisco IOS Release 15.2(5)E | 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 4: Field Descriptions for the show cable-diagnostics tdr Command Output***

| Field | Description |
|---|---|
| Interface | The interface on which TDR is run. |
| Speed | The speed of connection. |
| Local pair | The name of the pair of wires that TDR is testing on the local interface. |

| Field | Description |
|---|---|
| Pair length | 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
```

# show cluster

To display the cluster status and a summary of the cluster to which the switch belongs, use the **show cluster** EXEC command. This command can be entered on the cluster command switch and cluster member switches.

**show cluster**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

User EXEC

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E | This command was introduced. |

## Usage Guidelines

If you enter this command on a switch that is not a cluster member, the following error message appears:

```
Not a management cluster member.
```

On a cluster member switch, this command displays the identity of the cluster command switch, the switch member number, and the state of its connectivity with the cluster command switch.

On a cluster command switch stack or cluster command switch, this command displays the cluster name and the total number of members.

It also shows the cluster status and time since the status changed. If redundancy is enabled, it displays the primary and secondary command-switch information.

### Example

This example shows the output from the **show cluster** command entered on the cluster command switch:

```
Switch# show cluster
Command switch for cluster "Ajang"
    Total number of members:       7
    Status:                        1 members are unreachable
    Time since last status change: 0 days, 0 hours, 2 minutes
    Redundancy:                    Enabled
        Standby command switch:    Member 1
        Standby Group:             Ajang_standby
        Standby Group Number:      110
    Heartbeat interval:            8
    Heartbeat hold-time:           80
    Extended discovery hop count:  3
```

This example shows the output from the **show cluster** command entered on a cluster member switch:

```
Switch1# show cluster
Member switch for cluster "hapuna"
    Member number:               3
    Management IP address:       192.192.192.192
    Command switch mac address:  0000.0c07.ac14
    Heartbeat interval:          8
    Heartbeat hold-time:         80
```

This example shows the output from the **show cluster** command entered on a cluster member switch that has lost connectivity with member 1:

```
Switch# show cluster
Command switch for cluster "Ajang"
    Total number of members:       7
    Status:                        1 members are unreachable
    Time since last status change: 0 days, 0 hours, 5 minutes
    Redundancy:                    Disabled
    Heartbeat interval:            8
    Heartbeat hold-time:           80
    Extended discovery hop count:  3
```

This example shows the output from the **show cluster** command entered on a cluster member switch that has lost connectivity with the cluster command switch:

```
Switch# show cluster
Member switch for cluster "hapuna"
    Member number:              <UNKNOWN>
    Management IP address:      192.192.192.192
    Command switch mac address: 0000.0c07.ac14
    Heartbeat interval:         8
    Heartbeat hold-time:        80
```

# show cluster candidates

To display a list of candidate switches, use the **show cluster candidates** EXEC command.

**show cluster candidates** [**detail** | **mac-address** *H.H.H*]

## Syntax Description

| | |
|---|---|
| **detail** | (Optional) Displays detailed information for all candidates. |
| **mac-address** *H.H.H* | (Optional) Specifies the MAC address of the cluster candidate. |

## Command Modes

User EXEC

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E | This command was introduced. |

## Usage Guidelines

This command is available only on the cluster command switch stack or cluster command switch.

**Note** This feature is supported only on the LAN Base image.

If the switch is not a cluster command switch, the command displays an empty line at the prompt.

The SN in the display means *switch member number*. If E appears in the SN column, it means that the switch is discovered through extended discovery.

If E does not appear in the SN column, it means that the *switch member number* is the upstream neighbor of the candidate switch.

The hop count is the number of devices the candidate is located from the cluster command switch.

### Example

This example shows the output from the **show cluster candidates** command:

```
Switch# show cluster candidates
                                                                |---Upstream---|
    MAC Address    Name         Device Type   PortIf  FEC Hops  SN  PortIf FEC
    00d0.7961.c4c0 StLouis-2    WS-C2960-12T  Gi0/1        2    1   Fa0/11
    00d0.bbf5.e900 ldf-dist-128 WS-C3524-XL   Fa0/7        1    0   Fa0/24
    00e0.1e7e.be80 1900_Switch  1900          3        0   1    0   Fa0/11
    00e0.1e9f.7a00 Surfers-24   WS-C2924-XL   Fa0/5        1    0   Fa0/3
    00e0.1e9f.8c00 Surfers-12-2 WS-C2912-XL   Fa0/4        1    0   Fa0/7
    00e0.1e9f.8c40 Surfers-12-1 WS-C2912-XL   Fa0/1        1    0   Fa0/9
```

This example shows the output from the **show cluster candidates** that uses the MAC address of a cluster member switch directly connected to the cluster command switch:

```
Switch# show cluster candidates mac-address 00d0.7961.c4c0
Device 'Tahiti-12' with mac address number 00d0.7961.c4c0
    Device type:          cisco WS-C2960-12T
```

```
    Upstream MAC address: 00d0.796d.2f00 (Cluster Member 0)
    Local port:           Gi6/0/1 FEC number:
    Upstream port:        GI6/0/11 FEC Number:
Hops from cluster edge:   1
Hops from command device: 1
```

This example shows the output from the **show cluster candidates** that uses the MAC address of a cluster member switch that is three hops from the cluster edge:

```
Switch# show cluster candidates mac-address 0010.7bb6.1cc0
Device 'Ventura' with mac address number 0010.7bb6.1cc0
    Device type:          cisco WS-C2912MF-XL
    Upstream MAC address: 0010.7bb6.1cd4
    Local port:           Fa2/1  FEC number:
    Upstream port:        Fa0/24 FEC Number:
    Hops from cluster edge: 3
    Hops from command device: -
```

This example shows the output from the **show cluster candidates detail** command:

```
Switch# show cluster candidates detail
Device 'Tahiti-12' with mac address number 00d0.7961.c4c0
    Device type:          cisco WS-C3512-XL
    Upstream MAC address: 00d0.796d.2f00 (Cluster Member 1)
    Local port:           Fa0/3  FEC number:
    Upstream port:        Fa0/13 FEC Number:
    Hops from cluster edge: 1
    Hops from command device: 2
Device '1900_Switch' with mac address number 00e0.1e7e.be80
    Device type:          cisco 1900
    Upstream MAC address: 00d0.796d.2f00 (Cluster Member 2)
    Local port:           3      FEC number: 0
    Upstream port:        Fa0/11 FEC Number:
    Hops from cluster edge: 1
    Hops from command device: 2
Device 'Surfers-24' with mac address number 00e0.1e9f.7a00
    Device type:          cisco WS-C2924-XL
    Upstream MAC address: 00d0.796d.2f00 (Cluster Member 3)
    Local port:           Fa0/5 FEC number:
    Upstream port:        Fa0/3 FEC Number:
    Hops from cluster edge: 1
    Hops from command device: 2
```

# show cluster members

To display information about cluster members, use the **show cluster members** privileged EXEC command.

**show cluster members** [*n* | **detail**]

**Syntax Description**

| | |
|---|---|
| *n* | (Optional) Number that identifies a cluster member. The range is 0 to 15. |
| **detail** | (Optional) Displays detailed information for all cluster members. |

**Command Modes**

Privileged EXEC

**Command History**

| Release | Modification |
|---|---|
| Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E | This command was introduced. |

**Usage Guidelines**

This command is available only on the cluster command switch stack or cluster command switch.

**Note** This feature is supported only on the LAN Base image.

If the cluster has no members, this command displays an empty line at the prompt.

### Example

This example shows the output from the **show cluster members** command. The SN in the display means *switch number*.

```
Switch# show cluster members
                                          |---Upstream---|
SN MAC Address Name           PortIf  FEC Hops SN  PortIf  FEC  State
0 0002.4b29.2e00 StLouis1                  0                    Up (Cmdr)
1 0030.946c.d740 tal-switch-1 Fa0/13       1   0   Gi0/1        Up
2 0002.b922.7180 nms-2820     10      0    2   1   Fa0/18       Up
3 0002.4b29.4400 SanJuan2     Gi0/1        2   1   Fa0/11       Up
4 0002.4b28.c480 GenieTest    Gi0/2        2   1   Fa0/9        Up
```

This example shows the output from the **show cluster members** for cluster member 3:

```
Switch# show cluster members 3
Device 'SanJuan2' with member number 3
    Device type:           cisco WS-C2960
    MAC address:           0002.4b29.4400
    Upstream MAC address:  0030.946c.d740 (Cluster member 1)
    Local port:            Gi6/0/1   FEC number:
    Upstream port:         GI6/0/11  FEC Number:
    Hops from command device: 2
```

This example shows the output from the **show cluster members detail** command:

```
Switch# show cluster members detail
Device 'StLouis1' with member number 0 (Command Switch)
    Device type:          cisco WS-C2960
    MAC address:          0002.4b29.2e00
```

```
    Upstream MAC address:
    Local port:                   FEC number:
    Upstream port:                FEC Number:
    Hops from command device: 0
Device 'tal-switch-14' with member number 1
    Device type:          cisco WS-C3548-XL
    MAC address:          0030.946c.d740
   Upstream MAC address:  0002.4b29.2e00 (Cluster member 0)
    Local port:           Fa0/13   FEC number:
    Upstream port:        Gi0/1    FEC Number:
    Hops from command device: 1
Device 'nms-2820' with member number 2
    Device type:          cisco 2820
    MAC address:          0002.b922.7180
    Upstream MAC address: 0030.946c.d740 (Cluster member 1)
    Local port:           10       FEC number: 0
    Upstream port:        Fa0/18   FEC Number:
    Hops from command device: 2
Device 'SanJuan2' with member number 3
    Device type:          cisco WS-C2960
    MAC address:          0002.4b29.4400
    Upstream MAC address: 0030.946c.d740 (Cluster member 1)
    Local port:           Gi6/0/1  FEC number:
    Upstream port:        Fa6/0/11 FEC Number:
    Hops from command device: 2
Device 'GenieTest' with member number 4
    Device type:          cisco SeaHorse
    MAC address:          0002.4b28.c480
    Upstream MAC address: 0030.946c.d740 (Cluster member 1)
    Local port:           Gi0/2    FEC number:
    Upstream port:        Fa0/9    FEC Number:
    Hops from command device: 2
Device 'Palpatine' with member number 5
    Device type:          cisco WS-C2924M-XL
    MAC address:          00b0.6404.f8c0
    Upstream MAC address: 0002.4b29.2e00 (Cluster member 0)
    Local port:           Gi2/1    FEC number:
    Upstream port:        Gi0/7    FEC Number:
    Hops from command device: 1
```

# show ip name-server

To display all the name server IP addresses that have been maintained, enter the**show ip name-server** command.

**show ip name-server**

## Syntax Description

This command has no arguments or keywords.

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E | This command was introduced. |

### Example

```
Device# show ip name-server
192.0.2.1
192.0.2.2
2001:DB8::1
```

# show license right-to-use

To display information related to the right-to-use licenses on the device, use the **show license right-to-use** command in the privileged EXEC mode.

**show license right-to-use** [**default** | **detail** | **eula** | **summary** | **usage**]

## Syntax Description

| | |
|---|---|
| **default** | Displays the default license information. |
| **detail** | Displays detailed information of all the licenses in the switch stack. |
| **eula** | Displays the end user license agreement. |
| **summary** | Displays a summary of the license information on the entire switch stack. |
| **usage** | Displays detailed information about usage for all licenses in the switch stack. |

## Command Default

None

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS Release 15.2(6)E1 | This command was introduced. |

This example shows how to display the default license information:

```
Device# show license right-to-use default
slot         License Name                  Type
------------------------------------------------
0            lanlite                       Permanent
0            lanbase                       Permanent
```

This example shows how to display detailed information of all the licenses in the switch stack:

```
Device# show license right-to-use detail
Index 1
 License Name    : lanlite
 Period left     : 0  minute  0  second
 License Type: Permanent
 License State: Inactive
Index 2
 License Name    : lanbase
 Period left     : 0  minute  0  second
 License Type: Permanent
 License State: Active, In use

Index 3
```

```
 License Name    : dna-essentials
 Period left     : CSSM Managed
 License Type    : Subscription
 License State   : Active, In use

Index 4
 License Name    : dna-advantage
 Period left     : CSSM Managed
 License Type    : Subscription
 License State   : Not Activated
```

This example shows how to display summary of the license information on the entire switch stack:

```
Device# show license right-to-use summary
License Name                Type          Period left
-------------------------------------------------------
lanlite                     Permanent     0  minute  0  second
lanbase                     Permanent     0  minute  0  second
dna-essentials              Subscription  CSSM Managed
-------------------------------------------------------

License Level In Use: lanbase  addon: dna-essentials
License Level on Reboot: lanbase  addon: dna-essentials
```

This example shows how to display detailed information about usage for all licenses in the switch stack:

```
Device# show license right-to-use usage
slot         License Name                Type          In-use   EULA
-------------------------------------------------------------------------
0            lanlite                     Permanent     yes      yes
0            lanbase                     Permanent     yes      yes
             dna-essentials              Subscription  yes      yes
```

This example shows how to display the end user license agreement:

```
Device# show license right-to-use eula subscription
Feature name             EULA Accepted
------------             -------------
dna-essentials           yes
PLEASE READ THE FOLLOWING TERMS  CAREFULLY. INSTALLING THE LICENSE OR
LICENSE KEY PROVIDED FOR ANY CISCO SOFTWARE PRODUCT, PRODUCT FEATURE,
AND OR SUBSEQUENTLY PROVIDED SOFTWARE FEATURES (COLLECTIVELY, THE ?SOFTWARE?),
USING SUCH SOFTWARE, AND/OR ACTIVATION OF THE SOFTWARE COMMAND LINE INTERFACE
CONSTITUTES  YOUR  FULL ACCEPTANCE  OF  THE FOLLOWING TERMS.YOU MUST NOT PROCEED
FURTHER IF YOU ARE NOT WILLING TO BE BOUND BY ALL THE TERMS SET FORTH HEREIN.

Your use of the Software is subject to the Cisco End User License Agreement (EULA)
and any relevant supplemental terms (SEULA) found at
http://www.cisco.com/c/en/us/about/legal/cloud-and-software/software-terms.html.
You hereby acknowledge and agree that certain Software and/or features are licensed
for a particular term, that the license to such Software and/or features is valid only
for the applicable term and that such Software and/or features may be shut down or
otherwise terminated by Cisco after expiration of the applicable license term (e.g.,
90-day trial period). Cisco reserves the right to terminate any such Software feature
electronically or by any other means available. While Cisco may provide alerts, it is
your sole responsibility to monitor your usage of any such term Software feature to
```

```
ensure that your systems and networks are prepared for a shutdown of the Software feature.
To memorialize your acceptance of these terms and activate your license to use the Software,
please execute the command "license accept end user agreement force".
```

# show logging onboard

Display the on-board failure logging (OBFL) information using the **show logging onboard** privileged EXEC command.

**show logging onboard** [**module** [*switch number*]] {{**clilog** | **environment** | **message** | **poe** | **temperature** | **uptime** | **voltage**} [**continuous** | **detail** | **summary**] [**start** *hh:mm:ss day month year*] [**end** *hh:mm:ss day month year*] }

## Syntax Description

| | |
|---|---|
| **module** [*switch number*] | (Optional) Displays OBFL information about the specified switches.<br>Uses the *switch number* parameter to specify the switch number, which is the stack member number. If the switch is a standalone switch, the switch number is 1. If the switch is in a stack, the range is 1 to 8, depending on the switch member numbers in the stack.<br>For more information about this parameter, see the "Usage Guidelines" section for this command. |
| **clilog** | Displays the OBFL CLI commands that were entered on the standalone switch or specified stack members. |
| **environment** | Displays the unique device identifier (UDI) information for the standalone switch or specified stack members. For all the connected FRU devices, it displays the product identification (PID), the version identification (VID), and the serial number. |
| **message** | Displays the hardware-related system messages generated by the standalone switch or specified stack members. |
| **poe** | Displays the power consumption of PoE ports on the standalone switch or specified stack members. |
| **temperature** | Displays the temperature of the standalone switch or specified stack members. |
| **uptime** | Displays the time when the standalone switch or specified stack members start, the reason the standalone switch or specified members restart, and the length of time the standalone switch or specified stack members have been running since they last restarted. |
| **voltage** | Displays the system voltages of the standalone switch or the specified switch stack members. |
| **continuous** | (Optional) Displays the data in the *continuous* file. |
| **detail** | (Optional) Displays both the continuous and summary data. |
| **summary** | (Optional) Displays the data in the *summary* file. |
| **start** *hh:mm:ss day month year* | (Optional) Displays the data from the specified time and date. For more information, see the "Usage Guidelines" section. |
| **end** *hh:mm:ss day month year* | (Optional) Displays the data from the specified time and date. For more information, see the "Usage Guidelines" section. |

**Command Modes** Privileged EXEC

**Command History**

| Release | Modification |
|---|---|
| Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E | This command was introduced. |

**Usage Guidelines** When OBFL is enabled, the switch records OBFL data in a continuous file that contains all of the data. The continuous file is circular. When the continuous file is full, the switch combines the data into a summary file, which is also known as a historical file.

Creating the summary file frees up space in the continuous file so that the switch can write newer data to it.

If you enter the **module** keyword, but do not enter the switch number, the switch displays OBFL information about the stack members that support OBFL.

Use the **start** and **end** keywords to display data collected only during a particular time period. When specifying the start and end times, follow these guidelines:

- *hh:mm:ss*—Enter the time as a two-digit number for a 24-hour clock. Make sure to use the colons (:).

  For example, enter **13:32:45**.

- *day*—Enter the day of the month. The range is from 1 to 31.

- *month*—Enter the month in uppercase or lowercase letters. You can enter the full name of the month, such as **January** or **august**, or the first three letters of the month, such as **jan** or **Aug**

- *year*—Enter the year as a 4-digit number, such as 2008. The range is from 1993 to 2035.

**Note** This feature is supported only on the LAN Base image.

### Example

This example shows the output from the **show logging onboard clilog continuous** command:

```
Switch# show logging onboard clilog continuous
--------------------------------------------------------------------------------
CLI LOGGING CONTINUOUS INFORMATION
--------------------------------------------------------------------------------
MM/DD/YYYY HH:MM:SS COMMAND
--------------------------------------------------------------------------------
05/12/2006 15:33:17 show logging onboard temperature detail
05/12/2006 15:33:21 show logging onboard voltage detail
05/12/2006 15:33:32 show logging onboard poe detail
05/12/2006 16:14:09 show logging onboard temperature summary
...
<output truncated>
....
05/16/2006 13:07:53 no hw-module module logging onboard message level
05/16/2006 13:16:13 show logging onboard uptime continuous
05/16/2006 13:39:18 show logging onboard uptime summary
05/16/2006 13:45:57 show logging onboard clilog summary
--------------------------------------------------------------------------------
```

This example shows the output from the **show logging onboard poe continuous end 01:01:00 jan 2000** command on a switch:

```
Switch# show logging onboard message poe continuous end 01:01:00 jan 2000
POE CONTINUOUS INFORMATION
------------------------------------------------------------------------------
Sensor                   | ID |
------------------------------------------------------------------------------
Gi1/0/1                    1
Gi1/0/2                    2
Gi1/0/3                    3
Gi1/0/4                    4
...
<output truncated>
...
Gi1/0/21                  21
Gi1/0/22                  22
Gi1/0/23                  23
Gi1/0/24                  24
------------------------------------------------------------------------------
Time Stamp            |Sensor Watts
MM/DD/YYYY HH:MM:SS | Gi1/0/1 Gi1/0/2 Gi1/0/3 Gi1/0/4 Gi1/0/5 Gi1/0/6 Gi1/0/7 Gi1/0/8 Gi1/0/9
Gi1/0/10 Gi1/0/11 Gi1/0/12 Gi1/0/13 Gi1/0/14 Gi1/0/15 Gi1/0/16 Gi1/0/17 Gi1/0/18 Gi1/0/19
Gi1/0/20 Gi1/0/21
Gi1/0/22 Gi1/0/23 Gi1/0/24
------------------------------------------------------------------------------
03/01/1993 00:04:03   0.000   0.000   0.000   0.000  0.000  0.000  0.0  00  0.000  0.000
0.000   0.000   0.000   0.000 0.000   0.000   0. 000   0.000   0.000   0.000   0.000   0.000
0.000   0.000   0.000
03/01/1993 00:05:03   0.000 1.862    0.000   1.862  0.000  0.000  0.000  0.000  0.000  0.000
0.000   0.000   0.000   0.000 0.000   0.000   0.000   0.000   0.000   0.000   0.000   0.000
0.000   0.000
------------------------------------------------------------------------------
```

This example shows the output from the **show logging onboard status** command:

```
Switch# show logging onboard status
Devices registered with infra
                Slot no.: 0 Subslot no.: 0, Device obfl0:
Application name clilog :
                Path : obfl0:
                CLI enable status : enabled
                Platform enable status: enabled
Application name environment :
                Path : obfl0:
                CLI enable status : enabled
                Platform enable status: enabled
Application name errmsg :
                Path : obfl0:
                CLI enable status : enabled
                Platform enable status: enabled
Application name poe :
                Path : obfl0:
                CLI enable status : enabled
                Platform enable status: enabled
Application name temperature :
                Path : obfl0:
                CLI enable status : enabled
                Platform enable status: enabled
Application name uptime :
                Path : obfl0:
                CLI enable status : enabled
                Platform enable status: enabled
Application name voltage :
                Path : obfl0:
                CLI enable status : enabled
                Platform enable status: enabled
```

This example shows the output from the **show logging onboard temperature continuous** command:

```
Switch# show logging onboard temperature continuous
-------------------------------------------------------------------------------
TEMPERATURE CONTINUOUS INFORMATION
-------------------------------------------------------------------------------
Sensor                          | ID |
-------------------------------------------------------------------------------
Board temperature                 1
-------------------------------------------------------------------------------
       Time Stamp   |Sensor Temperature 0C
MM/DD/YYYY HH:MM:SS |  1   2   3   4   5   6   7   8   9  10  11  12
-------------------------------------------------------------------------------
05/12/2006 15:33:20   35  --  --  --  --  --  --  --  --  --  --  --
05/12/2006 16:31:21   35  --  --  --  --  --  --  --  --  --  --  --
05/12/2006 17:31:21   35  --  --  --  --  --  --  --  --  --  --  --
05/12/2006 18:31:21   35  --  --  --  --  --  --  --  --  --  --  --
05/12/2006 19:31:21   35  --  --  --  --  --  --  --  --  --  --  --
05/12/2006 20:31:21   35  --  --  --  --  --  --  --  --  --  --  --
05/12/2006 21:29:22   35  --  --  --  --  --  --  --  --  --  --  --
05/12/2006 22:29:22   35  --  --  --  --  --  --  --  --  --  --  --
05/12/2006 23:29:22   35  --  --  --  --  --  --  --  --  --  --  --
05/13/2006 00:29:22   35  --  --  --  --  --  --  --  --  --  --  --
05/13/2006 01:29:22   35  --  --  --  --  --  --  --  --  --  --  --
05/13/2006 02:27:23   35  --  --  --  --  --  --  --  --  --  --  --
05/13/2006 03:27:23   35  --  --  --  --  --  --  --  --  --  --  --
05/13/2006 04:27:23   35  --  --  --  --  --  --  --  --  --  --  --
05/13/2006 05:27:23   35  --  --  --  --  --  --  --  --  --  --  --
05/13/2006 06:27:23   35  --  --  --  --  --  --  --  --  --  --  --
05/13/2006 07:25:24   36  --  --  --  --  --  --  --  --  --  --  --
05/13/2006 08:25:24   35  --  --  --  --  --  --  --  --  --  --  --
<output truncated>
```

This example shows the output from the **show logging onboard uptime summary** command:

```
Switch# show logging onboard uptime summary
-------------------------------------------------------------------------------
UPTIME SUMMARY INFORMATION
-------------------------------------------------------------------------------
First customer power on : 03/01/1993 00:03:50
Total uptime            :   0 years   0 weeks   3 days   21 hours   55 minutes
Total downtime          :   0 years   0 weeks   0 days    0 hours    0 minutes
Number of resets        : 2
Number of slot changes  : 1
Current reset reason    : 0x0
Current reset timestamp : 03/01/1993 00:03:28
Current slot            : 1
Current uptime          : 0 years    0 weeks    0 days    0 hours   55 minutes
-------------------------------------------------------------------------------
Reset  |       |
Reason | Count |
-------------------------------------------------------------------------------
No historical data to display
-------------------------------------------------------------------------------
```

This example shows the output from the **show logging onboard voltage summary** command:

```
Switch# show logging onboard voltage summary
-------------------------------------------------------------------------------
VOLTAGE SUMMARY INFORMATION
-------------------------------------------------------------------------------
Number of sensors         : 8
Sampling frequency        : 60 seconds
Maximum time of storage   : 3600 minutes
-------------------------------------------------------------------------------
```

```
Sensor                    | ID | Maximum Voltage
--------------------------------------------------------------------------------
12.00V                      0   12.567
5.00V                       1    5.198
3.30V                       2    3.439
2.50V                       3    2.594
1.50V                       4    1.556
1.20V                       5    1.239
1.00V                       6    0.980
0.75V                       7    0.768
--------------------------------------------------------------------------------
Nominal Range                Sensor ID
--------------------------------------------------------------------------------
No historical data to display
--------------------------------------------------------------------------------
```

# show mac address-table

To display a specific MAC address table entry, use the **show mac address-table** command in EXEC mode.

**show mac-address-table**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

User EXEC

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E | This command was introduced. |

## Usage Guidelines

**Note** This feature is supported only on the LAN Base image.

This command can display static and dynamic entries or the MAC address table static and dynamic entries on a specific interface or VLAN.

### Example

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

```
Switch# show mac address-table
          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type    Ports
----    -----------       ----    -----
  All   0000.0000.0001    STATIC   CPU
  All   0000.0000.0002    STATIC   CPU
  All   0000.0000.0003    STATIC   CPU
  All   0000.0000.0009    STATIC   CPU
  All   0000.0000.0012    STATIC   CPU
  All   0180.c200.000b    STATIC   CPU
  All   0180.c200.000c    STATIC   CPU
  All   0180.c200.000d    STATIC   CPU
  All   0180.c200.000e    STATIC   CPU
  All   0180.c200.000f    STATIC   CPU
  All   0180.c200.0010    STATIC   CPU
    1   0030.9441.6327    DYNAMIC  Gi0/4
Total Mac Addresses for this criterion: 12
```

# show mac address-table address

To display MAC address table information for a specified MAC address, use the **show mac address-table address** command in EXEC mode.

**show mac address-table address** *mac-address* [**interface** *interface-id*] [**vlan** *vlan-id*]

## Syntax Description

| | |
|---|---|
| *mac-address* | The 48-bit MAC address; valid format is H.H.H. |
| **interface** *interface-id* | (Optional) Displays information for a specific interface. Valid interfaces include physical ports and port channels. |
| **vlan** *vlan-id* | (Optional) Displays entries for the specific VLAN only. The range is 1 to 4094. |

## Command Modes

User EXEC

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E | This command was introduced. |

### Example

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

```
Switch# show mac address-table address 0002.4b28.c482
           Mac Address Table
-------------------------------------------

Vlan   Mac Address      Type    Ports
----   -----------      ----    -----
All    0002.4b28.c482   STATIC  CPU
Total Mac Addresses for this criterion: 1
```

# show mac address-table aging-time

To display the aging time of address table entries, use the **show mac address-table aging-time** command in EXEC mode.

**show mac address-table aging-time** [**vlan** *vlan-id*]

## Syntax Description

| | |
|---|---|
| **vlan** *vlan-id* | (Optional) Displays aging time information for a specific VLAN. The range is 1 to 4094. |

## Command Modes

User EXEC

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E | This command was introduced. |

## Usage Guidelines

If no VLAN number is specified, the aging time for all VLANs appears. This command displays the aging time of a specific address table instance, all address table instances on a specified VLAN, or, if a specific VLAN is not specified, on all VLANs.

### Example

This example shows the output from the **show mac address-table aging-time** command:

```
Switch# show mac address-table aging-time

Vlan   Aging Time
----   ----------
   1   300
```

This example shows the output from the **show mac address-table aging-time vlan 10** command:

```
Switch# show mac address-table aging-time vlan 10

Vlan   Aging Time
----   ----------
  10   300
```

# show mac address-table count

To display the number of addresses present in all VLANs or the specified VLAN, use the **show mac address-table count** command in EXEC mode.

**show mac address-table count** [**vlan** *vlan-id*]

## Syntax Description

| | |
|---|---|
| **vlan** *vlan-id* | (Optional) Displays the number of addresses for a specific VLAN. The range is 1 to 4094. |

## Command Modes

User EXEC

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E | This command was introduced. |

## Usage Guidelines

If no VLAN number is specified, the address count for all VLANs appears.

### Example

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

```
Switch# show mac address-table count

Mac Entries for Vlan   : 1
---------------------------
Dynamic Address Count  : 2
Static Address Count   : 0
Total Mac Addresses    : 2
```

# show mac address-table dynamic

To display only dynamic MAC address table entries, use the **show mac address-table dynamic** command in EXEC mode.

**show mac address-table dynamic** [**address** *mac-address*] [**interface** *interface-id*] [**vlan** *vlan-id*]

## Syntax Description

| | |
|---|---|
| **address** *mac-address* | (Optional) Specifies a 48-bit MAC address; the valid format is H.H.H (available in privileged EXEC mode only). |
| **interface** *interface-id* | (Optional) Specifies an interface to match; valid interfaces include physical ports and port channels. |
| **vlan** *vlan-id* | (Optional) Displays entries for a specific VLAN; the range is 1 to 4094. |

## Command Modes

User EXEC

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E | This command was introduced. |

### Example

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

```
Switch# show mac address-table dynamic

          Mac Address Table
-------------------------------------------
Vlan   Mac Address     Type      Ports
----   -----------     ----      -----
   1   0030.b635.7862  DYNAMIC   Gi0/2
   1   00b0.6496.2741  DYNAMIC   Gi0/2
Total Mac Addresses for this criterion: 2
```

# show mac address-table interface

To display the MAC address table information for a specified interface on a specified VLAN, use the **show mac address-table interface** EXEC command.

**show mac address-table interface** *interface-id* [**vlan** *vlan-id*]

## Syntax Description

| | |
|---|---|
| *interface-id* | The interface type; valid interfaces include physical ports and port channels. |
| **vlan** *vlan-id* | (Optional) Displays entries for a specific VLAN; the range is 1 to 4094. |

## Command Modes

User EXEC

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E | This command was introduced. |

### Example

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

```
Switch# show mac address-table interface gigabitethernet0/2

          Mac Address Table
-------------------------------------------
Vlan Mac Address     Type     Ports
---- -----------     ----     -----
1    0030.b635.7862  DYNAMIC  Gi0/2
1    00b0.6496.2741  DYNAMIC  Gi0/2
Total Mac Addresses for this criterion: 2
```

# show mac address-table learning

To display the status of MAC address learning for all VLANs or a specified VLAN, use the **show mac address-table learning** command in EXEC mode.

**show mac address-table learning** [**vlan** *vlan-id*]

## Syntax Description

| | |
|---|---|
| **vlan** *vlan-id* | (Optional) Displays information for a specific VLAN. The range is 1 to 4094. |

## Command Modes

User EXEC

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E | This command was introduced. |

## Usage Guidelines

Use the **show mac address-table learning** command without any keywords to display configured VLANs and whether MAC address learning is enabled or disabled on them.

The default is that MAC address learning is enabled on all VLANs. Use the command with a specific VLAN ID to display the learning status on an individual VLAN.

**Note** This command is supported only on the LAN Base image.

### Example

This example shows the output from the **show mac address-table learning** command showing that MAC address learning is disabled on VLAN 200:

```
Switch# show mac address-table learning

VLAN      Learning Status
----      ---------------
1              yes
100            yes
200            no
```

# 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 Release 15.0(2)EXCisco IOS Release 15.2(5)E | 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 mac address-table multicast

To display information about the multicast MAC address table, use the **show mac-address-table multicast** command.

**show mac-address-table multicast** [**count** | {**igmp-snooping** [**count**]} | {**user** [**count**]} | {**vlan** *vlan_num*}]

## Syntax Description

| | |
|---|---|
| **count** | (Optional) Displays the number of multicast entries. |
| **igmp-snooping** | (Optional) Displays only the addresses learned by IGMP snooping. |
| **user** | (Optional) Displays only the user-entered static addresses. |
| **vlan** *vlan_num* | (Optional) Displays information for a specific VLAN only; valid values are from 1 to 4094. |

## Command History

| Release | Modification |
|---|---|
| Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E | This command was introduced. |

## Usage Guidelines

For the MAC address table entries that are used by the routed ports, the routed port name is displayed in the "vlan" column, not the internal VLAN number.

### Example

This example shows how to display multicast MAC address table information for a specific VLAN:

```
Switch# show mac-address-table multicast vlan 1

Multicast Entries
 vlan    mac address     type    ports
-------+---------------+-------+-----------------------------------------
   1    ffff.ffff.ffff   system Switch,Fa6/15
Switch#
```

This example shows how to display the number of multicast MAC entries for all VLANs:

```
Switch# show mac-address-table multicast count

MAC Entries for all vlans:
Multicast MAC Address Count:                  141
Total Multicast MAC Addresses Available:      16384
Switch#
```

# show mac address-table notification

To display the MAC address notification settings for all interfaces or the specified interface, use the **show mac address-table notification** command in EXEC mode.

```
show mac address-table notification {change [interface[interface-id]] | mac-move
| threshold}
```

## Syntax Description

| | |
|---|---|
| *change* | The MAC change notification feature parameters and history table. |
| **interface** | (Optional) Displays information for all interfaces. Valid interfaces include physical ports and port channels. |
| *interface-id* | (Optional) The specified interface. Valid interfaces include physical ports and port channels. |
| **mac-move** | Displays status for MAC address move notifications. |
| **threshold** | Displays status for MAC address-table threshold monitoring. |

## Command Default

By default, the MAC address notification, MAC move, and MAC threshold monitoring are disabled.

The default MAC utilization threshold is 50 percent.

The default time between MAC threshold notifications is 120 seconds.

## Command Modes

User EXEC

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E | This command was introduced. |

## Usage Guidelines

Use the **show mac address-table notification change** command without keywords to see if the MAC address change notification feature is enabled or disabled, the number of seconds in the MAC notification interval,

the maximum number of entries allowed in the history table, and the history table contents.

Use the **interface** keyword to display the notifications for all interfaces. If the interface ID is included, only the flags for that interface appear.

### Example

This example shows the output from the **show mac address-table notification change** command:

```
Switch# show mac address-table notification change

MAC Notification Feature is Enabled on the switch
Interval between Notification Traps : 60 secs
Number of MAC Addresses Added : 4
Number of MAC Addresses Removed : 4
Number of Notifications sent to NMS : 3
```

```
Maximum Number of entries configured in History Table : 100
Current History Table Length : 3
MAC Notification Traps are Enabled

History Table contents
------------------------------
History Index 0, Entry Timestamp 1032254, Despatch Timestamp 1032254
MAC Changed Message :
Operation: Added Vlan: 2 MAC Addr: 0000.0000.0001 Module: 0 Port: 1

History Index 1, Entry Timestamp 1038254, Despatch Timestamp 1038254
MAC Changed Message :
Operation: Added Vlan: 2 MAC Addr: 0000.0000.0000 Module: 0 Port: 1
Operation: Added Vlan: 2 MAC Addr: 0000.0000.0002 Module: 0 Port: 1
Operation: Added Vlan: 2 MAC Addr: 0000.0000.0003 Module: 0 Port: 1

History Index 2, Entry Timestamp 1074254, Despatch Timestamp 1074254
MAC Changed Message :
Operation: Deleted Vlan: 2 MAC Addr: 0000.0000.0001 Module: 0 Port: 1
Operation: Deleted Vlan: 2 MAC Addr: 0000.0000.0002 Module: 0 Port: 1
Operation: Deleted Vlan: 2 MAC Addr: 0000.0000.0003 Module: 0 Port: 1
```

# show mac address-table secure

To display only secure MAC address table entries, use the **show mac address-table secure** command in EXEC mode.

**show mac address-table secure** [**address** *mac-address*] [**interface** *interface-id*] [**vlan** *vlan-id*]

## Syntax Description

| | |
|---|---|
| **address** *mac-address* | (Optional) Specifies a 48-bit MAC address; the valid format is H.H.H (available in privileged EXEC mode only). |
| **interface** *interface-id* | (Optional) Specifies an interface to match; valid interfaces include physical ports and port channels. |
| **vlan** *vlan-id* | (Optional) Displays entries for a specific VLAN; the range is 1 to 4094. |

## Command Modes

User EXEC

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E | This command was introduced. |

### Example

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

```
Switch# show mac address-table secure

          Mac Address Table
-------------------------------------------
Vlan   Mac Address     Type      Ports
----   -----------     ----      -----
   1   0030.b635.7862  DYNAMIC   Gi0/2
   1   00b0.6496.2741  DYNAMIC   Gi0/2
Total Mac Addresses for this criterion: 2
```

# show mac address-table static

To display only static MAC address table entries, use the **show mac address-table static** command in EXEC mode.

**show mac address-table static** [**address** *mac-address*] [**interface** *interface-id*] [**vlan** *vlan-id*]

## Syntax Description

| | |
|---|---|
| **address** *mac-address* | (Optional) Specifies a 48-bit MAC address; the valid format is H.H.H (available in privileged EXEC mode only). |
| **interface** *interface-id* | (Optional) Specifies an interface to match; valid interfaces include physical ports and port channels. |
| **vlan** *vlan-id* | (Optional) Specifies the address for a specific VLAN. The range is from 1 to 4094. |

## Command Modes

User EXEC

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E | This command was introduced. |

### Example

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

```
Switch# show mac address-table static

            Mac Address Table
-------------------------------------------
Vlan    Mac Address     Type    Ports
----    -----------     ----    -----
All     0100.0ccc.cccc  STATIC  CPU
All     0180.c200.0000  STATIC  CPU
All     0100.0ccc.cccd  STATIC  CPU
All     0180.c200.0001  STATIC  CPU
All     0180.c200.0004  STATIC  CPU
All     0180.c200.0005  STATIC  CPU
  4     0001.0002.0004  STATIC  Drop
  6     0001.0002.0007  STATIC  Drop
Total Mac Addresses for this criterion: 8
```

# show mac address-table vlan

To display the MAC address table information for a specified VLAN, use the **show mac address-table vlan** command in EXEC mode.

**show mac address-table vlan** *vlan-id*

## Syntax Description

| | |
|---|---|
| *vlan-id* | The address for a specific VLAN. The range is 1 to 4094. |

## Command Modes

User EXEC

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E | This command was introduced. |

### Example

This example shows the output from the **show mac address-table vlan 1** command:

```
Switch# show mac address-table vlan 1

           Mac Address Table
-------------------------------------------
Vlan  Mac Address     Type    Ports
----  -----------     ----    -----
  1   0100.0ccc.cccc  STATIC  CPU
  1   0180.c200.0000  STATIC  CPU
  1   0100.0ccc.cccd  STATIC  CPU
  1   0180.c200.0001  STATIC  CPU
  1   0180.c200.0002  STATIC  CPU
  1   0180.c200.0003  STATIC  CPU
  1   0180.c200.0005  STATIC  CPU
  1   0180.c200.0006  STATIC  CPU
  1   0180.c200.0007  STATIC  CPU
Total Mac Addresses for this criterion: 9
```

# 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 Release 15.0(2)EXCisco IOS Release 15.2(5)E | 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 onboard switch

To display OBFL information use the **show onboard switch** privileged EXEC command.

**show onboard switch** *switch-number*{**clilog** | **environment** | **message** | **counter** | **temperature** | **uptime** | **voltage** | **status**}

## Syntax Description

| | |
|---|---|
| *switch-number* | Specifies the switch or stack member numbers. |
| **clilog** | Displays the OBFL CLI commands that were entered on a standalone switch or the specified stack members. |
| **environment** | Displays the UDI information for a standalone switch or the specified stack members. For all the connected FRU devices, it displays the PID, the VID, and the serial number. |
| **message** | Displays the hardware-related messages generated by a standalone switch or the specified stack members. |
| **counter** | Displays the counter information on a standalone switch or the specified stack members. |
| **temperature** | Displays the temperature of a standalone switch or the specified switch stack members. |
| **uptime** | Displays the time when a standalone switch or the specified stack members start, the reason the standalone switch or specified stack members restart, and the length of time that the standalone switch or specified stack members have been running since they last restarted. |
| **voltage** | Displays the system voltages of a standalone switch or the specified stack members. |
| **status** | Displays the status of a standalone switch or the specified stack members. |

## Command Modes

Priviledged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E | This command was introduced. |

### Example

The following example displays the OBFL CLI commands entered on a standalone switch or the specified stack member:

```
Switch# show onboard switch 1 clilog
```

The following example displays the UDI information for a standalone switch or the specified stack members. For all the connected FRU devices, it displays the PID, the VID, and the serial number.

```
Switch# show onboard switch 1 environment
```

The following example displays the hardware-related messages generated by a standalone switch or the specified stack members.

```
Switch# show onboard switch 1 message
```

The following example displays the counter information on a standalone switch or the specified stack members.

```
Switch# show onboard switch 1 counter
```

The following example displays the temperature of a standalone switch or the specified stack members.

```
Switch# show onboard switch 1 temperature
```

The following example displays the time when a standalone switch or the specified stack members start, the reason the standalone switch or the specified stack members restart, and the length of time that the standalone switch or the specified stack members have been running since they last restarted.

```
Switch# show onboard switch 1 uptime
```

The following example displays the system voltages of a standalone switch or the specified stack members.

```
Switch# show onboard switch 1 voltage
```

The following example displays the status of a standalone switch or the specified stack members.

```
Switch# show onboard switch 1 status
```

# 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 Release 15.0(2)EXCisco IOS Release 15.2(5)E | 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
```

# test cable-diagnostics prbs

To run the pseudo-random binary sequence (PRBS) feature on an interface, use the **test cable-diagnostics prbs** command in privileged EXEC mode.

**test cable-diagnostics prbs interface** *interface-id*

## Syntax Description

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

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E | This command was introduced. |

## Usage Guidelines

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

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

### Example

This example shows how to run PRBS on an interface:

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

# 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 Release 15.0(2)EXCisco IOS Release 15.2(5)E | This command was introduced. |

## Usage Guidelines

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

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

This example shows how to run TDR on an interface:

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

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

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

# traceroute mac

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

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

## Syntax Description

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

## Command Default

No default behavior or values.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E | This command was introduced. |

## Usage Guidelines

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

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

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

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

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

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

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

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

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

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

This feature is not supported in Token Ring VLANs.

## Examples

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

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

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

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

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

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

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

```
Device# traceroute mac 0000.0201.0501 0000.0201.0201 detail
  Source not directly connected, tracing source .....
  Source 0000.0201.0501 found on con5[WS-C3750E-24TD] (2.2.5.5)
  con5 / WS-C3750E-24TD / 2.2.5.5 :
          Gi0/0/1 [auto, auto] => Gi0/0/3 [auto, auto]
```

```
  con1 / WS-C3550-12G / 2.2.1.1 :
         Gi0/1 [auto, auto] => Gi0/2 [auto, auto]
  con2 / WS-C3550-24 / 2.2.2.2 :
         Gi0/2 [auto, auto] => Fa0/1 [auto, auto]
  Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
  Layer 2 trace completed.
```

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

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

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

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

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

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

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

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

# traceroute mac ip

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

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

## Syntax Description

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

## Command Default

No default behavior or values.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E | This command was introduced. |

## Usage Guidelines

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

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

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

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

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

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

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

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

This feature is not supported in Token Ring VLANs.

## Examples

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

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

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

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

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

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

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

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

# type

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

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

## Syntax Description

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

## Command Default

No default behavior or values.

## Command Modes

Boot loader

## Command History

| Release | Modification |
|---|---|
| Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E | This command was introduced. |

## Usage Guidelines

Filenames and directory names are case sensitive.

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

## Examples

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

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

# unset

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

**unset** *variable...*

## Syntax Description

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

## Command Default

No default behavior or values.

## Command Modes

Boot loader

## Command History

| Release | Modification |
|---|---|
| Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E | This command was introduced. |

## Usage Guidelines

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

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

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

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

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

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

### Example

This example shows how to unset the SWITCH_PRIORITY environment variable:

```
Device: unset SWITCH_PRIORITY
```

# version

To display the boot loader version, use the **version** command in boot loader mode.

**version**

## Syntax Description

This command has no arguments or keywords.

## Command Default

No default behavior or values.

## Command Modes

Boot loader

## Command History

| Release | Modification |
|---|---|
| Cisco IOS Release 15.0(2)EXCisco IOS Release 15.2(5)E | This command was introduced. |

## Examples

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

```
Device: version
C2960X Boot Loader (C2960X-HBOOT-M) Version 15.0(2r)EX, RELEASE SOFTWARE (fc1)
Compiled Wed 15-May-13 21:39 by rel
```