System Management Commands

- archive download-sw, on page 3
- archive tar, on page 6
- archive upload-sw, on page 10
- boot, on page 12
- boot buffersize, on page 13
- boot enable-break, on page 14
- boot host dhcp, on page 15
- boot host retry timeout, on page 16
- boot manual, on page 17
- boot system, on page 18
- cat, on page 19
- clear logging onboard, on page 20
- clear mac address-table, on page 21
- clear mac address-table move update, on page 22
- copy, on page 23
- debug matm move update, on page 24
- delete, on page 25
- dir, on page 26
- dying-gasp, on page 28
- help, on page 29
- hw-module, on page 30
- ip name-server, on page 32
- logging, on page 34
- logging buffered, on page 35
- logging console, on page 36
- logging file flash, on page 37
- logging history, on page 38
- logging history size, on page 39
- logging monitor, on page 40
- logging trap, on page 41
- mac address-table aging-time, on page 42
- mac address-table learning vlan, on page 43
- mac address-table notification, on page 45

- mac address-table static, on page 46
- mkdir, on page 47
- more, on page 48
- nmsp notification interval, on page 49
- rename, on page 51
- reset, on page 52
- rmdir, on page 53
- service sequence-numbers, on page 54
- set, on page 55
- show archive sw-upgrade history, on page 58
- show boot, on page 59
- show cable-diagnostics tdr, on page 61
- show dying-gasp, on page 63
- show mac address-table, on page 64
- show mac address-table address, on page 65
- show mac address-table aging-time, on page 66
- show mac address-table count, on page 67
- show mac address-table dynamic, on page 68
- show mac address-table interface, on page 69
- show mac address-table learning, on page 70
- show mac address-table move update, on page 71
- show mac address-table multicast, on page 72
- show mac address-table notification, on page 73
- show mac address-table static, on page 75
- show mac address-table vlan, on page 76
- show nmsp, on page 77
- show logging onboard , on page 78
- shutdown, on page 80
- test cable-diagnostics tdr, on page 81
- traceroute mac, on page 82
- traceroute mac ip, on page 85
- type, on page 87
- unset, on page 88
- version, on page 90

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.
/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 15.2(7)E1	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.

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 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
```

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. *source-url*—Specifies the source URL alias for the local 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 from which to extract. **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 15.2(7)E1	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)
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
<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: • 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** • Secure Copy Protocol (SCP): **scp:** [[*//username*@*location*] */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 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 15.2(7)E1	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 stack member 3 to a TFTP server at 172.20.140.2:

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

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 15.2(7)E1	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 15.2(7)E1	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:

```
Device(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 15.2(7)E1	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 15.2(7)E1	This command was introduced.

Example

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

```
Device(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 15.2(7)E1	This command was introduced.

Example

This example sets the timeout to 300 seconds:

```
Device(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 15.2(7)E1	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 15.2(7)E1	This command was introduced.

Example

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

```
Device(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 15.2(7)E1	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 15.2(7)E1	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:

```
Device# 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 15.2(7)E1	This command was introduced.

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

```
Device# 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 15.2(7)E1	This command was introduced.

Example

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

```
Device# 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.

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 15.2(7)E1	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 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 15.2(7)E1	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 15.2(7)E1	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 15.2(7)E1	This command was introduced.

Usage Guidelines

Directory names are case sensitive.

Examples

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

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

   96453632 bytes available (25732096 bytes used)
```

Table 1: dir Field Descriptions

Field	Description
2	Index number of the file.

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

dying-gasp

To enable dying gasp notifications, use the **dying-gasp** command in global configuration mode. To disable dying gasp notifications, use the **no** form of this command.

dying-gasp primary { **ethernet-oam** | **snmp-trap** | **syslog** } **secondary** { **ethernet-oam** | **snmp-trap** | **syslog** }

no dying-gasp

Syntax Description

primary	Enables dying gasp primary notifications.
ethernet-oam	Enables Ethernet-OAM notifications.
snmp-trap	Enables trap notifications sent to SNMP server.
syslog	Enables system logger.
secondary	Enables dying gasp secondary notifications.

Command Default

Dying gasp notifications are disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
Cisco IOS Release 15.2(7)E2	This command was introduced.

Usage Guidelines

The **ethernet-oam** keyword is not supported on Catalyst 1000 Series Switches.

Examples

The following example shows how to configure SNMP traps as primary notification and syslog as secondary notification:

```
Device> enable
Device# configure terminal
Device(config)# dying-gasp primary snmp-traps secondary syslog
```

Related Commands

Command	Description
show dying-gasp	Displays dying gasp configuration.

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 15.2(7)E1	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 member switch 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 15.2(7)E1	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 stack members 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 stack member 4 are stored in the flash memory when this command is entered on the active switch:

```
Device(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:

```
Device(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 15.2(7)E1	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
```

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 15.2(7)E1	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:

```
Device(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 15.2(7)E1	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:

```
Device(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 15.2(7)E1	This command was introduced.

Example

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

```
Device(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 15.2(7)E1	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:

```
Device(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 15.2(7)E1	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:

```
Device(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 15.2(7)E1	This command was introduced.

Example

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

```
Device(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 15.2(7)E1	This command was introduced.

Example

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

```
Device(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 15.2(7)E1	This command was introduced.

Example

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

```
Device(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 15.2(7)E1	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 15.2(7)E1	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:

```
Device(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.

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 15.2(7)E1	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 15.2(7)E1	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 15.2(7)E1	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 15.2(7)E1	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 15.2(7)E1	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
```

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 15.2(7)E1	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 15.2(7)E1	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 15.2(7)E1	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 15.2(7)E1	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:

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

Command Default

The environment variables have these default values:

MANUAL_BOOT: No (0)

BOOT: Null string

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

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

PS1 device:

CONFIG_FILE: config.text

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 15.2(7)E1	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 archive sw-upgrade history

To display the software image upgrade and downgrade history on a device, use the **show archive sw-upgrade history** command in privileged EXEC mode.

show archive sw-upgrade history

Command Modes

Privileged EXEC

Command History

Release	Modification
Cisco IOS Release 15.2(7)E3	This command was introduced.

Usage Guidelines

Use the **show archive sw-upgrade history** command to see the history of all software image upgrades and downgrades performed on the device. This command displays the image name, version, upgrade method and timeline for each upgrade that is done through Auto Install, PnP, archive CLI, or HTTP methods. Manual upgrades done through TFTP of tar files or binary files are not displayed.

If you have booted the Cisco IOS software, wait for ten minutes before using this command. This is because the software takes time to initialize after a boot.

Note This command displays the records of only the first 100 successful upgrades or downgrades (performed through Auto Install, PnP, archive CLI, or HTTP methods).

Example

The following example shows a sample output of the **show archive sw-upgrade history** command.

```
Device#show archive sw-upgrade history
File_name                                    Version                    Install Mode/Date
---------------------------------------     --------------
-----------------------------
c1000-universalk9-mz.152-7.1.88.E3.bin       152-7.1.88.E3         download-sw/UTC Mon Jul
 20 2020
c1000-universalk9-mz.152-7.1.86.E3.bin       152-7.1.86.E3                http/UTC Tue Jul
 21 2020
c1000-universalk9-mz.152-7.1.86.E3.bin       152-7.1.86.E3          auto-install/UTC Tue
Jul 23 2020
c1000-universalk9-mz.152-7.1.88.E3.bin       152-7.1.88.E3                 pnp/UTC Tue Jul
 28 2020
```

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 15.2(7)E1	This command was introduced.

Example

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

```
Device# 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. 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. 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. 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 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 15.2(7)E1	This command was introduced.

Usage Guidelines

TDR is supported only on 10/100/1000 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 3: 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: • The cable is properly connected, the link is up, and the interface speed is 1000 Mb/s. • The cable is open. • The cable has a short.
Remote pair	The name of the pair of wires to which the local pair is connected. TDR can learn about the remote pair only when the cable is properly connected and the link is up.
Pair status	The status of the pair of wires on which TDR is running: • Normal—The pair of wires is properly connected. • Not completed—The test is running and is not completed. • Not supported—The interface does not support TDR. • Open—The pair of wires is open . • Shorted—The pair of wires is shorted. • ImpedanceMis—The impedance is mismatched. • Short/Impedance Mismatched—The impedance mismatched or the cable is short. • InProgress—The diagnostic test is in progress.

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

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

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

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

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

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

show dying-gasp

To display dying gasp configuration, use the **show dying-gasp** command in privileged EXEC mode.

dying-gasp primary { **packets** [{ **ethernet-oam** | **snmp-trap** | **syslog** }] | **status** }

Syntax Description

packets	Displays dying gasp packet information.
ethernet-oam	(Optional) Displays dying gasp Ethernet-OAM packet information.
snmp-trap	(Optional) Displays dying gasp SNMP trap packet information.
syslog	(Optional) Displays dying gasp syslog packet information.
status	Displays dying gasp configuration status.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
Cisco IOS Release 15.2(7)E2	This command was introduced.

Usage Guidelines

The **ethernet-oam** keyword is not supported on Catalyst 1000 Series Switches.

Examples

The following is a sample output of the **show dying-gasp** command:

```
Device# show dying-gasp

Dying Gasp Configuration
SNMP Trap Enabled
Syslog Disabled
Ethernet OAM Disabled
```

The following is a sample output of the **show dying-gasp packets snmp-trap** command:

```
Device# show dying-gasp packets snmp-trap

SNMP Trap packet for server 10.1.1.2, link type IP
Interface, via GigabitEthernet1/0/0, local IP address 10.2.2.9
Encap type is ARPA, local hardware address 0022.bdd4.2f48
Next hop IP address 10.2.2.8, next hop hardware address 0000.0c07.ac09
SNMP Trap packet for server 10.1.1.4, link type IP
Interface, via GigabitEthernet1/0/1, local IP address 10.2.2.7
Encap type is ARPA, local hardware address 0012.001a.2f08
Next hop IP address 10.2.2.8, next hop hardware address 0cd0.0c02.ac10
```

Related Commands

Command	Description
dying-gasp	Enables dying gasp notifications.

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 15.2(7)E1	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:

```
Device# 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 15.2(7)E1	This command was introduced.

Example

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

```
Device# 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 15.2(7)E1	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:

```
Device# 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:

```
Device# 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 15.2(7)E1	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:

```
Device# 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 15.2(7)E1	This command was introduced.

Example

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

```
Device# 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 15.2(7)E1	This command was introduced.

Example

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

```
Device# 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 15.2(7)E1	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:

```
Device# 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 15.2(7)E1	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 15.2(7)E1	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:

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

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

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

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

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

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 15.2(7)E1	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:

```
Device# 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 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 15.2(7)E1	This command was introduced.

Example

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

```
Device# 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 15.2(7)E1	This command was introduced.

Example

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

```
Device# 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 15.2(7)E1	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 logging onboard

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

show logging onboard *switch-number*{**clilog** | **continuous** | **end** | **environment** | **message** | **module** | **poe** | **raw** | **start** | **status** | **summary** | **temperature** | **uptime** | **voltage**}

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.
continuous	Displays onboard logging continuous information.
detail	Displays detailed onboard logging information.
end	Displays ending time and date details.
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.
module	Specifies an individual module in the system.
poe	Displays POE details of standalone switch or the specified switch stack members.
raw	Displays onboard logging raw information.
start	Specifies starting time and date details.
status	Displays the status of a standalone switch or the specified stack members.
summary	Displays the onboard logging status information.
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.

Command Modes

Priviledged EXEC

Command History

Release	Modification
Cisco IOS Release 15.2(7)E1	This command was introduced.

Example

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

```
Device# show logging onboard 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.

```
Device# show logging onboard environment
```

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

```
Device# show logging onboard message
```

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

```
Device# show logging onboard 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.

```
Device# show logging onboard uptime
```

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

```
Device# show logging onboard voltage
```

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

```
Device# 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 15.2(7)E1	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 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 15.2(7)E1	This command was introduced.

Usage Guidelines

TDR is supported only on 10/100/1000 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 15.2(7)E1	This command was introduced.

Usage Guidelines

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

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

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

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

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

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

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

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

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

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

This feature is not supported in Token Ring VLANs.

Examples

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

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

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

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

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

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

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

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

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

```
Device# traceroute mac 0000.0011.1111 0000.0201.0201
  Error:Source Mac address not found.
  Layer2 trace 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 devices 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 15.2(7)E1	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 15.2(7)E1	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 boots automatically or manually.
	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 15.2(7)E1	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 15.2(7)E1	This command was introduced.

Examples

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

```
Device:version
C1000 Boot Loader (C1000-HBOOT-M) Version 15.2(7r)E, RELEASE SOFTWARE (fc1)
Compiled
```