software clean

To remove any and all packages and provisioning files that are no longer in use, use the **software clean** command in Privileged EXEC mode.

software clean[**file***file url*][**switch***nodes*] [**verbose**]

Syntax Description

file*file url*	Full path to wildcarded filename(s). Optional when running in installed mode. When no command options are specified, all unused package, bundle and provisioning files in the current boot directory will be cleaned.
switch*nodes*	(optional) Specifies which switch(es) should perform the clean operation using '1,2,4' and/or '2-4' notation. Default is all switches in the stack.
verbose	(optional) provides some additional info in the log files .

Command Default

No software package(s) will be cleaned by default.

Command Modes

Privileged EXEC

Command History

Release	Modification
IOS XE 3.2.0 SE	Command introduced.

Usage Guidelines

If no specific file to be deleted is indicated, the installer will search for unused packages and provisioning files on a given media device (eg., bootflash:, usb0: etc) to delete. One or more nodes may be given.

With no options specified for **software clean**, all unused packages and provisioning files on the currently booted device will be cleaned. The currently booted device is where the committed `packages.conf` file resides.

Examples

This example uses the 'software clean' command with no command options to clean the current boot directory, flash:, on a standalone switch that is running in installed mode.

```
infra-p2-3#dir flash:
Directory of flash:/

 7378  -rwx     2097152  Nov 15 2012 09:45:11 +00:00  nvram_config
 7379  drwx        4096  Nov 15 2012 09:19:24 +00:00  mnt
 7396  -rwx        1244  Nov 14 2012 18:32:55 +00:00  packages.conf.00-
 7390  -rwx    74390300  Nov 15 2012 09:18:17 +00:00  cat3k_caa-base.SSA.03.09.17.EMP.pkg
 7383  -rwx    74601776  Nov 14 2012 18:31:59 +00:00  cat3k_caa-base.SSA.03.09.16.EMD.pkg
 7384  -rwx     2732724  Nov 14 2012 18:32:08 +00:00  cat3k_caa-drivers.SSA.
03.09.16.EMD.pkg
 7385  -rwx    49886128  Nov 14 2012 18:32:02 +00:00  cat3k_caa-infra.SSA.03.09.16.EMD.pkg
 7387  -rwx    30579500  Nov 14 2012 18:32:05 +00:00  cat3k_caa-iosd-universalk9.SSA.
150-9.16.EMD.pkg
 7386  -rwx         556   Nov 9 2012 09:58:21 +00:00  vlan.dat
 7389  -rwx    62814928  Nov 14 2012 18:32:08 +00:00  cat3k_caa-wcm.SSA.03.09.16.EMD.pkg
 7388  -rwx    18193120  Nov 14 2012 18:32:03 +00:00  cat3k_caa-platform.SSA.
03.09.16.EMD.pkg
 7397  -rwx        1243  Nov 15 2012 09:18:55 +00:00  packages.conf
 7391  -rwx     2734772  Nov 15 2012 09:18:17 +00:00  cat3k_caa-drivers.SSA.
03.09.17.EMP.pkg
 7392  -rwx    32465772  Nov 15 2012 09:18:24 +00:00  cat3k_caa-infra.SSA.03.09.17.EMP.pkg
 7393  -rwx    30384940  Nov 15 2012 09:18:35 +00:00  cat3k_caa-iosd-universalk9.SSA.
150-9.17.EMP.pkg
 7394  -rwx    18143968  Nov 15 2012 09:18:39 +00:00  cat3k_caa-platform.SSA.
03.09.17.EMP.pkg
 7395  -rwx    62638800  Nov 15 2012 09:18:51 +00:00  cat3k_caa-wcm.SSA.03.09.17.EMP.pkg

712413184 bytes total (208535552 bytes free)
infra-p2-3#
infra-p2-3#software clean
Preparing clean operation ...
[2]: Cleaning up unnecessary package files
[2]: No path specified, will use booted path flash:packages.conf
[2]: Cleaning flash:
[2]: Preparing packages list to delete ...
    cat3k_caa-base.SSA.03.09.17.EMP.pkg
        File is in use, will not delete.
    cat3k_caa-drivers.SSA.03.09.17.EMP.pkg
        File is in use, will not delete.
    cat3k_caa-infra.SSA.03.09.17.EMP.pkg
        File is in use, will not delete.
    cat3k_caa-iosd-universalk9.SSA.150-9.17.EMP.pkg
        File is in use, will not delete.
    cat3k_caa-platform.SSA.03.09.17.EMP.pkg
        File is in use, will not delete.
    cat3k_caa-wcm.SSA.03.09.17.EMP.pkg
        File is in use, will not delete.
    packages.conf
        File is in use, will not delete.
[2]: Files that will be deleted:
    cat3k_caa-base.SSA.03.09.16.EMD.pkg
    cat3k_caa-drivers.SSA.03.09.16.EMD.pkg
    cat3k_caa-infra.SSA.03.09.16.EMD.pkg
    cat3k_caa-iosd-universalk9.SSA.150-9.16.EMD.pkg
    cat3k_caa-platform.SSA.03.09.16.EMD.pkg
    cat3k_caa-wcm.SSA.03.09.16.EMD.pkg
    packages.conf.00-

[2]: Do you want to proceed with the deletion? [yes/no]: y
[2]: Clean up completed
```

```
infra-p2-3#
infra-p2-3#dir flash:
Directory of flash:/

 7378  -rwx     2097152  Nov 15 2012 09:45:11 +00:00  nvram_config
 7379  drwx        4096  Nov 15 2012 09:19:24 +00:00  mnt
 7390  -rwx    74390300  Nov 15 2012 09:18:17 +00:00  cat3k_caa-base.SSA.03.09.17.EMP.pkg
 7386  -rwx         556   Nov 9 2012 09:58:21 +00:00  vlan.dat
 7397  -rwx        1243  Nov 15 2012 09:18:55 +00:00  packages.conf
 7391  -rwx     2734772  Nov 15 2012 09:18:17 +00:00  cat3k_caa-drivers.SSA.
03.09.17.EMP.pkg
 7392  -rwx    32465772  Nov 15 2012 09:18:24 +00:00  cat3k_caa-infra.SSA.03.09.17.EMP.pkg
 7393  -rwx    30384940  Nov 15 2012 09:18:35 +00:00  cat3k_caa-iosd-universalk9.SSA.
150-9.17.EMP.pkg
 7394  -rwx    18143968  Nov 15 2012 09:18:39 +00:00  cat3k_caa-platform.SSA.
03.09.17.EMP.pkg
 7395  -rwx    62638800  Nov 15 2012 09:18:51 +00:00  cat3k_caa-wcm.SSA.03.09.17.EMP.pkg

712413184 bytes total (447623168 bytes free)
infra-p2-3#
```

Related Commands

Command	Description
software install file	Install Cisco IOS XE files.
software commit	Use this command to commit a package set that was installed using the **auto-rollback** command option of the **software install** command.
software expand	Use this command to expand individual IOS XE Software packages and the provisioning file from a specified bundle to a specific destination directory.
software install source switch	Use this command to install the running IOS XE software packages from one stack member to one or more other stack members.
software rollback	Use this command to roll back the committed Cisco IOS XE Software to a previous installation point.

software commit

To commit a package set that was installed using the **auto-rollback** command option of the **software install** command, use the **software commit** command in Privileged EXEC mode.

software commit[**switch***node*] [**verbose**]

Syntax Description

switch*nodes*	(optional) specifies which switch(es) should perform the commit operation using '1,2,4' and/or '2-4' notation. Default is all switches in the stack
verbose	(optional) provides some additional info in the log files

Command Default

No software package(s) will be committed by default.

Command Modes

Privileged EXEC

Command History

Release	Modification
IOS XE 3.2.0 SE	Command introduced.

Usage Guidelines

The **software commit** command cancels the rollback timer, if it is running, and commits a software upgrade. A commit makes an upgrade, ie. a package set, persistent. A committed package set will run after a node is reloaded.

Examples

This example uses the 'software install file' command with the 'auto-rollback' command option to install the bundle onto both switches in a stack via tftp . After the switches reload with the new software, the 'software commit' command is used to stop the rollback timer and commit the candidate package set.

```
infra-p2-3#software install file tftp://172.19.211.47/cat3k_caa-universalk9.SSA.
03.09.19.EMP.150-9.19.EMP.bin auto-rollback 45
Preparing install operation ...
[2]: Downloading file tftp://172.19.211.47/cat3k_caa-universalk9.SSA.03.09.19.EMP.
150-9.19.EMP.bin to active switch 2
[2]: Finished downloading file tftp://172.19.211.47/cat3k_caa-universalk9.SSA.
03.09.19.EMP.150-9.19.EMP.bin to active switch 2
[2]: Copying software from active switch 2 to switch 1
[2]: Finished copying software to switch 1
[1 2]: Starting install operation
[1 2]: Expanding bundle cat3k_caa-universalk9.SSA.03.09.19.EMP.150-9.19.EMP.bin
[1 2]: Copying package files
[1 2]: Package files copied
[1 2]: Finished expanding bundle cat3k_caa-universalk9.SSA.03.09.19.EMP.150-9.19.EMP.bin
[1 2]: Verifying and copying expanded package files to flash:
[1 2]: Verified and copied expanded package files to flash:
[1 2]: Starting compatibility checks
[1 2]: Finished compatibility checks
[1 2]: Starting application pre-installation processing
[1 2]: Finished application pre-installation processing
[1]: Old files list:
    Removed cat3k_caa-base.SSA.03.09.17.EMP.pkg
    Removed cat3k_caa-drivers.SSA.03.09.17.EMP.pkg
    Removed cat3k_caa-infra.SSA.03.09.17.EMP.pkg
    Removed cat3k_caa-iosd-universalk9.SSA.150-9.17.EMP.pkg
    Removed cat3k_caa-platform.SSA.03.09.17.EMP.pkg
    Removed cat3k_caa-wcm.SSA.03.09.17.EMP.pkg
[2]: Old files list:
    Removed cat3k_caa-base.SSA.03.09.17.EMP.pkg
    Removed cat3k_caa-drivers.SSA.03.09.17.EMP.pkg
    Removed cat3k_caa-infra.SSA.03.09.17.EMP.pkg
    Removed cat3k_caa-iosd-universalk9.SSA.150-9.17.EMP.pkg
    Removed cat3k_caa-platform.SSA.03.09.17.EMP.pkg
    Removed cat3k_caa-wcm.SSA.03.09.17.EMP.pkg
[1]: New files list:
    Added cat3k_caa-base.SSA.03.09.19.EMP.pkg
    Added cat3k_caa-drivers.SSA.03.09.19.EMP.pkg
    Added cat3k_caa-infra.SSA.03.09.19.EMP.pkg
    Added cat3k_caa-iosd-universalk9.SSA.150-9.19.EMP.pkg
    Added cat3k_caa-platform.SSA.03.09.19.EMP.pkg
    Added cat3k_caa-wcm.SSA.03.09.19.EMP.pkg
[2]: New files list:
    Added cat3k_caa-base.SSA.03.09.19.EMP.pkg
    Added cat3k_caa-drivers.SSA.03.09.19.EMP.pkg
    Added cat3k_caa-infra.SSA.03.09.19.EMP.pkg
    Added cat3k_caa-iosd-universalk9.SSA.150-9.19.EMP.pkg
    Added cat3k_caa-platform.SSA.03.09.19.EMP.pkg
    Added cat3k_caa-wcm.SSA.03.09.19.EMP.pkg
[1 2]: Creating pending provisioning file
[1 2]: Finished installing software.  New software will load on reboot.
[1 2]: Setting rollback timer to 45 minutes

[1 2]: Do you want to proceed with reload? [yes/no]: y
[1]: Reloading
[2]: Pausing before reload
*Nov 15 10:24:24.891: %STACKMGR-1-RELOAD_REQUEST: 2 stack-mgr:  Received reload request
for switch 1, reason User requested reload
*Nov 15 10:24:25.051: %STACKMGR-1-STACK_LINK_CHANGE: 2 stack-mgr:  Stack port 2 on switch
2 is down
*Nov 15 10:24:25.051: %STACKMGR-1-SWITCH_REMOVED: 2 stack-mgr:  Switch 1 has been removed
from the stack
*Nov 15 10:24:25.146: %REDUNDANCY-3-STANDBY_LOST: Standby processor fault
(PEER_NOT_PRESENT)
*Nov 15 10:24:25.146: %REDUNDANCY-5-PEER_MONITOR_EVENT: Active detected a standby removal
(raw-event=PEER_NOT_PRESENT(3))

*Nov 15 10:24:25.146: %REDUNDANCY-3-STANDBY_LOST: Standby processor fault (PEER_DOWN)
*Nov 15 10:24:25.146: %REDUNDANCY-5-PEER_MONITOR_EVENT: Active detected standby down or
crashed (raw-event=PEER_DOWN(2))
```

```
*Nov 15 10:24:25.146: %REDUNDANCY-3-STANDBY_LOST: Standby processor fault
(PEER_REDUNDANCY_STATE_CHANGE)
*Nov 15 10:24:25.146: %REDUNDANCY-5-PEER_MONITOR_EVENT: Active detected a standby removal
(raw-event=PEER_REDUNDANCY_STATE_CHANGE(5))

*Nov 15 10:24:27.054: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/1, changed state to
down
*Nov 15 10:24:28.057: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet1/0/1, changed state to down
[2]: Reloading

infra-p2-3#
*Nov 15 10:24:39.911: %STACKMGR-1-RELOAD_REQUEST: 2 stack-mgr:  Received reload request
for switch 2, reason User requested reload
*Nov 15 10:24:39.912: %STACKMGR-1-RELOAD: 2 stack-mgr:  reloading due to reason User
requested reload
*Nov 15 10:24:40.423: %IOSXE-3-PLATFORM: 2 process sysmgr: Reset/Reload requested by
[stack-manager].

< Switches were reloaded and booted with the newly installed software>

*Nov 15 10:34:21.345: %AUTHMGR_SPI-6-START: Auth Manager SPI server started (infra-p2-3-1)
*Nov 15 10:34:24.612: %HA_CONFIG_SYNC-6-BULK_CFGSYNC_SUCCEED: Bulk Sync succeeded
*Nov 15 10:34:24.624: %RF-5-RF_TERMINAL_STATE: Terminal state reached for (SSO)
*Nov 15 10:34:24.510: %SSH-5-DISABLED: SSH 1.99 has been disabled (infra-p2-3-1)
*Nov 15 10:34:24.511: %SSH-5-ENABLED: SSH 1.99 has been enabled (infra-p2-3-1)
infra-p2-3#
infra-p2-3#show software installer rollback-timer
Switch#     Status      Duration
---------------------------------
1           active      00:31:28
2           active      00:31:43

infra-p2-3#
infra-p2-3#software commit
Preparing commit operation ...
[1 2]: Starting commit operation
[1 2]: Finished committing software changes.


infra-p2-3#
infra-p2-3#show software installer rollback-timer
Switch#     Status      Duration
---------------------------------
1           inactive       -
2           inactive       -

infra-p2-3#
```

Related Commands

Command	Description
software clean	Use this command to remove any and all packages and provisioning files that are no longer in use.
software install file	Install Cisco IOS XE files.
software expand	Use this command to expand individual IOS XE Software packages and the provisioning file from a specified bundle to a specific destination directory.

Command	Description
software install source switch	Use this command to install the running IOS XE software packages from one stack member to one or more other stack members.
software rollback	Use this command to roll back the committed Cisco IOS XE Software to a previous installation point.

software expand

To expand individual IOS XE Software packages and the provisioning file from a specified bundle to a specific destination directory, use the **software expand** command in Privileged EXEC mode.
To expand the individual IOS XE Software packages and the provisioning file from the running bundle, use the **software expand running** command in Privileged EXEC mode.

software expand {**file** *source url* | **running**}[**to***destination url*] [**switch***nodes*][**verbose**]

Syntax Description

file*source url*	URL of the bundle to be expanded. If a network URL is specified, the **to** keyword must also be used to specify the destination location. The **file** and **running** keywords are mutually exclusive
running	Specifies that the packages from the running bundle should be expanded . The **to** keyword must also be used to specify the destination location . The **file** and **running** keywords are mutually exclusive . The running command option is not allowed when running in installed mode.

to*destination url*	Specifies the local or UFS directory where the expanded bundle contents are copied to. **Note** If this option is not entered, the contents are extracted into the same directory as the source bundle. This keyword is mandatory when the source URL is a network URL, and also when the **running** keyword is used .
switch*nodes*	(optional) Specifies which switch(es) should perform the expand operation using '1,2,4' and/or '2-4' notation. Default is all switches in the stack.
verbose	(optional) provides some additional info in the log files

Command Default

Command is used to expand an IOS XE software bundle. The contents are extracted into the same directory as the source bundle by default.

Command Modes

Privileged EXEC

Command History

Release	Modification
IOS XE 3.2.0 SE	Command introduced.

Usage Guidelines

If the **to** option is not entered, the contents will be extracted into the default installation location for the platform.

The bundle file is unchanged after the operation is complete.

Examples

This example uses the following steps to prepare a switch for booting in installed mode, i.e., booting a package provisioning file (packages.conf)

1. Boot in bundle mode using 'boot flash:<bundle name>' Can also boot from usbflash0 : or via tftp

```
switch: b tftp://172.19.211.47/cat3k_caa-universalk9.SSA.03.09.17.EMP.150-9.17.EMP.bin
Reading full image into
memory.....................................................................................
```

```
.....................................................................................
.....................................done
Nova Bundle Image
--------------------------------------
Kernel Address    : 0x6042fef4
Kernel Size       : 0x317ccc/3243212
Initramfs Address : 0x60747bc0
Initramfs Size    : 0xdbf2f9/14414585
Compression Format: .mzip

Bootable image at @ ram:0x6042fef4
Bootable image segment 0 address range [0x81100000, 0x81b80000] is in range [0x80180000,
0x90000000].
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
File "tftp://172.19.211.47/cat3k_caa-universalk9.SSA.03.09.17.EMP.150-9.17.EMP.bin"
uncompressed and installed, entry point: 0x811060f0
Loading Linux kernel with entry point 0x811060f0 ...
Bootloader: Done loading app on core_mask: 0xf

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

All packages are Digitally Signed
Starting System Services

:
:

*Nov 15 10:49:35.746: %LINEPROTO-5-UPDOWN: Line protocol on Interface
TenGigabitEthernet2/1/1, changed state to down
*Nov 15 10:49:35.746: %LINEPROTO-5-UPDOWN: Line protocol on Interface
TenGigabitEthernet2/1/2, changed state to down
*Nov 15 10:49:36.822: %LINK-3-UPDOWN: Interface GigabitEthernet2/0/1, changed state to up
infra-p2-3>
infra-p2-3>enable
infra-p2-3#
```

2. Use the 'software clean file flash:' command to remove any unused package, bundle and provisioning files from flash:

```
infra-p2-3#software clean file flash:
Preparing clean operation ...
[2]: Cleaning up unnecessary package files
[2]: Preparing packages list to delete ...
[2]: Files that will be deleted:
    cat3k_caa-base.SSA.03.09.19.EMP.pkg
    cat3k_caa-drivers.SSA.03.09.19.EMP.pkg
    cat3k_caa-infra.SSA.03.09.19.EMP.pkg
    cat3k_caa-iosd-universalk9.SSA.150-9.17.EMP.pkg
    cat3k_caa-iosd-universalk9.SSA.150-9.19.EMP.pkg
    cat3k_caa-platform.SSA.03.09.19.EMP.pkg
    cat3k_caa-wcm.SSA.03.09.19.EMP.pkg
    packages.conf

[2]: Do you want to proceed with the deletion? [yes/no]: yes
[2]: Clean up completed


infra-p2-3#
```

3. Use the 'software expand running to flash:' command to expand the running bundle to flash:

```
infra-p2-3#software expand running to flash:
Preparing expand operation ...
[2]: Expanding the running bundle
[2]: Copying package files
[2]: Package files copied
[2]: Finished expanding the running bundle


infra-p2-3#
infra-p2-3#dir flash:
Directory of flash:/

 7378  -rwx     2097152  Nov 15 2012 10:49:37 +00:00  nvram_config
```

```
14753  drwx        4096  Nov 15 2012 10:20:27 +00:00  mnt
 7381  -rw-    74390300  Nov 15 2012 10:54:24 +00:00  cat3k_caa-base.SSA.03.09.17.EMP.pkg
 7382  -rw-     2734772  Nov 15 2012 10:54:24 +00:00  cat3k_caa-drivers.SSA.
03.09.17.EMP.pkg
 7383  -rw-    32465772  Nov 15 2012 10:54:24 +00:00  cat3k_caa-infra.SSA.03.09.17.EMP.pkg
 7384  -rw-    30384940  Nov 15 2012 10:54:24 +00:00  cat3k_caa-iosd-universalk9.SSA.
150-9.17.EMP.pkg
 7385  -rw-    18143968  Nov 15 2012 10:54:24 +00:00  cat3k_caa-platform.SSA.
03.09.17.EMP.pkg
 7380  -rw-        1243  Nov 15 2012 10:55:03 +00:00  packages.conf
 7386  -rwx         556   Nov 9 2012 09:58:21 +00:00  vlan.dat
 7387  -rw-    62638800  Nov 15 2012 10:54:24 +00:00  cat3k_caa-wcm.SSA.03.09.17.EMP.pkg

712413184 bytes total (447627264 bytes free)
infra-p2-3#
```

4. Reload the switch

```
infra-p2-3#reload
Reload command is being issued on Active unit, this will reload the whole stack
Proceed with reload? [confirm]

*Nov 15 10:56:35.800: %SYS-5-RELOAD: Reload requested by console. Reload Reason: Reload
command.
*Nov 15 10:56:36.569: %STACKMGR-1-RELOAD_REQUEST: 2 stack-mgr:  Received reload request
for
all switches, reason Reload command
*Nov 15 10:56:36.570: %STACKMGR-1-RELOAD: 2 stack-mgr:  reloading due to reason Reload
command
*Nov 15 10:56:37.071: %IOSXE-3-PLATFORM: 2 process sysmgr: Reset/Reload requested by
[stack-manager].
<Thu Nov 15 10:56:37 2012> Message from sysmgr: Reset Reason:Reset/Reload requested by
[stack-manager]. [Reload command]
```

5. Boot the installed packages using 'boot flash:packages.conf '

```
switch: boot flash:packages.conf
Getting rest of image
Reading full image into memory....done
Reading full base package into memory...: done = 74390300
Nova Bundle Image
--------------------------------------
Kernel Address    : 0x6042f354
Kernel Size       : 0x317ccc/3243212
Initramfs Address : 0x60747020
Initramfs Size    : 0xdbf2f9/14414585
Compression Format: .mzip

Bootable image at @ ram:0x6042f354
Bootable image segment 0 address range [0x81100000, 0x81b80000] is in range
[0x80180000, 0x90000000].
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
boot_system: 377
Loading Linux kernel with entry point 0x811060f0 ...
Bootloader: Done loading app on core_mask: 0xf

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

All packages are Digitally Signed
Starting System Services

:
:

*Nov 15 11:05:23.202: %LINEPROTO-5-UPDOWN: Line protocol on Interface
TenGigabitEthernet2/1/1, changed state to down
*Nov 15 11:05:23.202: %LINEPROTO-5-UPDOWN: Line protocol on Interface
TenGigabitEthernet2/1/2, changed state to down
*Nov 15 11:05:24.286: %LINK-3-UPDOWN: Interface GigabitEthernet2/0/1, changed state to up
infra-p2-3>
```

Related Commands

Command	Description
software clean	Use this command to remove any and all packages and provisioning files that are no longer in use.
software install file	Install Cisco IOS XE files.
software commit	Use this command to commit a package set that was installed using the **auto-rollback** command option of the **software install** command.
software install source switch	Use this command to install the running IOS XE software packages from one stack member to one or more other stack members.
software rollback	Use this command to roll back the committed Cisco IOS XE Software to a previous installation point.

software install file

To install IOS XE Software files, use the **software install file** command in Privileged EXEC mode.

software install file *bundle url* [**switch***nodes*] [**auto-rollback***minutes*][**force**][**on-reboot**] [**provisioning-file***provisioning-file url*][**force**][**new**][**verbose**]

Syntax Description

file *bundle url*	Specify the url of the bundle file to be installed.
switch*nodes*	(optional) Specifies which switch(es) should perform the install operation using '1,2,4' and/or '2-4' notation. Default is all switches in the stack.
auto-rollback*minutes*	(optional) Used to start the rollback timer for the specified number of minutes. If not used, the software is automatically committed after installation. A value to zero means the rollback timer is never started and the software is not automatically committed (need to use 'software commit '). If set to another value, the 'software commit' command must be used to commit the software before the timer expires (else it will automatically rollback to the original software).

on-reboot	(optional) Indicates that the user should not prompted to reload when the installation operation completes. The user must then use the reload command to boot the system with the newly installed packages.
provisioning-file*provisioning-file url*	(optional) Specifies the provisioning file to be updated by the installation. Default is the running provisioning file. Valid locations are flash: or usbflash0:
force	(optional) Specifies that the operation will be forced. Forced means that the installation will proceed despite any remote package incompatibilities. Force should not generally be required, and should be used with caution. Local package compatibility checks are enforced regardless of this command option.
new	(optional) Indicates that the post-install package set should contain only the packages being installed. Without this option, the post-install package set is a merged set of the currently installed software and the new packages being installed.
verbose	(optional) provides some additional info in the log files

Command Default Command is used to install IOS XE software. No software will be installed by default.

Command Modes Privileged EXEC

Command History

Release	Modification
IOS XE 3.2.0 SE	Command introduced.

Usage Guidelines

The **software install file** command is used to install package files from a software bundle when the system is running in installed mode. By default, the command will install software on all nodes in the system.

The following tasks are performed during the **software install file** operation.

- For a network installation, download the specified software bundle into memory on the active node (or standalone node is a standalone system).

- In a multi-node system, copy the software bundle to each node if the file does not already exist on the node. If installing a bundle that resides in local media on the active node (flash: or usbflash0:), the bundle file (.bin) is copied to the corresponding local device on each node. If installing a bundle via the network, the bundle is copied to memory on each node in the system.

- Expand the package files from the specified bundle into flash: on each node after verifying each package's digital signature

- Perform compatibility checks on all nodes in the system to ensure that the software running on all nodes after installation will be compatible. This task is skipped if the **force** command option is used.

- Start the auto-rollback timer if the **auto-rollback** command option was used. The newly installed packages will be automatically rolled back if the auto-rollback timer expires before the 'software commit' command is issued.

- Update the package provisioning file (packages.conf) and save a copy of the original provisioning file for use during auto-rollback or user-initiated rollback (**software rollback** command).

- Commit the newly installed software packages if the **auto-rollback** command option was not used.

- Prompt the user to reload (if the **on-reboot** command option was not used).

Note The **software install file** command cannot be used if the system is running in bundle mode. In this case, the **software expand** command can be used to prepare the system to boot in installed mode.

Examples

The following example installs the cat3k_caa-universalk9.SSA.03.09.19.EMP.150-9.19.EMP.bin bundle from a tftp server. The bundle is first downloaded to RAM, then the package files included in the bundle are extracted and copied to flash:. The .bin file itself is not copied to flash:.

Note You need IOSd IP connectivity to install via tftp .

```
infra-p2-3#software install file tftp://172.19.211.47/
cat3k_caa-universalk9.SSA.03.09.19.EMP.150-9.19.EMP.bin
Preparing install operation ...
[2]: Downloading file tftp://172.19.211.47/
cat3k_caa-universalk9.SSA.03.09.19.EMP.150-9.19.EMP.bin to active switch 2
[2]: Finished downloading file tftp://172.19.211.47/
cat3k_caa-universalk9.SSA.03.09.19.EMP.150-9.19.EMP.bin to active switch 2
[2]: Starting install operation
[2]: Expanding bundle cat3k_caa-universalk9.SSA.03.09.19.EMP.150-9.19.EMP.bin
```

```
[2]: Copying package files
[2]: Package files copied
[2]: Finished expanding bundle cat3k_caa-universalk9.SSA.03.09.19.EMP.150-9.19.EMP.bin
[2]: Verifying and copying expanded package files to flash:
[2]: Verified and copied expanded package files to flash:
[2]: Starting compatibility checks
[2]: Finished compatibility checks
[2]: Starting application pre-installation processing
[2]: Finished application pre-installation processing
[2]: Old files list:
    Removed cat3k_caa-base.SSA.03.09.17.EMP.pkg
    Removed cat3k_caa-drivers.SSA.03.09.17.EMP.pkg
    Removed cat3k_caa-infra.SSA.03.09.17.EMP.pkg
    Removed cat3k_caa-iosd-universalk9.SSA.150-9.17.EMP.pkg
    Removed cat3k_caa-platform.SSA.03.09.17.EMP.pkg
    Removed cat3k_caa-wcm.SSA.03.09.17.EMP.pkg
[2]: New files list:
    Added cat3k_caa-base.SSA.03.09.19.EMP.pkg
    Added cat3k_caa-drivers.SSA.03.09.19.EMP.pkg
    Added cat3k_caa-infra.SSA.03.09.19.EMP.pkg
    Added cat3k_caa-iosd-universalk9.SSA.150-9.19.EMP.pkg
    Added cat3k_caa-platform.SSA.03.09.19.EMP.pkg
    Added cat3k_caa-wcm.SSA.03.09.19.EMP.pkg
[2]: Creating pending provisioning file
[2]: Finished installing software.  New software will load on reboot.
[2]: Committing provisioning file

[2]: Do you want to proceed with reload? [yes/no]: n

infra-p2-3#
```

Related Commands

Command	Description
software clean	Use this command to remove any and all packages and provisioning files that are no longer in use.
software commit	Use this command to commit a package set that was installed using the **auto-rollback** command option of the **software install** command.
software expand	Use this command to expand individual IOS XE Software packages and the provisioning file from a specified bundle to a specific destination directory.
software install source switch	Use this command to install the running IOS XE software packages from one stack member to one or more other stack members.
software rollback	Use this command to roll back the committed Cisco IOS XE Software to a previous installation point.

software install source switch

To install the running IOS XE software packages from one stack member to one or more other stack members, use the **software install source switch** command in Privileged EXEC mode.

software install source switch*node* [**switch***node*] [**auto-rollback***minutes*][**force**][**on-reboot**] [**verbose**][**new**][**provisioning-file***provisioning-file url*]

Syntax Description

switch*node*	Specifies which switch in the stack to use as the package source. Only a single switch may be specified and there is no default value
switch*nodes*	(optional) Specifies which switch(es) should perform the install operation using '1,2,4' and/or '2-4' notation. Default is all switches in the stack.

auto-rollback*minutes*	(optional) Used to start the rollback timer for the specified number of minutes. If not used, the software is automatically committed after installation. A value to zero means the rollback timer is never started and the software is not automatically committed (need to use 'software commit '). If set to another value, the 'software commit' command must be used to commit the software before the timer expires (else it will automatically rollback to the original software).
force	(optional) Specifies that the operation will be forced. Forced means that the installation will proceed despite any remote package incompatibilities. Force should not generally be required, and should be used with caution. Local package compatibility checks are enforced regardless of this command option.
on-reboot	(optional) Indicates that the user should not prompted to reload when the installation operation completes. The user must then use the reload command to boot the system with the newly installed packages.
verbose	(optional) provides some additional info in the log files
new	(optional) Indicates that the post-install package set should contain only the packages being installed. Without this option, the post-install package set is a merged set of the currently installed software and the new packages being installed.

provisioning-file*provisioning-file url*	(optional) Specifies the provisioning file to be updated by the installation. Default is the running provisioning file. Valid locations are flash: or usbflash0:

Command Default

Command is used to install IOS XE software. No software will be installed by default.

Command Modes

Privileged EXEC

Command History

Release	Modification
IOS XE 3.2.0 SE	Command introduced.

Usage Guidelines

The **software install source switch** command is used to install the running package files from one stack member to one or more other stack members while the system is running in installed mode.

The following tasks are performed during the **software install source switch** operation.

- Copy the running software packages from flash: on the specified source switch to flash: on all other switches specified in the command.

- Perform compatibility checks on all switches in the stack to ensure that the software running on all stack members after installation will be compatible. This task is skipped if the **force** command option is used.

- Start the auto-rollback timer if the **auto-rollback** command option was used. The newly installed packages will be automatically rolled back if the auto-rollback timer expires before the **software commit** command is issued.

- Update the package provisioning file (packages.conf) and save a copy of the original provisioning file for use during auto-rollback or user-initiated rollback (**software rollback** command).

- Commit the newly installed software packages if the **auto-rollback** command option was not used.

- Prompt the user to reload (if the **on-reboot** command option was not used).

Note The **software install source switch** command cannot be used if the system is running in bundle mode. In this case, the **software expand** command can be used to prepare the system to boot in installed mode.

Examples

In the following example, the switches in a 2-member stack are running different (but compatible) software packages. The **software install source switch** command is used to install the currently running packages on the standby switch (switch 1) to the active switch (switch 2).

```
infra-p2-3#show version running
Package: Base, version: 03.09.19.EMP, status: active
  File: cat3k_caa-base.SSA.03.09.19.EMP.pkg, on: Switch1
  Built: Thu Nov 15 01:52:19 PST 2012, by: udonthi

Package: Drivers, version: 03.09.19.EMP, status: active
  File: cat3k_caa-drivers.SSA.03.09.19.EMP.pkg, on: Switch1
  Built: Thu Nov 15 01:54:53 PST 2012, by: udonthi

Package: Infra, version: 03.09.19.EMP, status: active
  File: cat3k_caa-infra.SSA.03.09.19.EMP.pkg, on: Switch1
  Built: Thu Nov 15 01:53:08 PST 2012, by: udonthi

Package: IOS, version: 150-9.19.EMP, status: active
  File: cat3k_caa-iosd-universalk9.SSA.150-9.19.EMP.pkg, on: Switch1
  Built: Thu Nov 15 01:54:09 PST 2012, by: udonthi

Package: Platform, version: 03.09.19.EMP, status: active
  File: cat3k_caa-platform.SSA.03.09.19.EMP.pkg, on: Switch1
  Built: Thu Nov 15 01:53:39 PST 2012, by: udonthi

Package: WCM, version: 03.09.19.EMP, status: active
  File: cat3k_caa-wcm.SSA.03.09.19.EMP.pkg, on: Switch1
  Built: Thu Nov 15 01:54:34 PST 2012, by: udonthi


Package: Base, version: 03.09.17.EMP, status: active
  File: cat3k_caa-base.SSA.03.09.17.EMP.pkg, on: Switch2
  Built: Mon Nov 12 20:27:51 PST 2012, by: udonthi

Package: Drivers, version: 03.09.17.EMP, status: active
  File: cat3k_caa-drivers.SSA.03.09.17.EMP.pkg, on: Switch2
  Built: Mon Nov 12 20:31:01 PST 2012, by: udonthi

Package: Infra, version: 03.09.17.EMP, status: active
  File: cat3k_caa-infra.SSA.03.09.17.EMP.pkg, on: Switch2
  Built: Mon Nov 12 20:28:53 PST 2012, by: udonthi

Package: IOS, version: 150-9.17.EMP, status: active
  File: cat3k_caa-iosd-universalk9.SSA.150-9.17.EMP.pkg, on: Switch2
  Built: Mon Nov 12 20:29:58 PST 2012, by: udonthi

Package: Platform, version: 03.09.17.EMP, status: active
  File: cat3k_caa-platform.SSA.03.09.17.EMP.pkg, on: Switch2
  Built: Mon Nov 12 20:29:33 PST 2012, by: udonthi

Package: WCM, version: 03.09.17.EMP, status: active
  File: cat3k_caa-wcm.SSA.03.09.17.EMP.pkg, on: Switch2
  Built: Mon Nov 12 20:30:29 PST 2012, by: udonthi



infra-p2-3#
infra-p2-3#software install source switch 1
Preparing install operation ...
[2]: Copying software from source switch 1 to switch 2
[2]: Finished copying software to switch 2
[2]: Starting install operation
[2]: Starting compatibility checks
[2]: Finished compatibility checks
[2]: Starting application pre-installation processing
[2]: Finished application pre-installation processing
[2]: Old files list:
    Removed cat3k_caa-base.SSA.03.09.17.EMP.pkg
    Removed cat3k_caa-drivers.SSA.03.09.17.EMP.pkg
    Removed cat3k_caa-infra.SSA.03.09.17.EMP.pkg
    Removed cat3k_caa-iosd-universalk9.SSA.150-9.17.EMP.pkg
    Removed cat3k_caa-platform.SSA.03.09.17.EMP.pkg
    Removed cat3k_caa-wcm.SSA.03.09.17.EMP.pkg
```

```
[2]: New files list:
    Added cat3k_caa-base.SSA.03.09.19.EMP.pkg
    Added cat3k_caa-drivers.SSA.03.09.19.EMP.pkg
    Added cat3k_caa-infra.SSA.03.09.19.EMP.pkg
    Added cat3k_caa-iosd-universalk9.SSA.150-9.19.EMP.pkg
    Added cat3k_caa-platform.SSA.03.09.19.EMP.pkg
    Added cat3k_caa-wcm.SSA.03.09.19.EMP.pkg
[2]: Creating pending provisioning file
[2]: Finished installing software.  New software will load on reboot.
[2]: Committing provisioning file

[2]: Do you want to proceed with reload? [yes/no]: no

infra-p2-3#
```

Related Commands

Command	Description
software clean	Use this command to remove any and all packages and provisioning files that are no longer in use.
software install file	Install Cisco IOS XE files.
software commit	Use this command to commit a package set that was installed using the **auto-rollback** command option of the **software install** command.
software expand	Use this command to expand individual IOS XE Software packages and the provisioning file from a specified bundle to a specific destination directory.
software rollback	Use this command to roll back the committed Cisco IOS XE Software to a previous installation point.

software rollback

To roll back the committed Cisco IOS XE Software to a previous installation point, use the **software rollback** command in Privileged EXEC mode.

software rollback [**switch***node*] [**as-booted**][**provisioning-file***provisioning-file url*][**on-reboot**] [**force**][**verbose**]

Syntax Description

switch*nodes*	(optional) specifies which switch(es) should perform the rollback operation using '1,2,4' and/or '2-4' notation. Default is all switches in the stack
as-booted	(optional) Used to rollback any installations that have occurred since bootup and commit the booted packages.conf file.
provisioning-file*provisioning-file url*	(optional) Specifies the provisioning file to be updated by the rollback. Default is the running provisioning file. Valid locations are flash: or usbflash0:
on-reboot	(optional) Indicates that the user should not prompted to reload when the rollback operation completes. The user must then use the reload command to boot the system with the newly installed packages.

force	(optional) Specifies that the operation will be forced. Forced means that the rollback will proceed despite any remote package incompatibilities. Force should not generally be required, and should be used with caution. Local package compatibility checks are enforced regardless of this command option.
verbose	(optional) provides some additional info in the log files

Command Default

No software will be rolled-back by default.

Command Modes

Privileged EXEC

Command History

Release	Modification
IOS XE 3.2.0 SE	Command introduced.

Usage Guidelines

The **software rollback** command rolls back the committed software, ie. set of packages, to a previous installation point.

The software rollback functionality relies on the existence of one or more **rollback provisioning files** in flash:, along with all of the .pkg files listed in the rollback provisioning file(s).

The rollback provisioning files are visible in flash: as packages.conf.00-, packages.conf.01-, etc.

- packages.conf.00- is a snapshot of the packages.conf file as it looked prior to the last installation operation.

- packages.conf.01- is a snapshot of the packages.conf file as it looked two installations ago. (This pattern continues for all provisioning files.)

When the **software rollback** command is used, packages.conf.00- becomes packages.conf, packages.conf.01- becomes packages.conf.00-, etc.

Note If the **software clean** command is used, future attempts to do a software rollback will fail if the rollback provisioning file and/or the packages listed in it have been cleaned.

Examples

This example uses the 'software rollback' command to revert to the previously installed package set (packages.conf.00 -).

```
infra-p2-3#software rollback
Preparing rollback operation ...
[2]: Starting rollback operation
[2]: Starting compatibility checks
[2]: Finished compatibility checks
[2]: Starting application pre-installation processing
[2]: Finished application pre-installation processing
[2]: Old files list:
    Removed cat3k_caa-base.SSA.03.09.19.EMP.pkg
    Removed cat3k_caa-drivers.SSA.03.09.19.EMP.pkg
    Removed cat3k_caa-infra.SSA.03.09.19.EMP.pkg
    Removed cat3k_caa-iosd-universalk9.SSA.150-9.19.EMP.pkg
    Removed cat3k_caa-platform.SSA.03.09.19.EMP.pkg
    Removed cat3k_caa-wcm.SSA.03.09.19.EMP.pkg
[2]: New files list:
    Added cat3k_caa-base.SSA.03.09.17.EMP.pkg
    Added cat3k_caa-drivers.SSA.03.09.17.EMP.pkg
    Added cat3k_caa-infra.SSA.03.09.17.EMP.pkg
    Added cat3k_caa-iosd-universalk9.SSA.150-9.17.EMP.pkg
    Added cat3k_caa-platform.SSA.03.09.17.EMP.pkg
    Added cat3k_caa-wcm.SSA.03.09.17.EMP.pkg
[2]: Creating pending provisioning file
[2]: Finished rolling back software changes. New software will load on reboot.

[2]: Do you want to proceed with reload? [yes/no]: n

infra-p2-3#
```

Related Commands

Command	Description
software clean	Use this command to remove any and all packages and provisioning files that are no longer in use.
software install file	Install Cisco IOS XE files.
software commit	Use this command to commit a package set that was installed using the **auto-rollback** command option of the **software install** command.
software expand	Use this command to expand individual IOS XE Software packages and the provisioning file from a specified bundle to a specific destination directory.
software install source switch	Use this command to install the running IOS XE software packages from one stack member to one or more other stack members.

test cable-diagnostics

To test the condition of 10-Gigabit Ethernet links or copper cables on 48-port 10/100/1000 BASE-T modules, use the **test cable-diagnostics**command in privileged EXEC mode.

test cable-diagnostics tdr interface *type number*

Syntax Description

tdr	Activates the TDR test for copper cables on 48-port 10/100/1000 BASE-T modules.
interface *type*	Specifies the interface type; see the “Usage Guidelines” section for valid values.
number	Module and port number.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(17a)SX	Support for this command was introduced on the Cisco 7600 series routers.
12.2(17b)SXA	This command was changed to provide support for the 4-port 10GBASE-E serial 10-Gigabit Ethernet module (WS-X6704-10GE).

Release	Modification
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Cable diagnostics can help you detect whether your cable has connectivity problems.

The TDR test guidelines are as follows:

- TDR can test cables up to a maximum length of 115 meters.
- The TDR test is supported on Cisco 7600 series routers running Release 12.2(17a)SX and later releases on specific mdoules. See the Release Notes for Cisco IOS Release 12.2SX on the Catalyst 6500 and Cisco 7600 Supervisor Engine 720, Supervisor Engine 32, and Supervisor Engine 2 for the list of the modules that support TDR.
- The valid values for **interface** *type*are **fastethernet** and **gigabitethernet**.
- Do not start the test at the same time on both ends of the cable. Starting the test at both ends of the cable at the same time can lead to false test results.
- Do not change the port configuration during any cable diagnostics test. This action may result in incorrect test results.
- The interface must be up before running the TDR test. If the port is down, the **test cable-diagnostics tdr** command is rejected and the following message is displayed:

```
Router# test cable-diagnostics tdr interface gigabitethernet2/12
% Interface Gi2/12 is administratively down
% Use 'no shutdown' to enable interface before TDR test start.
```

- If the port speed is 1000 and the link is up, do not disable the auto-MDIX feature.
- For fixed 10/100 ports, before running the TDR test, disable auto-MDIX on both sides of the cable. Failure to do so can lead to misleading results.
- For all other conditions, you must disable the auto-MDIX feature on both ends of the cable (use the **no mdix auto**command). Failure to disable auto-MDIX will interfere with the TDR test and generate false results.
- If a link partner has auto-MDIX enabled, this action will interfere with the TDR-cable diagnostics test and test results will be misleading. The workaround is to disable auto-MDIX on the link partner.
- If you change the port speed from 1000 to 10/100, enter the **no mdix auto**command before running the TDR test. Note that entering the **speed 1000** command enables auto-MDIX regardless of whether the **no mdix auto**command has been run.

Examples

This example shows how to run the TDR-cable diagnostics:

```
Router # test cable-diagnostics tdr interface gigabitethernet2/1
TDR test started on interface Gi2/1
A TDR test can take a few seconds to run on an interface
Use 'show cable-diagnostics tdr' to read the TDR results.
```

Related Commands

Command	Description
clear cable-diagnostics tdr	Clears a specific interface or clears all interfaces that support TDR.
show cable-diagnostics tdr	Displays the test results for the TDR cable diagnostics.

traceroute mac

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

traceroute mac *source-mac-address* {*destination-mac-address* | **interface** *type interface-number destination-mac-address*} [**vlan** *vlan-id*] [**detail**]

traceroute mac interface *type interface-number source-mac-address* {*destination-mac-address* | **interface** *type interface-number destination-mac-address*} [**vlan** *vlan-id*] [**detail**]

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

Syntax Description

source-mac-address	Media Access Control (MAC) address of the source switch in hexadecimal format.
destination-mac-address	MAC address of the destination switch in hexadecimal format.
interface *type*	Specifies the interface where the MAC address resides; valid values are **FastEthernet**, **GigabitEthernet**, and **Port-channel**.
interface-number	Module and port number or the port-channel number; valid values for the port channel are from 1 to 282.
vlan *vlan-id*	(Optional) Specifies the virtual local area network (VLAN) on which to trace the Layer 2 path that the packets take from the source switch to the destination switch; valid values are from 1 to 4094.
detail	(Optional) Displays detailed information about the Layer 2 trace.
ip	Specifies the IP address where the MAC address resides.
source-ip-address	IP address of the source switch as a 32-bit quantity in dotted-decimal format.

source-hostname	IP hostname of the source switch.
destination-ip-address	IP address of the destination switch as a 32-bit quantity in dotted-decimal format.
destination-hostname	IP hostname of the destination switch.

Command Default

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported on the Cisco 7600 series router that is configured with a Supervisor Engine 2.

Do not use leading zeros when entering a VLAN ID.

For Layer 2 traceroute to functional properly, you must enable CDP on all of the switches in the network. Do not disable CDP.

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

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

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

When multiple devices are attached to one port through hubs (for example, multiple CDP neighbors are detected on a port), the Layer 2 traceroute utility terminates at that hop and displays an error message.

This feature is not supported in Token Ring VLANs.

Examples

This example shows how to display detailed information about the Layer 2 path:

```
Router# traceroute mac 0001.0000.0204 0001.0000.0304 detail
Source 1001.0000.0204 found on VAYU[WS-C6509] (10.1.1.10)
1 VAYU / WS-C6509 / 10.1.1.10 :
Gi6/1 [full, 1000M] => Po100 [auto, auto]
2 PANI / WS-C6509 / 10.1.1.12 :
Po100 [auto, auto] => Po110 [auto, auto]
3 BUMI / WS-C6509 / 10.1.1.13 :
Po110 [auto, auto] => Po120 [auto, auto]
4 AGNI / WS-C6509 / 10.1.1.11 :
Po120 [auto, auto] => Gi8/12 [full, 1000M]
Destination 1001.0000.0304 found on AGNI[WS-C6509] (10.1.1.11)
Layer 2 trace completed.
Router#
```

This example shows the output when the switch is not connected to the source switch:

```
Router# traceroute mac 0000.0201.0501 0000.0201.0201 detail
Source not directly connected, tracing source .....
Source 1000.0201.0501 found on con5[WS-C6509] (10.2.5.5)
con5 / WS-C6509 / 10.2.5.5 :
        Fa0/1 [auto, auto] =>Gi0/1 [auto, auto]
con1 / WS-C6509 / 10.2.1.1 :
        Gi0/1 [auto, auto] =>Gi0/2 [auto, auto]
con2 / WS-C6509 / 10.2.2.2 :
        Gi0/2 [auto, auto] =>Fa0/1 [auto, auto]
Destination 1000.0201.0201 found on con2[WS-C6509] (10.2.2.2)
Layer 2 trace completed.
Router#
```

This example shows the output when the switch cannot find the destination port for the source MAC address:

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

This example shows the output when the source and destination devices are in different VLANs:

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

This example shows the output when the destination MAC address is a multicast address:

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

This example shows the output when the source and destination switches belong to multiple VLANs:

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

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

```
Router# traceroute mac interface fastethernet0/1 0000.0201.0601 interface fastethernet0/3
0000.0201.0201
Source 1000.0201.0601 found on con6[WS-C6509] (10.2.6.6)
con6 (10.2.6.6) :Fa0/1 =>Fa0/3
con5                (10.2.5.5       )  :    Fa0/3 =>Gi0/1
con1                (10.2.1.1       )  :    Gi0/1 =>Gi0/2
```

```
con2                (10.2.2.2        )  :    Gi0/2 =>Fa0/1
Destination 1000.0201.0201 found on con2[WS-C6509] (10.2.2.2)
Layer 2 trace completed
Router#
```

This example shows how to display detailed traceroute information:

```
Router# traceroute mac ip 10.2.66.66 10.2.22.22 detail
Translating IP to mac.....
10.2.66.66 =>0000.0201.0601
10.2.22.22 =>0000.0201.0201
Source 0000.0201.0601 found on con6[WS-C6509] (10.2.6.6)
con6 / WS-C6509 / 10.2.6.6 :
        Fa0/1 [auto, auto] =>Fa0/3 [auto, auto]
con5 / WS-C6509 / 10.2.5.5 :
        Fa0/3 [auto, auto] =>Gi0/1 [auto, auto]
con1 / WS-C6509 / 10.2.1.1 :
        Gi0/1 [auto, auto] =>Gi0/2 [auto, auto]
con2 / WS-C6509 / 10.2.2.2 :
        Gi0/2 [auto, auto] =>Fa0/1 [auto, auto]
Destination 0000.0201.0201 found on con2[WS-C6509] (10.2.2.2)
Layer 2 trace completed.
Router#
```

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

```
Router# traceroute mac ip con6 con2
Translating IP to mac .....
10.2.66.66 =>0000.0201.0601
10.2.22.22 =>0000.0201.0201
Source 0000.0201.0601 found on con6
con6 (10.2.6.6) :Fa0/1 =>Fa0/3
con5                (10.2.5.5        )  :    Fa0/3 =>Gi0/1
con1                (10.2.1.1        )  :    Gi0/1 =>Gi0/2
con2                (10.2.2.2        )  :    Gi0/2 =>Fa0/1
Destination 0000.0201.0201 found on con2
Layer 2 trace completed
Router#
```

This example shows the output when ARP cannot associate the source IP address with the corresponding MAC address:

```
Router# traceroute mac ip 10.2.66.66 10.2.77.77
Arp failed for destination 10.2.77.77.
Layer2 trace aborted.
Router#
```

upgrade rom-monitor

To set the execution preference on a read-only memory monitor (ROMMON), use the **upgrade rom-monitor** command in privileged EXEC or diagnostic mode.

upgrade rom-monitor slot *num* {**sp** | **rp**} **file** *filename*

upgrade rom-monitor slot *num* {**sp** | **rp**} {**invalidate** | **preference**} {**region1** | **region2**}

Cisco ASR 1000 Series Aggregation Services Routers

upgrade rom-monitor filename *URL slot*

Syntax Description

slot *num*	Specifies the slot number of the ROMMON to be upgraded.
sp	Upgrades the ROMMON of the Switch Processor.
rp	Upgrades the ROMMON of the Route Processor.
file *filename*	Specifies the name of the S-record (SREC) file; see the “Usage Guidelines” section for valid values.
invalidate	Invalidates the ROMMON of the selected region.
preference	Sets the execution preference on a ROMMON of the selected region.
region1	Selects the ROMMON in region 1.
region2	Selects the ROMMON in region 2.
filename	Specifies the ROMMON package filename.
URL	The URL to a ROMMON file. The URL always begins with a file system, such as **bootflash:**, **harddisk:**, **obfl:**, **stby-harddisk:**, or **usb**[**0**-**1**], then specifies the path to the file.

slot	The slot that contains the hardware that will receive the ROMMON upgrade. Options are: • *number* --the number of the Session Initiation Protocol (SIP) slot that requires the ROMMON upgrade • **all** --All hardware on the router • **F0** --Embedded-Service-Processor slot 0 • **F1** --Embedded-Service-Processor slot 1 • **FP** --All installed Embedded-Service-Processors • **R0** --Route-Processor slot 0 • **R1** --Route-Processor slot 1 • **RP** --Route-Processor

Command Default

This command has no default settings.

Command Modes

Privileged EXEC (#) Diagnostic (diag)

Command History

Release	Modification
12.2(14)SX	This command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	This command was modified. Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(24)T	This command was integrated into Cisco IOS Release 12.4(24)T.
Cisco IOS XE Release 2.1	This command was integrated into Cisco ASR 1000 Series Routers, and introduced in diagnostic mode.

Usage Guidelines

Caution If you enter the **upgrade rom-monitor** command from a Telnet session instead of a console connection, service may be interrupted.

The **slot** *num*keyword and argument combination is required for this command to function properly.

The **sp** or **rp**keyword is required if you installed a supervisor engine in the specified slot.

Valid values for **file** *filename* are the following:

- **bootflash:**
- **disk0:**
- **disk1:**
- **flash:**
- **ftp:**
- **rcp:**
- **sup-bootflash:**
- **sup-slot0:**
- **tftp:**

On Cisco ASR 1000 Series Routers, this command can be used to upgrade ROMMON in privileged EXEC and diagnostic mode. The hardware receiving the ROMMON upgrade must be reloaded to complete the upgrade.

From Cisco IOS Release 12.4(24)T, you can use the **upgrade rom-monitor** command on Cisco 3200 series routers to upgrade ROMMON and the system bootstrap, if a newer version of ROMMON is available on the system.

Examples

This example shows how to upgrade the new ROMMON image to the flash device on a Supervisor Engine 2:

```
Router# upgrade rom-monitor
 slot 1 sp file tftp://dirt/tftpboot-users/A2_71059.srec
ROMMON image upgrade in progress
   Erasing flash
   Programming flash
   Verifying new image
   ROMMON image upgrade complete
   The card must be reset for this to take effect
Router#
```

In the following example, a ROMMON upgrade is performed to upgrade to Cisco IOS Release 12.2(33r)XN1 on a Cisco ASR 1000 Series Router using an ROMMON image stored on the bootflash: file system. All hardware is upgraded on the Cisco ASR 1000 Series Router in this example, and the router is then reloaded to complete the procedure.

```
Router# show rom-monitor 0
System Bootstrap, Version 12.2(33)XN1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2007 by cisco Systems, Inc.
Router# show rom-monitor F0
System Bootstrap, Version 12.2(33)XN1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2007 by cisco Systems, Inc.
Router# show rom-monitor R0
System Bootstrap, Version 12.2(33)XN1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2007 by cisco Systems, Inc.
Router# copy tftp bootflash:
Address or name of remote host []? 127.23.16.81

Source filename []? auto/tftp-boot/asr1000-rommon.122-33r.XN1.pkg
Destination filename [asr1000-rommon.122-33r.XN1.pkg]?
Accessing tftp://127.23.16.81/auto/tftp-boot/asr1000-rommon.122-33r.XN1.pkg...
Loading auto/tftp-boot/asr1000-rommon.122-33r.XN1.pkg from 127.23.16.81 (via
GigabitEthernet0): !!!
```

```
[OK - 553164 bytes]
553164 bytes copied in 1.048 secs (527828 bytes/sec)
Router# dir bootflash:
Directory of bootflash:/
   11  drwx       16384   Dec 2 2004 12:02:09 +00:00  lost+found
14401  drwx        4096   Dec 2 2004 12:05:05 +00:00  .ssh
86401  drwx        4096   Dec 2 2004 12:05:07 +00:00  .rollback_timer
   12  -rw-    33554432  Nov 20 2007 19:53:47 +00:00  nvram_00100
   13  -rw-     6401536  Dec 23 2004 19:45:11 +00:00  mcp-fpd-pkg.122-test.pkg
28801  drwx        4096   Nov 1 2007 17:00:36 +00:00  .installer   15  -rw-      553164
Nov 28 2007 15:33:49 +00:00  asr1000-rommon.122-33r.XN1.pkg
   16  -rw-    51716300  Nov 14 2007 16:39:59 +00:00  asr1000rp1-
espbase.v122_33_xn_asr_rls0_throttle.pkg
   17  -rw-    21850316  Nov 14 2007 16:41:23 +00:00  asr1000rp1-rpaccess-
k9.v122_33_xn_asr_rls0_throttle.pkg
   18  -rw-    21221580  Nov 14 2007 16:42:21 +00:00  asr1000rp1-
rpbase.v122_33_xn_asr_rls0_throttle.pkg
   19  -rw-    27576524  Nov 14 2007 16:43:50 +00:00  asr1000rp1-
rpcontrol.v122_33_xn_asr_rls0_throttle.pkg
   20  -rw-    48478412  Nov 14 2007 16:45:50 +00:00  asr1000rp1-rpios-
advipservicesk9.v122_33_xn_asr_rls0_throttle.pkg
   21  -rw-    36942028  Nov 14 2007 16:47:17 +00:00  asr1000rp1-
sipbase.v122_33_xn_asr_rls0_throttle.pkg
   22  -rw-    14749900  Nov 14 2007 16:48:17 +00:00  asr1000rp1-
sipspa.v122_33_xn_asr_rls0_throttle.pkg
   23  -rw-        6049  Nov 14 2007 16:49:29 +00:00  packages.conf
   14  -rw-   213225676  Nov 20 2007 19:53:13 +00:00  asr1000rp1-
advipservicesk9.v122_33_xn_asr_rls0_throttle.bin
928833536 bytes total (451940352 bytes free)
Router# upgrade rom-monitor filename bootflash:/asr1000-rommon.122-33r.XN1.pkg all
Upgrade rom-monitor on Route-Processor 0
Target copying rom-monitor image file
Checking upgrade image...
1966080+0 records in
3840+0 records out
Upgrade image MD5 signature is 253f15daf89eea22b1db92d440d03608
Burning upgrade partition...
1966080+0 records in
3840+0 records out
Checking upgrade partition...
Upgrade flash partition MD5 signature is 253f15daf89eea22b1db92d440d03608
ROMMON upgrade complete.
To make the new ROMMON permanent, you must restart the RP.
Upgrade rom-monitor on Embedded-Service-Processor 0
Target copying rom-monitor image file
Checking upgrade image...
1966080+0 records in
3840+0 records out
Upgrade image MD5 signature is 253f15daf89eea22b1db92d440d03608
Burning upgrade partition...
1966080+0 records in
3840+0 records out
Checking upgrade partition...
Upgrade flash partition MD5 signature is 253f15daf89eea22b1db92d440d03608
ROMMON upgrade complete.
To make the new ROMMON permanent, you must restart the linecard.
Upgrade rom-monitor on SPA-Inter-Processor 0
Target copying rom-monitor image file
Checking upgrade image...
1966080+0 records in
3840+0 records out
Upgrade image MD5 signature is 253f15daf89eea22b1db92d440d03608
Burning upgrade partition...
1966080+0 records in
3840+0 records out
Checking upgrade partition...
Upgrade flash partition MD5 signature is 253f15daf89eea22b1db92d440d03608
ROMMON upgrade complete.
To make the new ROMMON permanent, you must restart the linecard.
Upgrade rom-monitor on SPA-Inter-Processor 1
Target copying rom-monitor image file
Checking upgrade image...
1966080+0 records in
```

```
3840+0 records out
Upgrade image MD5 signature is 253f15daf89eea22b1db92d440d03608
Burning upgrade partition...
1966080+0 records in
3840+0 records out
Checking upgrade partition...
Upgrade flash partition MD5 signature is 253f15daf89eea22b1db92d440d03608
ROMMON upgrade complete.
To make the new ROMMON permanent, you must restart the linecard.
Router# reload
<reload bootup output removed for brevity>
Router# show rom-monitor 0
System Bootstrap, Version 12.2(33r)XN1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2007 by cisco Systems, Inc.
Router# show rom-monitor F0
System Bootstrap, Version 12.2(33r)XN1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2007 by cisco Systems, Inc.
Router# show rom-monitor R0
System Bootstrap, Version 12.2(33r)XN1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 2007 by cisco Systems, Inc.
```

Related Commands

Command	Description
show rom-monitor	Displays the ROMMON status.

verify

To verify the checksum of a file on a flash memory file system or compute a Message Digest 5 (MD5) signature for a file, use the **verify** command in privileged EXEC mode.

verify [**/md5** [*md5-value*]] *filesystem* **:** [*file-url*]

Cisco 7600 Series Router

verify {**/md5** *flash-filesystem* [*expected-md5-signature*] | **/ios** *flash-filesystem* | *flash-filesystem*}

Syntax Description

/md5	(Optional) Calculates and displays the MD5 value for the specified software image. Compare this value with the value available on Cisco.com for this image.
md5-value	(Optional) The known MD5 value for the specified image. When an MD5 value is specified in the command, the system calculates the MD5 value for the specified image and display a message verifying that the MD5 values match or that there is a mismatch.
filesystem **:**	File system or directory containing the files to list, followed by a colon. Standard file system keywords for this command are **flash:** and **bootflash:**.
file-url	(Optional) The name of the files to display on a specified device. The files can be of any type. You can use wildcards in the filename. A wildcard character (*) matches all patterns. Strings after a wildcard are ignored.

Cisco 7600 Series Router

/md5 *flash-filesystem*	Computes an MD5 signature for a file; valid values are **bootflash:**, **disk0:**, **disk1:**, **flash:**, or **sup-bootflash:**.
expected-md5-signature	(Optional) MD5 signature.
/ios *flash-filesystem*	Verifies the compressed Cisco IOS image checksum; valid values are **bootflash:**, **disk0:**, **disk1:**, **flash:**, or **sup-bootflash:**.
flash-filesystem	Device where the Flash memory resides; valid values are **bootflash:**, **disk0:**, **disk1:**, **flash:**, or **sup-bootflash:**.

Command Default

The current working device is the default device (file system).

Command Modes

Privileged EXEC

Command History

Release	Modification
11.0	This command was introduced.
12.2(4)T	The **/md5** keyword was added.
12.2(18)S	The **verify** command was enhanced to verify the hash that is contained in the image, and the output was enhanced to show the hash value in addition to the entire hash image (CCO hash).
12.0(26)S	The **verify** command enhancements were integrated into Cisco IOS Release 12.0(26)S.
12.2(14)SX	Support for this command was added for the Supervisor Engine 720.
12.3(4)T	The **verify** command enhancements were integrated into Cisco IOS Release 12.3(4)T.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command replaces the **copy verify** and **copy verify flash** commands.

Use the **verify** command to verify the checksum of a file before using it.

Each software image that is distributed on disk uses a single checksum for the entire image. This checksum is displayed only when the image is copied into flash memory; it is not displayed when the image file is copied from one disk to another.

Supported Platforms Other than the Cisco 7600 Series Router

Before loading or duplicating a new image, record the checksum and MD5 information for the image so that you can verify the checksum when you copy the image into flash memory or onto a server. A variety of image information is available on Cisco.com. For example, you can get the Release, Feature Set, Size, BSD Checksum, Router Checksum, MD5, and Publication Date information by clicking on the image file name prior to downloading it from the Software Center on Cisco.com.

To display the contents of flash memory, use the **show flash** command. The flash contents listing does not include the checksum of individual files. To recompute and verify the image checksum after the image has been copied into flash memory, use the **verify** command. Note, however, that the **verify** command only performs a check on the integrity of the file after it has been saved in the file system. It is possible for a corrupt image to be transferred to the router and saved in the file system without detection. If a corrupt image is transferred successfully to the router, the software will be unable to tell that the image is corrupted and the file will verify successfully.

To use the message-digest5 (MD5) hash algorithm to ensure file validation, use the **verify** command with the **/md5** option. MD5 is an algorithm (defined in RFC 1321) that is used to verify data integrity through the creation of a unique 128-bit message digest. The **/md5** option of the **verify** command allows you to check the integrity of a Cisco IOS software image by comparing its MD5 checksum value against a known MD5 checksum value for the image. MD5 values are now made available on Cisco.com for all Cisco IOS software images for comparison against local system image values.

To perform the MD5 integrity check, issue the **verify** command using the **/md5** keyword. For example, issuing the **verify flash:c7200-is-mz.122-2.T.bin /md5**command will calculate and display the MD5 value for the software image. Compare this value with the value available on Cisco.com for this image.

Alternatively, you can get the MD5 value from Cisco.com first, then specify this value in the command syntax. For example, issuing the **verify flash:c7200-is-mz.122-2.T.bin /md5 8b5f3062c4caeccae72571440e962233** command will display a message verifying that the MD5 values match or that there is a mismatch. A mismatch in MD5 values means that either the image is corrupt or the wrong MD5 value was entered.

Cisco 7600 Series Router

The Readme file, which is included with the image on the disk, lists the name, file size, and checksum of the image. Review the contents of the Readme file before loading or duplicating the new image so that you can verify the checksum when you copy it into the flash memory or onto a server.

Use the **verify /md5** command to verify the MD5 signature of a file before using it. This command validates the integrity of a copied file by comparing a precomputed MD5 signature with the signature that is computed by this command. If the two MD5 signatures match, the copied file is identical to the original file.

You can find the MD5 signature that is posted on the Cisco.com page with the image.

You can use the **verify /md5** command in one of the following ways:

- Verify the MD5 signatures manually by entering the **verify /md5** *filename* command.

Check the displayed signature against the MD5 signature that is posted on the Cisco.com page.

- Allow the system to compare the MD5 signatures by entering the **verify /md5** *flash-filesystem:filenam expected-md5-signature* command.

After completing the comparison, the system returns with a verified message. If an error is detected, the output is similar to the following:

```
Router# verify /md5 disk0:c6msfc2-jsv-mz 0f
.
.
.
Done
!
 %Error verifying disk0:c6msfc2-jsv-mz
 Computed signature  = 0f369ed9e98756f179d4f29d6e7755d3
 Submitted signature = 0f
```

To display the contents of the flash memory, enter the **show flash** command. The listing of the flash contents does not include the checksum of the individual files. To recompute and verify the image checksum after the image has been copied into the flash memory, enter the **verify** command.

A colon (:) is required after the specified device.

Examples

Supported Platforms Other than Cisco 7600 Series Router

The following example shows how to use the **verify** command to check the integrity of the file c7200-js-mz on the flash memory card inserted in slot 0:

```
Router# dir slot0:

Directory of slot0:/
  1  -rw-     4720148   Aug 29 1997 17:49:36  hampton/nitro/c7200-j-mz
  2  -rw-     4767328   Oct 01 1997 18:42:53  c7200-js-mz
  5  -rw-         639   Oct 02 1997 12:09:32  rally
  7  -rw-         639   Oct 02 1997 12:37:13  the_time
20578304 bytes total (3104544 bytes free)
Router# verify slot0:c7200-js-mz

Verified slot0:c7200-js-mz
```

In the following example, the **/md5** keyword is used to display the MD5 value for the image:

```
Router# verify /md5 disk1:

Verify filename []? c7200-js-mz

.
.
.
Done
!
verify /md5 (disk1:c7200-js-mz) = 0f369ed9e98756f179d4f29d6e7755d3
```

In the following example, the known MD5 value for the image (obtained from Cisco.com) is specified in the **verify** command, and the system checks the value against the stored value:

```
Router# verify /md5 disk1:c7200-js-mz ?
  WORD  Expected md5 signature
  <cr>
router# verify /md5 disk1:c7200-js-mz 0f369ed9e98756f179d4f29d6e7755d3
.
.
.
Done
!
Verified (disk1:c7200-js-mz) = 0f369ed9e98756f179d4f29d6e7755d3
```

The following example shows how the output of the **verify** command was enhanced to show the hash value in addition to the entire hash image (CCO hash):

```
Router# verify disk0:c7200-js-mz
%Filesystem does not support verify operations
Verifying file integrity of disk0:c7200-js-mz
.
.
.
Done
!
Embedded Hash           MD5 :CFA258948C4ECE52085DCF428A426DCD
Computed Hash               MD5 :CFA258948C4ECE52085DCF428A426DCD
CCO Hash                MD5 :44A7B9BDDD9638128C35528466318183
Signature Verified
```

Cisco 7600 Series Router

This example shows how to use the **verify** command:

```
Router# verify cat6k_r47_1.cbi
.
.
.
File cat6k_r47_1.cbi verified OK.
```

This example shows how to check the MD5 signature manually:

```
Router# verify /md5 c6msfc2-jsv-mz
.
.
.
Done
!
 verify /md5 (disk0:c6msfc2-jsv-mz) = 0f369ed9e98756f179d4f29d6e7755d3
```

This example shows how to allow the system to compare the MD5 signatures:

```
Router# verify /md5 disk0:c6msfc2-jsv-mz 0f369ed9e98756f179d4f29d6e7755d3
.
.
.
Done
!
 verified /md5 (disk0:c6sup12-jsv-mz) = 0f369ed9e98756f179d4f29d6e7755d3
Router#
```

This example shows how to verify the compressed checksum of the Cisco IOS image:

```
Router# verify /ios disk0:c6k222-jsv-mz
Verified compressed IOS image checksum for disk0:c6k222-jsv-mz
```

Related Commands

Command	Description
cd	Changes the default directory or file system.
copy	Copies any file from a source to a destination.
copy /noverify	Disables the automatic image verification for the current copy operation.

Command	Description
dir	Displays a list of files on a file system.
file verify auto	Verifies the compressed Cisco IOS image checksum.
pwd	Displays the current setting of the cd command.
show file systems	Lists available file systems.
show flash	Displays the layout and contents of flash memory.

vtp

To configure the global VLAN Trunking Protocol (VTP) state, use the **vtp** command in global configuration mode. To return to the default value, use the **no** form of this command.

vtp {**domain** *domain-name* | **file** *filename* | **interface** *interface-name* [**only**] | **mode** {**client** | **off** | **server** | **transparent**} {**vlan** | **mst** | **unknown**} | **password** *password-value* [**hidden** | **secret**] | **pruning** | **version** {**1** | **2** | **3**}}

no vtp

Syntax Description

domain *domain-name*	Sets the VTP administrative domain name.
file *filename*	Sets the ASCII name of the IFS file system file where the VTP configuration is stored.
interface *interface-name*	Sets the name of the preferred source for the VTP-updater ID for this device.
only	(Optional) Specifies to use only this interface's IP address as the VTP-IP updater address.
mode client	Sets the type of VTP-device mode to client mode.
mode off	Sets the type of VTP-device mode to off mode.
mode server	Sets the type of VTP-device mode to server mode.
mode transparent	Sets the type of VTP-device mode to transparent mode.
vlan	Specifies VTP version 3 VLAN instances.
mst	Specifies VTP version 3 MST instances.
unknown	Specifies VTP version 3 for all other instances.

password *password-value*	Specifies the administrative-domain password.
hidden	(Optional) Specifies that the VTP version 3 secret key generated from the password be saved in the const_nvram:vlan.dat file.
secret	(Optional) Allows you to directly configure the VTP version 3 password secret key.
pruning	Enables the administrative domain to permit pruning.
version {**1** | **2** | **3**}	Specifies the administrative-domain VTP version number.

Command Default

The defaults are as follows:

- **vtp domain** and **vtp interface** co mmands have no default settings.
- *filename* is const-nvram:vlan.dat .
- VTP mode is **mode server** for VLANs and **transparent** for all other features.
- No password is configured.
- Pruning is disabled.
- Administrative-domain VTP version number 1.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(14)SX	This command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Cisco IOS Release 12.2(17d)SXB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	The **mode off**keyword combination was added.
12.2(33)SXI	Support for VTP version 3 was added.

Usage Guidelines

Note The **vtp pruning**, **vtp password**, and **vtp version** commands are also available in privileged EXEC mode. We recommend that you use these commands in global configuration mode only; do not use these commands in privileged EXEC mode.

Extended-range VLANs are not supported by VTP.

When you define the domain-name value , the dom ain name is case sensitive and can be from 1 to 32 characters.

The *filename* and *interface-name*values are ASCII strings from 1 to 255 characters.

You must configure a password on each network device in the management domain when the switch is in secure mode.

Caution If you configure VTP in secure mode, the management domain does not function properly if you do not assign a management domain password to each network device in the domain.

A VTP version 2-capable network device can operate in the same VTP domain as a network device running VTP version 1 if VTP version 2 is disabled on the VTP version 2-capable network device (VTP version 2 is disabled by default).

Do not enable VTP version 2 on a network device unless all of the network devices in the same VTP domain are version 2-capable. When you enable VTP version 2 on a network device, all of the version 2-capable network devices in the domain enable VTP version 2.

In a Token Ring environment, you must enable VTP version 2 for VLAN switching to function properly.

Enabling or disabling VTP pruning on a VTP server enables or disables VTP pruning for the entire management domain.

Configuring VLANs as pruning eligible or pruning ineligible on a Cisco 7600 series router affects pruning eligibility for those VLANs on that switch only; it does not affect pruning eligibility on all network devices in the VTP domain.

The **vtp password**, **vtp pruning**, and **vtp version** commands are not placed in startup memory but are included in the VTP transparent-mode startup configuration file.

Extended-range VLANs are not supported by VTP.

You can configure the **pruning** keyword in VTP-server mode; the **version** keyword is configurable in VTP-server mode or VTP transparent mode.

The password-value argument is an ASCII string from 8 to 64 characters identifying the administrative domain for the device.

VTP pruning causes information about each pruning-eligible VLAN to be removed from VTP updates if there are no stations belonging to that VLAN.

All Cisco 7600 series routers in a VTP domain must run the same version of VTP. VTP version 1 and VTP version 2 do not operate on Cisco 7600 series routers in the same VTP domain.

If all Cisco 7600 series routers in a domain are VTP version 2-capable, you need only to enable VTP version 2 on one Cisco 7600 series router; the version number is then propagated to the other version 2-capable Cisco 7600 series routers in the VTP domain.

If you toggle the version 2 mode, certain default VLAN parameters are modified.

If you enter the **vtp mode off** command, it sets the device to off. If you enter the **no vtp mode off** command, it resets the device to the VTP server mode.

In VTP version 3, the VTP mode has to be specified on a per-feature basis. Use the **vlan** and **mst** keywords to configure the VTP mode on VLAN and MST instances. To configure the VTP mode for any other feature, use the **unknown** keyword. When you convert from either VTP version 1 or 2 to version 3, the current mode configuration will be preserved.

With VTP version 3, a new method is available for hiding the VTP password from the configuration file. When you use the **hidden** keyword, the secret key that is generated from the password string is saved in the const_nvram:vlan.dat file. If you use the **secret** keyword, you can directly configure the password secret key. By using the **secret** keyword, you can distribute the password in the secret key format rather than in the cleartext format.

Examples

This example shows how to set the device's management domain:

```
Router(config)#
vtp domain DomainName1
```

This example shows how to specify the file in the IFS-file system where the VTP configuration is stored:

```
Router(config)#
vtp file vtpconfig
Setting device to store VLAN database at filename vtpconfig.
```

This example shows how to set the VTP mode to client:

```
Router(config)#
vtp mode client
Setting device to VTP CLIENT mode.
```

This example shows how to disable VTP mode globally:

```
Router(config)# vtp mode off
Setting device to VTP OFF mode.
```

This example shows how to reset the device to the VTP server mode:

```
Router(config)# no vtp mode off
Setting device to VTP OFF mode.
```

Related Commands

Command	Description
show vtp	Displays the VTP statistics and domain information.
vtp (interface configuration)	Enables VTP on a per-port basis.