Release Notes for the Catalyst 3750 Switch Cisco IOS Release 12.1(11)AX

May 2003

The Cisco IOS Release 12.1(11)AX runs on all Catalyst 3750 switches. Catalyst 3750 switches support stacking through Cisco StackWise technology. Unless otherwise noted, the term *switch* refers to a standalone switch and to a switch stack.

These release notes include important information about this Cisco IOS release and any limitations, restrictions, and caveats that apply to it. Verify that these release notes are correct for your switch:

- If you are installing a new switch, refer to the IOS release label on the rear panel of your switch.
- If your switch is on, use the **show version** privileged EXEC command. See the "Determining the Software Version and Feature Set" section on page 4.
- If you are upgrading to a new release, refer to the software upgrade filename for the software version.

For the complete list of Catalyst 3750 switch documentation, see the "Related Documentation" section on page 17.

You can download the switch software from these sites:

- http://www.cisco.com/kobayashi/sw-center/sw-lan.shtml

  (for registered Cisco.com users with a login password)
- http://www.cisco.com/public/sw-center/sw-lan.shtml

  (for nonregistered Cisco.com users)

This software release is part of a special release of Cisco IOS software that is not released on the same 8-week maintenance cycle that is used for other platforms. As maintenance releases and future software releases become available, they will be posted to Cisco.com (previously Cisco Connection Online [CCO]) in the Cisco IOS software area.

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Contents

This information is in the release notes:

System Requirements

These are the system requirements for this software release:

- "Hardware Supported" section on page 2
- "Software Compatibility" section on page 3

Hardware Supported

Table 1 lists the hardware supported by this software release.

Table 1 Supported Hardware

Switch	Description
Catalyst 3750-24TS	24 10/100 Ethernet ports and 2 small form-factor pluggable (SFP) module slots
Catalyst 3750G-24T	24 10/100/1000 Ethernet ports
Catalyst 3750G-24TS	24 10/100/1000 Ethernet ports and 4 SFP module slots
Catalyst 3750-48TS	48 10/100 Ethernet ports and 4 SFP module slots
SFP modules	1000BASE-SX and 1000BASE-LX
Redundant power system	Cisco RPS 300 Redundant Power System for the Catalyst 3750G-24TS, 3750G-24T, and 3750-48TS switch models (not supported on the Catalyst 3750-24TS switch) Cisco RPS 675 Redundant Power System for the entire Catalyst 3750 switch family

Software Compatibility

For information about the recommended platforms for web-based management, operating systems and browser support, Java plug-in guidelines and installation procedures, refer to the *Catalyst 3750 Switch Hardware Installation Guide*.

Creating Clusters with Different Releases of IOS Software

When a cluster consists of a mixture of Catalyst switches, we strongly recommend using only Catalyst 3750 switches as the command and standby command switches. The Catalyst 3750 switch can be part of a cluster as a standalone switch or as a switch stack. In a cluster, a switch stack is treated as a single entity.

When the command switch is a Catalyst 3750 switch, all standby command switches must also be Catalyst 3750 switches. The Catalyst 3750 switch that has the latest software should be the command switch. If the command switch is a Catalyst 3750 Gigabit Ethernet switch and the standby command switch is a Catalyst 3750 Fast Ethernet switch, command switch port speeds are reduced if the standby command switch takes over.

Table 2 lists the cluster capabilities and software versions for the switches. The switches are listed in the order of highest to lowest end switch. A lower-end switch cannot be the command switch of a switch listed above it in the table (for example, a Catalyst 2950 switch cannot be the command switch of a cluster that has Catalyst 2970 or Catalyst 3550 switches.)

Table 2 Switch Software and Cluster Capability

Switch	IOS Release	Cluster Capability
Catalyst 3750	12.1(11)AX	Member or command switch
Catalyst 3550	12.1(4)EA1 or later	Member or command switch
Catalyst 2970	12.1(11)AX	Member or command switch
Catalyst 2950	12.1(5.2)WC(1) or later	Member or command switch
Catalyst 2955	12.1(12c)EA1 or later	Member or command switch
Catalyst 3500 XL	12.0(5.1)XU or later	Member or command switch
Catalyst 2950	12.0(5.2)WC(1) or later	Member or command switch
Catalyst 2900 XL (8-MB switches)	12.0(5.1)XU or later	Member or command switch
Catalyst 2900 XL (4-MB switches)	11.2(8.5)SA6 (recommended)	Member switch only[1]
Catalyst 1900 and 2820	9.00(-A or -EN) or later	Member switch only

[1] Catalyst 2900 XL (4-MB) switches appear in the front-panel and topology views of the Cluster Management Suite (CMS). However, CMS does not support configuration or monitoring of these switches.

Some versions of the Catalyst 2900 XL software do not support clustering, and if you have a cluster with switches that are running different versions of IOS software, software features added on the latest release might not be reflected on switches running the older versions. For example, if you start CMS on a Catalyst 2900 XL switch running Release 11.2(8)SA6, the windows and functionality can be different from a switch running Release 12.0(5)WC(1) or later.

Note The CMS is not forward-compatible, which means that if a member switch is running a software version that is newer than the release running on the command switch, the new features are not available on the member switch. If the member switch is a new device supported by a software release that is later than the software release on the command switch, the command switch cannot recognize the member switch, and it is displayed as an unknown device in the Front Panel view. You cannot configure any parameters or generate a report through CMS for that member; instead, you must launch the Device Manager application to configure and to obtain reports for that member.

Downloading Software

These are the procedures for downloading software:

- "Determining the Software Version and Feature Set" section on page 4
- "Determining Which Files to Use" section on page 5
- "Upgrading a Switch by Using CMS" section on page 5
- "Upgrading a Switch by Using the CLI" section on page 5
- "Recovering from a Software Failure" section on page 6

Note Before downloading software, read this section for important information.

Determining the Software Version and Feature Set

The Cisco IOS image is stored as a .bin file in a directory that is named with the Cisco IOS release. A subdirectory contains the files needed for web management. The image is stored on the system board Flash device (flash:).

You can use the **show version** privileged EXEC command to see the software version that is running on your switch. The second line displays C3750-I5-M for the enhanced multilayer software image (EMI) or C3750-I9-M for the standard multilayer software image (SMI).

Note Although the **show version** output always shows the software image running on the switch (Layer 2 or Layer 2/3), the model name shown at the end of this display is the factory configuration (SMI or EMI) and does not change if you upgrade the software image.

You can also use the **dir** *filesystem***:** privileged EXEC command to see the directory names of other software images that you might have stored in Flash memory.

Determining Which Files to Use

The upgrade procedures in these release notes describe how to perform the upgrade by using a combined .tar file. This file contains both the IOS image file and the files needed for the CMS. You must use the combined .tar file to upgrade the switch through the CMS. To upgrade the switch through the CLI, use the .tar file and the **archive download-sw** privileged EXEC command.

Table 3 lists the software filenames for this software release.

Table 3 Cisco IOS Software Image Files for Catalyst 3750 Switches

Filename	Description
c3750-i9-tar.121-11.AX.tar	IOS SMI image file and CMS files. This image has Layer 2+ features including access control lists (ACLs), quality of service (QoS), static routing, and the Routing Information Protocol (RIP).
c3750-i5-tar.121-11.AX.tar	IOS EMI image file and CMS files. This image has both Layer 2+ and full Layer 3 features. It includes Layer 2+ features and full Layer 3 routing (IP unicast routing, IP multicast routing, and fallback bridging). To distinguish it from the Layer 2+ static routing and RIP, the EMI includes protocols such as the Enhanced Interior Gateway Routing Protocol (EIGRP) and Open Shortest Path First (OSPF) Protocol.

Upgrading a Switch by Using CMS

You can upgrade switch software by using CMS. From the menu bar, select **Administration > Software Upgrade**. For detailed instructions, click **Help**.

Upgrading a Switch by Using the CLI

This procedure is for copying the combined .tar file to the Catalyst 3750 switch. You copy the file to the switch from a TFTP server and extract the files. You can download an image file and replace or keep the current image.

To download software, and if necessary, the TFTP server application, follow these steps:

Step 1 Use Table 3 on page 5 to identify the file that you want to download.

Step 2 Download the software image file.

- If you have a SmartNet support contract, go to this URL and log in to download the appropriate files:

  http://www.cisco.com/kobayashi/sw-center/sw-lan.shtml

- If you do not have a SmartNet contract, go to this URL and follow the instructions to register on Cisco.com and download the appropriate files:

  http://www.cisco.com/public/sw-center/sw-lan.shtml

To download the SMI and EMI files, select **Catalyst 3750 software**.

Step 3 Download the Cisco TFTP server from the URL link from Step 2, if necessary. The information on this page describes how to download and configure the TFTP server.

Step 4 Copy the image to the appropriate TFTP directory on the workstation, and make sure the TFTP server is properly configured.

For more information, refer to Appendix B in the software configuration guide for this release.

Step 5 Log in to the switch through the console port or a Telnet session.

Step 6 Check your VLAN 1 configuration by using the **show interfaces vlan 1** privileged EXEC command, and verify that VLAN 1 is part of the same network as the TFTP server. (Check the *Internet address is* line near the top of the display.)

Step 7 Download the image file from the TFTP server to the switch. If you are installing the same version of software that is currently on the switch, overwrite the current image by using this privileged EXEC command:

```
archive download-sw /overwrite /reload tftp:[[//location]/directory]/image-name.tar
```

The **/overwrite** option overwrites the software image in Flash memory with the downloaded one.

The **/reload** option reloads the system after downloading the image unless the configuration has been changed and not been saved.

For *//location*, specify the IP address of the TFTP server.

For */directory/image-name***.tar**, specify the directory (optional) and the image to download. Directory and image names are case sensitive.

This example shows how to download an image from a TFTP server at 198.30.20.19 and to overwrite the image on the switch:

```
Switch# archive download-sw /overwrite tftp://198.30.20.19/c3750-i5-tar.121-11.AX.tar
```

You can also download the image file from the TFTP server to the switch and keep the current image by replacing the **/overwrite** option with the **/leave-old-sw** option.

Recovering from a Software Failure

Switch software can be corrupted during an upgrade, by downloading the wrong file to the switch, and by deleting the image file. In all of these cases, the switch does not pass the power-on self-test (POST), and there is no connectivity. You can use the XMODEM protocol to recover from this failure.

For detailed recovery procedures, refer to the “Troubleshooting” chapter in the software configuration guide for this release.

Installation Notes

You can assign IP information to your switch by using these methods:

- The setup program (Refer to the *Catalyst 3750 Switch Hardware Installation Guide*.)
- The Dynamic Host Configuration Protocol (DHCP)-based autoconfiguration (Refer to the *Catalyst 3750 Switch Software Configuration Guide*.)
- Manually assigning an IP address (Refer to the *Catalyst 3750 Switch Software Configuration Guide*.)

New Features

These are the new supported hardware and the new software features provided this release:

- "New Hardware Features" section on page 7
- "New Software Features" section on page 7

New Hardware Features

For a list of all supported hardware, see the "Hardware Supported" section on page 2.

New Software Features

This release is the first software release for the Catalyst 3750 switch. For a detailed list of key features for this software release, refer to the *Catalyst 3750 Switch Software Configuration Guide*.

Limitations and Restrictions

You should review this section before you begin working with the switch. These are known limitations that will not be fixed, and there is not always a workaround. Some features might not work as documented, and some features could be affected by recent changes to the switch hardware or software.

These are the limitations and restrictions:

- "IOS Limitations and Restrictions" section on page 7
- "Cluster Limitations and Restrictions" section on page 9
- "CMS Limitations and Restrictions" section on page 10

IOS Limitations and Restrictions

These limitations apply to IOS configuration:

- Non-reverse-path forwarded (RPF) IP multicast traffic to a group that is bridged in a VLAN is leaked onto a trunk port in the VLAN even if the port is not a member of the group in the VLAN, but it is a member of the group in some other VLAN. Because unnecessary traffic is sent on the trunk port, it needlessly reduces the bandwidth of the port. There is no workaround for this problem because non-RPF traffic is continuous in certain topologies. As long as the trunk port is a member on a trunk port in at least one VLAN, this problem for the non-RPF traffic occurs. (CSCdu25219)
- If the number of multicast routes and Internet Group Management Protocol (IGMP) groups are more than the maximum number specified with the **show sdm prefer** global configuration command, the traffic received on unknown groups is flooded in the received VLAN even though the **show ip igmp snooping multicast-table** privileged EXEC command output shows otherwise. The workaround is to reduce the number of multicast routes and IGMP snooping groups to less than the maximum supported value. (CSCdy09008)

- After the stack master switch failover and when the previous stack master rejoins the stack, some Layer 3 configuration on routed port interfaces belonging to the previous stack master might be lost (for example, the IP address, bridge groups, and so forth). This problem occurs under these conditions:
  - When the configuration of the stack has been modified but not saved.
  - The stack master switch fails, and a new switch in the stack is elected to become the new stack master.
  - The previous stack master rejoins the stack.
  - There is at least one port on the previous stack master physically configured as a routed port with some Layer 3 configuration.

  The workaround for this problem is to save the configuration by using the **write memory** privileged EXEC command. If the problem has already occurred, reconfigure the lost settings on the routed port. (CSCdy29217)
- If the switch stack is a designated bridge in the LAN and another switch is connected to the switch stack through redundant links and has one of these redundant ports in a blocking state, sometimes the spanning-tree state topology is not the same after configuration changes in the LAN. For example, if the root bridge has some ports that go down and then come back up, the switch stack might no longer be a designated bridge after the spanning-tree states stabilizes. Another switch in the LAN that had blocked ports might become the designated bridge. In some situations, the designated bridge selection behavior is not deterministic. The workaround is to shut down the root port or the blocked port on the switch stack by using the **shutdown** interface configuration command and to bring the same port up later by using the **no shutdown** interface configuration command. (CSCdy40828)
- An egress SPAN copy of routed unicast traffic might show an incorrect destination MAC address on both local and remote SPAN sessions. This limitation does not apply to bridged packets. The workaround for local SPAN is to use the replicate option. For a remote SPAN session, there is no workaround. This is a hardware limitation. (CSCdy72835)
- Egress SPAN routed packets (both unicast and multicast) show the incorrect source MAC address. For remote SPAN packets, the source MAC address should be the MAC address of the egress VLAN, but instead the packet shows the MAC address of the remote SPAN (RSPAN) VLAN. For local SPAN packets with native encapsulation on the destination port, the packet shows the MAC address of VLAN 1. This problem does not appear with local SPAN when the encapsulation replicate option is used. This limitation does not apply to bridged packets. The workaround is to use the **encapsulate replicate** keywords in the **monitor session** global configuration command. Otherwise, there is no workaround. This is a hardware limitation. (CSCdy81521)
- IGMP filtering is applied to packets that are forwarded through hardware. It is not applied to packets that are forwarded through software. Hence, with multicast routing enabled, the first few packets are sent from a port even when IGMP filtering is set to deny those groups on that port. There is no workaround. (CSCdy82818)
- The Catalyst 3750 switch treats frames received with mixed encapsulation (802.1Q and Inter-Switch Link [ISL]) as frames with FCS errors, increments the error counters, and causes the LED to blink amber. This happens when an ISL-unaware device receives an ISL-encapsulated packet and forwards the frame to an 802.1Q trunk interface. There is no workaround. (CSCdz33708)
- IP-option software-forwarded traffic is sometimes leaked unnecessarily on a trunk port. Suppose the trunk port in question is member of an IP multicast group in VLAN X, but it is not a member in VLAN Y. In VLAN Y, there is another port that has membership to the group, and VLAN Y is the output interface for the multicast route entry corresponding to the group. IP options traffic received

on an input interface VLAN (other than VLAN Y) is unnecessarily sent on the trunk port in VLAN Y because the trunk port is forwarding in VLAN Y (even though the port has no group membership in VLAN Y). There is no workaround. (CSCdz42909)

- When you use the **ip access-group** interface configuration command with a router ACL to deny access to a group in a VLAN, multicast data to the group that is received in the VLAN is always flooded in the VLAN regardless of IGMP group membership in the VLAN. This provides reachability to directly connected clients, if any, in the VLAN. The workaround is to not apply a router ACL set to deny access to a VLAN interface. Apply the security through other means; for example, apply VLAN maps to the VLAN instead of using a router ACL for the group. (CSCdz86110)
- SNAP-encapsulated IP packets are dropped without an error message being reported at the interface. The switch does not support SNAP-encapsulated IP packets. There is no workaround. (CSCdz89142)
- During periods of very high traffic, when two RSPAN source sessions are configured, the VLAN ID of packets in one RSPAN session might overwrite the VLAN ID of the other RSPAN session. If this occurs, packets intended for one RSPAN VLAN are incorrectly sent to the other RSPAN VLAN. This problem does not affect RSPAN destination sessions. The workaround is to configure only one RSPAN source session. (CSCea72326)
- A Gigabit Ethernet connection between a SGMII (Serial Gigabit Media Independent Interface) port (3/4, 7/8, 11/12, 15/16, 19/20, and 23/24) and an Intel Pro/1000T Server Adapter NIC might loose connectivity on the Catalyst 3750G-24T and Catalyst 3750G-24TS switches. The link activates correctly, but might subsequently stop exchanging data. This is an Intel product defect. The workaround is to use RGMII (Reduced Gigabit Media Independent Interface) ports (1/2, 5/6, 9/10, 13/14, 17/18, and 21/22) instead of SGMII ports. Alternatively, use the **speed 1000** interface configuration command to force the speed of the port to 1000. (CSCea77032)
- The egress SPAN data rate might degrade when fallback bridging or multicast routing is enabled. The amount of degradation depends on the processor loading. Typically, the switch can egress SPAN up to 40,000 packets per second (64-byte packets). As long as the total traffic being monitored is below this limit, there is no degradation. However, if the traffic being monitored exceeds the limit, only a portion of the source stream is spanned. When this occurs, the following console message appears: `Decreased egress SPAN rate`. In all cases, normal traffic is not affected; the degradation limits only how much of the original source stream can be egress spanned. If fallback bridging and multicast routing are disabled, egress SPAN is not degraded. There is no workaround. If possible, disable fallback bridging and multicast routing. If possible, use ingress SPAN to observe the same traffic. (CSCeb01216)

Cluster Limitations and Restrictions

These limitations apply to cluster configuration:

- When there is a transition from the cluster active command switch to the standby command switch, Catalyst 1900, Catalyst 2820, and Catalyst 2900 4-MB switches that are cluster members might lose their cluster configuration. You must manually add these switches back to the cluster. (CSCds32517, CSCds44529, CSCds55711, CSCds55787, CSCdt70872)
- When a Catalyst 2900 XL or Catalyst 3500 XL cluster command switch is connected to a Catalyst 3550 or to a Catalyst 3750 switch, the command switch does not find any cluster candidates beyond the Catalyst 3550 or the Catalyst 3750 switch if it is not a member of the cluster. You must add the Catalyst 3550 or the Catalyst 3750 switch to the cluster. You can then see any cluster candidates connected to it. (CSCdt09918)

- If both the active command-switch and the standby command switch fail at the same time, the cluster is not automatically recreated. Even if there is a third passive command switch, it might not recreate all cluster members because it might not have all the latest cluster configuration information. You must manually recreate the cluster if both the active and standby command switches simultaneously fail. (CSCdt43501)

CMS Limitations and Restrictions

These limitations apply to CMS configuration:

- Host names and Domain Name System (DNS) server names that contain commas on a cluster command switch, member switch, or candidate switch can cause CMS to behave unexpectedly. You can avoid this instability in the interface by not using commas in host names or DNS names. Do not enter commas when entering multiple DNS names in the IP Configuration tab of the IP Management window in CMS.
- Access control entries (ACEs) that contain the **host** keyword precede all other ACEs in standard access control lists (ACLs). You can reposition the ACEs in a standard ACL with one restriction: No ACE with the **any** keyword or a wildcard mask can precede an ACE with the **host** keyword.
- CMS performance degrades if the Topology View is open for several hours on a Solaris machine. The cause might be a memory leak. The workaround is to close the browser, reopen it, and launch CMS again. (CSCds29230)
- If you are printing a Topology View or Front Panel View that contains many devices and are running Solaris 2.6 with JDK1.2.2, you might get an *Out of Memory* error message. The workaround is to close the browser, re-open it, and launch CMS again. Before you perform any other task, bring up the view that you want to print, and click **Print** in the **CMS** menu.(CSCds80920)
- If a PC running CMS has low memory and CMS is running continuously for 2 to 3 days, the PC runs out of memory. The workaround is to relaunch CMS. (CSCdv88724)
- When a VLAN or a range of VLANs is already configured and you specify a VLAN filter for a SPAN session, the current configuration for that session is overwritten with the new entry. Although the CLI appends new entries after the existing ones, CMS recreates the whole session, overwrites the current entry, and provides only a single VLAN filter per entry. The workaround is to use the CLI. It is the only method for specifying multiple VLANs for filtering in a SPAN session. (CSCdw93904)
- CMS temporarily halts while starting with Netscape version 4.75 and Java Runtime Environment (JRE) 1.3.1 or 1.4.0 on Windows 98. This also happens with Netscape version 6.2 and JRE 1.3.1 on Windows 98. When you bring up CMS, it halts while determining network information. The workaround is to click once outside of the CMS window. Then CMS should proceed. (CSCdz69724)
- When you add a new member with a username and password that is different from the existing cluster members username and password, CMS produces an exception error because of an authentication failure. The workaround is to add the new member without any username and password. When the new member is added to the cluster, remove the existing username and password from the Username and Password fields, enter a new username and password, and then apply it to all cluster members. (CSCdz07957)
- When the Link Graphs application has run for hours displaying packet drop and error information, sometimes the X-axis crosses the Y-axis at a negative y value instead of at y = 0. This condition occurs with all supported operating systems, browsers, and Java plug-ins. There is no workaround. (CSCdz32584)

Important Notes

These are the important notes related to this software release:

- "Switch Stack Notes" section on page 11
- "IOS Notes" section on page 11
- "Cluster Notes" section on page 11
- "CMS Notes" section on page 11

Switch Stack Notes

Always power off a switch before adding or removing it from a switch stack.

IOS Notes

There are no IOS configuration notes to report.

Cluster Notes

There are no cluster configuration notes to report.

CMS Notes

These notes apply to CMS configuration:

- If you use CMS on Windows 2000, it might not apply configuration changes if you change the enable password from the CLI during your CMS session. You have to restart CMS and enter the new password when prompted. Platforms other than Windows 2000 prompt you for the new enable password when it is changed.
- CMS does not display QoS classes that are created through the CLI if these classes have multiple match statements. When using CMS, you cannot create classes that match more than one match statement. CMS does not display policies that have such classes.
- If you use Internet Explorer Version 5.5 and select a URL with a nonstandard port at the end of the address (for example, *www.add.com*:84), you must enter *http://* as the URL prefix. Otherwise, you cannot launch CMS.
- Within an ACL, you can change the sequence of ACEs that have the **host** keyword. However, because such ACEs are independent of each other, the change has no effect on the way the ACL filters traffic.
- If you use the Netscape browser to view the CMS GUI and you resize the browser window while CMS is initializing, CMS does not resize to fit the window.

  Resize the browser window again when CMS is not busy.
- CMS does not start if the temporary directory on your computer runs out of memory. This problem can occur because of a bug in the 1.2.2 version of the Java plug-in. The plug-in creates temporary files in the directory whenever it runs CMS, and the directory eventually runs out of plug-in space.

The workaround is to remove all the jar_cache*.tmp files from the temporary directory. The path to the directory is different for different operating systems:

Solaris: /var/tmp
Windows NT and Windows 2000: \TEMP
Windows 95 and 98: \Windows\Temp

- In the Front Panel view or the Topology view, CMS does not display error messages in read-only mode for these switches:
  - Catalyst 2900 XL or Catalyst 3500 XL member switches running Release 12.0(5)WC2 or earlier
  - Catalyst 2950 member switches running Release 12.0(5)WC2 or earlier
  - Catalyst 3550 member switches running Release 12.1(6)EA1 or earlier

  In the Front Panel view, if the switch is running one of the previously listed software releases, the device LEDs do not appear. In the Topology view, if the member is a Long-Reach Ethernet (LRE) switch, the customer premises equipment (CPE) connected to the switch does not appear. The Bandwidth and Link graphs also do not appear in these views.

  To view switch information, you need to upgrade the member switch software. For information about upgrading switch software, see the "Downloading Software" section on page 4.

Open Caveats

These are the open caveats with possible unexpected activity in this software release:

- "Open IOS Caveats" section on page 12
- "Open CMS Caveats" section on page 16

Open IOS Caveats

These are the severity 3 IOS configuration caveats:

- CSCdz11708

  The user-configured IP address is removed when the previously acquired Dynamic Host Configuration Protocol (DHCP) IP address lease expires.

  This problem occurs under these conditions:
  - When the switch is booted without a configuration (no config.text file in Flash memory).
  - When the switch is connected to a DHCP server that is configured to give an address to it (the dynamic IP address is assigned to VLAN 1).
  - An IP address is configured on VLAN 1 before the dynamic address lease assigned to VLAN 1 expires.

  The workaround is to reconfigure the lost IP address configuration by using the **ip address** interface configuration command on VLAN 1.

- CSCdz29910

  While in the interface-range configuration mode, if you use the **no channel-group** interface configuration command or change the channel-group mode by using the **channel-group** command, an assert-fail message with traceback information appears.

The workaround is to not remove a channel group or change the channel-group mode while in interface-range configuration mode.

- CSCdz30046

  When multicast VLAN registration (MVR) groups are added or deleted, the receiver port that joined the groups after the addition still receives traffic even after the group is deleted. The correct behavior is that MVR data traffic to the group should stop flowing to the receiver port immediately after the **no mvr group** *ip-address* global configuration command is entered.

  The workaround is to disable MVR by using the **no mvr** global configuration command and then to re-enable it by using the **mvr** command. Add and delete the groups that have problems by using the **mvr group** *ip-address* and the **no mvr group** *ip-address* global configuration commands.

- CSCdz41019

  In a switch stack, if the stack master switch is reloaded at the same time that an EtherChannel link on a stack member goes down, a new stack master switch is elected but fails shortly thereafter.

  There is no workaround.

- CSCdz60348

  When an output ACL for a VLAN is full, the switch drops all the packets routed or sent to that VLAN. Because of a hardware problem, the switch cannot use software to forward. This problem occurs for all Layer 3 features, such as unicast routing, multicast routing, and fallback bridging.

  There is no workaround.

- CSCdz69741

  If there is a lot of SNMP polling activity and MAC notification traps being sent on the switch, entering the **mac-address-table notification history-size** *value* global configuration command to change the MAC address notification table history size might cause the switch to fail.

  The workaround is to disable the MAC notification traps by using the **no mac-address-table notification** command, wait for 10 seconds, and then enter the **mac-address-table notification history-size** command. After entering this command, re-enable the MAC notification traps by using the **mac-address-table notification** command.

- CSCdz79082

  A broadcast storm occurs in a bridge group under these conditions:

  - When a port in the VLAN in which fallback bridging is enabled receives a non-IP packet with the bridge protocol data unit (BPDU) indicator bit set in the ISL header.
  - The destination MAC address has not been learned in the bridge group and at least one port in the VLAN is in the blocking state.

  The broadcast storm ceases as soon as the MAC address is learned in the bridge group.

  The workaround is to make sure that all ports in a VLAN that are participating in fallback bridging are in the forwarding state.

- CSCdz80499

  Known unicast (secured addresses) are flooded within a bridge group under these conditions:

  If secure addresses are learned or configured on a port and the VLAN on this port is part of a bridge group, non-IP traffic destined to the secure addresses is flooded within the bridge group.

  The workaround is to disable fallback bridging. To remove an interface from a bridge group and to remove the bridge group, use the **no bridge-group** *bridge-group* interface configuration command. Another workaround is to disable port security on all ports in all VLANs participating in fallback bridging by using the **no switchport port-security** interface configuration command.

- CSCea02137

  When an undefined aggregate policer is configured in a policy-map, the switch automatically generates the wrong aggregate policer for it.

  The workaround is to configure an aggregate policer by using the **mls qos aggregate-policer** global configuration command before configuring the policy-map.

- CSCea02851

  When you are in policy-map class configuration mode and configure an aggregate policer with the **police aggregate** policy-map class configuration command, causing the number of aggregate policers to exceed 63, the aggregate policer is still retained in the policy map. This over-limit policer cannot be attached again and creates inconsistent behavior

  The workaround is to manually delete the over-limit policer by using the **no police aggregate** *aggregate-policer-name* policy-map class configuration command.

- CSCea21883

  Under some heavy load conditions with bridge groups and SPAN enabled (where the packets are dropped at the port because of flooding), the %SUPQ-4-CPUHB_RECV_STARVE message appears. This can be due to loops in the spanning trees. During this condition, the port output rate is reduced to recover from the condition. The message means that this condition has occurred.

  The workaround is to check the traffic pattern and the configuration of the switch to see why the port is dropping packets. Reconfigure or change the traffic pattern. If this is not possible, reduce the port output line rate by using the **srr-queue bandwidth limit 65** interface configuration command on the ports where heavy traffic is seen. If the message is not recurring, it was a transient condition, and the switch recovered from it.

- CSCea35481

  An extended access list with permit or forward actions using Layer 4 information might incorrectly forward fragmented packets. The first packet of a fragmented packet is correctly forwarded by hardware, but subsequent packets with nonzero offsets are forwarded by software or dropped.

  There is no workaround.

- CSCea54285

  You cannot set the VTP mode to transparent(3) using SNMP.

  The workaround is to set the VTP mode to transparent using the **vtp mode transparent** interface configuration command.

- CSCea67031

  The switch can take several minutes to generate and optimize the forwarding rules after you configure a complex VLAN map. For example, a complex VLAN map might contain multiple sequences that use the same VLAN map ACL, where the individual ACL clauses include one or more deny clauses (nonterminating–not the last deny). During the optimization process, the switch might not respond to commands.

  The workaround is to minimize the use of complex VLAN map ACLs. Otherwise, wait 10 to 15 minutes for the optimization to complete.

- CSCea75726

  When snooping is disabled and a spanning tree loop exists, incoming IGMP report and leave messages generate a storm of such messages in the network.

  The workaround is to enable snooping. Alternatively, shut down the blocked ports.

- CSCea86944

  Gigabit Ethernet ports configured for RGMII mode (1/2, 5/6, 9/10, 13/14, 17/18, and 21/22) might fail an internal loopback test during system startup on the Catalyst 3750G-24T and Catalyst 3750G-24TS switches. If this occurs, the port is permanently shut down and unusable. On reboot, the port might operate normally.

  The workaround is to use other ports until the next software release.

- CSCea88723

  A routed port that uses an IP ACL might not correctly filter packets after an administrative shutdown and restart. The problem can occur after the following sequence:

  - An IP ACL is applied to a routed port using the **ip access-group** interface configuration command.
  - The routed port is shut down by using the **shutdown** interface configuration command.
  - The ACL is modified or another interface is changed between routed port and switched port using the **switchport** and **no switchport** interface configuration commands.
  - The routed port is re-enabled by issuing the **no shutdown** interface configuration command.

  The workaround is to always remove the IP ACL from the routed port after an administrative shutdown and then reapply the IP ACL after re-enabling the port.

- CSCeb01226

  Gigabit Ethernet ports might have FCS errors when operating at Gigabit speeds on the Catalyst 3750G-24T and Catalyst 3750G-24TS switches. The FCS error rate for this condition is very low.

  The workaround is to restart the ports by using the **shutdown** and then **no shutdown** interface configuration commands.

- CSCeb05555

  The RSPAN feature incorrectly spans all local link control packets with a destination MAC address of 0100.0CCC.CCCC on trunk ports that carry the RSPAN VLAN. As a result, trunk ports carrying the RSPAN VLAN incorrectly combine control packets from RSPAN source ports with normal local control packets. The resulting problems vary from confusing results to improper protocol operation. The following list describes problems that can occur with selected protocols:

  - Cisco Discovery Protocol (CDP) could provide incorrect information. For example, CDP could incorrectly list a neighbor switch that is actually a neighbor on the RSPAN source port.
  - Dynamic Trunking Protocol (DTP) could fail to work properly on trunks that are carrying the RSPAN VLAN.
  - Port Aggregration Protocol (PAgP) could fail to work properly on EtherChannels that are carrying the RSPAN VLAN.
  - VLAN Trunking Protocol (VTP) could incorrectly propagate VTP pruning messages on the wrong interface. For example, a pruning message intended for an RSPAN source port could also appear on the trunk port carrying the RSPAN VLAN.
  - Unidirectional Link Detection Protocol (UDLD) and any other protocol that uses 0100.00CC.CCCC as the destination MAC address could not operate properly on trunk ports that carry the RSPAN VLAN.

  The following list describes workarounds:

  - If necessary, disable CDP by using the **no cdp enable** interface configuration command on all interfaces used as RSPAN sources.

- Do not use DTP on trunks carrying the RSPAN VLAN. Instead, use the **switchport trunk encapsulation** *encapsulation-type*, **switchport mode trunk**, and **switchport nonegotiate** interface configuration commands to create an unconditional trunk and to disable DTP negotiation.
- Do not use PAgP on trunks carrying the RSPAN VLAN. Instead, use the **channel-group** *channel-number* **mode on** interface configuration command to form the EtherChannel without negotiation.
- Prune the RSPAN VLAN from all trunk ports where it is not needed. For example, by using the **switchport trunk allowed vlan except** *rspan-vlan-id* interface configuration command to exclude specific RSPAN VLANs.

Open CMS Caveats

These are the severity 3 CMS configuration caveats:

- CSCdz52326

  In the Voice VLAN window, you cannot configure a voice VLAN when the VLAN mode is set to dynamic desirable or dynamic auto.

  The workaround is to configure the voice VLAN with static-access mode. In the Voice VLAN window, select the interface to modify, and click **Modify** to display the Modify Voice VLAN window. In the VLAN Mode drop-down list, select **Static Access**, and click **OK**. Then launch the VLAN window by selecting **VLAN > VLAN** from the menu bar. Click the **Configure Ports** tab. Select the port, and click **Modify** to launch the Modify Port Mode window. In the Administrative Mode drop-down list, select **Trunk Desirable** or **Trunk Auto**, and click **OK**.

- CSCea01123

  Certain Simple Network Management Protocol (SNMP) traps are not shown on the SNMP Trap Managers tab even though they are configured. For example, suppose you click the **Administration > SNMP > Trap Managers** tab, create a trap manager, click the vlancreate and vlandelete checkboxes along with other traps, and click **Apply**. When you select the new trap manager entry in the Current Managers list, the vlancreate and vlandelete options are not shown.

  There is no workaround.

- CSCea12761

  In the Topology View, when you right-click a device in an expanded stack to display the Device Properties window, all devices are shown as having the model number of the stack master switch. This happens even if there are several model numbers within the stack. This condition occurs with all supported operating systems, browsers, and Java plug-ins.

  There is no workaround.

- CSCea13508

  From the Users and Passwords window (**Administration > Users and Passwords**), there is no provision for enabling or disabling the login for console or VTY lines. The **line console 0 login** global configuration command is not supported in CMS.

  There is no workaround.

- CSCea15587

  Whenever a given VLAN has multiple router ports associated with it, the IGMP Router tab on the IGMP Report window (**Reports > Multicast > IGMP Report**) shows only one router port, but it should show all router ports on a given VLAN.

The workaround is to obtain the same information from the Multicast Router Ports tab on the IGMP Snooping window by selecting **Device > IGMP Snooping** from the menu bar. This tab shows all the applicable router ports.

- CSCea16267

  When you select the **Device > QoS > Policies** window and try to modify a policy, you might receive a null-pointer exception error, which prevents you from modifying the policy. The error happens if the policy uses a class that has an ACL match statement and the ACL is deleted.

  The workaround is to remove the class from the policy.

- CSCea26106 You might not be able to create or modify an EtherChannel if the ports in the EtherChannel do not meet these requirements:
  - Port group members must belong to the same set of VLANs and must be all static-access or all trunk ports. The native VLAN ID, trunk VLANs, and pruning VLANs must be the same for trunk ports.
  - Port monitoring (also known as Switched Port Analyzer [SPAN]), port security, 802.1X should not be enabled on the port.
  - Dynamic-access ports cannot be grouped.

  The workaround is to make sure that the channel-group members belong to the same allowed range of VLANs and that members are either all static-access or all trunk ports. For all trunk ports, the native VLAN, allowed VLANs on the trunk, and the VLANs in the pruning-eligible list must be the same. Do not assign a port to an EtherChannel when SPAN, port security, or 802.1X is configured on the port. Dynamic-access ports cannot belong to a channel group.

- CSCea80729

  The **Refresh** button of the CMS Inventory Report does not update the System Uptime.

  The workaround is to click the **Refresh** icon on the browser toolbar instead.

Related Documentation

These documents provide complete information about the switch and are available from this Cisco.com site:

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat3750/index.htm

You can order printed copies of documents with a DOC-xxxxxx= number from the Cisco.com sites and from the telephone numbers listed in the "Obtaining Documentation" section on page 18.

- *Catalyst 3750 Switch Software Configuration Guide* (order number DOC-7815164=)
- *Catalyst 3750 Switch Command Reference* (order number DOC-7815165=)
- *Catalyst 3750 Switch System Message Guide* (order number DOC-7815166=)
- Cluster Management Suite (CMS) online help (available only from the switch CMS software)
- *Catalyst 3750 Switch Hardware Installation Guide* (order number DOC-7815136=)
- *Cisco Small Form-Factor Pluggable Modules Installation Notes* (not orderable but available on Cisco.com)

Obtaining Documentation

Cisco provides several ways to obtain documentation, technical assistance, and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation on the World Wide Web at this URL:

http://www.cisco.com/univercd/home/home.htm

You can access the Cisco website at this URL:

http://www.cisco.com

International Cisco websites can be accessed from this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which may have shipped with your product. The Documentation CD-ROM is updated regularly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual or quarterly subscription.

Registered Cisco.com users can order a single Documentation CD-ROM (product number DOC-CONDOCCD=) through the Cisco Ordering tool:

http://www.cisco.com/en/US/partner/ordering/ordering_place_order_ordering_tool_launch.html

All users can order monthly or quarterly subscriptions through the online Subscription Store:

http://www.cisco.com/go/subscription

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/en/US/partner/ordering/index.shtml

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. On the Cisco Documentation home page, click **Feedback** at the top of the page.

You can e-mail your comments to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Customer Document Ordering
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com, which includes the Cisco Technical Assistance Center (TAC) website, as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from the Cisco TAC website. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC website, including TAC tools and utilities.

Cisco.com

Cisco.com offers a suite of interactive, networked services that let you access Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com provides a broad range of features and services to help you with these tasks:

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

To obtain customized information and service, you can self-register on Cisco.com at this URL:

http://tools.cisco.com/RPF/register/register.do

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available: the Cisco TAC website and the Cisco TAC Escalation Center. The type of support that you choose depends on the priority of the problem and the conditions stated in service contracts, when applicable.

We categorize Cisco TAC inquiries according to urgency:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration. There is little or no impact to your business operations.
- Priority level 3 (P3)—Operational performance of the network is impaired, but most business operations remain functional. You and Cisco are willing to commit resources during normal business hours to restore service to satisfactory levels.
- Priority level 2 (P2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively impacted by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.
- Priority level 1 (P1)—An existing network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Cisco TAC Website

The Cisco TAC website provides online documents and tools to help troubleshoot and resolve technical issues with Cisco products and technologies. To access the Cisco TAC website, go to this URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC website. Some services on the Cisco TAC website require a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to this URL to register:

http://tools.cisco.com/RPF/register/register.do

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC website, you can open a case online at this URL:

http://www.cisco.com/tac/caseopen

If you have Internet access, we recommend that you open P3 and P4 cases online so that you can fully describe the situation and attach any necessary files.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. These classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

Before calling, please check with your network operations center to determine the Cisco support services to which your company is entitled: for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). When you call the center, please have available your service agreement number and your product serial number.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The *Cisco Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the *Cisco Product Catalog* at this URL:

  http://www.cisco.com/en/US/products/products_catalog_links_launch.html

- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: *Internetworking Terms and Acronyms Dictionary, Internetworking Technology Handbook, Internetworking Troubleshooting Guide,* and the *Internetworking Design Guide.* For current Cisco Press titles and other information, go to Cisco Press online at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access *Packet* magazine at this URL:

  http://www.cisco.com/go/packet

- iQ Magazine is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. You can access iQ Magazine at this URL:

  http://www.cisco.com/go/iqmagazine

This document is to be used with the documentation listed in the "Related Documentation" section.