Release Notes for the Catalyst 3560E-12D Switches, Cisco IOS Release 12.2(40)EX

October 22, 2007

Cisco IOS Release 12.2(40)EX runs only on Catalyst 3560E-12D switches.

For information on other releases of the Catalyst 3560-E switches, see the release notes at this site:

http://www.cisco.com/en/US/products/ps7077/prod_release_note09186a0080899d76.html

These release notes include important information about Cisco IOS Release 12.2(40)EX 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, see the Cisco IOS release label on the rear panel of your switch.
- If your switch is on, use the **show version** privileged EXEC command. See the "Finding the Software Version and Feature Set" section on page 5.
- If you are upgrading to a new release, see the software upgrade filename for the software version. See the "Deciding Which Files to Use" section on page 5.

You can download the switch software from this site (registered Cisco.com users with a login password):

http://tools.cisco.com/support/downloads/go/MDFTree.x?butype=switches

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 in the Cisco IOS software area.

For the complete list of Catalyst 3560-E switch documentation, see the "Related Documentation" section on page 26.

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

Contents

This information is in the release notes:

System Requirements

The system requirements are described in these sections:

Hardware Supported

Table 1 lists the hardware supported on this release.

Table 1 Catalyst 3560E-12D Switch Supported Hardware

Switch Hardware	Description	Supported by Minimum Cisco IOS Release
Cisco Catalyst 3560E-12D	12 10-Gigabit Ethernet X2 module slots	Cisco IOS Release 12.2(40)EX
Cisco X2 transceiver modules	X2-10GB-SR V02 or later X2-10GB-LR V03 or later X2-10GB-ER V02 or later X2-10GB-CX4 V03 or later X2-10GB-LX4 V03 or later X2-10GB-LRM	Cisco IOS Release 12.2(40)EX
Cisco TwinGig Converter Module	Dual SFP[1] X2 converter module to allow the switch to support SFP Gigabit Ethernet modules	Cisco IOS Release 12.2(40)EX

Table 1 Catalyst 3560E-12D Switch Supported Hardware (continued)

Switch Hardware	Description	Supported by Minimum Cisco IOS Release
SFP modules	1000BASE-LX/LH 1000BASE-SX 1000BASE-ZX 1000BASE-BX10-D 1000BASE-BX10-U 1000BASE-T 100BASE-FX CWDM[2]	Cisco IOS Release 12.2(40)EX
C3K-PWR-300WAC	300-W AC power supply module for Catalyst 3560E-12D switches	Cisco IOS Release 12.2(40)EX
C3K-PWR-300WDC	300-W DC power supply module for Catalyst 3560E-12D switches	Cisco IOS Release 12.2(40)EX
C3K-FAN-16CFM	Fan module for Catalyst 3560E-12D switches	Cisco IOS Release 12.2(40)EX

1. SFP = small form-factor pluggable.
2. CWDM = coarse wavelength-division multiplexer.

Device Manager System Requirements

These sections describe the hardware and software requirements for using the device manager:

- "Hardware Requirements" section on page 3
- "Software Requirements" section on page 3

Hardware Requirements

Table 2 lists the minimum hardware requirements for running the device manager.

Table 2 Minimum Hardware Requirements

Processor Speed	DRAM	Number of Colors	Resolution	Font Size
Intel Pentium II[1]	64 MB[2]	256	1024 x 768	Small

1. We recommend Intel Pentium 4.
2. We recommend 256-MB DRAM.

Software Requirements

Table 3 lists the supported operating systems and browsers for using the device manager. The device manager verifies the browser version when starting a session to ensure that the browser is supported.

Note The device manager does not require a plug-in.

Table 3 Supported Operating Systems and Browsers

Operating System	Minimum Service Pack or Patch	Microsoft Internet Explorer[1]	Netscape Navigator
Windows 2000	None	5.5 or 6.0	7.1
Windows XP	None	5.5 or 6.0	7.1

1. Service Pack 1 or higher is required for Internet Explorer 5.5.

Cluster Compatibility

You cannot create and manage switch clusters through the device manager. To create and manage switch clusters, use the command-line interface (CLI) or the Network Assistant application.

When creating a switch cluster or adding a switch to a cluster, follow these guidelines:

- When you create a switch cluster, we recommend configuring the highest-end switch in your cluster as the command switch.
- If you are managing the cluster through Network Assistant, the switch with the latest software should be the command switch.
- The standby command switch must be the same type as the command switch. For example, if the command switch is a Catalyst 3750-E switch, all standby command switches must be Catalyst 3750-E switches.

For additional information about clustering, see *Getting Started with Cisco Network Assistant* and *Release Notes for Cisco Network Assistant* (not orderable but available on Cisco.com), the software configuration guide, and the command reference.

CNA Compatibility

Cisco IOS Release 12.2(40)EX and later is only compatible with Cisco Network Assistant 5.0 and later. You can download Network Assistant from this URL:

http://www.cisco.com/pcgi-bin/tablebuild.pl/NetworkAssistant

For more information about Cisco Network Assistant, see the *Release Notes for Cisco Network Assistant* on Cisco.com.

Upgrading the Switch Software

These are the procedures for downloading software. Before downloading software, read this section for important information:

Finding 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 of the display shows the version.

Note Although the **show version** output always shows the software image running on the switch, the model name shown at the end of this display is the factory configuration (IP base feature set or IP services feature set) and does not change if you upgrade the software license.

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.

Deciding 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 the Cisco IOS image file and the files needed for the embedded device manager. You must use the combined tar file to upgrade the switch through the device manager. To upgrade the switch through the command-line interface (CLI), use the tar file and the **archive download-sw** privileged EXEC command.

Table 4 lists the filenames for this software release.

Note For IPv6 routing and IPv6 ACL capability on the Catalyst 3560E-12D switch, you must get the advanced IP services software license from Cisco.

Table 4 Cisco IOS Software Image Files for Catalyst 3560E-12D Switches

Filename	Description
c3560e-universal-tar.122-40.EX.tar	Catalyst 3560E-12D switch universal image and device manager files. This image has all the supported features that are enabled by the software license installed on the switch.
c3560e-universalk9-tar.122-40.EX.tar	Catalyst 3560E-12D switch universal cryptographic image and device manager files. This image has the Kerberos, SSH, SSL, and SNMPv3 in addition to the features supported in the universal image.

The universal software images support multiple feature sets. Use the software activation feature to deploy a software license and to enable a specific feature set. For information about software activation, see the *Cisco Software Activation and Compatibility Document* on Cisco.com:

http://www.cisco.com/en/US/products/ps7077/tsd_products_support_series_home.html

Archiving Software Images

Before upgrading your switch software, make sure that you have archived copies of the current Cisco IOS release and the Cisco IOS release from which you are upgrading. You should keep these archived images until you have upgraded all devices in the network to the new Cisco IOS image and until you have verified that the new Cisco IOS image works properly in your network.

Cisco routinely removes old Cisco IOS versions from Cisco.com. See *Product Bulletin 2863* for more information:

http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/prod_bulletin0900aecd80281c0e.html

You can copy the bin software image file on the flash memory to the appropriate TFTP directory on a host by using the **copy flash: tftp:** privileged EXEC command.

Note Although you can copy any file on the flash memory to the TFTP server, it is time-consuming to copy all of the HTML files in the tar file. We recommend that you download the tar file from Cisco.com and archive it on an internal host in your network.

You can also configure the switch as a TFTP server to copy files from one switch to another without using an external TFTP server by using the **tftp-server** global configuration command. For more information about the **tftp-server** command, see the "Basic File Transfer Services Commands" section of the *Cisco IOS Configuration Fundamentals Command Reference, Release 12.2,* at this URL:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_command_reference_book09186a00800811e0.html

Upgrading a Switch by Using the Device Manager or Network Assistant

You can upgrade switch software by using the device manager or Network Assistant. For detailed instructions, click **Help**.

Note When using the device manager to upgrade your switch, do not use or close your browser session after the upgrade process begins. Wait until after the upgrade process completes.

Upgrading a Switch by Using the CLI

This procedure is for copying the combined tar file to the 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, follow these steps:

Step 1 Use Table 4 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

To download the universal software image files for a Catalyst 3560E-12D switch, click **Catalyst 3560-E software**. To obtain authorization and to download the cryptographic software files, click **Catalyst 3560-E 3DES Cryptographic Software**.

Step 3 Copy the image to the appropriate TFTP directory on the workstation, and make sure that the TFTP server is properly configured.

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

Step 4 Log into the switch through the console port or a Telnet session.

Step 5 (Optional) Ensure that you have IP connectivity to the TFTP server by entering this privileged EXEC command:

```
Switch# ping tftp-server-address
```

For more information about assigning an IP address and default gateway to the switch, see the software configuration guide for this release.

Step 6 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 entering this privileged EXEC command:

```
Switch# 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 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/c3560e-universal-tar.122-40.EX.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

For additional recovery procedures, see 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 Express Setup program, as described in the switch getting started guide.
- The CLI-based setup program, as described in the switch hardware installation guide.
- The DHCP-based autoconfiguration, as described in the switch software configuration guide.
- Manually assigning an IP address, as described in the switch software configuration guide.

New Features

This section describes the new supported hardware and the new and updated software features provided in this release.

New Hardware Features

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

New Software Features

This is the new software feature for this release:

Fan failures—When this feature is enabled, the Catalyst 3560E-12D switch automatically shuts down when more than one fan fails.

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.

This section contains these limitations:

Cisco IOS Limitations

Unless otherwise noted, these limitations apply to the Catalyst 3560E-12D switches:

Access Control List

These are the access control list (ACL) limitations:

- The Catalyst 3560-E switch has 964 TCAM entries available for ACLs in the default and routing SDM templates instead of the 1024 entries that are available on the Catalyst 3560 switch.

  There is no workaround. (CSCse33114)

- When a MAC access list is used to block packets from a specific source MAC address, that MAC address is entered in the switch MAC-address table.

  The workaround is to block traffic from the specific MAC address by using the **mac address-table static** *mac-addr* **vlan** *vlan-id* **drop** global configuration command. (CSCse73823)

Address Resolution Protocol

This is an Address Resolution Protocol limitation:

- The switch might place a port in an error-disabled state due to an Address Resolution Protocol (ARP) rate limit exception even when the ARP traffic on the port is not exceeding the configured limit. This could happen when the burst interval setting is 1 second, the default.

  The workaround is to set the burst interval to more than 1 second. We recommend setting the burst interval to 3 seconds even if you are not experiencing this problem.(CSCse06827))

Cisco X2 Transceiver Modules and SFP Modules

These are the Cisco X2 transceiver module and SFP module limitations:

- Cisco X2-10GB-LR transceiver modules with a version identification number lower than V03 might show intermittent frame check sequence (FCS) errors or be ejected from the switch during periods of operational shock greater than 50g. There is no workaround. (CSCse14048)
- Cisco X2-10GB-CX4 transceiver modules with a version identification number lower than V03 might be difficult to insert because of a dimensional tolerance discrepancy. The workaround is to use modules with a version identification number of V03 or later. (CSCsg28558)
- Switches with the Cisco X2-10GB-LX4 transceiver modules with a version identification number prior to V03 might intermittently fail. The workaround is to use Cisco X2-10GB-LX4 transceiver modules with a version identification number of V03 or later. (CSCsh60076)
- Cisco GLC-GE-100FX SFP modules with a serial number between OPC0926xxxx and OPC0945xxxx might show intermittent *module not valid*, data, status, link-flapping, and FCS errors. The workaround is to use modules with serial numbers that are not in the specified range. (CSCsh59585)
- When switches are installed closely together and the uplink ports of adjacent switches are in use, you might have problems accessing the SFP module bale-clasp latch to remove the SFP module or the SFP cable (Ethernet or fiber). Use one of these workarounds:
  - Allow space between the switches when installing them.
  - In a switch stack, plan the SFP module and cable installation so that uplinks in adjacent stack members are not all in use.
  - Use long, small screwdriver to access the latch then remove the SFP module and cable. (CSCsd57938)
- When a Cisco X2-10GB-CX4 transceiver module is in the X2 transceiver module port and you enter the **show controllers ethernet-controller tengigabitethernet** privileged EXEC command, the command displays some fields as unspecified. This is the expected behavior based IEEE 802.3ae. (CSCsd47344)

- The far-end fault optional facility is not supported on the GLC-GE-100FX SFP module. The workaround is to configure aggressive UDLD. (CSCsh70244).

Configuration

These are the configuration limitations:

- When an excessive number (more than 100 packets per second) of Address Resolution Protocol (ARP) packets are sent to a Network Admission Control (NAC) Layer 2 IP-configured member port, a switch might display a message similar to this:

  ```
  PLATFORM_RPC-3-MSG_THROTTLED: RPC Msg Dropped by throttle mechanism: type 0, class
  51, max_msg 128, total throttled 984323
  -Traceback= 6625EC 5DB4C0 5DAA98 55CA80 A2F2E0 A268D8
  ```

  No workaround is necessary. Under normal conditions, the switch generates this notification when snooping the next ARP packet. (CSCse47548)

- When there is a VLAN with protected ports configured in fallback bridge group, packets might not be forwarded between the protected ports.

  The workaround is to not configure VLANs with protected ports as part of a fallback bridge group. (CSCsg40322)

  When a switch port configuration is set at 10 Mb/s half duplex, sometimes the port does not send in one direction until the port traffic is stopped and then restarted. You can detect the condition by using the **show controller ethernet-controller** or the **show interfaces** privileged EXEC commands.

  The workaround is to stop the traffic in the direction in which it is not being forwarded, and then restart it after 2 seconds. You can also use the **shutdown** interface configuration command followed by the **no shutdown** command on the interface. (CSCsh04301)

- When line rate traffic is passing through a dynamic port, and you enter the **switchport access vlan dynamic** interface configuration command for a range of ports, the VLANs might not be assigned correctly. One or more VLANs with a null ID appears in the MAC address table instead.

  The workaround is to enter the **switchport access vlan dynamic** interface configuration command separately on each port.(CSCsi26392)

IEEE 802.1x Authentication

These are the IEEE 802.1x authentication limitations:

- If a supplicant using a Marvel Yukon network interface card (NIC) is connected an IEEE 802.1x-authorized port in multihost mode, the extra MAC address of 0c00.0000.0000 appears in the MAC address table.

  Use one of these workarounds (CSCsd90495):

  - Configure the port for single-host mode to prevent the extra MAC address from appearing in the MAC address table.
  - Replace the NIC card with a new card.

- When MAC authentication bypass is configured to use Extensible Authentication Protocol (EAP) for authorization and critical authentication is configured to assign a critical port to an access VLAN:

  - If the connected device is supposed to be unauthorized, the connected device might be authorized on the VLAN that is assigned to the critical port instead of to a guest VLAN.

  - If the device is supposed to be authorized, it is authorized on the VLAN that is assigned to the critical port.

  Use one of these workarounds (CSCse04534):

  - Configure MAC authentication bypass to not use EAP.
  - Define your network access profiles to not use MAC authentication bypass. For more information, see the Cisco Access Control Server (ACS) documentation.

Multicasting

These are the multicasting limitations:

- Multicast packets with a time-to-live (TTL) value of 0 or 1 are flooded in the incoming VLAN when all of these conditions are met:
  - Multicast routing is enabled in the VLAN.
  - The source IP address of the packet belongs to the directly connected network.
  - The TTL value is either 0 or 1.

  The workaround is to not generate multicast packets with a TTL value of 0 or 1, or disable multicast routing in the VLAN. (CSCeh21660)
- Multicast packets denied by the multicast boundary access list are flooded in the incoming VLAN when all of these conditions are met:
  - Multicast routing is enabled in the VLAN.
  - The source IP address of the multicast packet belongs to a directly connected network.
  - The packet is denied by the IP multicast boundary access-list configured on the VLAN.

  There is no workaround. (CSCei08359)
- Reverse path forwarding (RPF) failed multicast traffic might cause a flood of Protocol Independent Multicast (PIM) messages in the VLAN when a packet source IP address is not reachable.

  The workaround is to not send RPF-failed multicast traffic, or make sure that the source IP address of the RPF-failed packet is reachable. (CSCsd28944)
- If the **clear ip mroute** privileged EXEC command is used when multicast packets are present, it might cause temporary flooding of incoming multicast traffic in the VLAN.

  There is no workaround. (CSCsd45753)
- When you configure the **ip igmp max-groups** *number* and **ip igmp max-groups action replace** interface configuration commands and the number of reports exceed the configured max-groups value, the number of groups might temporarily exceed the configured max-groups value. No workaround is necessary because the problem corrects itself when the rate or number of IGMP reports are reduced. (CSCse27757)

QoS

These are the quality of service (QoS) limitations:

- When QoS is enabled and the egress port receives pause frames at the line rate, the port cannot send packets.

  There is no workaround. (CSCeh18677)

- Egress shaped round robin (SRR) sharing weights do not work properly with system jumbo MTU frames.

  There is no workaround. (CSCsc63334)

- In a hierarchical policy map, if the VLAN-level policy map is attached to a VLAN interface and the name of the interface-level policy map is the same as that for another VLAN-level policy map, the switch rejects the configuration, and the VLAN-level policy map is removed from the interface.

  The workaround is to use a different name for the interface-level policy map. (CSCsd84001)

- If the ingress queue has low buffer settings and the switch sends multiple data streams of system jumbo MTU frames at the same time at the line rate, the frames are dropped at the ingress.

  There is no workaround. (CSCsd72001)

- When you use the **srr-queue bandwidth limit** interface configuration command to limit port bandwidth, packets that are less than 256 bytes can cause inaccurate port bandwidth readings. The accuracy is improved when the packet size is greater than 512 bytes. There is no workaround. (CSCsg79627)

Routing

This is the routing limitation:

- When the PBR is enabled and QoS is enabled with DSCP settings, the CPU utilization might be high if traffic is sent to unknown destinations.

  The workaround is to not send traffic to unknown destinations. (CSCse97660)

SPAN and RSPAN

These are the SPAN and Remote SPAN (RSPAN) limitations.

- When egress SPAN is running on a 10-Gigabit Ethernet port, only about 12 percent of the egress traffic is monitored.

  There is no workaround. This is a hardware limitation. (CSCei10129)

- When the **logging event-spanning-tree** interface configuration command is configured and logging to the console is enabled, a topology change might generate a large number of logging messages, causing high CPU utilization. CPU utilization can increase with the number of spanning-tree instances and the number of interfaces configured with the **logging event-spanning-tree** interface configuration command. This condition adversely affects how the switch operates and could cause problems such as STP convergence delay.

  High CPU utilization can also occur with other conditions, such as when debug messages are logged at a high rate to the console.

  Use one of these workarounds:

  - Disable logging to the console.
  - Rate-limit logging messages to the console. (CSCsg91027)
  - Remove the **logging event spanning-tree** interface configuration command from the interfaces.

- The far-end fault optional facility is not supported on the GLC-GE-100FX SFP module.

  The workaround is to configure aggressive UDLD. (CSCsh70244).

Device Manager Limitations

This is the device manager limitation:

- When you are prompted to accept the security certificate and you click *No*, you only see a blank screen, and the device manager does not launch.

  The workaround is to click *Yes* when you are prompted to accept the certificate. (CSCef45718)

Important Notes

These sections describe the important notes related to this software release for the Catalyst 3560E-12D switch:

- "Cisco IOS Notes" section on page 13
- "Device Manager Notes" section on page 13

Cisco IOS Notes

These notes apply to Cisco IOS software:

- If the switch requests information from the Cisco Secure Access Control Server (ACS) and the message exchange times out because the server does not respond, a message similar to this appears:

  ```
  00:02:57: %RADIUS-4-RADIUS_DEAD: RADIUS server 172.20.246.206:1645,1646 is not
  responding.
  ```

  If this message appears, make sure that there is network connectivity between the switch and the ACS. You should also make sure that the switch has been properly configured as an AAA client on the ACS.

- If the switch has interfaces with automatic QoS for voice over IP (VoIP) configured and you upgrade the switch software to Cisco IOS Release 12.2(40)SE (or later), when you enter the **auto qos voip cisco-phone** interface configuration command on another interface, you might see this message:

  ```
  AutoQoS Error: ciscophone input service policy was not properly applied
  policy map AutoQoS-Police-CiscoPhone not configured
  ```

  If this happens, enter the **no auto qos voip cisco-phone** interface command on all interface with this configuration to delete it. Then enter the **auto qos voip cisco-phone** command on each of these interfaces to reapply the configuration.

Device Manager Notes

These notes apply to the device manager:

- You cannot create and manage switch clusters through the device manager. To create and manage switch clusters, use the CLI or Cisco Network Assistant.
- When the switch is running a localized version of the device manager, the switch displays settings and status only in English letters. Input entries on the switch can only be in English letters.
- For device manager session on Internet Explorer, popup messages in Japanese or in simplified Chinese can appear as garbled text. These messages appear properly if your operating system is in Japanese or Chinese.

- We recommend this browser setting to speed up the time needed to display the device manager from Microsoft Internet Explorer.

  From Microsoft Internet Explorer:

  1. Choose **Tools > Internet Options**.
  2. Click **Settings** in the "Temporary Internet files" area.
  3. From the Settings window, choose **Automatically**.
  4. Click **OK**.
  5. Click **OK** to exit the Internet Options window.
- The HTTP server interface must be enabled to display the device manager. By default, the HTTP server is enabled on the switch. Use the **show running-config** privileged EXEC command to see if the HTTP server is enabled or disabled.

Beginning in privileged EXEC mode, follow these steps to configure the HTTP server interface:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**ip http authentication** {**aaa** | **enable** | **local**}	Configure the HTTP server interface for the type of authentication that you want to use. • **aaa**—Enable the authentication, authorization, and accounting feature. You must enter the **aaa new-model** interface configuration command for the **aaa** keyword to appear. • **enable**—Enable password, which is the default method of HTTP server user authentication, is used. • **local**—Local user database, as defined on the Cisco router or access server, is used.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show running-config**	Verify your entries.

- The device manager uses the HTTP protocol (the default is port 80) and the default method of authentication (the enable password) to communicate with the switch through any of its Ethernet ports and to allow switch management from a standard web browser.

  If you change the HTTP port, you must include the new port number when you enter the IP address in the browser **Location** or **Address** field (for example, http://10.1.126.45:184 where 184 is the new HTTP port number). You should write down the port number through which you are connected. Use care when changing the switch IP information.

  If you are *not* using the default method of authentication (the enable password), you need to configure the HTTP server interface with the method of authentication used on the switch.

Beginning in privileged EXEC mode, follow these steps to configure the HTTP server interface:

	Command	Purpose
Step 1	**configure terminal**	Enter global configuration mode.
Step 2	**ip http authentication** {**enable** | **local** | **tacacs**}	Configure the HTTP server interface for the type of authentication that you want to use. • **enable**—Enable password, which is the default method of HTTP server user authentication, is used. • **local**—Local user database, as defined on the Cisco router or access server, is used. • **tacacs**—TACACS server is used.
Step 3	**end**	Return to privileged EXEC mode.
Step 4	**show running-config**	Verify your entries.

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.cisco.com:84*), you must enter *http://* as the URL prefix. Otherwise, you cannot launch the device manager.

Open Caveats

This section describes the open caveats with possible unexpected activity in this software release. Unless otherwise noted, these severity 3 Cisco IOS configuration caveats apply to the switch:

- CSCsg58889

  If IEEE 802.1Q tunneling and Layer 2 protocol tunneling are configured first on physical ports, and the ports are then added to an unconfigured port channel, the port channel might stop forwarding traffic if one or more physical ports in the EtherChannel are shut down.

  These are the workarounds:

  – Remove and reapply the Layer 2 protocol tunneling configuration on the port channel.

  – Configure the port channel first, next configure the physical ports, and then add them to the port channel.

- CSCsg77818

  When a switch interface is configured with trust boundary and Cisco Discovery Protocol (CDP) or the CDP table is repeatedly disabled, enabled, or cleared, the switch might reload.

  The workaround is to avoid repeatedly disabling, enabling, or clearing CDP or the CDP table when trust boundary is configured on an interface. Or, disable trust boundary first before repeatedly disabling, enabling, or clearing CDP or the CDP table.

- CSCsh12472

  The switch might display tracebacks similar to this example when an EtherChannel interface port-channel type changes from Layer 2 to Layer 3 or the reverse:

  ```
  15:50:11: %COMMON_FIB-4-FIBNULLHWIDB: Missing hwidb for fibhwidb Port-channel1
  (ifindex 1632) -Traceback= A585C B881B8 B891CC 2F4F70 5550E8 564EAC 851338 84AF0C
  4CEB50 859DF4 A7BF28 A98260 882658 879A58
  ```

  There is no workaround.

- CSCsh70377

  When a secondary VLAN is disassociated from the primary VLAN, duplicate MAC addresses on the primary VLAN remain in the MAC address table.

  The workaround is to disassociate the secondary VLAN from the primary VLAN by entering these commands (in this order):

  clear port-security {**all** | **interface** *interface-id*) privileged EXEC command

  primary-vlan association remove *vlan-id* VLAN configuration mode command.

- CSCsi01526

  Traceback messages appear if you enter the **no switchport** interface configuration command to change a Layer 2 interface that belongs to a port channel to a routed port.

  There is no workaround.

- CSCsi06399

  When a RIP network and IP address are configured on an interface, a traceback error occurs after you enter the **shutdown**, **no shutdown, switchport** and **no switchport** interface configuration commands.

  The workaround is to configure the RIP network and the IP address after you configure the interface.

- CSCsi16162

  When you enter an all 0s route with an all 1s mask in the routing table and the next hop is entered as an interface, a traceback message appears.

  The workaround is to use an IP address as the next hop instead of an interface.

- CSCsi50367

  When changing a switch port access VLAN from static to dynamic or the reverse, a message similar to this might appear:

  ```
  01:43:55: PSECURE: Assert failure: is_etherchnl(hwidb_or_null swidb)):
  ../switch/psecure/psecure_ifc.c: 412: psecure_get_vlanid (l2a1-5) 01:43:55Traceback=
  804484 809604 802258 806904 70FC 8D70 5C97BC 6901DC 6903CC 9EF8D8 9E6CC4 (l2a1-5)
  ```

  There is no workaround necessary. This message does not affect switch functionality.

- CSCsi67680

  When unicast routing is disabled and then re-enabled, virtual routing and forwarding (VRF) routing is disabled on the switch interfaces.

  The workaround is to enter the **shut** and **no shut** interface configuration commands on the affected interfaces.

- CSCsi70454

  The configuration file used for the configuration replacement feature requires the character string *end\n* at the end of the file. The Windows Notepad text editor does not add the *end\n* string, and the configuration rollback does not work.

  These are the workarounds. (You only need to do one of these.)

  - Do not use a configuration file that is stored by or edited with Windows Notepad.
  - Manually add the character string *end\n* to the end of the file.

  The workaround is to configure routed IPv4 multicast and IPv6 unicast traffic in different switch ports.

- CSCsi71768

  If you upgrade the software image from Cisco IOS Release 12.2(25)SEE2 to Cisco IOS Release 12.2(35)SE1, the IPv6 static routes are in the switch configuration but might not be in the routing table.

  The workaround is to specify the egress interface on the IPv6 static route.

- CSCsj10198

  When a per-port per-VLAN policy map (a hierarchical VLAN-based policy map) is attached to a VLAN interface, and you remove the child-policy policer from the policy map and then add it back, the policy map fails to re-attach to the same SVI.

  The workaround is to delete the child policy, which removes it from the parent policy. Then recreate the child policy (with the same or a different name) and reference it in the parent policy. The parent policy then successfully attaches to the SVI.

- CSCsj77933

  In Cisco IOS Release 12.2(35)SE and Cisco IOS Release 12.2(37)SE, if you enter a space before a comma in the **define interface-range** or the **interface range global** configuration command, the space before the comma is not saved in the switch configuration.

  There is no workaround.

Resolved Caveat

This section describes the caveat that has been resolved in this release:

- CSCsi63999

  Changing the spanning tree mode from rapid STP to MSTP no longer causes tracebacks when the virtual port error-disable feature is enabled when the STP mode is changed.

Documentation Updates

These sections provide updates to the product documentation:

Updates to the Software Configuration Guide

These are the updates to the Software Configuration Guide for the Catalyst 3750-E and Catalyst 3560-E switches:

EIGRP Routing Note

If the switch is running the IP base feature set, you can configure complete EIGRP routing. However, the configuration is not implemented because the IP base feature set supports only EIGRP stub routing, as described in the "Configuring IP Unicast Routing" chapter of the software configuration guide.

After you have entered the **eigrp stub** router configuration command, only the **eigrp stub connected summary** command takes effect. Although the CLI help might show the **receive-only** and **static** keywords and you can enter these keywords, the switch running the IP base image always behaves as if the **connected** and **summary** keywords were configured.

Configuring Source-Specific Multicast

This section describes how to configure source-specific multicast (SSM). For a complete description of the SSM commands in this section, refer to the "IP Multicast Routing Commands" chapter of the *Cisco IOS IP Command Reference, Volume 3 of 3: Multicast*. To locate documentation for other commands that appear in this chapter, use the command reference master index, or search online.

The SSM feature is an extension of IP multicast in which datagram traffic is forwarded to receivers from only those multicast sources that the receivers have explicitly joined. For multicast groups configured for SSM, only SSM distribution trees (no shared trees) are created.

SSM Components Overview

SSM is a datagram delivery model that best supports one-to-many applications, also known as broadcast applications. SSM is a core networking technology for the Cisco implementation of IP multicast solutions targeted for audio and video broadcast application environments. The switch supports these components that support the implementation of SSM:

- Protocol independent multicast source-specific mode (PIM-SSM)

  PIM-SSM is the routing protocol that supports the implementation of SSM and is derived from PIM sparse mode (PIM-SM).

- Internet Group Management Protocol version 3 (IGMPv3)

To run SSM with IGMPv3, SSM must be supported in the Cisco IOS router, the host where the application is running, and the application itself.

How SSM Differs from Internet Standard Multicast

The current IP multicast infrastructure in the Internet and many enterprise intranets is based on the PIM-SM protocol and Multicast Source Discovery Protocol (MSDP). These protocols have the limitations of the Internet Standard Multicast (ISM) service model. For example, with ISM, the network must maintain knowledge about which hosts in the network are actively sending multicast traffic.

The ISM service consists of the delivery of IP datagrams from any source to a group of receivers called the multicast host group. The datagram traffic for the multicast host group consists of datagrams with an arbitrary IP unicast source address S and the multicast group address G as the IP destination address. Systems receive this traffic by becoming members of the host group.

Membership in a host group simply requires signalling the host group through IGMP version 1, 2, or 3. In SSM, delivery of datagrams is based on (S, G) channels. In both SSM and ISM, no signalling is required to become a source. However, in SSM, receivers must subscribe or unsubscribe to (S, G) channels to receive or not receive traffic from specific sources. In other words, receivers can receive traffic only from (S, G) channels to which they are subscribed, whereas in ISM, receivers need not know the IP addresses of sources from which they receive their traffic. The proposed standard approach for channel subscription signalling use IGMP include mode membership reports, which are supported only in IGMP version 3.

SSM IP Address Range

SSM can coexist with the ISM service by applying the SSM delivery model to a configured subset of the IP multicast group address range. Cisco IOS software allows SSM configuration for the IP multicast address range of 224.0.0.0 through 239.255.255.255. When an SSM range is defined, existing IP multicast receiver applications do not receive any traffic when they try to use an address in the SSM range (unless the application is modified to use an explicit (S, G) channel subscription).

SSM Operations

An established network, in which IP multicast service is based on PIM-SM, can support SSM services. SSM can also be deployed alone in a network without the full range of protocols that are required for interdomain PIM-SM (for example, MSDP, Auto-RP, or bootstrap router [BSR]) if only SSM service is needed.

If SSM is deployed in a network already configured for PIM-SM, only the last-hop routers support SSM. Routers that are not directly connected to receivers do not require support for SSM. In general, these not-last-hop routers must only run PIM-SM in the SSM range and might need additional access control configuration to suppress MSDP signalling, registering, or PIM-SM shared tree operations from occurring within the SSM range.

Use the **ip pim ssm** global configuration command to configure the SSM range and to enable SSM. This configuration has the following effects:

- For groups within the SSM range, (S, G) channel subscriptions are accepted through IGMPv3 include-mode membership reports.
- PIM operations within the SSM range of addresses change to PIM-SSM, a mode derived from PIM-SM. In this mode, only PIM (S, G) join and prune messages are generated by the router, and no (S, G) rendezvous point tree (RPT) or (*, G) RPT messages are generated. Incoming messages related to RPT operations are ignored or rejected, and incoming PIM register messages are

immediately answered with register-stop messages. PIM-SSM is backward-compatible with PIM-SM unless a router is a last-hop router. Therefore, routers that are not last-hop routers can run PIM-SM for SSM groups (for example, if they do not yet support SSM).

- No MSDP source-active (SA) messages within the SSM range are accepted, generated, or forwarded.

IGMPv3 Host Signalling

In IGMPv3, hosts signal membership to last hop routers of multicast groups. Hosts can signal group membership with filtering capabilities with respect to sources. A host can either signal that it wants to receive traffic from all sources sending to a group except for some specific sources (called exclude mode), or that it wants to receive traffic only from some specific sources sending to the group (called include mode).

IGMPv3 can operate with both ISM and SSM. In ISM, both exclude and include mode reports are applicable. In SSM, only include mode reports are accepted by the last-hop router. Exclude mode reports are ignored.

Configuration Guidelines

This section contains the guidelines for configuring SSM.

Legacy Applications Within the SSM Range Restrictions

Existing applications in a network predating SSM do not work within the SSM range unless they are modified to support (S, G) channel subscriptions. Therefore, enabling SSM in a network can cause problems for existing applications if they use addresses within the designated SSM range.

Address Management Restrictions

Address management is still necessary to some degree when SSM is used with Layer 2 switching mechanisms. Cisco Group Management Protocol (CGMP), IGMP snooping, or Router-Port Group Management Protocol (RGMP) support only group-specific filtering, not (S, G) channel-specific filtering. If different receivers in a switched network request different (S, G) channels sharing the same group, they do not benefit from these existing mechanisms. Instead, both receivers receive all (S, G) channel traffic and filter out the unwanted traffic on input. Because SSM can re-use the group addresses in the SSM range for many independent applications, this situation can lead to decreased traffic filtering in a switched network. For this reason, it is important to use random IP addresses from the SSM range for an application to minimize the chance for re-use of a single address within the SSM range between different applications. For example, an application service providing a set of television channels should, even with SSM, use a different group for each television (S, G) channel. This setup guarantees that multiple receivers to different channels within the same application service never experience traffic aliasing in networks that include Layer 2 switches.

IGMP Snooping and CGMP Limitations

IGMPv3 uses new membership report messages that might not be correctly recognized by older IGMP snooping switches.

For more information about switching issues related to IGMP (especially with CGMP), refer to the “Configuring IGMP Version 3” section of the “Configuring IP Multicast Routing” chapter.

State Maintenance Limitations

In PIM-SSM, the last hop router continues to periodically send (S, G) join messages if appropriate (S, G) subscriptions are on the interfaces. Therefore, as long as receivers send (S, G) subscriptions, the shortest path tree (SPT) state from the receivers to the source is maintained, even if the source does not send traffic for longer periods of time (or even never).

This case is opposite to PIM-SM, where (S, G) state is maintained only if the source is sending traffic and receivers are joining the group. If a source stops sending traffic for more than 3 minutes in PIM-SM, the (S, G) state is deleted and only re-established after packets from the source arrive again through the RPT. Because no mechanism in PIM-SSM notifies a receiver that a source is active, the network must maintain the (S, G) state in PIM-SSM as long as receivers are requesting receipt of that channel.

Configuring SSM

Beginning in privileged EXEC mode, follow these steps to configure SSM:

	Command	Purpose
Step 1	**ip pim ssm** [**default** | **range** *access-list*]	Define the SSM range of IP multicast addresses.
Step 2	**interface** type number	Select an interface that is connected to hosts on which IGMPv3 can be enabled, and enter the interface configuration mode.
Step 3	**ip pim** {**sparse-mode** | **sparse-dense-mode**}	Enable PIM on an interface. You must use either **sparse mode** or **sparse-dense mode**.
Step 4	**ip igmp version 3**	Enable IGMPv3 on this interface. The default version of IGMP is set to Version 2.

Monitoring SSM

Beginning in privileged EXEC mode, follow these steps to monitor SSM.

Command	Purpose
Router# **show ip igmp groups detail**	Display the (S, G) channel subscription through IGMPv3.
Router# **show ip mroute**	Display whether a multicast group supports SSM service or whether a source-specific host report was received.

Updates to the Command References

These are the updates to the Command Reference for the Catalyst 3750-E and Catalyst 3560-E switches:

- The usage guidelines for the **set** and **unset** bootloader commands in the command reference is incorrect.

  These are the correct usage guidelines for the **set** command:

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

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

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

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

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

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

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

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

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

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

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

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

The bootloader prompt string (PS1) can be up to 120 printable characters except the equal sign (=).

These are the correct guidelines for the **unset** command:

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

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

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

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

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

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

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

Updates to the System Message Guides

These are the updates to System Message Guide for the Catalyst 3750-E and Catalyst 3560-E switches:

Error Message `DOT1X_SWITCH-5-ERR_ADDING_ADDRESS: Unable to add address [enet] on [chars]`

Explanation The client MAC address could not be added to the MAC address table because the hardware memory is full or the address is a secure address on another port. [enet] is the supplicant MAC address, and [chars] is the interface. This message might appear if the IEEE 802.1x feature is enabled.

Recommended Action If the hardware memory is full, remove some of the dynamic MAC addresses. If the client address is on another port, manually remove it from that port.

Error Message `SPANTREE-6-PORTADD_ALL_VLANS: [chars] added to all Vlans`

Explanation The interface has been added to all VLANs. [chars] is the added interface.

Recommended Action No action is required.

Error Message `SPANTREE-6-PORTDEL_ALL_VLANS: [chars] deleted from all Vlans`

Explanation The interface has been deleted from all VLANs. [chars] is the deleted interface.

Recommended Action No action is required.

Error Message `SW_VLAN-6-VTP_DOMAIN_NAME_CHG: VTP domain name changed to [chars].`

Explanation The VLAN Trunking Protocol (VTP) domain name was changed through the configuration to the name specified in the message. [chars] is the changed domain name.

Recommended Action No action is required.

Error Message `PLATFORM_UCAST-6-PREFIX: One or more, more specific prefixes could not be programmed into TCAM and are being covered by a less specific prefix`

Explanation A more specific prefix could not be programmed into Ternary Content Addressable Memory (TCAM) and is covered by a less specific prefix. This could be a temporary condition. The output of the **show platform ip unicast failed route** privileged EXEC command lists the failed prefixes.

Recommended Action No action is required.

Error Message `PLATFORM_HCEF-3-ADJ: [chars]`

Explanation This message appears when an unsupported feature is configured on a switch running Cisco IOS Release 12.2(25)SE. [chars] is the error message.

Recommended Action Determine if a generic routing encapsulation (GRE) tunnel or the **ip cef accounting** global configuration command are configured. Only Distance Vector Multicast Routing Protocol (DVMRP) tunnels are supported. If the GRE tunnel is configured, remove the tunnel, or

upgrade the switch software to a Cisco IOS release when the GRE feature is needed. If the **ip cef accounting** command is configured, remove it by using the **no ip cef accounting** global configuration command.

Note Cisco IOS Release12.2(25)SEB2 does not support the **ip cef accounting** command.

Error Message `PLATFORM_IPv6_UCAST-6-PREFIX: One or more, more specific prefixes could not be programmed into TCAM and are being covered by a less specific prefix`

Explanation A more specific prefix could not be programmed into Ternary Content Addressable Memory (TCAM) and is covered by a less specific prefix. This could be a temporary condition. The output of the **show platform ipv6 unicast retry route** privileged EXEC command lists the failed prefixes.

Recommended Action No action is required.

Error Message `EC-5-CANNOT_BUNDLE1: Port-channel [chars] is down, port [chars] will remain stand-alone.`

Explanation The aggregation port is down. The port remains standalone until the aggregation port is up. The first [chars] is the EtherChannel. The second [chars] is the port number.

Recommended Action Ensure that the other ports in the bundle have the same configuration]

Error Message `ILPOWER-3-CONTROLLER_PORT_ERR:Controller port error, Interface Fa0/7:Power given, but link is not up.`

Explanation The inline-power-controller reported an error on an interface.

Recommended Action Enter the **shutdown** and **no shutdown** interface configuration commands on the affected interfaces. Upgrade to Cisco IOS Release12.1(14)EA1 or later, which provides an electrostatic discharge (ESD) recovery mechanism.

Updates to the Regulatory Compliance and Safety Information

This section includes an update to the Regulatory Compliance and Safety information for the Catalyst 3750-E and Catalyst 3560-E switches.

- Warning Statement 345 no longer applies to the Catalyst 3560E-12D switches.
- Warning Statement 248 replaces warning Statement 266 for the Catalyst 3560E-12D switches:

Statement 248—Unit Mounting Warning

Warning **This unit is intended to be mounted on a wall. Please read the wall mounting instructions carefully before beginning installation. Failure to use the correct hardware or to follow the correct procedures could result in a hazardous situation to people and damage to the system.** Statement 248

Waarschuwing **Deze eenheid dient aan een wand te worden bevestigd. Lees voordat u met de installatie begint, de instructies voor wandmontage aandachtig door. Het niet gebruiken van de juiste apparatuur of het niet volgen van de juiste procedures kan leiden tot gevaarlijke situaties of beschadiging van het systeem.**

Varoitus **Tämä laite on tarkoitettu seinälle asennettavaksi. Lue seinäasennusohjeet huolellisesti ennen asennuksen aloittamista. Väärien työkalujen käyttäminen tai ohjeiden noudattamatta jättäminen voi aiheuttaa henkilövahinkoja ja vioittaa laitetta.**

Attention **Cette unité est conçue pour être montée sur un mur. Veuillez lire attentivement les instructions de montage avant de commencer l'installation. L'utilisation d'un matériel incorrect ou l'application inappropriée des procédures peut être à l'origine d'accidents et endommager le système.**

Warnung **Diese Einheit ist für die Montage an einer Wand bestimmt. Lesen Sie die Montageanweisungen sorgfältig durch, bevor Sie mit der Installation beginnen. Nichtverwenden der korrekten Hardware oder Nichtbefolgen der korrekten Vorgehensweise stellt eine potentielle Gefahrenquelle dar und könnte das System beschädigen.**

Avvertenza **L'unità deve essere montata a parete. Leggere attentamente le istruzioni di montaggio a parete prima di procedere all'installazione. L'impiego di utensili non adeguati o di procedure non corrette può comportare un rischio per le persone e per il sistema stesso.**

Advarsel **Denne enheten er beregnet på veggmontering. Les instruksjonene om veggmontering nøye før du begynner installeringen. Hvis du ikke bruker riktig maskinutstyr eller følger de korrekte prosedyrer, kan det medføre risiko for personskade og skade på systemet.**

Aviso **Esta unidade foi concebida para ser montada numa parede. Leia atentamente as instruções de montagem em parede antes de iniciar a instalação. A utilização de material incorrecto ou o não seguimento dos procedimentos correctos podem dar origem a uma situação perigosa para o pessoal e danificar o sistema.**

¡Advertencia! **Esta unidad está diseñada para ser montada en la pared. Leer las instrucciones de montaje en pared cuidadosamente antes de comenzar la instalación. En caso de no utilizar los materiales apropiados o no seguir el procedimiento correcto, se podría crear una situación peligrosa y ocasionar daños al sistema.**

Varning! **Den här enheten är utformad för väggmontering. Läs noga anvisningarna för väggmontering innan du börjar installera. Om du inte använder rätt maskinvara eller inte följer anvisningarna kan det orsaka fara för personskada eller skador på systemet.**

Related Documentation

These documents provide complete information about the Catalyst 3560-E switch and are available on Cisco.com:

http://www.cisco.com/en/US/products/ps7078/tsd_products_support_series_home.html

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 URL referenced in the "Obtaining Documentation, Obtaining Support, and Security Guidelines" section on page 27.

These documents provide complete information about the switches:

- *Catalyst 3560-E Switch Getting Started Guide* (not orderable but available on Cisco.com)
- *Catalyst 3750-E and Catalyst 3560-E Switch Hardware Installation Guide* (not orderable but available on Cisco.com)
- *Regulatory Compliance and Safety Information for the Catalyst 3750-E and Catalyst 3560-E Switch* (not orderable but available on Cisco.com)
- *Release Notes for the Catalyst 3750-E and Catalyst 3560-E Switch* (not orderable but available on Cisco.com)
- *Catalyst 3750-E and Catalyst 3560-E Switch Software Configuration Guide* (not orderable but available on Cisco.com)
- *Catalyst 3750-E and Catalyst 3560-E Switch Command Reference* (not orderable but available on Cisco.com)
- *Catalyst 3750-E and Catalyst 3560-E Switch System Message Guide* (not orderable but available on Cisco.com)
- *Cisco Software Activation and Compatibility Document* (not orderable but available on Cisco.com)
- *Documentation Updates for the Catalyst 3560E-12D Switches* (not orderable but available on Cisco.com)
- *Installation Notes for the Catalyst 3750-E, Catalyst 3560-E Switches, and RPS 2300 Power Supply Modules* (order number DOC-7817570=)
- *Installation Notes for the Catalyst 3750-E and Catalyst 3560-E Switch Fan Module* (order number DOC-7817571=)
- *Installation Notes for the Cisco TwinGig Converter Module* (order number DOC-7817572=)
- *Cisco Redundant Power System 2300 Hardware Installation Guide* (order number DOC-7817647=)
- *Cisco Redundant Power System 2300 Compatibility Matrix* (not orderable but available on Cisco.com)
- Device manager online help (available on the switch)

These compatibility matrix documents are available from this Cisco.com site:

http://www.cisco.com/en/US/products/hw/modules/ps5455/products_device_support_tables_list.html

- *Cisco Gigabit Ethernet Transceiver Modules Compatibility Matrix* (not orderable but available on Cisco.com)
- *Cisco 100-Megabit Ethernet SFP Modules Compatibility Matrix* (not orderable but available on Cisco.com)
- *Cisco Small Form-Factor Pluggable Modules Compatibility Matrix* (not orderable but available on Cisco.com)

- *Compatibility Matrix for 1000BASE-T Small Form-Factor Pluggable Modules* (not orderable but available on Cisco.com)

For other information about related products, see these documents:

- *Getting Started with Cisco Network Assistant* (not orderable but available on Cisco.com)
- *Release Notes for Cisco Network Assistant* (not orderable but available on Cisco.com)
- *Network Admission Control Software Configuration Guide* (not orderable but is available on Cisco.com)

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

---

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