Release Notes for the Cisco IE 3000 Switch, Cisco IOS Release 12.2(58)SE1 and Later

Revised December 22, 2011

Note Cisco IOS Release 12.2(58)SE images for all platforms were removed from Cisco.com because of a severe defect, CSCto62631. The solution for the defect is in Cisco IOS Release 12.2(58)SE1.

Cisco IOS Release 12.2(58)SE1 runs on all Cisco IE 3000 switches.

These release notes include important information about Cisco IOS Release 12.2(58)SE1, and any limitations, restrictions, and caveats that apply to the releases. 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 4.
- 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 4.

You can download the switch software from this site (registered Cisco.com users with a login password): http://www.cisco.com/cisco/software/navigator.html?a=ahttp://www.cisco.com/cisco/web/download/index.htmli=rpm

Contents

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

System Requirements

Supported Hardware

Switches and Modules

Table 1 Cisco IE 3000 Switch Models

Switch Model	Description
Cisco IE-3000-4TC	4 10/100BASE-T Ethernet ports and 2 dual-purpose ports, each with a 10/100/1000BASE-T copper port and an SFP (small form-factor pluggable) module slot
Cisco IE-3000-8TC	8 10/100BASE-T Ethernet ports and 2 dual-purpose ports
Cisco IE-3000-4TC-E	4 10/100BASE-T Ethernet ports and 2 dual-purpose ports (supports the IP services software feature set)
Cisco IE-3000-8TC-E	8 10/100BASE-T Ethernet ports and 2 dual-purpose ports (supports the IP services software feature set)
Cisco IEM-3000-8TM	Expansion module with 8 10/100BASE-T copper Ethernet ports
Cisco IEM-3000-8FM	Expansion module with 8 100BASE-FX fiber-optic Ethernet ports

SFP Modules

Table 2 SFP Models

Type of SFP	SFP Models
Industrial temperature modules	GLC-FE-100FX-RGD GLC-SX-MM-RGD GLC-FE-100LX-RGD GLC-LX-SM-RGD GLC-ZX-SM-RGD

Table 2 SFP Models (continued)

Type of SFP	SFP Models
Extended temperature modules	100BASE-BX
Commercial temperature modules	CWDM 1000BASE-BX GLC-FE-100EX (Cisco IOS Release 12.2(55)SE and later.) **Note** 100EX SFP support is Version -02 (10-2262-02) or later

Device Manager System Requirements

Hardware

Table 3 Minimum Hardware Requirements

Processor Speed	DRAM	Number of Colors	Resolution	Font Size
233 MHz minimum[1]	512 MB[2]	256	1024 x 768	Small

1. We recommend 1 GHz.
2. We recommend 1 GB DRAM.

Software

- Windows 2000, XP, Vista, and Windows Server 2003.
- Internet Explorer 6.0, 7.0, Firefox 1.5, 2.0 or later with JavaScript enabled.

The device manager verifies the browser version when starting a session and does not require a plug-in.

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 Cisco IE 3000 switch, all standby command switches must be Cisco IE 3000 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 12.2(46)SE1 and later is only compatible with Cisco Network Assistant (CNA) 5.4 and later.

Note CNA 5.4 does not support the cisco-ie-macros that were introduced in Cisco 12.2(55)SE and later. Using the new Smartport role names will cause CNA errors.

You can download Cisco Network Assistant from this URL: http://www.cisco.com/cisco/software/navigator.html?mdfid=279230132http://www.cisco.com/pcgi-bin/tablebuild.pl/NetworkAssistanti=rp

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

Upgrading the Switch Software

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 compact flash memory card.

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.

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.

If you download the IP services image and plan to use Layer 3 functionality, you must use the Switch Database Management (SDM) routing template. To see which template is currently active template, enter the **show sdm prefer** privileged EXEC command. If necessary, change the SDM template to the routing template by entering the **sdm prefer routing** global configuration command. You will be prompted to reload the switch to activate the new template.

Note The switch must be running Cisco IOS Release 12.2(52)SE or later to configure the routing template.

Table 4 Cisco IOS Software Image Files

Filename	Description
ies-lanbasek9-tar.122-58.SE1.tar	Cisco IE 3000 cryptographic image file and device manager files with Layer 2+, Kerberos, and SSH features.
ies-ipservicesk9-tar.122-58.SE1.tar	Cisco IE 3000 IP services cryptographic image and device manager files with Kerberos, SSH, Layer 2+, and full Layer 3 features.

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 to 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/prod/collateral/iosswrel/ps8802/ps6969/ps1835/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*:
http://www.cisco.com/en/US/docs/ios/fundamentals/command/reference/cf_t1.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.

Note Make sure that the compact flash card is inserted into the switch before downloading the software.

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:

a. If you are a registered customer, go to this URL and log in.

http://www.cisco.com/cisco/software/navigator.html?a=ahttp://www.cisco.com/cisco/web/download/index.htmli=rpm

b. Navigate to **Switches > Industrial Ethernet Switches**.

c. Navigate to your switch model.

d. Click **IOS Software**, then select the latest IOS release.

e. Download the image you identified in Step 1.

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 the *Cisco IE 3000 Switch Software Configuration Guide*.

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/image-name.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 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 Software Features

- Protocol storm protection to control the rate of incoming protocol traffic to a switch by dropping packets that exceed a specified ingress rate
- Call Home to provide e-mail-based and web-based notification of critical system events. Users with a service contract directly with Cisco Systems can register Call Home devices for the Cisco Smart Call Home service that generates automatic service requests with the Cisco TAC.
- IETF IP-MIB and IP-FORWARD-MIB(RFC4292 and RFC4293) updates to support the IP version 6 (IPv6)-only and the IPv6 part of the protocol-version independent (PVI) objects and tables.
- Network Time Protocol version 4 (NTPv4) to support both IPv4 and IPv6 and compatibility with NTPv3.
- DHCPv6 bulk-lease query to support new bulk lease query type (as defined in RFC5460).
- The DHCPv6 relay source configuration feature to configure a source address for DHCPv6 relay agent.
- Enhancements to RADIUS, TACACS+, and SSH to function over IPv6.
- NSF IETF mode for OSPFv2—OSPFv2 graceful restart support for IPv4. (IP services feature set only)
- NSF IETF mode for OSPFv3—OSPFv3 graceful restart support for IPv6. (IP services feature set only)

- Support for the Virtual Router Redundancy Protocol (VRRPv4), which dynamically assigns responsibility for one or more virtual routers to the VRRP routers on a LAN, allowing multiple routers on a multiaccess link to utilize the same virtual IP address.
- Precision Time Protocol (PTP) enhancement to allow PTP messages passing through the expansion module ports.
- Profinet topology editor functions with the Simatic Step 7 application when Simatic Step 7 runs version v5.4 SP5 HF5 (v5.4.5.5).
- Common Industrial Protocol (CIP) enhancement to initiate a time domain reflectometery (TDR) cable diagnostics test and to query the result via CIP protocol.

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

Configuration

- A static IP address might be removed when the previously acquired DHCP IP address lease expires.

  This problem occurs under these conditions:

  - When the switch is booted up 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).
  - When an IP address is configured on VLAN 1 before the dynamic address lease assigned to VLAN 1 expires.

  The workaround is to reconfigure the static IP address. (CSCea71176 and CSCdz11708)

- When connected to some third-party devices that send early preambles, a switch port operating at 100 Mb/s full duplex or 100 Mb/s half duplex might bounce the line protocol up and down. The problem is observed only when the switch is receiving frames.

  The workaround is to configure the port for 10 Mb/s and half duplex or to connect a hub or a nonaffected device to the switch. (CSCed39091)

- When port security is enabled on an interface in restricted mode and the **switchport block unicast interface** command has been entered on that interface, MAC addresses are incorrectly forwarded when they should be blocked

  The workaround is to enter the **no switchport block unicast** interface configuration command on that specific interface. (CSCee93822)

- A traceback error occurs if a crypto key is generated after an SSL client session.

  There is no workaround. This is a cosmetic error and does not affect the functionality of the switch. (CSCef59331)

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

  The workaround is to configure aggressive UDLD. (CSCsh70244)

- When you enter the **boot host retry timeout** global configuration command to specify the amount of time that the client should keep trying to download the configuration and you do not enter a timeout value, the default value is zero, which should mean that the client keeps trying indefinitely. However, the client does not keep trying to download the configuration.

  The workaround is to always enter a non zero value for the timeout value when you enter the **boot host retry timeout** *timeout-value* command. (CSCsk65142)

- On a switch running both Resilient Ethernet Protocol (REP) and Bidirectional Forwarding Detection (BFD), when the REP link status layer (LSL) age-out value is less than 1 second, the REP link flaps if the BFD interface is shut down and then brought back up.

  The workaround is to use the **rep lsl-age-out timer** interface configuration command to configure the REP LSL age timer for more than 1000 milliseconds (1 second). (CSCsz40613)

Ethernet

- Traffic on EtherChannel ports is not perfectly load-balanced. Egress traffic on EtherChannel ports are distributed to member ports on load balance configuration and traffic characteristics like MAC or IP address. More than one traffic stream may map to same member ports based on hashing results calculated by the ASIC.

  If this happens, uneven traffic distribution will happen on EtherChannel ports.

  Changing the load balance distribution method or changing the number of ports in the EtherChannel can resolve this problem.

  Use any of these workarounds to improve EtherChannel load balancing:

  - for random source-ip and dest-ip traffic, configure load balance method as **src-dst-ip**
  - for incrementing source-ip traffic, configure load balance method as **src-ip**
  - for incrementing dest-ip traffic, configure load balance method as **dst-ip**
  - Configure the number of ports in the EtherChannel so that the number is equal to a power of 2 (i.e. 2, 4, or 8)

For example, with load balance configured as **dst-ip** with 150 distinct incrementing destination IP addresses, and the number of ports in the EtherChannel set to either 2, 4, or 8, load distribution is optimal.(CSCeh81991)

IP

- When the rate of received DHCP requests exceeds 2,000 packets per minute for a long time, the response time might be slow when you are using the console.

  The workaround is to use rate limiting on DHCP traffic to prevent a denial of service attack from occurring. (CSCeb59166)

Multicasting

- If the number of multicast routes and Internet Group Management Protocol (IGMP) groups are more than the maximum number specified by 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)

- 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)

- If an IGMP report packet has two multicast group records, the switch removes or adds interfaces depending on the order of the records in the packet:
  - If the ALLOW_NEW_SOURCE record is before the BLOCK_OLD_SOURCE record, the switch removes the port from the group.
  - If the BLOCK_OLD_SOURCE record is before the ALLOW_NEW_SOURCE record, the switch adds the port to the group.

  There is no workaround. (CSCec20128)

- When IGMP snooping is disabled and you enter the **switchport block multicast** interface configuration command, IP multicast traffic is not blocked.

  The **switchport block multicast** interface configuration command is only applicable to non-IP multicast traffic.

  There is no workaround. (CSCee16865)

- Incomplete multicast traffic can be seen under either of these conditions:
  - You disable IP multicast routing or re-enable it globally on an interface.
  - A switch mroute table temporarily runs out of resources and recovers later.

  The workaround is to enter the **clear ip mroute** privileged EXEC command on the interface. (CSCef42436)

- After you configure a switch to join a multicast group by entering the **ip igmp join-group** *group-address* interface configuration command, the switch does not receive join packets from the client, and the switch port connected to the client is removed from the IGMP snooping forwarding table.

  Use one of these workarounds:

  - Cancel membership in the multicast group by using the **no ip igmp join-group** *group-address* interface configuration command on an SVI.
  - Disable IGMP snooping on the VLAN interface by using the **no ip igmp snooping vlan** *vlan-id* global configuration command. (CSCeh90425)

QoS

- Some switch queues are disabled if the buffer size or threshold level is set too low with the **mls qos queue-set output** global configuration command. The ratio of buffer size to threshold level should be greater than 10 to avoid disabling the queue.

  The workaround is to choose compatible buffer sizes and threshold levels. (CSCea76893)
- When auto-QoS is enabled on the switch, priority queuing is not enabled. Instead, the switch uses shaped round robin (SRR) as the queuing mechanism. The auto-QoS feature is designed on each platform based on the feature set and hardware limitations, and the queuing mechanism supported on each platform might be different.

  There is no workaround. (CSCee22591)
- If you configure a large number of input interface VLANs in a class map, a traceback message similar to this might appear:

  ```
  01:01:32: %BIT-4-OUTOFRANGE: bit 1321 is not in the expected range of 0 to 1024
  ```

  There is no impact to switch functionality.

  There is no workaround. (CSCtg32101)

SPAN and RSPAN

- Cisco Discovery Protocol (CDP), VLAN Trunking Protocol (VTP), and Port Aggregation Protocol (PAgP) packets received from a SPAN source are not sent to the destination interfaces of a local SPAN session.

  The workaround is to use the **monitor session** *session_number* **destination** {**interface** *interface-id* **encapsulation replicate**} global configuration command for local SPAN. (CSCed24036)

Trunking

- The switch treats frames received with mixed encapsulation (IEEE 802.1Q and Inter-Switch Link [ISL]) as frames with FCS errors, increments the error counters, and the port LED blinks amber. This happens when an ISL-unaware device receives an ISL-encapsulated packet and forwards the frame to an IEEE 802.1Q trunk interface.

  There is no workaround. (CSCdz33708)
- IP traffic with IP options set is sometimes leaked on a trunk port. For example, a trunk port is a member of an IP multicast group in VLAN X but is not a member in VLAN Y. If VLAN Y is the output interface for the multicast route entry assigned to the multicast group and an interface in VLAN Y belongs to the same multicast group, the IP-option traffic received on an input VLAN interface other than one in VLAN Y is 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).

- For trunk ports or access ports configured with IEEE 802.1Q tagging, inconsistent statistics might appear in the **show interfaces counters** privileged EXEC command output. Valid IEEE 802.1Q frames of 64 to 66 bytes are correctly forwarded even though the port LED blinks amber, and the frames are not counted on the interface statistics.

  There is no workaround. (CSCec35100).

VLAN

- If the number of VLANs times the number of trunk ports exceeds the recommended limit of 13,000, the switch can fail.

  The workaround is to reduce the number of VLANs or trunks. (CSCeb31087)
- 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)
- When many VLANs are configured on the switch, high CPU utilization occurs when many links are flapping at the same time.

  The workaround is to remove unnecessary VLANs to reduce CPU utilization when many links are flapping. (CSCtl04815)

Device Manager Limitations

- 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)
- When you successfully upgrade an image by using device manager and click *No* when prompted to reload the image, device manager becomes unusable.

  The workaround is to manually reload the switch. (CSCsj88169)

Important Notes

Device Manager Notes

- You cannot create and manage switch clusters through the device manager. To create and manage switch clusters, use the CLI or Cisco Network Assistant.
- 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.

Open Caveats

- CSCtg98453

  When you make port security changes on an interface, such as configuring aging time, violations, or aging type, error messages and tracebacks might appear.

  There is no workaround.

- CSCtl32991

  Unicast EIGRP packets destined for the switch are sent to the host queue instead of to the higher priority routing protocol queue.

  Note This does not occur when packets are routed through the switch to another destination.

  There is no workaround.

- CSCtl60247

  When a switch running Multiple Spanning Tree (MST) is connected to a switch running Rapid Spanning Tree Protocol (RSTP), the MST switch acts as the root bridge and runs per-VLAN spanning tree (PVST) simulation mode on boundary ports connected to the RST switch. If the allowed VLAN on all trunk ports connecting these switches is changed to a VLAN other than VLAN 1 and the root port of the RSTP switch is shut down and then enabled, the boundary ports connected to the root port move immediately to the forward state without going through the PVST+ slow transition.

  There is no workaround.

- CSCtl81217

  When a switch is using a DHCP server to assign IP addresses and an interface on the switch has RIP enabled, if the switch reloads, the interface loses some RIP configuration (specifically RIP authentication mode and RIP authentication key-chain). This does not happen when the IP address is statically configured on the interface. The problem occurs only when you configure RIP before an IP address is assigned by the DHCP server.

  There is no workaround, but you can use an embedded event manager (EEM) script to add the interface configuration commands on the interface:

  ip rip authentication mode

  ip rip key-chain

- CSCtn08650

  If you try to use Device manager to upgrade the IP services image on the switch to Cisco IOS Release 12.2(58)SE, the upgrade might not successfully complete. It hangs at the step “Loading the tar file to the switch.”

  The workaround is to use the CLI to upgrade the IP services image.

Resolved Caveats

Caveats Resolved in Cisco IOS Release 12.2(55)SE4

- CSCtj83964

  On a switch running Protocol-Independent Multicast (PIM) and Source Specific Multicast (SSM), multicast traffic might not be sent to the correct port after the switch reloads.

  The workaround is to enter the **clear ip route** privileged EXEC command or reconfigure PIM and SSM after a reload.

- CSCtl51859

  Neighbor discovery fails for IPv6 hosts connected to the switch when the IPv6 MLD snooping feature is enabled globally on the switch.

  The workaround is to disable IPv6 MLD snooping on the switch.

Caveats Resolved in Cisco IOS Release 12.2(58)SE2

- CSCtq01926

  When you configure a port to be in a dynamic VLAN by entering the **switchport access vlan dynamic** interface configuration command on it, the switch might reload when it processes ARP requests on the port.

  The workaround is to configure static VLANs for these ports.

Caveats Resolved in Cisco IOS Release 12.2(58)SE1

- CSCtg00542

  A Link Aggregation Control Protocol (LACP) bundle takes up to 70 seconds to form when NetFlow sampling is enabled.

  The workaround is to disable NetFlow sampling.

- CSCtg11547

  When you configure a switch to send messages to a syslog server in a VPN Routing and Forwarding (VRF) instance, the messages are not sent to the server.

  The workaround is to remove the VRF configuration.

- CSCtg71149

  When ports in an EtherChannel are linking up, the message `EC-5-CANNOT_BUNDLE2` might appear. This condition is often self-correcting, indicated by the appearance of `EC-5-COMPATIBLE` message following the first message. On occasion, the issue does not self-correct, and the ports may remain unbundled.

  The workaround is to reload the switch or to restore the EtherChannel bundle by shutting down and then enabling the member ports and the EtherChannel in this order:

  - Enter the **shutdown** interface configuration command on each member port.
  - Enter the **shutdown** command on the port-channel interface.
  - Enter the **no shutdown** command on each member port.

  Enter the **no shutdown** command on the port-channel interface.

- CSCth77163

When you connect a Cisco IE 3000 switch configured with Resilient Ethernet Protocol (REP) to a Catalyst 3750 running Cisco IOS Release 12.2(53)SE2, traffic to the Catalyst 3750 suddenly stops.

The workaround is to configure STP instead of REP on the Cisco IE 3000.

- CSCti37197

  Enabling the Cisco Discovery Protocol (CDP) on a tunnel interface causes the switch to fail when a a CDP packet is received on the interface.

Note Tunnels are not supported on these platforms.

The workaround is to use the **no cdp enable** interface configuration command to disable CDP on the interface.

- CSCti45352

  When a FlexLinks backup interface is configured on a switch, the backup interface incorrectly shows that all VLANs are in the forwarding state.

  The workaround is to use the **show interface trunk** interface configuration command to display the status of the backup link.

- CSCti78365

  The config.text.backup file is present after the switch is restored to the factory defaults.

  There is no workaround.

- CSCti95834

  When you enter the **ipv6 traffic-filter** interface configuration command, it might not filter traffic as expected, and it might allow traffic to pass through.

  There is no workaround.

- CSCtj30207

  The auto-install terminates if the switch receives an IP address from the DHCP server with the default router set.

  There is no workaround.

- CSCtj03875

  When you disconnect the spanning tree protocol (STP) peer link, the STP port path cost configuration changes.

  There is no workaround.

- CSCtj75471

  When a spanning-tree bridge protocol data unit (BPDU) is received on an 802.1Q trunk port and has a VLAN ID is greater than or equal to 4095, the spanning-tree lookup process fails.

  There is no workaround.

- CSCtj88307

  When you enter the **default interface**, **switchport**, or **no switchport** interface configuration command on the switch, this message appears: *`EMAC phy access error, port 0, retrying.....`*

  There is no workaround.

- CSCtk11275

  On a switch running Cisco IOS Release 12.2(55)SE with the **parser config cache interface** global configuration command in the configuration, when you use the CISCO-MAC-NOTIFICATION-MIB to enable the SNMP MAC address notification trap, the trap is enabled, but the trap setting does not appear in the switch configuration.

  The workaround is to remove the **parser config cache interface** command from the configuration.

- CSCtl09690

  The switch repeatedly displays this Precision Time Protocol (PTP) error message when it receives PTP messages from two colliding host on the same port:

  Potential PTP source collision on port (*port number*)

  There is no workaround.

- CSCtl42740

  When 802.1x MAC authentication bypass with multidomain authentication and critical VLAN are enabled on an interface on a switch running Cisco IOS Release 12.2(53)SE or later, if the switch loses connectivity with the AAA server, the switch might experience high CPU usage and show these messages:

  ```
  AUTH-EVENT (Gi0/15) Received clear security violation
  AUTH-EVENT (Gi0/15) dot1x_is_mab_interested_in_mac: Still waiting for a MAC on port
  GigabitEthernet0/15
  ```

  There is no workaround.

- CSCtl80678

  The port manager callback might cause more than 90% CPU usage for up to 20 minutes under these conditions:

  - Link comes up simultaneously on multiple dot1q trunk ports.
  - VLAN Trunking Protocol (VTP) pruning is enabled.

  The workaround is to disable VTP pruning.

- CSCto62631

  A switch running Cisco IOS Release 12.2(58)SE might reload if:

  - SSH version 2 is configured on the switch, and
  - a customized login banner was configured by using the **banner login** *message* global configuration command

  Use one of these workarounds:

  - Disable the login banner by entering the **no login banner** command.
  - Disable SSH on the switch.
  - Downgrade to a software version prior to Cisco IOS Release 12.2(58)SE.

- CSCto07919

  Cisco IOS Software is affected by two vulnerabilities that cause a Cisco IOS device to reload when processing IP version 6 (IPv6) packets over a Multiprotocol Label Switching (MPLS) domain. These vulnerabilities are:

  – Crafted IPv6 Packet May Cause MPLS-Configured Device to Reload

  – ICMPv6 Packet May Cause MPLS-Configured Device to Reload

  Cisco has released free software updates that address these vulnerabilities.

  Workarounds that mitigate these vulnerabilities are available.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20110928-ipv6mpls.shtml.

Documentation Updates

Note The "Supported MIBs" appendix is no longer in the software configuration guide. To locate and download MIBs for a specific Cisco product and release, use the Cisco MIB Locator: http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml.

Updates to the Getting Started Guide

Express Setup

When you launch Express Setup, you are prompted for the switch password. Enter the default password, *cisco*. The switch ignores text in the username field. Before you complete and exit Express Setup, you must change the password from the default password, *cisco*.

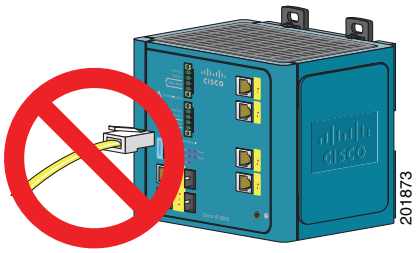
In the "Running Express Setup" section of the *Cisco IE 3000 Switch Getting Started Guide*, Steps 8 to 10 have changed.

Running Express Setup:

To run Express Setup:

Step 1 Make sure that nothing is connected to the switch.

During Express Setup, the switch acts as a DHCP server. If your PC has a static IP address, change your PC settings before you begin to temporarily use DHCP.



Step 2 Connect power to the switch.

See the wiring instructions in the "Grounding the Switch" section and the "Wiring the DC Power Source" section.

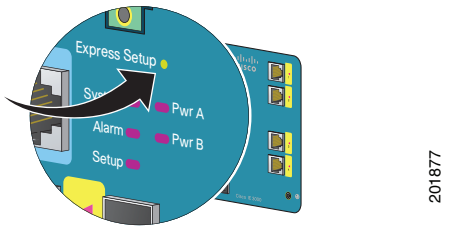
Step 3 When the switch powers on, it begins the power-on self-test (POST). During POST, the System LED blinks while a series of tests verify that the switch functions properly. Wait for the switch to complete POST, which takes approximately 1 minute.

Step 4 Make sure that POST has completed by verifying that the System LED is solid green. If the switch has not been configured, the Setup LED blinks green. If the Setup LED stops blinking, you can still continue with the next step.

If the switch fails POST, the System LED turns red. See the "In Case of Difficulty" section if your switch fails POST.

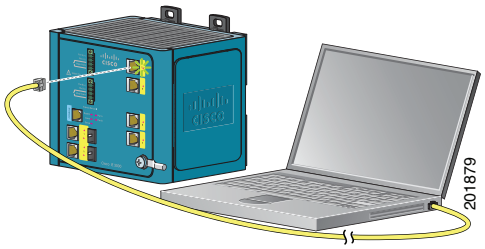
Step 5 Press the Express Setup button. This button is recessed behind the front panel, so you can use a simple tool, such as a paper clip.

When you press the Express Setup button, a switch port LED begins blinking green.



Step 6 Connect a Category 5 Ethernet cable (not provided) from the blinking switch port to the Ethernet port on your PC.

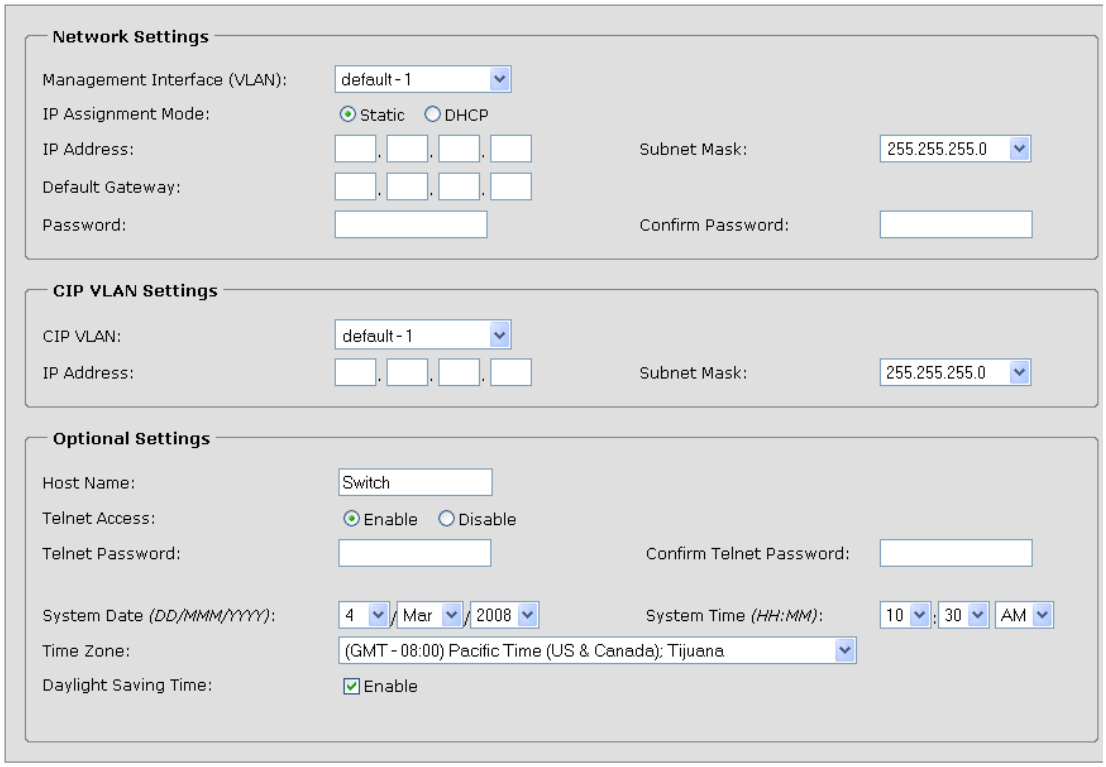
The port LEDs on your PC and the switch blink green while the switch configures the connection.



Step 7 When the Setup LED turns solid green, start a browser session on the PC.

Step 8 The Express Setup window automatically appears. If the window does not appear, verify that any proxy settings or pop-up blockers are disabled on your browser and that any wireless client is disabled on your PC. You might also need to enter a URL in your browser, such as *Cisco.com* or another well-known website. If you need help, see the "In Case of Difficulty" section.

Note If the switch has been previously configured, the device manager page appears. You can use it to change the switch IP address.



Step 9 Enter the network settings. All entries must be in English letters and Arabic numbers.

- **Management Interface (VLAN)**: We recommend using the default, **VLAN 1**. The management VLAN establishes an IP connection to the switch.
- **IP Assignment Mode**: We recommend using the default, **Static**, which means that the switch always has the IP address that you assign. Use the **DHCP** setting when you want the switch to automatically obtain an IP address from a DHCP server.
- **IP Address**: Enter the IP address for the switch. Later, you can use the IP address to access the switch through the device manager.
- **Subnet Mask**: Select a mask from the drop-down list.
- **Default Gateway**: Enter the IP address of the router.
- **Password**: Enter a password. The password can be from 1 to 25 alphanumeric characters, can start with a number, is case sensitive, allows embedded spaces, but does not allow spaces at the beginning or end. In the **Confirm Password** field, enter the password again.

For more information about the network settings, click **Help** on the toolbar.

Step 10 Enter the Control Industrial Protocol (CIP) VLAN settings:

- **CIP VLAN**: Enter the VLAN on which CIP will be enabled. The CIP VLAN can be the same as the management VLAN, or you can isolate CIP traffic on another VLAN that is already configured on the switch. The default CIP VLAN ID is **VLAN 1**.
- **IP Address**: Enter the IP address for the CIP VLAN. If the CIP VLAN is different from the management VLAN, you must specify an IP address for the CIP VLAN. Make sure that the IP address that you assign to the switch is not being used by another device in your network.
- **Subnet Mask**: Select a mask from the drop-down list.

For more information about the CIP VLAN settings, click **Help** on the toolbar.

Step 11 Enter the Optional Settings now, or enter them later by using the device manager interface:

- Enter a **Host Name** for the switch.
- Select **Enable** or **Disable** for Telnet access. If enabled, enter and confirm the Telnet password in the **Password** fields.
- The date and time fields are populated from your PC.
- Click **Enable** to use Daylight Saving Time.

For more information about the optional settings, click **Help** on the toolbar.

Step 12 Click **Submit** to save the information that you entered and to finish the basic configuration. You have completed the initial switch setup. If you click **Cancel**, the fields are cleared, and you can start over.

Step 13 Turn off DC power at the source, disconnect all cables to the switch, and install the switch in your network. See the "Managing the Switch" section for information about configuring and managing the switch.

Warning Statement 1067

This warning statement has been removed from the *Cisco IE 3000 Switch Getting Started Guide* on Cisco.com.

Grounding the Switch

Step 6: Use a ratcheting torque screwdriver to tighten the ground screw and ring terminal lug to the switch front panel to 8.5 in-lb, the maximum recommended torque.

Wiring the DC Power Source

Step 6: Use a ratcheting torque flathead screwdriver to torque the power and relay connector captive screws (above the installed wire leads) to 2 in-lb, the maximum recommended torque.

Resetting the Switch

Follow these steps to return your switch to the factory default settings. These are reasons why you might want to reset the switch:

- You installed the switch in your network and cannot connect to it because you assigned the wrong IP address.
- You want to clear all configurations from the switch and assign a new IP address.
- You want to reset the password on the switch.

Caution Resetting the switch deletes the configuration and reboots the switch.

To reset the password on the switch:

1. Power off the switch.
2. Power on the switch, and at the same time, press and hold down the Express Setup button until all the system LEDs turn red.
3. Release the Express Setup button, and the switch continues to boot.

After the switch restarts, continue to run Express Setup.

Updates to the Regulatory Compliance and Safety Information for the Cisco IE 3000 Switch

Warning Statement 1067

Warning statement 1067 has been removed from the *Regulatory Compliance and Safety Information for the Cisco IE 3000 Switch* on Cisco.com.

Compliance Labels

Figure 1 Compliance Label for the Cisco IE 3000 Switch

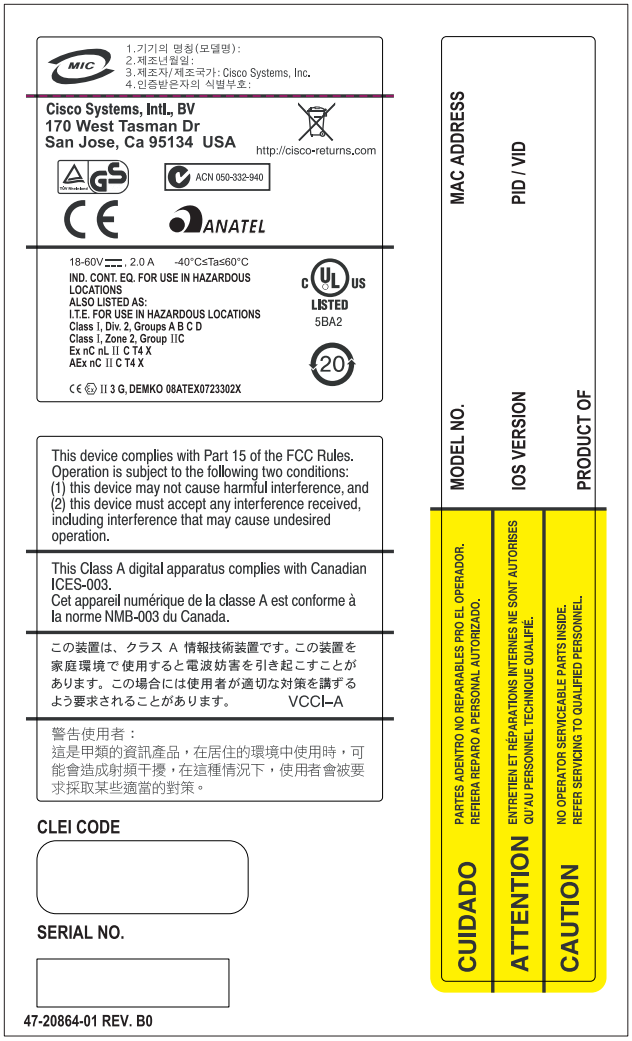
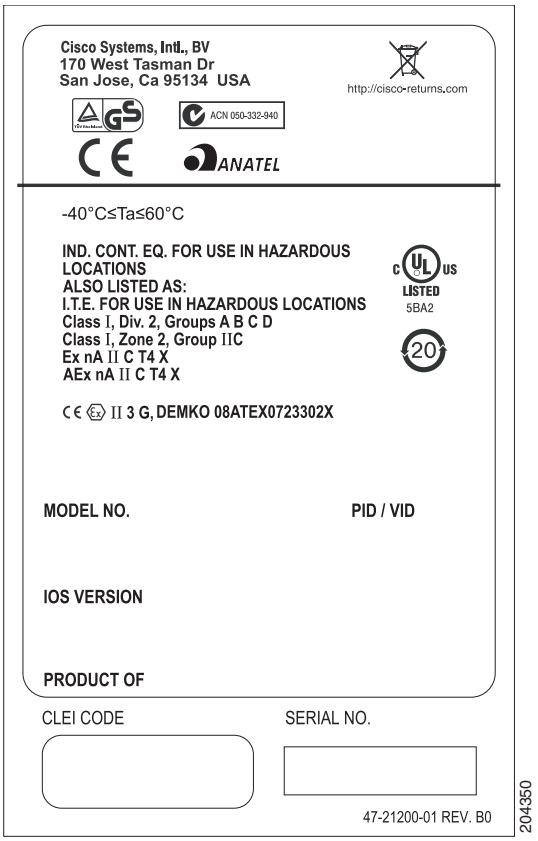


Figure 2 Compliance Label for the Cisco IE 3000 Switch Extension Module



Updates to the Hardware Installation Guide

This update is for the "Overview" chapter. These switches were added:

Table 5 Cisco IE 3000 Switch Model Descriptions

Switch Model	Description
Cisco IE-3000-4TC-E	4 10/100BASE-T Ethernet ports and 2 dual-purpose ports (supports the IP services software feature set)
Cisco IE-3000-8TC-E	8 10/100BASE-T Ethernet ports and 2 dual-purpose ports (supports the IP services software feature set)

This update is for the "Technical Specifications" chapter.

The technical specifications listed in Table A-2 for the Cisco IE-3000-8TC and IE-3000-4TC switches also apply to the Cisco IE-3000-4TC-E and IE-3000-4TC-E switches.

Updates to the Software Configuration Guide

Correction to the "Clustering Switches" Chapter

In the "Candidate Switch and Cluster Member Switch Characteristics" section, the requirements should include:

- The **ip http server** global configuration command must be configured on the switch.

Correction to the "Configuring Network Security with ACLs" Chapter

There is an error in the "Creating a Numbered Extended ACL" section. Contrary to the note in this section, ICMP echo-replies can be filtered.

Correction to the "Unsupported Commands" Chapter

The "Miscellaneous" section of the "Unsupported Commands" chapter should include the **logging discriminator** global configuration command.

Updates to the System Message Guide

New System Messages

Error Message `IP-3-SBINIT: Error initializing [chars] subblock data structure. [chars]`

Explanation The subblock data structure was not initialized. [chars] is the structure identifier.

Recommended Action No action is required.

Error Message `AUTHMGR-7-STOPPING: Stopping '[chars]' for client [enet] on Interface [chars] AuditSessionID [chars]`

Explanation The authentication process has been stopped. The first [chars] is the authentication method, [enet] is the Ethernet address of the host, the second [chars] is the interface for the host, and the third [chars] is the session ID.

Recommended Action No action is required.

Error Message `AUTHMGR-7-NOMOREMETHODS: Exhausted all authentication methods for client ([chars]) on Interface [chars] AuditSessionID [chars]`

Explanation All available authentication methods have been tried. The first [chars] is the client identifier, the second [chars]s is the interface for the client, and the third [chars] is the session ID.

Recommended Action No action is required.

Modified System Messages

Error Message `AUTHMGR-5-MACMOVE: MAC address ([enet]) moved from Interface [chars] to Interface [chars]`

Explanation The client moved to a new interface but did not log off from the first interface. [enet] is the MAC address of the client, the first [chars] is the earlier interface, and the second [chars] is the newer interface.

Recommended Action No action is required.

Error Message `AUTHMGR-5-MACREPLACE: MAC address ([enet]) on Interface [chars] is replaced by MAC ([enet])`

Explanation A new client has triggered a violation that caused an existing client to be replaced. The first [enet] is the first client, [chars] is the interface, the second [enet] is the new client.

Recommended Action No action is required.

Error Message `MAB-5-FAIL: Authentication failed for client ([chars]) on Interface [chars] AuditSessionID [chars]`

Explanation Authentication was unsuccessful. The first [chars] is the client, the second [chars] is the interface, and the third [chars] is the session ID.

Recommended Action No action is required.

Error Message `MAB-5-SUCCESS: Authentication successful for client ([chars]) on Interface [chars] AuditSessionID [chars]`

Explanation Authentication was successful. The first [chars] is the client, the second [chars] is the interface, and the third [chars] is the session ID.

Recommended Action No action is required.

Deleted System Messages

Error Message `IP-3-STCKYARPOVR: Attempt to overwrite Sticky ARP entry: [inet], hw: [enet] by hw: [enet]\n", MSGDEF_LIMIT_FAST`

Explanation Multiple stations are configured with the same IP address in a private VLAN. (This could be a case of IP address theft.) [inet] is the IP address that is configured, the first [enet] is the original MAC address associated with the IP address, and the second [enet] is the MAC address that triggered this message.

Recommended Action Change the IP address of one of the two systems.

Related Documentation

User documentation in HTML format includes the latest documentation updates and might be more current than the complete book PDF available on Cisco.com.

These documents provide complete information about the Cisco IE 3000 switches and are available at Cisco.com:
http://www.cisco.com/en/US/products/ps9703/tsd_products_support_series_home.html

- *Cisco IE 3000 Switch Software Configuration Guide*
- *Cisco IE 3000 Switch Command Reference*
- *Cisco IE 3000 Switch System Message Guide*
- *Cisco IE 3000 Switch Hardware Installation Guide*
- *Cisco IE 3000 Switch Getting Started Guide*—available in English, simplified Chinese, French, German, Italian, Japanese, Brazilian Portuguese and Spanish

For other information about related products, see these documents:

- Device manager online help (available on the switch)
- *Getting Started with Cisco Network Assistant*
- *Release Notes for Cisco Network Assistant*

These SFP module installation notes are available from this Cisco.com site:
http://www.cisco.com/en/US/products/hw/modules/ps5455/prod_installation_guides_list.html

- *Cisco Small Form-Factor Pluggable Modules Installation Notes*
- *Cisco CWDM GBIC and CWDM SFP Installation Note*

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 Small Form-Factor Pluggable Modules Compatibility Matrix
- Compatibility Matrix for 1000BASE-T Small Form-Factor Pluggable Modules

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation:
http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

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