Release Notes for the Cisco IE 3000 Switch, Cisco IOS Release 12.2(46)SE1 and later

Revised September 9, 2009

Cisco IOS Release 12.2(46)SE1 and later runs on all Cisco IE 3000 switches.

These release notes include important information about Cisco IOS Release 12.2(46)SE1 and later, 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 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.

For the complete list of Cisco IE 3000 switch documentation, see the "Related Documentation" section on page 25.

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

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

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.

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

This section lists the hardware and SFP modules that the switch supports.

Switches and Modules

Table 1 lists the hardware supported on this release.

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 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

These are the SFP modules that the switch supports:

Table 2 SFP Models

Type of SFP	SFP Models
Industrial temperature SFP modules	GLC-FE-100FX-RGD GLC-SX-MM-RGD GLC-FE-100LX-RGD GLC-LX-SM-RGD GLC-ZX-SM-RGD
Extended temperature SFP modules	100BASE-BX
Commercial temperature SFP modules	CWDM 1000BASE-BX

Device Manager System Requirements

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

- Hardware Requirements, page 3
- Software Requirements, page 3

Hardware Requirements

Table 3 lists the minimum hardware requirements for running the device manager.

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 Requirements

Table 4 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 4 Supported Operating Systems and Browsers

Operating System	Minimum Service Pack or Patch	Microsoft Internet Explorer	Mozilla FireFox
Windows 2000	None	6.0 or 7.0	1.5 or 2.0
Windows 2003	None	6.0 or 7.0	1.5 or 2.0

Table 4 Supported Operating Systems and Browsers (continued)

Operating System	Minimum Service Pack or Patch	Microsoft Internet Explorer	Mozilla FireFox
Windows XP	None	6.0 or 7.0	1.5 or 2.0
Vista	None	6.0 or 7.0	1.5 or 2.0

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 this release. Using the new Smartport role names will cause CNA errors.

You can download Cisco 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, page 5
- Deciding Which Files to Use, page 5
- Archiving Software Images, page 5

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 5 lists the filenames for this software release.

Table 5 Cisco IOS Software Image Files

Filename	Description
ies-lanbase-tar.122-46.SE2.tar	Catalyst IE 3000 image file and device manager files. This image has Layer 2+ features.
ies-lanbasek9-tar.122-46.SE2.tar	Catalyst IE 3000 cryptographic image file and device manager files. This image has the Kerberos and SSH 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/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_chapter09186a00800ca744.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 5 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 image for a Cisco IE 3000 switch, click **Cisco IE 3000 software**. To obtain authorization and to download the cryptographic software files, **click Cisco IE 3000 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 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/ies-lanbase-tar.122-46.SE1.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

These sections describe the new supported hardware and the new and updated software features provided in this release:

- New Hardware Features, page 8
- New Software Features, page 8

New Hardware Features

There are no new hardware features for this release. For a list of all supported hardware, see the "Hardware Supported" section on page 2.

New Software Features

- Support for Precision Time Protocol (PTP) as defined in the IEEE 1588 standard to synchronize the real-time clocks of the devices in a network with nanosecond accuracy
- DHCP server port-based address allocation (also referred to as DHCP persistence) for the preassignment of an IP address to a switch port
- IPv6 host support for basic IPv6 management
- Support for cisco-ie macros that are optimized for Industrial Automation traffic
- These enhancements have been made to the CIP (Common Industrial Protocol) feature (CSCsq767881, CSCsu01070, CSCsu89122):
  - When CIP is enabled on the IE 3000, you can specify the VLAN ID to be used as the CIP interface.
  - The device manager Express Setup page includes fields for IP address and mask for the CIP VLAN.
  - CIP indicates when the compact flash card is unplugged or not operating.

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

These limitations apply to the Cisco IE 3000 switches:

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)

- 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.
  - Remove the **logging event spanning-tree** interface configuration command from the interfaces. (CSCsg91027)

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

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

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 IG MP 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)

- Entering the **shutdown** and the **no shutdown** interface configuration commands on the internal link can disrupt the PoE operation. If a new IP phone is added while the internal link is in shutdown state, the IP phone does not get inline power if the internal link is brought up within 5 minutes.

  The workaround is to enter the **shutdown** and the **no shutdown** interface configuration commands on the Fast Ethernet interface of a new IP phone that is attached to the service module port after the internal link is brought up. (CSCeh45465)

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)

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)

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

- CSCsk65142

  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.

- CSCsm95883

  When an unsuccessful forward open request message is returned on the switch, the response does not contain the connection serial number, vendor ID, or vendor serial number information. Only the general and extended error codes are returned.

  This problem only applies to unsuccessful forward open response messages.

  The workaround is to enable the **CIP debug** command to determine the cause of the forward open failure.

- CSCsr13187

  The **show cip object tcp/ip interface** privileged EXEC command displays an old value for the domain name after it has been unconfigured with the **no ip domain-name** global configuration command.

  The workaround is to ignore the domain name output of the **show cip object tcp/ip interface** privileged EXEC command.

- CSCsv63055

  When you configure PTP in forward mode by entering the ptp mode forward global configuration command, the PTP page in device manager breaks due to a parser error.

  There is no workaround. No PTP information is displayed when PTP is in forward mode.

- CSCsv69430

  The device manager Legend incorrectly shows solid green for the Alarm and Setup LEDs in the Off state. The correct color of these LEDs in the Off state is solid black (dark).

  There is no workaround.

Resolved Caveats

These are the caveats that have been resolved in these releases:

- "Cisco IOS Caveats Resolved in Cisco IOS Release 12.2(46)SE2" section on page 15
- "Cisco IOS Caveats Resolved in Cisco IOS Release 12.2(46)SE1" section on page 17

Cisco IOS Caveats Resolved in Cisco IOS Release 12.2(46)SE2

- CSCsk64158

  Symptoms: Several features within Cisco IOS software are affected by a crafted UDP packet vulnerability. If any of the affected features are enabled, a successful attack will result in a blocked input queue on the inbound interface. Only crafted UDP packets destined for the device could result in the interface being blocked, transit traffic will not block the interface.

  Cisco has released free software updates that address this vulnerability.

  Workarounds that mitigate this vulnerability are available in the workarounds section of the advisory. This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090325-udp.shtml

- CSCsm27071

  A vulnerability in the handling of IP sockets can cause devices to be vulnerable to a denial of service attack when any of several features of Cisco IOS software are enabled. A sequence of specially crafted TCP/IP packets could cause any of the following results:

  - The configured feature may stop accepting new connections or sessions.
  - The memory of the device may be consumed.
  - The device may experience prolonged high CPU utilization.
  - The device may reload. Cisco has released free software updates that address this vulnerability.

  Workarounds that mitigate this vulnerability are available in the "workarounds" section of the advisory. The advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090325-ip.shtml

- CSCsr29468

  Cisco IOS software contains a vulnerability in multiple features that could allow an attacker to cause a denial of service (DoS) condition on the affected device. A sequence of specially crafted TCP packets can cause the vulnerable device to reload.

  Cisco has released free software updates that address this vulnerability.

  Several mitigation strategies are outlined in the workarounds section of this advisory.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090325-tcp.shtml

- CSCsv04836

  Multiple Cisco products are affected by denial of service (DoS) vulnerabilities that manipulate the state of Transmission Control Protocol (TCP) connections. By manipulating the state of a TCP connection, an attacker could force the TCP connection to remain in a long-lived state, possibly indefinitely. If enough TCP connections are forced into a long-lived or indefinite state, resources on a system under attack may be consumed, preventing new TCP connections from being accepted. In some cases, a system reboot may be necessary to recover normal system operation. To exploit these vulnerabilities, an attacker must be able to complete a TCP three-way handshake with a vulnerable system.

  In addition to these vulnerabilities, Cisco Nexus 5000 devices contain a TCP DoS vulnerability that may result in a system crash. This additional vulnerability was found as a result of testing the TCP state manipulation vulnerabilities.

  Cisco has released free software updates for download from the Cisco website 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-20090908-tcp24.shtml.

- CSCsv38112

  During switch bootup, the switch alarm-relay circuit no longer changes states (from open to closed and back to open again).

- CSCsv38166

  The server side of the Secure Copy (SCP) implementation in Cisco IOS software contains a vulnerability that could allow authenticated users with an attached command-line interface (CLI) view to transfer files to and from a Cisco IOS device that is configured to be an SCP server, regardless of what users are authorized to do, per the CLI view configuration. This vulnerability could allow valid users to retrieve or write to any file on the device's file system, including the device's saved configuration and Cisco IOS image files, even if the CLI view attached to the user does not allow it. This configuration file may include passwords or other sensitive information.

  The Cisco IOS SCP server is an optional service that is disabled by default. CLI views are a fundamental component of the Cisco IOS Role-Based CLI Access feature, which is also disabled by default. Devices that are not specifically configured to enable the Cisco IOS SCP server, or that are configured to use it but do not use role-based CLI access, are not affected by this vulnerability.

  This vulnerability does not apply to the Cisco IOS SCP client feature.

  Cisco has released free software updates that address this vulnerability.

  There are no workarounds available for this vulnerability apart from disabling either the SCP server or the CLI view feature if these services are not required by administrators.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20090325-scp.shtml

- CSCsw93341

  Smartport macros can now be configured using RSLogix Add-on Profile (AOP). In previous releases, some macros were incorrectly applied twice. (AOP cannot configure multiple macros, and an error was reported to the management node.)

Cisco IOS Caveats Resolved in Cisco IOS Release 12.2(46)SE1

- CSCsc96474

  These traceback messages such as these no longer appear when a large number of IEEE 802.1x supplicants repeatedly try to log in and log out.

  ```
  Jan 3 17:54:32 L3A3 307: Jan 3 18:04:13.459: %SM-4-BADEVENT: Event 'eapReq' is invalid
  for the current state 'auth_bend_idle': dot1x_auth_bend Fa9
  Jan 3 17:54:32 L3A3 308: -Traceback= B37A84 18DAB0 2FF6C0 2FF260 8F2B64 8E912C Jan 3
  19:06:13 L3A3 309: Jan 3 19:15:54.720: %SM-4-BADEVENT: Event 'eapReq_no_reAuthMax' is
  invalid for the current ate 'auth_restart': dot1x_auth Fa4
  ```

- CSCsd03580

  When IEEE 802.1x is globally disabled on the switch by using the **no dot1x system-auth-control** global configuration command, interface level IEEE 802.1x configuration commands, including the **dot1x timeout** and **dot1x mac-auth-bypass** commands, are now available.

- CSCsi70454

  The configuration file used for the configuration replacement feature no longer requires the character string *end\n* at the end of the file.

- CSCsj87991

  A switch configured for Link Layer Discovery Protocol (LLDP) now correctly reports the enabled switch capabilities in the LLDP type, length, and value (TLV) attributes. System capabilities appear correctly, and the enabled capabilities are now identified if the switch is configured only as a Layer 2 switch.

- CSCso00078

  When two IE 3000 switches are connected with both copper and fiber connections on the same port. and a 100FX-FE SFP module is connected to the switch, when you change the media-type from SFP to copper, the copper link now correctly comes up.

- CSCsq19944

  When configuring a switch management VLAN to be another VLAN during Express Setup, the PC no longer loses the network connection to the switch if it remains connected to the same port.

- CSCsq52244

  When a diagnostic or port mirroring role is defined on an interface and you change it to another port role, the port role icon in device manager is now correct.

- CSCsq76774

  If you remove the secure MAC address from an interface through CIP (Common Industrial Protocol), the **switchport port-security violation restrict** CLI configuration no longer remains on the interface.

- CSCsu04337

  In a Multi Domain Authentication (MDA) setup with per-virtual port error-disable configured, when authenticated data and voice clients on the member switch port are dynamically assigned to VLANs and a second data client causes a security violation, only the data virtual port is error-disabled. The voice virtual port is no longer error-disabled at the same time.

- CSCsr13171

  When the switch IP address is successfully changed via CIP, the expected successful CIP response is now returned. When changing the domain name or switch host name, odd-length strings with the required padding are no longer rejected by the switch.

- CSCsu65129

  When an IEEE 802.1x client is directly connected to an interface configured for 802.1x multi-domain with no IP phone attached, the interface is initially assigned to the guest VLAN. Once the 802.1x supplicant allows access to the guest VLAN and an EAPOL packet is detected, the interface now correctly reverts to an unauthorized state, and IEEE 802.1x authentication restarts.

- CSCsu82979

  The CIP revision has been incremented to 2.001 in this release.

Documentation Updates

These sections provide updates to the product documentation:

Updates to the Cisco IE 3000 Switch Software Configuration Guide and Command Reference

The default mode for the **ptp** global configuration command has been changed to **e2etransparent.**

The ptp **mode forward** option has been added to the **ptp** global configuration command.

When PTP mode is forward, all incoming PTP packets pass through all ports on the switch as normal multicast traffic. In this mode, the switch does not generate any PTP packets, and no other PTP configuration is available, including **priority** or **ptp** interface configuration commands.

When the switch is in PTP forward mode, if you enter the **show ptp clock** or **show ptp port** privileged EXEC commands, you see a message that no information is available in forwarding mode.

See the **ptp (global configuration)** command on the next page for the correct syntax.

Note that the “Configuring PTP” chapter in the software configuration guide for this release also contains the wrong information for ptp mode default and does not include the ptp forward option.

ptp (global configuration)

Use the **ptp** global configuration command to set the clock properties for the Precision Time Protocol (PTP). Use the **no** form of this command to return to the default end-to-end transparent clock mode.

ptp {**mode** {**boundary** | **e2etransparent** | **forward**} | **priority1** *value* | **priority2** *value*}

no ptp {**mode** | **priority1** | **priority2**}

Syntax Description

mode	Configure the clock mode.
boundary	Set the switch to boundary clock mode.
e2etransparent	Set the switch to end-to-end transparent clock mode. This is the default.
forward	Set the switch to forward mode. In this mode, incoming PTP packets pass through the switch as normal multicast traffic.
priority1 *value*	Set the local clock priority1 value. The range is 0 to 255; the default priority number is 128. This keyword is available only when the switch is in boundary mode.
priority2 *value*	Set the local clock priority2 value. The range is 0 to 255; the default priority number is 128. This keyword is available only when the switch is in boundary mode.

Defaults

The default mode is end-to-end transparent clock mode.

Command Modes

Global configuration

Command History

Release	Modification
12.2(46)SE1	This command was introduced.

Usage Guidelines

The **ptp priority1** and **ptp priority2** commands are only available when the switch is in boundary mode**.**

When the switch is in PTP forward mode, no PTP configuration is available except configuring PTP mode to another mode. You cannot configure per-port PTP when the switch is in forward mode.

If you enter the **show ptp clock** or **show ptp port** privileged EXEC command when the switch is in PTP forward mode, an error message is generated that no information is available.

Examples

This example shows how to configure the clock to end-to-end transparent mode:

```
Switch(config)# ptp mode e2etransparent
```

This example shows how to configure the local clock priority1 value to 55 when PTP mode is boundary:

```
Switch(config)# ptp mode priority1 55
```

Related Commands

Command	Description
ptp (interface configuration)	Sets the PTP clock properties for a port.
show ptp	Displays the PTP properties that are configured on the port.
debug ptp	Enables debugging of the PTP activity.

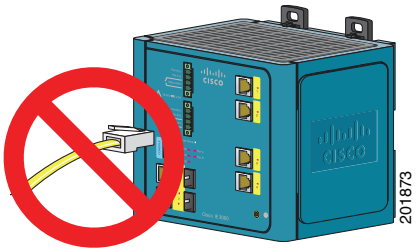
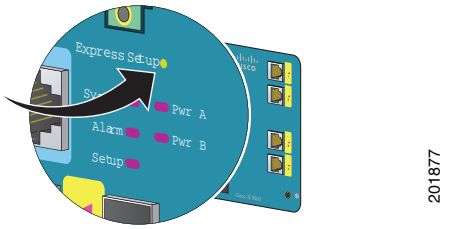
Updates to the Cisco IE 3000 Switch Getting Started Guide

Express Setup

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

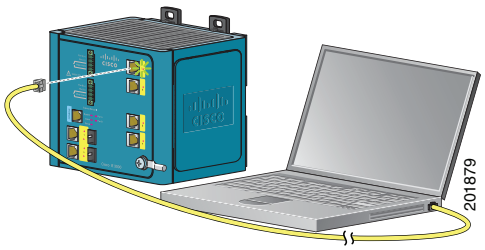
Running Express Setup:

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.

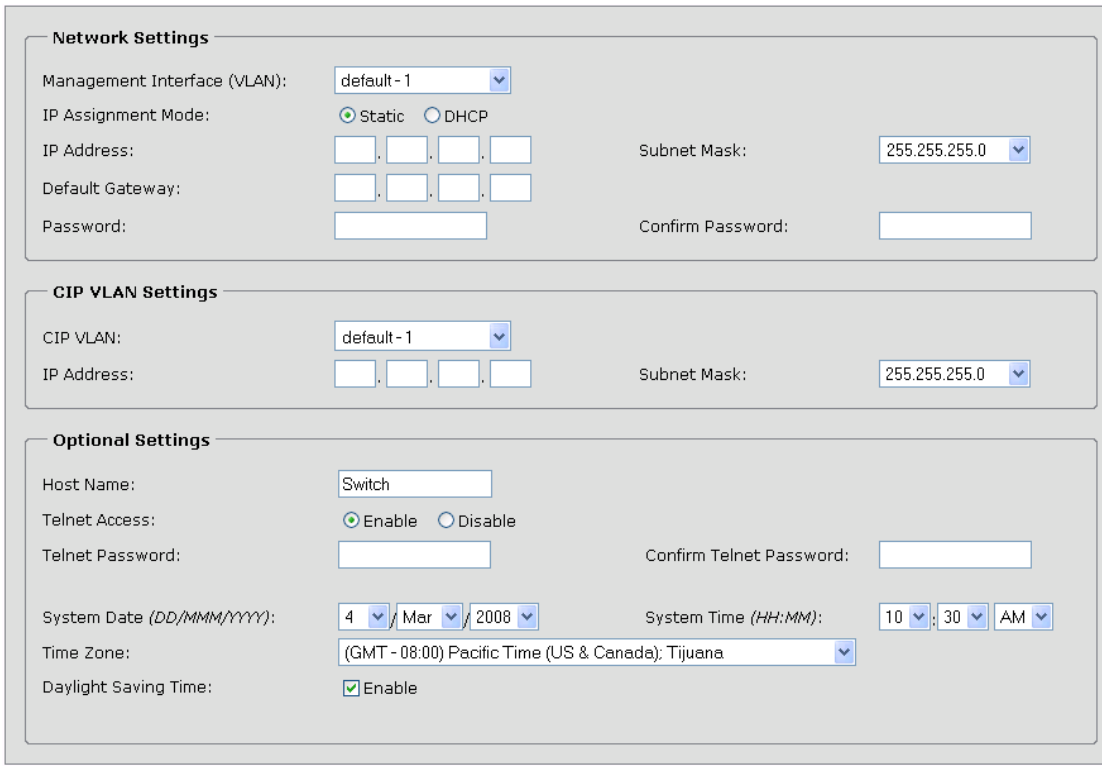
The port LEDs on your PC and the switch blink green while the switch configures the connection.



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

The compliance labels for the switch are shown in Figure 1 and Figure 2.

Figure 1 Compliance Label for the Cisco IE 3000 Switch

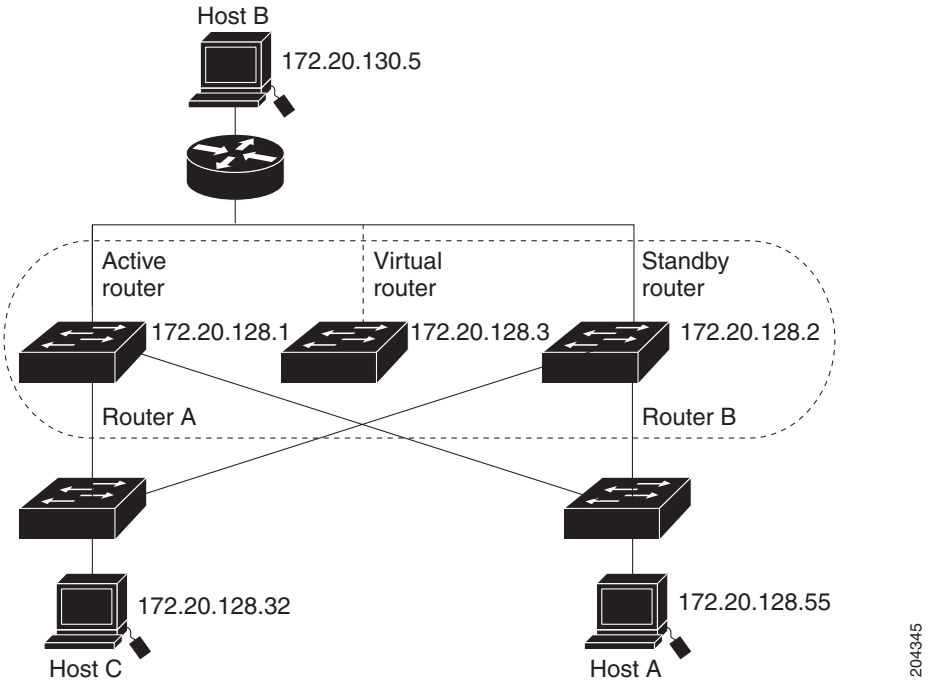
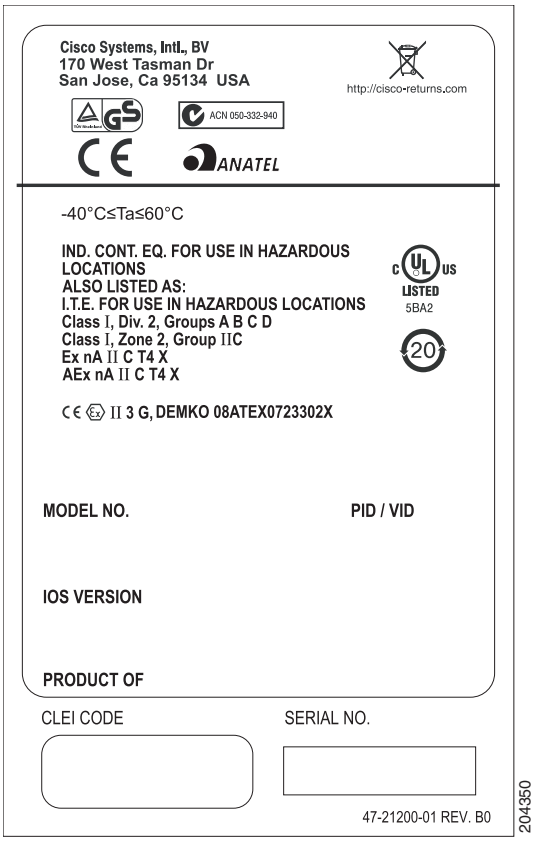


Figure 2 Compliance Label for the Cisco IE 3000 Switch Extension Module



Related Documentation

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, at:

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.