# Release Notes for Cisco 2600 XM Series Routers and Cisco 2800 Integrated Service Routers with Cisco IOS Release 12.4(15)SW

**November 30, 2007**
**Cisco IOS Release 12.4(15)SW**
**Fourth Release**

These release notes describe new features and significant software components for the Cisco 2600XM series routers and the Cisco 2800 integrated service routers that support the Cisco IOS Release 12.4(15)SW releases. These release notes are updated as needed to describe new memory requirements, new features, new hardware support, software platform deferrals, microcode or modem code changes, related document changes, and any other important changes. Use these release notes with the *Cross-Platform Release Notes for Cisco IOS Release 12.4T* located on Cisco.com.

For a list of the software caveats that apply to Release 12.4(15)SW, see the "Caveats" section on page 9 and *Caveats for Cisco IOS Release 12.4(11)T*. The online caveats document is updated for every maintenance release and is located on Cisco.com

## Contents




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

# Inheritance Information

Cisco IOS Release 12.4(11)SW is based on Cisco IOS Release 12.4(11)T. All features in Cisco IOS Release 12.4(11)T are in Cisco IOS Release 12.4(11)SW.

Table 1 lists sections of the *Cross-Platform Release Notes for Cisco IOS Release 12.4(15)SW* that apply to Cisco IOS Release 12.4(11)SW.

***Table 1 References for the Cross-Platform Release Notes for Cisco IOS Release 12.4T***

| Topic | Location |
|---|---|
| • Introductory information about the Cisco Cisco 2600XM series routers and the Cisco 2800 integrated service routers<br>• Hardware Supported<br>• Feature Set Tables | On Cisco.com at the following link:<br>http://www.cisco.com/en/US/products/ps6441/prod_release_note09186a00804a19a2.html |
| • Determining the Software Version<br>• Upgrading to a New Software Release | On Cisco.com at the following link:<br>http://www.cisco.com/en/US/products/ps6441/prod_release_note09186a00804a19ec.html |
| • Feature Descriptions (New and Changed Information)<br>• MIBs<br>• Important Notes | On Cisco.com at the following link:<br>http://www.cisco.com/en/US/products/ps6441/prod_release_note09186a00804a19ae.html |
| • Related Documentation<br>• Obtaining Documentation<br>• Obtaining Technical Assistance | On Cisco.com at the following link:<br>http://www.cisco.com/en/US/products/ps6441/prod_release_note09186a00804a196b.html |

# System Requirements

This section describes the system requirements for Release 12.4(15)SW and includes the following sections:

# Memory Requirements

Table 2 describes memory requirements for the Cisco IOS feature sets that are supported by Cisco IOS Cisco IOS Release 12.4(11)SW on the Cisco 2600XM series routers and the Cisco 2800 integrated service routers.

***Table 2 Recommended Memory for the Cisco 2600 and Cisco 2600XM Series Routers and the Cisco 2800 Integrated Service Routers with Cisco IOS Release 12.4(15)SW***

| Platform | Image Name | Feature Set | Image | Flash Memory (MB) | DRAM (MB) |
|---|---|---|---|---|---|
| 2650XM<br>2651XM | IP Transfer Point (M3UA/SUA) | Cisco 2600 Series IOS IP Transfer Point (M3UA/SUA) | c2600-itpk9-mz | 32 | 128 |
| | | Cisco 2600 Series IOS IP Transfer Point (STP/M2PA) | | | |
| | | Cisco 2600 Series IOS ITP MAP Gateway Base | | | |
| Cisco 2811 | IP Transfer Point (SLT) | Cisco 2800 Series IOS IP Transfer Point (SLT) | c2800nm-ipss7-mz | 32 | 156 |
| | IP Transfer Point (M3UA/SUA) | Cisco 2800 Series IOS IP Transfer Point (M3UA/SUA) | c2800nm-itpk9-mz | | |
| | IP Transfer Point (STP/M2PA) | Cisco 2800 Series IOS IP Transfer Point (STP/M2PA) | c2800nm-itpk9-mz | | |
| | IP MAP Gateway Base | Cisco 2800 Series IOS IP MAP Gateway Base | c2800nm-itpk9-mz | | |
| Cisco 2691 | Cisco 2691 Enterprise Services | Enterprise Services | c2691-entservicesk9-mz | | |
| | Cisco 2691 IP Base w/o Crypto | IP Base w/o Crypto | c2691-ipbase-mz | | |

# Hardware Supported

Cisco IOS Release 12.4(15)SW supports the following platforms:

- Cisco 2650XM series
- Cisco 2651XM series
- Cisco 2811 integrated service routers

For descriptions of existing hardware features and supported modules, see the hardware installation guides, configuration and command reference guides, and additional documents specific to the Cisco 2600XM series and Cisco 2800 integrated service routers, which are available on Cisco.com at the following locations:

- Cisco 2600XM series routers:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/2600/index.htm

- Cisco 2800 integrated service routers:

  http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/2800/index.htm

This URL is subject to change without notice. If it changes, point your web browser to Cisco.com, and click the following path:

**Cisco Product Documentation**: **Access Servers and Access Routers**: **Modular Access Routers**

# Determining the Software Version

To determine which version of Cisco IOS software is currently running on your router, log in to the router and enter the **show version** EXEC command. The following sample output from the **show version** command indicates the version number.

```
Router> show version
Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-Y7-MZ), Version 12.4(15)SW, EARLY DEPLOYMENT RELEASE
SOFTWARE (fc1)
Synched to technology version 12.4(15)T
```

# Upgrading to a New Software Release

For general information about upgrading to a new software release, refer to the *Software Installation and Upgrade Procedures* located at http://www.cisco.com/warp/public/130/upgrade_index.shtml.

# Feature Set Tables

The Cisco IOS software is packaged in feature sets consisting of software images, depending on the platform. Each feature set contains a specific set of Cisco IOS features. Release 12.4(15)SW supports the same feature sets as Releases 12.4 and 12.4(15)T, but Release 12.4(15)SW includes new features supported by the Cisco 2600XM series routers and the Cisco 2800 integrated service routers.

**Caution** The Cisco IOS images with strong encryption (including, but not limited to, 168-bit [3DES] data encryption feature sets) are subject to United States government export controls and have limited distribution. Strong encryption images to be installed outside the United States will likely require an export license. Customer orders can be denied or subject to delay as a result of United States government regulations. When applicable, the purchaser/user must obtain local import and use authorizations for all encryption strengths. Please contact your sales representative or distributor for more information, or send an e-mail to export@cisco.com.

Table 3 lists the feature and feature sets supported in Cisco IOS Release 12.4(15)SW

The tables use the following conventions:

- In—The number in the ‘In’ column indicates the Cisco IOS release in which the feature was introduced. For example, “12.4(15)SW” indicates that the feature was introduced in 12.4(15)SW. If a cell in this column is empty, the feature was included in a previous release or in the initial base release.
- Yes—The feature is supported in the software image.

- No—The feature is not supported in the software image.

**Note** These feature set tables contain only a selected list of features, which are cumulative for Release 12.4(11)*nn* early deployment releases only (*nn* identifies each early deployment release). The tables do not list all features in each image—additional features are listed in *Cross-Platform Release Notes for Cisco IOS Release 12.4(11)T* and Release 12.4(15)T Cisco IOS documentation.

***Table 3 Cisco IOS Release 12.4(15)SW Feature List for Cisco 2691 and Cisco 2600XM Series Routers***

| Feature | In | Image |
|---|---|---|
| C-Link Backup Routing of M3UA/SUA Traffic | Yes | See Table 2 for image names. |
| GWS SCCP Error Return | | |
| MLR SCCP Error Return | | |
| Multiple HSL PVCs per Physical ATM interface | | |
| SCCP/MAP Address Modification for SRI-SM Messages | | |
| Enhanced Loadsharing | | |
| Integrated GWS and MLR Triggers | | |

# New and Changed Information

This section contains the following information:



## New Hardware Features in Release 12.4(15)SW

There are no new hardware features in this release.

# New Software Features in Release 12.4(15)SW

## Saving a GWS Table or a GWS Configuration to a Remote or Local File

Platforms: Cisco 2600XM, Cisco 2800 Integrated Services Router

In Cisco IOS 12.2(18)IXE and later releases, you can save a GWS table or a general GWS configuration to a local or remote file system. The GWS table file is made up of a number of table entries. The general GWS configuration file is made up of action sets, table sub mode commands, linkset table, AS table and global table.

Saving a GWS table or a GWS configuration to a remote or local file is documented in *IP Transfer Point (ITP) on the Cisco 2600 Platform*.

## Saving an MLR Table or an MLR Configuration to a Remote or Local File

Platforms: Cisco 2600XM, Cisco 2800 Integrated Services Router

In Cisco IOS 12.2(18)IXE and later releases, you can save an MLR table or a general MLR configuration to a local or remote file system. The general MLR configuration file includes MLR global options, MLR result groups, loading MLR address table command, MLR rulesets, MLR modify profiles, and MLR routing tables. The MLR address table file is made up of a number of table entries.

Saving an MLR Table or an MLR configuration to a remote or local file is documented in *IP Transfer Point (ITP) on the Cisco 2600 Platform*.

# New Hardware Features in Release 12.4(11)SW3

There are no new hardware features in this release.

# New Software Features in Release 12.4(11)SW3

There are no new software features in this release.

# New Hardware Features in Release 12.4(11)SW2

There are no new hardware features on the Cisco 2600XM series routers and the Cisco 2800 integrated service routers in Cisco IOS Release 12.4(11)SW2

# New Software Features in Release 12.4(11)SW2

The following new software features are supported by the Cisco 2600XM and Cisco 2800 series routers for Cisco IOS Release 12.4(11)SW2:

• Enhanced Loadsharing, page 7

• Integrated GWS and MLR Triggers, page 7

### Enhanced Loadsharing

The Enhanced Loadsharing feature creates a 3-bit hash from a subset of bits (6 each) taken from the Originating Point Code (OPC) and Destination Point Code (DPC). Concatenating this hash with the SLS yields a 7-bit value that is then used to select a link (SLC) from a 128 entry SLS->SLC mapping table. This results in a much more even load distribution among available links.

The feature also allows flexibility in choosing the subset of bits from the OPC and DPC using the opc-shift and dpc-shift parameters and simultaneous configuration of sls-shift, at the global and/or linkset level.

Refer to the following document for more information about Enhanced Loadsharing:

*IP Transfer Point*

### Integrated GWS and MLR Triggers

In Cisco IOS 12.4(11)SW2 and later releases, Multi Layer Routing (MLR) triggers and Gateway Screening (GWS) are integrated. GWS determines which packets are intercepted by MLR. You can configure MLR triggers using the GWS infrastructure, GWS tables, and MLR variables.

Refer to the following document for more information about Integrated GWS and MLR Triggers:

*IP Transfer Point*

## New Hardware Features in Release 12.4(11)SW1

The following new hardware feature is supported by the Cisco 2811 in Cisco IOS Release 12.4(18)SW1:

### Support for the VWIC Module (VWIC-2T1/E1-RAN)

Platforms: Cisco 2811

The Cisco VWIC-2T1/E1-RAN is a general-purpose T1/E1 voice/WAN interface card (VWIC) that features advanced processing and T1/E1 protection switching and is specifically designed for the Cisco RAN Optimization solution.

## New Software Features in Release 12.4(11)SW1

There are no new software features on the Cisco 2600XM series routers and the Cisco 2800 integrated service routers in Cisco IOS Release 12.4(11)SW1

## New Hardware Features in Release 12.4(11)SW

There are no new hardware features on the Cisco 2600XM series routers or the Cisco 2800 integrated service routers in Cisco IOS Release 12.4(11)SW.

# New Software Features in Release 12.4(11)SW

The following new software features are supported by the Cisco Cisco 2600XM series routers and the Cisco 2800 integrated service routers in Cisco IOS Release 12.4(11)SW:



## C-Link Backup Routing of M3UA/SUA Traffic

Cisco IOS Release 12.4(11)SW supports a C-link Backup Routing feature that provides backup routing to MTP3 User Adaptation Layer (M3UA) and SCCP User Adaptation (SUA) application servers (ASs). It uses a Message Transfer Part Level 3 (MTP3)/M2PA linkset to a remote signaling gateway (SG) serving the same ASs over Stream Control Transmission Protocol (SCTP)/IP. This configurable software feature is available to any IP Transfer Point (ITP) running a sigtran protocol (M3UA and/or SUA) and offloaded MTP3. The remote SG that is reachable through the C-link may be another ITP, or any SG serving the same ASs.

Refer to the following document for more information: *IP Transfer Point (ITP)*

## GWS SCCP Error Return

Cisco IOS Release 12.4(11)SW allows you to configure Gateway Screening (GWS) to return a unitdata service (UDTS) to the source of the Signaling Connection Control Part (SCCP) packet when the SCCP packet is dropped. You configure a return UDTS when you define the gateway screening action set in enhanced GWS.

Refer to the following document for more information: *IP Transfer Point (ITP)*

## MLR SCCP Error Return

Cisco IOS Release 12.4(11)SW allows you to configure Multi Layer Routing (MLR) to return a unitdata service (UDTS) to the source of the Signaling Connection Control Part (SCCP) packet when the SCCP packet is blocked. You configure this by specifying an optional sccp-error parameter on block results in MLR rules and MLR address tables.

Refer to the following document for more information: *IP Transfer Point (ITP)*

## Multiple HSL PVCs per Physical ATM interface

Cisco IOS Release 12.4(11)SW allows multiple High Speed Link (HSL) permanent virtual circuits (PVCs) per physical Asynchronous Transfer Mode (ATM) interface. This is done through the support of subinterface configuration on the ATM link. Prior to Cisco IOS Release 12.4(11)SW, you could only configure the ATM interface, not any subinterfaces. The ability to create additional subinterfaces allows for more qssals, since only one qssal is allowed per interface or subinterface.

Refer to the following document for more information: *IP Transfer Point (ITP)*

### SCCP/MAP Address Modification for SRI-SM Messages

Cisco IOS Release 12.4(11)SW permits Signaling Connection Control Part (SCCP) and MAP address modification using a Multi-Layer Routing (MLR) **modify-profile**. MLR currently supports modifying only the service center address (orig-smsc) and the calling party address (CgPA) for SRI-SM messages.

With Cisco IOS Release 12.4(11)SW, the user can also now optionally configure the desired action for failed modifications using the **modify-failure** command within the MLR options submode. A user can also configure the **preserve-opc** function within the global MLR options submode. The **preserve-opc** function retains the original Originating Point Code (OPC). The user may configure MLR to return a unitdata service (UDTS) to the source of the SCCP packet when the SCCP packet is blocked by specifying an optional **sccp-error** parameter on block results.

Refer to the following document for more information: *IP Transfer Point (ITP)*

## New Features in Release 12.4(11)T

For information regarding the features supported in Cisco IOS Release 12.4T, see the Cross-Platform Release Notes and New Feature Documentation links at the following location on Cisco.com:
http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124relnt/xprn124/index.htm

# MIBs

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

http://tools.cisco.com/ITDIT/MIBS/servlet/index

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

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

# Limitations and Restrictions

There are no known limitations or restrictions in this release.

# Caveats

Caveats describe unexpected behavior or defects in the Cisco IOS software releases. Severity 1 caveats are the most serious caveats, severity 2 caveats are less serious, and severity 3 caveats are the least serious of these three severity levels.

Caveats in Cisco IOS Release 12.4(11)T are also in Cisco IOS Release 12.4(11)SW. For information on caveats in Cisco IOS Release 12.4(11)T, refer to the *Caveats for Cisco IOS Release 12.4(11)T* document. This document lists severity 1 and 2 caveats; the documents are located on Cisco.com.

**Note** If you have an account with Cisco.com, you can also use the Bug Toolkit to find select caveats of any severity. To reach the Bug Toolkit, log in to Cisco.com and go to: http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

Because Cisco IOS Release 12.4(11)SW is the initial base release, there are no resolved caveats. For a list of the resolved caveats, refer to the next set of release notes for this release version.

# Open Caveats—Cisco IOS Release 12.4(15)SW

- CSCsh35975

  Bad VCD msg observed traffic on the other links and subinterfaces does not seem to be affected.

  Condition: The below steps cause the condition:

  1. shut the main interface and its sub-interfaces that are used in links
  2. no shut the main interface but keep the sub-interfaces shut

  Workaround: There are no known workarounds

- CSCsd34549

  An unexpected config_state value is seen during reload or switchover.

  Condition: This is seen after an IMA card reloads or switches over.

  Workaround: There are no known workarounds

- CSCsd73254

  On the ITP 2600 platform, if a specific software error on the active RP causes the active RP to fail, the standby SUP may not detect the failure. Instead, the active SUP may reload the ITP to restore ITP manageability.

  Condition: This has only been observed in specific lab tests that force a specific software failure on the active RP.

  Workaround: There are no known workarounds

# Resolved Caveats—Cisco IOS Release 12.4(15)SW

- CSCek63758

  MSU Rates spike after clearing counters

  Condition: This problem occurs on all ITP platforms

  Workaround: There are no known workarounds

- CSCsg27676

  The SGMP link between ITP mates may flap when an ASP becomes active

  Condition: This problem occurs on all ITP platforms

  Workaround: There are no known workarounds

- CSCsg58153

  The PA has crashed and is unresponsive

  Condition: Bad circuits on uplink links cause all the SS7 links to go down and flap continuously

  Workaround: The fix is to bring the PA up once it has crashed

- CSCsh69956

  Syslog messages and SNMP traps are not generated for clock transitions on the PA-A3-8T1IMA

  Condition: This problem occurs on all ITP platforms

  Workaround: There are no known workarounds.

- CSCsi40918

  The RSP crashed causing a switchover to standby RSP.

  Condition: This crash occurred during normal router operations.

  Workaround: There are no known workarounds.

- CSCsi60319

  The MMSC gateway feature of the ITP is not returning the responding HLR E.164 address to the SMPP client when the HLR responds with an ERROR or REJECT component.

  Condition: This problem only affects the MMSC gateway feature when clients submit a GetIMSI request and an HLR responds with an error.

  Workaround: There are no known workarounds.

- CSCsi64297

  A VIP crashes while processing GTT traffic.

  Condition: This problem occurs with MTP3 offload enabled with a VIP performing GTT on both UDT and XUDT SCCP messages.

  Workaround: There are no known workarounds.

- CSCsi68966

  SCCP fails to route messages to XUA PCs even though they are available.

  Condition : This problem is timing related and only occurs on a reboot of the entire system or card.

  Workaround: GTAs entered in config should point to AS name directly instead of PC.

- CSCsi79035

  The M3UA ASP multi-homing test fails when one interface is disconnected even though there are multiple local-ip addresses configured on multiple interfaces. The output of the show ip sctp instance shows only one local-ip address when it should have shown two.

  Condition: When M3UA ASPs have local-ip addresses from different FlexWANs, then sometimes only one IP address is used by the SCTP instance.

  Workaround: Doing shutdown and no shutdown of the affected M3UA instance clears the problem. The output of the command show ip sctp instance will now show two local-ip addresses.

- CSCsi98081

  A buffer leak caused by a large quantity of SNMP traps.

  Condition: This problem occurs on all ITP platforms

  Workaround: There are no known workarounds.

- CSCsj36934

7507MX crashes due to a bus error: System returned to ROM by bus error at PC 0x4107D360 TLB (load or instruction fetch) exception, CPU signal 10, PC = 0x4107D360

Condition: This occurs during normal operations.

Workaround: There are no known workarounds.

- CSCsj60899

  Flexwan crash while processing outbound m3ua sccp msu xudt.

  Condition: ITP may experience a LC crash while processing an XUDT SCCP Message that is routed to an M3UA destination. The XUDT must contain the optional importance parameter.

  Workaroudn: There are no known workarounds.

- CSCsj99422

  New ASP binding during NSO bulk sync causes SYNCERR.

  Condition: This occurs on an NSO switchover on ITP running m3ua/sua traffic.

  Workaround: There are no known workarounds.

- CSCsk15118

  ITP may crash while performing SCCP instance address conversion

  Condition: This occurs when the following three conditions are met:

  a. sccp instance conversion where address conversion is used between instances
  b. MSU with more than 16 digits in the received called party address
  c. The called party address does not match an entry in the selected prefix conversion table.

  Workaround: Ensure that all prefix conversion tables have default entries that will match all possible addresses.

  For example,

  cs7 instance 0 gtt address-conversion E164toE164 ...

  update in-address 0 out-address 0 update

  in-address 1 out-address 1 update

  in-address 2 out-address 2 update

  in-address 3 out-address 3 update

  in-address 4 out-address 4 update

  in-address 5 out-address 5 update

  in-address 6 out-address 6 update

  in-address 7 out-address 7 update

  in-address 8 out-address 8 update

  in-address 9 out-address 9

- CSCsk25247

  An ITP M2PA link will stop processing received messages and will eventually fail after receiving an SCTP DATA chunk that is 300 bytes or more. The DATA chunk is an invalid message because it is larger than the maximum MSU size allowed on the link, and is discarded before the Forward

Sequence Number (FSN) in the M2PA header is updated for the link. This causes all subsequent messages received over the link to be dropped due to an invalid FSN. The link will eventually fail if an SLTM/SLTA is dropped, or when the remote peer can no longer buffer forwarded messages.

The output of 'show cs7 m2pa statistics' and 'show cs7 m2pa' may be used to identify that this problem is occurring. 'show cs7 m2pa statistics' will show an elevated number of UnexpectedFSN_rcvd errors. 'show cs7 m2pa state' will show that the 'bsnr' field is not incrementing despite data chunks being received over the association.

Condition: This occurs when ITP receives an SCTP DATA chunk that is 300 bytes or more over an active M2PA link.

Workaround:

Identify the source of the invalid MSU and prevent it from forwarding the MSU to the ITP

shut / no shut the linkset to recover the affected links. This, however, will not prevent the problem from re-occurring.

- CSCsk50308

  When configuring an mtp3 route to an m3ua/sua point code, the initial route status is "available" even though the m3ua/sua point code is locally inactive.

  This occurs only upon initial route configuration.

  Workaround: Do one of the following:

  1. Bring the m3ua/sua point code active to match the route availability.
  2. Execute an mtp3 restart.

- CSCsk56500

  The removal of a card leaves the controller configuration intact.

  Condition: This happens on 2811 ITPs only when the no card type <t1|e1> command is issued. The result is the controller configuration remains in the show running-configuration output.

  Workaround: There should be no reason to issue a no card type command in an operating system. A reload is required to change the card type on all ITP systems.

- CSCsi34398

  When unconfiguring and reconfiguring OC3 ATM interfaces and associated linksets, with multi-pvc feature, including sub-interface and IP protocol, system may reload unexpectedly.

  Condition: The exact sequence of operation to recreate that problem has not been identified. Some conditions under an OC3 ATM interface, configuring and unconfiguring sub-interfaces, as well as ip protocol and atm nni.

  Workaround: Avoid configuring and unconfiguring multiple times. Once the system is configured, it remains stable.

- CSCsh33248

  A traceback similar to the following is observed:

  %FIB-4-FIBNULLIDB: Missing idb for fibidb ATM4/1/0.1 (if_number 76).

  -Traceback= 40603CD0 413473C8 4134867C 40C9CFB0 40CA08FC 40CA177C

  %FIB-4-FIBNULLIDB: Missing idb for fibidb ATM4/1/0.1 (if_number 76).

  -Traceback= 40603CD0 4133485C 41334990 4132A58C 4132AB68 4132E490 4132C5FC

  %FIB-SP-STDBY-4-FIBXDRINV: Invalid format. invalid if_number

  %CEF: fibidb ATM4/1/0.1(76) has no idb

Condition: In a multi-pvc configuration and after a switchover, configuration of a non-existent sub-interface may cause the trace back above.

Workaround: Don't unconfigure non-existent sub-interfaces

- CSCse11887

  IPCALLOCFAIL occurs during OIR of FlexWAN.

  Condition: The problem occurs intermittently during FlexWAN OIR.

  Workaround: There are no known workarounds.

- CSCsf10777

  An ATMPA-3-CMDFAIL may occur when you extract the Flexwan from the chassis.

  Condition: Occurs only when the Flexwan contains an E1 IMA PA, and the Flexwan is extracted from the chassis. Once the Flexwan is reinserted no additional symptoms occur.

  Workaround: There are no known workarounds if the Flexwan is extracted.

## Open Caveats—Cisco IOS Release 12.4(11)SW3

There are no known open caveats for Cisco IOS Release 12.4(11)SW3.

## Resolved Caveats—Cisco IOS Release 12.4(11)SW3

All the caveats listed in this section are resolved in Cisco IOS Release 12.4(11)SW3. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCsj44081

  Improper use of data structures occurred in Cisco IOS. The Cisco IOS software has been enhanced with the introduction of additional software checks to signal the improper use of data structures. The %DATACORRUPTION-1-DATAINCONSISTENCY error message is now preceded by a timestamp, and the error message is then followed by a traceback.

  Workaround: There is no workaround.

- CSCsi68841

  After configuring cs7 grouping, ITP crashed during normal traffic processing.

  Workaround: There are no known workarounds.

- CSCsj53415

  When traffic goes through GTT which results in going to an xUA AS, but is blocked by outbound GWS, the buffer is lost. Eventually all buffers are exhausted and the links fail and do not recover. Show buffers show a huge number of CS7 buffers and a huge number of misses in the global pool. The CS7 buffers keep increasing until the links fail.

  Workaround: If the links fail, a reload of the individual line card that contains the inbound links or reload of the entire router is required. Removing the outbound GWS rule prevents the problem.

## Open Caveats—Cisco IOS Release 12.4(11)SW2

There are no known open caveats for Cisco IOS Release 12.4(11)SW2.

# Resolved Caveats—Cisco IOS Release 12.4(11)SW2

All the caveats listed in this section are resolved in Cisco IOS Release 12.4(11)SW2. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCsg11686

  ITP sends an SIE instead of an SIN when a failed link is reactivating.

  Conditions: This issue occurs when a linkset has two links and one of the links is brought out of service (for example, as a result of a remote disconnect). Although the linkset status remains "available" when the failed link is re-activated, the ITP sends an SIE instead of an SIN (as shown by the increase of the OMLSSU_XMIT_SIECount by 1 for the failed link in the output of show cs7 mtp2 statistics command). Because one link is still available, an SIN should be sent instead of an SIE.

  Workaround: There are no known workarounds.

- CSCsg27676

  The Signaling Gateway Mate Protocol (SGMP) link between ITP mates may fail when an Application Server Process (ASP) becomes active.

  This issue occurs when an ASP configured for a loadshare bindings Application Server (AS) becomes active, and thousands of ASP bindings exist on the ITP.

  There are no known workarounds.

- CSCsh59560

  Cisco IP Transfer Point (ITP) running Cisco IOS Release 12.4(11)SW reports the Message Transfer Part Level 3 (MTP3) route as Avail, but the destination is reported as INACC.

  Conditions: This issue occurs during a system boot while processing a large route table because the MTP3 restart may not complete before the mtp3 timers expire. As a result, the system may be in an intermediate state where routes are available but the destination is inaccessible.

  Workaround: Reduce the number of routes to 8000 total routes/4000 destinations.

- CSCsh69956

  Syslog messages and Simple Network Management Protocol (SNMP) traps are not generated for clock transitions on the Inverse Multiplexing over ATM (IMA) port adapter.

  Workaround: There are no known workarounds.

- CSCsi60319

  The responding Home Location Register (HLR) E.164 address is not returned to the Short Message Peer-to-Peer (SMPP) client when handling error responses from an HLR.

  Conditions: This condition only affects the Multimedia Message Service Center (MMSC) gateway feature when clients submit a GetIMSI request and an HLR responds with an error.

  Workaround: There are no known workarounds.

# Open Caveats—Cisco IOS Release 12.4(11)SW1

There are no open caveats in this release.

# Resolved Caveats—Cisco IOS Release 12.4(11)SW1

- CSCsd85587

  A vulnerability has been discovered in a third party cryptographic library which is used by a number of Cisco products. This vulnerability may be triggered when a malformed Abstract Syntax Notation One (ASN.1) object is parsed. Due to the nature of the vulnerability it may be possible, in some cases, to trigger this vulnerability without a valid certificate or valid application-layer credentials (such as a valid username or password).

  Successful repeated exploitation of any of these vulnerabilities may lead to a sustained Denial-of-Service (DoS); however, vulnerabilities are not known to compromise either the confidentiality or integrity of the data or the device. These vulnerabilities are not believed to allow an attacker will not be able to decrypt any previously encrypted information.

  The vulnerable cryptographic library is used in the following Cisco products:

  - Cisco IOS, documented as Cisco bug ID CSCsd85587
  - Cisco IOS XR, documented as Cisco bug ID CSCsg41084
  - Cisco PIX and ASA Security Appliances, documented as Cisco bug ID CSCse91999
  - Cisco Unified CallManager, documented as Cisco bug ID CSCsg44348
  - Cisco Firewall Service Module (FWSM)

  This vulnerability is also being tracked by CERT/CC as VU#754281.

  Cisco has made free software available to address this vulnerability for affected customers. There are no workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070522-crypto.shtml.

**Note** Another related advisory is posted together with this Advisory. It also describes vulnerabilities related to cryptography that affect Cisco IOS. A combined software table for Cisco IOS only is available at http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml and can be used to choose a software release which fixes all security vulnerabilities published as of May 22, 2007. The related advisory is published at http://www.cisco.com/warp/public/707/cisco-sa-20070522-SSL.shtml.

# Open Caveats—Cisco IOS Release 12.4(11)SW

- CSCsh59560: MTP3 Route avail; Dest/MAP Status INACC after router boot

  Symptoms: Cisco IP Transfer Point (ITP) running Cisco IOS Release 12.4(11)SW reports the Message Transfer Part Level 3 (MTP3) route as Avail, but the destination is reported as INACC.

  Conditions: This issue occurs during a system boot while processing a large route table because the MTP3 restart may not complete before the mtp3 timers expire. As a result, the system may be in an intermediate state where routes are available but the destination is inaccessible.

  Workaround: Reduce the number of routes 8000 total routes/4000 destinations.

# Resolved Caveats—Cisco IOS Release 12.4(11)SW

There are no resolved caveats in this release.

# Related Documentation

The following sections describe the documentation available for the Cisco 2691 and Cisco 2600XM series routers. Typically, these documents consist of hardware and software installation guides, Cisco IOS configuration and command references, system error messages, feature modules, and other documents. Documentation is available as printed manuals or electronic documents, except for feature modules, which are available online on Cisco.com.

Use these release notes with the documents listed in the following sections:

- Release-Specific Documents
- Platform-Specific Documents

## Release-Specific Documents

The following documents are specific to Release 12.4 and apply to Cisco IOS Release 12.4(11)SW. They are located on Cisco.com and the Documentation CD (under the heading Service & Support**)**:

- To reach the *Cross-Platform Release Notes for Cisco IOS Release 12.4(11)T*, click this path:

  **Technical Documents**: **Cisco IOS Software**: **Release 12.4**: **Release Notes**: **Cisco IOS Release 12.4(11)T**

- To see other features that are supported on various Cisco platforms in Cisco IOS Cisco IOS Release 12.4(11)SW, go to the following document on Cisco.com:

  *Cisco IOS Release 12.4 Special and Early Deployments*

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124relnt/rnspls/rnxc.htm

- To reach product bulletins, field notices, and other release-specific documents, click this path:

  **Technical Documents**: **Product Bulletins**

- To reach the *Caveats for Cisco IOS Release 12.4* and *Caveats for Cisco IOS Release 12.4(11)T* documents, which contain caveats applicable to all platforms for all maintenance releases of Release 12.4, click this path:

  **Technical Documents**: **Cisco IOS Software**: **Release 12.4**: **Caveats**

**Note** If you have an account with Cisco.com, you can also use the Bug Toolkit to find selected caveats of any severity. To reach the Bug Toolkit, log in to Cisco.com, and go to: http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

## Platform-Specific Documents

Hardware installation guides, configuration and command reference guides, and additional documents specific to the Cisco 2600XM series routers and the Cisco 2800 integrated service routers are available on Cisco.com at the following locations:

- Cisco 2600XM Series Routers:

  http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/2600/index.htm

- Cisco 2800 Integrated Service Routers:

  http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/2800/index.htm

# Cisco Feature Navigator

Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a particular set of features and which features are supported in a particular Cisco IOS image. Feature Navigator is available 24 hours a day, 7 days a week.

To access Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, e-mail the Contact Database Administration group at cdbadmin@cisco.com. If you do not have an account on Cisco.com, go to http://www.cisco.com/register and follow the directions to set up an account.

To use Feature Navigator, you must have a JavaScript-enabled web browser such as Netscape 3.0 or later, or Internet Explorer 4.0 or later. Internet Explorer 4.0 always has JavaScript enabled. To enable JavaScript for Netscape 3.x or Netscape 4.x, follow the instructions provided with the web browser. For JavaScript support and enabling instructions for other browsers, check with the browser vendor.

Feature Navigator is updated when major Cisco IOS software releases and technology releases occur. You can access Feature Navigator at the following URL:

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

# Cisco IOS Software Documentation Set

The Cisco IOS software documentation set consists of the Cisco IOS configuration guides, Cisco IOS command references, and several other supporting documents that are shipped with your order in electronic form on the Documentation CD-ROM—unless you specifically ordered printed versions.

## Documentation Modules

Each module in the Cisco IOS documentation set consists of one or more configuration guides and one or more corresponding command references. Chapters in a configuration guide describe protocols, configuration tasks, and Cisco IOS software functionality, and contain comprehensive configuration examples. Chapters in a command reference provide complete command syntax information. Use each configuration guide with its corresponding command reference. The Cisco IOS software documentation set is available on Cisco.com.

## Release 12.4 Documentation Set

Table 3 on page 5 describes the contents of the Cisco IOS Release 12.4 software documentation set, which is available in both electronic and printed form.

**Note** You can find the most current Cisco IOS documentation on Cisco.com. These electronic documents may contain updates and modifications made after the hard-copy documents were printed.

**Note** Some aspects of the complete Cisco IOS Release 12.4 software documentation set might not apply to the Cisco 2600XM series routers and the Cisco 2800 integrated service routers.

## Cisco IOS Release 12.4T Documentation Set

Table 4 lists the Cisco IOS Release 12.4T configuration guides and command references.

**Note** Some of the configuration guides in the following table reference Cisco IOS Release12.4 versions of these documents. In these instances, no distinct Cisco IOS Release 12.4T version of the guide exists and the necessary configuration information is in the Cisco IOS Release12.4 version of the document. Keep in mind that Cisco IOS Release 12.4(11)SW is based on Cisco IOS Release 12.4(11)T. All features in Cisco IOS Release 12.4(11)T are in Cisco IOS Release 12.4(11)SW. The references to Cisco IOS Release12.4 configuration guides in the following table do not indicate that all features in Cisco IOS Release 12.4 are in Cisco IOS Release 12.4(11)SW.

***Table 4 Cisco IOS Release 12.4T Configuration Guides and Command References***

| Configuration Guide and Command Reference Titles | Description |
|---|---|
| **IP** | |
| *Cisco IOS BGP Configuration Guide*, Release 12.4T | The configuration guide describes configuration tasks to configure various advanced Border Gateway Protocol (BGP) features, such as BGP next-hop address tracking, BGP Nonstop Forwarding (NSF) awareness, and route dampening. BGP is an interdomain routing protocol designed to provide loop-free routing between organizations. |
| *Cisco IOS DHCP Configuration Guide*, Release 12.4T | The configuration guide describes the concepts and the tasks needed to configure the Cisco IOS Dynamic Host Configuration Protocol (DHCP). |
| *Cisco IOS IP Addressing Services Configuration Guide*, Release 12.4<br>*Cisco IOS IP Addressing Services Command Reference*, Release 12.4T | The configuration guide is a task-oriented guide to configuring IP addressing and services, including Network Address Translation (NAT), Domain Name System (DNS), and Dynamic Host Configuration Protocol (DHCP). The command reference provides detailed information about the commands used in the configuration guide. |
| *Cisco IOS IP Application Services Configuration Guide*, Release 12.4T<br>*Cisco IOS Application Services Command Reference*, Release 12.4T | The configuration guide is a task-oriented guide to configuring IP application services, including IP access lists, Web Cache Communication Protocol (WCCP), Gateway Load Balancing Protocol (GLBP), Server Load Balancing (SLB), Hot Standby Router Protocol (HSRP), and Virtual Router Redundancy Protocol (VRRP). The command reference provides detailed information about the commands used in the configuration guide. |
| *Cisco IOS IP Mobility Configuration Guide*, Release 12.4<br>*Cisco IOS IP Mobility Command Reference*, Release 12.4T | The configuration guide is a task-oriented guide to configuring Mobile IP and Cisco Mobile Networks. The command reference provides detailed information about the commands used in the configuration guide. |
| *Cisco IOS IP Multicast Configuration Guide*, Release 12.4<br>*Cisco IOS IP Multicast Command Reference*, Release 12.4T | The configuration guide is a task-oriented guide to configuring IP multicast, including Protocol Independent Multicast (PIM), Internet Group Management Protocol (IGMP), Distance Vector Multicast Routing Protocol (DVMRP), and Multicast Source Discovery Protocol (MSDP). The command reference provides detailed information about the commands used in the configuration guide. |

*Table 4 Cisco IOS Release 12.4T Configuration Guides and Command References (continued)*

| Configuration Guide and Command Reference Titles | Description |
|---|---|
| *Cisco IOS IP Routing Protocols Configuration Guide*, Release 12.4<br>*Cisco IOS IP Routing Protocols Command Reference*, Release 12.4T | The configuration guide is a task-oriented guide to configuring IP routing protocols, including Border Gateway Protocol (BGP), Intermediate System-to-Intermediate System (IS-IS), and Open Shortest Path First (OSPF). The command reference provides detailed information about the commands used in the configuration guide. |
| *Cisco IOS IP Switching Configuration Guide*, Release 12.4<br>*Cisco IOS IP Switching Command Reference*, Release 12.4T | The configuration guide is a task-oriented guide to configuring IP switching features, including Cisco Express Forwarding (CEF), fast switching, and Multicast Distributed Switching (MDS). The command reference provides detailed information about the commands used in the configuration guide. |
| *Cisco IOS IPv6 Configuration Guide*, Release 12.4T<br>*Cisco IOS IPv6 Command Reference*, Release 12.4T | The configuration guide is a task-oriented guide to configuring IP version 6 (IPv6), including IPv6 broadband access, IPv6 data-link layer, IPv6 multicast routing, IPv6 quality of service (QoS), IPv6 routing, IPv6 services and management, and IPv6 tunnel services. The command reference provides detailed information about the commands used in the configuration guide. |
| *Cisco IOS NAT Configuration Guide*, Release 12.4T | The configuration guide contains configuration documentation for s configuring NAT for IP address conservation and using application level gateways with NAT. |
| *Cisco IOS Optimized Edge Routing Configuration Guide*, Release 12.4T<br>*Cisco IOS Optimized Edge Routing Command Reference*, Release 12.4T | The configuration guide is a task-oriented guide to configuring Optimized Edge Routing (OER) features, including OER prefix learning, OER prefix monitoring, OER operational modes, and OER policy configuration. The command reference provides detailed information about the commands used in the configuration guide. |
| **Security and VPN** | |
| *Cisco IOS Security Configuration Guide*, Release 12.4T<br>*Cisco IOS Security Command Reference*, Release 12.4T | The configuration guide is a task-oriented guide to configuring various aspects of security, including terminal access security, network access security, accounting, traffic filters, router access, and network data encryption with router authentication. The command reference provides detailed information about the commands used in the configuration guide. |
| **QoS** | |
| *Cisco IOS Quality of Service Solutions Configuration Guide*, Release 12.4T<br>*Cisco IOS Quality of Service Solutions Command Reference*, Release 12.4T | The configuration guide is a task-oriented guide to configuring quality of service (QoS) features, including traffic classification and marking, traffic policing and shaping, congestion management, congestion avoidance, and signaling. The command reference provides detailed information about the commands used in the configuration guide. |
| **LAN Switching** | |
| *Cisco IOS LAN Switching Configuration Guide*, Release 12.4<br>*Cisco IOS LAN Switching Command Reference*, Release 12.4T | The configuration guide is a task-oriented guide to local-area network (LAN) switching features, including configuring routing between virtual LANs (VLANs) using Inter-Switch Link (ISL) encapsulation, IEEE 802.10 encapsulation, and IEEE 802.1Q encapsulation. The command reference provides detailed information about the commands used in the configuration guide. |

*Table 4 Cisco IOS Release 12.4T Configuration Guides and Command References (continued)*

| Configuration Guide and Command Reference Titles | Description |
|---|---|
| **Multiprotocol Label Switching (MPLS)** | |
| *Cisco IOS Multiprotocol Label Switching Configuration Guide*, Release 12.4<br>*Cisco IOS Multiprotocol Label Switching Command Reference*, Release 12.4T | The configuration guide is a task-oriented guide to configuring Multiprotocol Label Switching (MPLS), including MPLS Label Distribution Protocol, MPLS traffic engineering, and MPLS Virtual Private Networks (VPNs). The command reference provides detailed information about the commands used in the configuration guide. |
| **Network Management** | |
| *Cisco IOS IP SLAs Monitoring Technology Configuration Guide*, Release 12.4<br>*Cisco IOS IP SLAs Command Reference*, Release 12.4T | The configuration guide is a task-oriented guide to configuring the Cisco IOS IP Service Level Assurances (IP SLAs) feature. The command reference provides detailed information about the commands used in the configuration guide. |
| *Cisco IOS NetFlow Configuration Guide*, Release 12.4T<br>*Cisco IOS NetFlow Command Reference*, Release 12.4T | The configuration guide is a task-oriented guide to NetFlow features, including configuring NetFlow to analyze network traffic data, configuring NetFlow aggregation caches and export features, and configuring Simple Network Management Protocol (SNMP) and NetFlow MIB features. The command reference provides detailed information about the commands used in the configuration guide. |
| *Cisco IOS Network Management Configuration Guide*, Release 12.4<br>*Cisco IOS Network Management Command Reference*, Release 12.4T | The configuration guide is a task-oriented guide to network management features, including performing basic system management, performing troubleshooting and fault management, configuring Cisco Discovery Protocol (CDP), configuring Cisco Networking Services (CNS), configuring DistributedDirector, and configuring Simple Network Management Protocol (SNMP). The command reference provides detailed information about the commands used in the configuration guide. |
| **Voice** | |
| *Cisco CallManager and Cisco IOS Interoperability Configuration Guide*, Release 12.4T | The configuration guide provides configuration information about Cisco IOS voice features for Cisco Unified CallManager and Cisco IOS Interoperability. |
| *Cisco IOS Voice Configuration Library*<br>*Cisco IOS Voice Command Reference* | The configuration library is a task-oriented collection of configuration guides, application guides, a troubleshooting guide, feature documents, a library preface, a voice glossary, and more. It also covers Cisco IOS support for voice call control protocols, interoperability, physical and virtual interface management, and troubleshooting. In addition, the library includes documentation for IP telephony applications. The command reference provides detailed information about the commands used in the configuration library. |
| **Wireless / Mobility** | |
| *Cisco IOS Mobile Wireless Gateway GPRS Support Node Configuration Guide*, Release 12.4<br>*Cisco IOS Mobile Wireless Gateway GPRS Support Node Command Reference*, Release 12.4T | The configuration guide is a task-oriented guide to understanding and configuring a Cisco IOS Gateway GPRS Support Node (GGSN) in a 2.5G General Packet Radio Service (GPRS) and 3G Universal Mobile Telecommunication System (UMTS) network. The command reference provides detailed information about the commands used in the configuration guide. |

*Table 4 Cisco IOS Release 12.4T Configuration Guides and Command References (continued)*

| Configuration Guide and Command Reference Titles | Description |
|---|---|
| *Cisco IOS Mobile Wireless Home Agent Configuration Guide*, Release 12.4<br>*Cisco IOS Mobile Wireless Home Agent Command Reference*, Release 12.4T | The configuration guide is a task-oriented guide to understanding and configuring the Cisco Mobile Wireless Home Agent, which is an anchor point for mobile terminals for which Mobile IP or Proxy Mobile IP services are provided. The command reference provides detailed information about the commands used in the configuration guide. |
| *Cisco IOS Mobile Wireless Packet Data Serving Node Configuration Guide*, Release 12.4<br>*Cisco IOS Mobile Wireless Packet Data Serving Node Command Reference*, Release 12.4T | The configuration guide is a task-oriented guide to understanding and configuring the Cisco Packet Data Serving Node (PDSN), a wireless gateway between the mobile infrastructure and standard IP networks that enables packet data services in a Code Division Multiple Access (CDMA) environment. The command reference provides detailed information about the commands used in the configuration guide. |
| *Cisco IOS Mobile Wireless Radio Access Networking Configuration Guide*, Release 12.4<br>*Cisco IOS Mobile Wireless Radio Access Networking Command Reference*, Release 12.4T | The configuration guide is a task-oriented guide to understanding and configuring Cisco IOS Radio Access Network products. The command reference provides detailed information about the commands used in the configuration guide. |
| *Cisco IOS Wireless LAN Configuration Guide*, Release 12.4T | The configuration guide provides the conceptual information, configuration tasks, and examples to help you configure and monitor a “wireless-aware” router using the Cisco IOS CLI, which can be used through a console port or Telnet session. |
| **Long Reach Ethernet (LRE) and Digital Subscriber Line (xDSL)** | |
| *Cisco IOS Broadband Access Aggregation and DSL Configuration Guide*, Release 12.4<br>*Cisco IOS Broadband Access Aggregation and DSL Command Reference*, Release 12.4T | The configuration guide is a task-oriented guide to configuring broadband access aggregation and digital subscriber line features. The command reference provides detailed information about the commands used in the configuration guide. |
| *Cisco IOS Service Selection Gateway Configuration Guide*, Release 12.4<br>*Cisco IOS Service Selection Gateway Command Reference*, Release 12.4T | The configuration guide is a task-oriented guide to configuring Service Selection Gateway (SSG) features, including subscriber authentication, service access, and accounting. The command reference provides detailed information about the commands used in the configuration guide. |
| **Dial—Access** | |
| *Cisco IOS Dial Technologies Configuration Guide*, Release 12.4<br>*Cisco IOS Dial Technologies Command Reference*, Release 12.4T | The configuration guide is a task-oriented guide to configuring lines, modems, and ISDN services. This guide also contains information about configuring dialup solutions, including solutions for remote sites dialing in to a central office, Internet service providers (ISPs), ISP customers at home offices, enterprise WAN system administrators implementing dial-on-demand routing, and other corporate environments. The command reference provides detailed information about the commands used in the configuration guide. |

*Table 4 Cisco IOS Release 12.4T Configuration Guides and Command References (continued)*

| Configuration Guide and Command Reference Titles | Description |
|---|---|
| *Cisco IOS VPDN Configuration Guide*, Release 12.4T<br>*Cisco IOS VPDN Command Reference*, Release 12.4T | This book contains the commands used to configure and maintain a Cisco IOS virtual private dialup network (VPDN). The commands are listed alphabetically. |
| **Asynchronous Transfer Mode (ATM)** | |
| *Cisco IOS Asynchronous Transfer Mode Configuration Guide*, Release 12.4<br>*Cisco IOS Asynchronous Transfer Mode Command Reference*, Release 12.4T | The configuration guide is a task-oriented guide to configuring Asynchronous Transfer Mode (ATM), including WAN ATM, LAN ATM, and multiprotocol over ATM (MPOA). The command reference provides detailed information about the commands used in the configuration guide. |
| **WAN** | |
| *Cisco IOS Wide-Area Networking Configuration Guide*, Release 12.4<br>*Cisco IOS Wide-Area Networking Command Reference*, Release 12.4T | The configuration guide is a task-oriented guide to configuring wide-area network (WAN) features, including: Layer 2 Tunneling Protocol Version 3 (L2TPv3); Frame Relay; Link Access Procedure, Balanced (LAPB); and X.25. The command reference provides detailed information about the commands used in the configuration guide. |
| **System Management** | |
| *Cisco IOS Configuration Fundamentals Configuration Guide*, Release 12.4<br>*Cisco IOS Configuration Fundamentals Command Reference*, Release 12.4T | The configuration guide is a task-oriented guide to using Cisco IOS software to configure and maintain Cisco routers and access servers, including information about using the Cisco IOS command-line interface (CLI), loading and maintaining system images, using the Cisco IOS file system, using the Cisco IOS Web browser user interface (UI), and configuring basic file transfer services. The command reference provides detailed information about the commands used in the configuration guide. |
| *Cisco IOS Interface and Hardware Component Configuration Guide*, Release 12.4<br>*Cisco IOS Interface and Hardware Component Command Reference*, Release 12.4T | The configuration guide is a task-oriented guide to configuring and managing interfaces and hardware components, including dial shelves, LAN interfaces, logical interfaces, serial interfaces, and virtual interfaces. The command reference provides detailed information about the commands used in the configuration guide. |

*Table 4 Cisco IOS Release 12.4T Configuration Guides and Command References (continued)*

| Configuration Guide and Command Reference Titles | Description |
|---|---|
| **IBM Technologies** | |
| *Cisco IOS Bridging and IBM Networking Configuration Guide*, Release 12.4<br>*Cisco IOS Bridging Command Reference*, Release 12.4T<br>*Cisco IOS IBM Networking Command Reference*, Release 12.4T | The configuration guide is a task-oriented guide to configuring:<br>• Bridging features, including: transparent and source-route transparent (SRT) bridging, source-route bridging (SRB), Token Ring Inter-Switch Link (TRISL), and Token Ring Route Switch Module (TRRSM).<br>• IBM network features, including: data-link switching plus (DLSw+), serial tunnel (STUN), and block serial tunnel (BSTUN); Logical Link Control, type 2 (LLC2), and Synchronous Data Link Control (SDLC); IBM Network Media Translation, including SDLC Logical Link Control (SDLLC) and Qualified Logical Link Control (QLLC); downstream physical unit (DSPU), Systems Network Architecture (SNA) service point, SNA Frame Relay Access, Advanced Peer-to-Peer Networking (APPN), native client interface architecture (NCIA) client/server topologies, and IBM Channel Attach.<br>The two command references provide detailed information about the commands used in the configuration guide. |
| **Additional and Legacy Protocols** | |
| *Cisco IOS AppleTalk Configuration Guide*, Release 12.4<br>*Cisco IOS AppleTalk Command Reference*, Release 12.4T | The configuration guide is a task-oriented guide to configuring the AppleTalk protocol. The command reference provides detailed information about the commands used in the configuration guide. |
| *Cisco IOS DECnet Configuration Guide*, Release 12.4<br>*Cisco IOS DECnet Command Reference*, Release 12.4T | The configuration guide is a task-oriented guide to configuring the DECnet protocol. The command reference provides detailed information about the commands used in the configuration guide. |
| *Cisco IOS ISO CLNS Configuration Guide*, Release 12.4<br>*Cisco IOS ISO CLNS Command Reference*, Release 12.4T | The configuration guide is a task-oriented guide to configuring International Organization for Standardization (ISO) Connectionless Network Service (CLNS). The command reference provides detailed information about the commands used in the configuration guide. |
| *Cisco IOS Novell IPX Configuration Guide*, Release 12.4<br>*Cisco IOS Novell IPX Command Reference*, Release 12.4T | The configuration guide is a task-oriented guide to configuring the Novell Internetwork Packet Exchange (IPX) protocol. The command reference provides detailed information about the commands used in the configuration guide. |
| *Cisco IOS Terminal Services Configuration Guide*, Release 12.4<br>*Cisco IOS Terminal Services Command Reference*, Release 12.4T | The configuration guide is a task-oriented guide to configuring terminal services, including DEC, local-area transport (LAT), and X.25 packet assembler/disassembler (PAD). The command reference provides detailed information about the commands used in the configuration guide. |

Table 5 lists the documents and resources that support the Cisco IOS Release 12.4T software configuration guides and command references.

***Table 5 Cisco IOS Release 12.4T Supporting Documents and Resources***

| Document Title | Description |
|---|---|
| *Cisco IOS Master Commands List*, Release 12.4T | An alphabetical listing of all the commands documented in the Cisco IOS Release 12.4T command references. |
| *Cisco IOS New, Modified, Replaced, and Removed Commands*, Release 12.4T | A listing of all the new, modified, replaced and removed commands for the Cisco IOS Release 12.4T release, grouped by maintenance release and ordered alphabetically within each group. |
| *System Messages for Cisco IOS Release 12.4 T* | These publications list and describe Cisco IOS system messages for Cisco IOS Release 12.4T. Not all system messages indicate problems with your system. Some are purely informational, and others may help diagnose problems with communications lines, internal hardware, or the system software. |
| *Cisco IOS Debug Command Reference*, Release 12.4T | This publication contains an alphabetical listing of the **debug** commands and their descriptions. Documentation for each command includes a brief description of its use, command syntax, and usage guidelines. |
| *Cisco IOS Fax and Modem Services over IP Application Guide*, Release 12.4T | The application guide includes descriptions and configuration instructions for fax and modem transmission capabilities on Cisco Voice over IP (VoIP) networks. |
| *Cross-Platform Release Notes for Cisco IOS Release 12.4T* | This documentation describes general release information, including information about supported platforms, feature sets, platform-specific notes, and Cisco IOS software defects. |
| *Dictionary of Internetworking Terms and Acronyms* | This publication compiles and defines the terms and acronyms used in the internetworking industry. |
| RFCs | RFCs are standards documents maintained by the Internet Engineering Task Force (IETF). Cisco IOS software documentation references supported RFCs when applicable. The full text of referenced RFCs may be obtained at the following URL:<br>http://www.rfc-editor.org/ |
| MIBs | MIBs are used for network monitoring. To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br>http://www.cisco.com/go/mibs |

# Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

## Cisco.com

You can access the most current Cisco documentation at this URL:

http://www.cisco.com/techsupport

You can access the Cisco website at this URL:

http://www.cisco.com

You can access international Cisco websites at this URL:

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

## Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

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

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

# Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco documentation to bug-doc@cisco.com.

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

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

We appreciate your comments.

# Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

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

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

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

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

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

## Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com

  An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- Nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

**Tip** We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.*x* through 8.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

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

The link on this page has the current PGP key ID in use.

# Service and Support

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

## Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you with these tasks:

- Streamline business processes and improve productivity
- Resolve technical issues with online support

- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

If you want to obtain customized information and service, you can self-register on Cisco.com. To access Cisco.com, go to this URL:

http://www.cisco.com

# Technical Assistance Center

The Cisco Technical Assistance Center (TAC) is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two levels of support are available: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Cisco TAC inquiries are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

The Cisco TAC resource that you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

## Cisco TAC Web Site

You can use the Cisco TAC Web Site to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to this URL:

http://www.cisco.com/tac

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

http://www.cisco.com/register/

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

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

If you have Internet access, we recommend that you open P3 and P4 cases through the Cisco TAC Web Site.

## Cisco TAC Escalation Center

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

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

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

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

---

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