Release Notes for Cisco 7000 Family for Cisco IOS Release 12.4 SW

March 30, 2008

Cisco IOS Release 12.4(15)SW1

These release notes for the Cisco 7000 family describe the enhancements provided in Cisco IOS Release 12.4(15)SW1. Cisco IOS Release 12.4(15)SW1 supports the IP Transfer Point (ITP) product on Cisco 7200 and 7301 series routers and uses the ITP functionality of Cisco IOS Release 12.2(25)SW8 as its base. Cisco IOS Release 12.4(15)SW1 is not a general purpose release. These release notes are updated as needed.

For a list of the software caveats that apply to Cisco IOS Release 12.4(15)SW1, see the "Caveats for Cisco IOS Release 12.4 SW" section on page 13 and *Caveats for Cisco IOS Release 12.4T*. The caveats document is updated for every maintenance release and is located on Cisco.com.

Use these release notes with *Cross-Platform Release Notes for Cisco IOS Release 12.4T* located on Cisco.com.

Cisco recommends that you view the field notices for this release to see if your software or hardware platforms are affected. If you have an account on Cisco.com, you can find field notices at http://www.cisco.com/warp/customer/tech_tips/index/fn.html. If you do not have a Cisco.com login account, you can find field notices at http://www.cisco.com/warp/public/tech_tips/index/fn.html.

Contents

These release notes describe the following topics:

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

Inheritance Information

Cisco IOS Release 12.4(15)SW1 is based on Cisco IOS Release 12.4(15)T. All features in Cisco IOS Release 12.4(15)T are in Cisco IOS Release 12.4(15)SW1.

Table 1 lists sections of the *Cross-Platform Release Notes for Cisco IOS Release 12.4T* that apply to Cisco IOS Release 12.4(15)SW1.

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

Topic	Location
• Introductory information about the Cisco 7200 and Cisco 7301 series routers • Hardware Supported • Feature Set Tables	On Cisco.com at: **Products & Services > IOS Software > Cisco IOS Software Releases 12.4T > General Information> Release Notes > Cross-Platform Release Notes for Cisco IOS Release 12.4T, Part 2 > Platform-Specific Information** Or at: http://www.cisco.com/en/US/products/ps6441/prod_release_note09186a00804a19a2.html
• Determining the Software Version • Upgrading to a New Software Release	On Cisco.com at: **Products & Services > IOS Software > Cisco IOS Software Releases 12.4T > General Information> Release Notes > Cross-Platform Release Notes for Cisco IOS Release 12.4T, Part 1 > System Requirements** Or at: http://www.cisco.com/en/US/products/ps6441/prod_release_note09186a00804a19ec.html

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

Topic	Location
• Feature Descriptions (New and Changed Information) • MIBs • Important Notes	On Cisco.com at: **Products & Services > IOS Software > Cisco IOS Software Releases 12.4T > General Information> Release Notes > Cross-Platform Release Notes for Cisco IOS Release 12.4T, Part 3 > New Features and Important Notes** Or at: http://www.cisco.com/en/US/products/ps6441/prod_release_note09186a00804a19ae.html
• Related Documentation • Obtaining Documentation • Obtaining Technical Assistance	On Cisco.com at: **Products & Services > IOS Software > Cisco IOS Software Releases 12.4T > General Information> Release Notes > Cross-Platform Release Notes for Cisco IOS Release 12.2T, Part 4 > Related Documentation** Or at: http://www.cisco.com/en/US/products/ps6441/prod_release_note09186a00804a196b.html

System Requirements

This section describes the system requirements for Cisco IOS Release 12.4(15)SW1 and includes the following sections:

Memory Recommendations

Table 2 Memory Recommendations for Cisco IOS Release 12.4(15)SW1

Platforms	Feature Sets	Image Name	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
Cisco 7200	IP Standard Feature Set	IP Transfer Point	c7200-itpk9-mz	32 MB Flash	256 MB DRAM	FLASH
Cisco 7301	IP Standard Feature Set	IP Transfer Point	c7301-itpk9-mz	32 MB Flash	256 MB DRAM	FLASH

Supported Hardware

Cisco IOS Release 12.4(15)SW1 supports the following Cisco 7000 platforms:

- Cisco 7200 series routers
- Cisco 7301 series routers

For detailed descriptions of the new hardware features, see the "New and Changed Information" section on page 6.

Determining the Software Version

To determine the version of Cisco IOS software running on your Cisco 7200 or Cisco 7301 series router, log in to the router and enter the **show version** EXEC command. For example:

```
Router> show version
Cisco Internetwork Operating System Software
IOS (tm) 7301 Software (c7301-itpk9-mz), Version 12.4(15)SW1, RELEASE SOFTWARE
```

Upgrading to a New Software Release

For information about selecting a new Cisco IOS software release, please refer to *How to Choose a Cisco IOS Software Release* at:

http://www.cisco.com/warp/public/130/choosing_ios.shtml

For information about upgrading to a new software release, refer to the appropriate platform-specific document:

- Cisco 7200 Series, 7300 Series, 7400 Series, and 7500 Series Routers

  http://www.cisco.com/en/US/products/hw/routers/ps133/products_tech_note09186a0080094c07.shtml

For *Cisco IOS Upgrade Ordering Instructions*, refer to the document at the following location:

http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/957_pp.htm

To choose a new Cisco IOS software release by comparing feature support or memory requirements, use Cisco Feature Navigator. Cisco Feature Navigator is a web-based tool that enables you to determine which Cisco IOS and Catalyst OS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or by feature set (software image). Under the release section, you can compare Cisco IOS software releases side by side to display both the features unique to each software release and the features that the releases have in common.

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

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

To choose a new Cisco IOS software release based on information about defects that affect that software, use Bug Toolkit at:

http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

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.

Cisco IOS Release 12.4(15)SW1 supports the same feature sets as Cisco IOS Release 12.4(15)T, but Cisco IOS Release 12.4(15)SW1 can include new features supported by the Cisco 7200 and Cisco 7301 series routers.

Caution Cisco IOS images with strong encryption (including, but not limited to, 168-bit Triple Data Encryption Standard [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 are likely to require an export license. Customer orders may be denied or subject to delay because of United States government regulations. When applicable, purchaser and 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.

Cisco IOS software images are subject to deferral. Cisco recommends that you view the deferral notices at the following location to determine if your software release is affected:

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

Table 3 lists the features and feature sets supported by the Cisco 7200 and Cisco 7301 series routers in Cisco IOS Release 12.4(15)SW1 and uses the following conventions:

- Yes—The feature is supported in the software image.
- No—The feature is not supported in the software image.
- In—The number in the "In" column indicates the Cisco IOS release in which the feature was introduced. For example, "(11) 3" would mean a feature was introduced in12.4(11)SW3. If a cell in this column is empty, the feature was included in the initial base release.

Note These release notes are not cumulative and list only features that are new to Cisco IOS Release 12.4(15)SW1. The parent release for Cisco IOS Release 12.4(15)SW1 is Cisco IOS Release 12.4(15)T. For information about inherited features, refer to Cisco.com or Cisco Feature Navigator. For Cisco.com, either go to Cisco.com and select the appropriate software release under **Products and Service** and **IOS Software** or go to http://www.cisco.com/univercd/home/index.htm and select the appropriate software release under **Cisco IOS Software** and **Release Notes**. You can use the Cisco Feature Navigator tool at http://www.cisco.com/go/fn.

Table 3 Feature List by Feature Set for the Cisco 7000 Family Routers

Features	In	Software Images by Feature Sets	
		c7200-itpk9-mz	c7301-itpk9-mz
Accounting Support for xUA and Virtual Linkset	(15) 1	Yes	Yes
C-Link Backup Routing of M3UA/SUA Traffic		Yes	Yes
Enhanced Loadsharing	(11) 2	Yes	Yes
Enhanced MLR Modification CdPA (and CgPA)	(15)	Yes	Yes
Enhancing GTT Address Conversion Flexibility	(15)	Yes	Yes
Extending the Application Group to 64 Entries per Group	(15)	Yes	Yes

Table 3 Feature List by Feature Set for the Cisco 7000 Family Routers

Features	In	Software Images by Feature Sets	
		c7200-itpk9-mz	c7301-itpk9-mz
GWS SCCP Error Return		Yes	Yes
Integrated GWS and MLR Triggers	(11)2	Yes	Yes
MLR Routing to M3UA AS without Modifying the DPC	(15)	Yes	Yes
MLR SCCP Error Return		Yes	Yes
Multiple HSL PVCs per Physical ATM interface		Yes	Yes
Saving, Loading, and Non-Disruptive Replacement of a GWS Configuration or GWS Table to a Remote or Local File	(15)	Yes	Yes
Saving, Loading, and Non-Disruptive Replacement of an MLR Configuration to a Remote or Local File	(15)	Yes	Yes
SCCP/MAP Address Modification for SRI-SM Messages		Yes	Yes
Support for 16 Application Server Processes (ASPs) per Application Server (AS)	(15) 1	Yes	Yes
Support for GTT Inter-Instance	(15) 1	Yes	Yes
Support for the cs7 mtp3 rct-opc-from-tfc Command	(15) 1	Yes	Yes
Support for TTC Variant Conversion	(15) 1	Yes	Yes
Translation Type (TT) Modification within an Application Group	(15)	Yes	Yes
TTMAP support for xUA AS	(15)	Yes	Yes

New and Changed Information

The following sections list the new hardware and software features supported by the Cisco 7200 and Cisco 7301 series routers for Cisco IOS Release 12.4(15)SW1.

New Hardware Features in Release 12.4(15)SW1

No new hardware features are supported by the Cisco IOS Release 12.4(15)SW1.

New Software Features in Release 12.4(15)SW1

The following new software features are supported in Cisco IOS Release 12.4(15)SW1:

- Accounting Support for xUA and Virtual Linkset, page 7
- Support for 16 Application Server Processes (ASPs) per Application Server (AS), page 7
- Support for GTT Inter-Instance, page 7
- Support for the cs7 mtp3 rct-opc-from-tfc Command, page 7
- Support for TTC Variant Conversion, page 7

Accounting Support for xUA and Virtual Linkset

In Cisco IOS 12.4(15)SW1 and later releases, Cisco ITP supports accounting for the combination of M3UA and SUA functionality (xUA). This feature applies the existing linkset-based accounting to xUA AS use. Accounting is also provided for virtual linksets between instances.

Refer to the following document for more information about Accounting Support for xUA and Virtual Linkset:

IP Transfer Point (ITP)

Support for 16 Application Server Processes (ASPs) per Application Server (AS)

In Cisco IOS 12.4(15)SW1 and later releases, Cisco ITP supports 16 ASPs per AS.

Support for GTT Inter-Instance

In Cisco IOS 12.4(15)SW1 and later releases, Global Title Translation (GTT) Inter-Instance support enhances Cisco ITP's capability of routing MSU inter-instance based on global title when configuring instance conversion after GTT. This allows Cisco ITP to use the GTT process on an MSU in one instance and send it to another instance for subsequent GTT processing. The feature also addresses inter-instance looping prevention.

Refer to the following document for more information about GTT Inter-Instance:

IP Transfer Point (ITP)

Support for the cs7 mtp3 rct-opc-from-tfc Command

In Cisco IOS 12.4(15)SW1 and later releases, Cisco ITP provides the ability to configure the operation of sending Routeset Congestion Test (RCT) messages to use the destination point code (DPC) found on the last received TFC as the source for the Origin Point Code (OPC) on the next RCT procedure. By default, Cisco ITP uses its local point code as the OPC parameter on an RCT.

Refer to the following document for more information about the **cs7 mtp3 rct-opc-from-tfc** command:

ITP Command Set: A - D chapter of the *IP Transfer Point (ITP)*

Support for TTC Variant Conversion

In Cisco IOS 12.4(15)SW1 and later releases, Cisco ITP provides MTP3/SCCP conversion ability between TTC and ANSI/ITU variants. A similar conversion between ITU and ANSI is already supported.

Refer to the following document for more information about TTC Variant Conversion:

IP Transfer Point (ITP)

New Hardware Features in Release 12.4(15)SW

There are no new hardware features supported in Cisco IOS Release 12.4(15)SW.

New Software Features in Release 12.4(15)SW

The following new software features are supported by the Cisco 7200 and Cisco 7301 series routers for Cisco IOS Release 12.4(15)SW:

Enhanced MLR Modification CdPA (and CgPA)

This feature allows Multi Layer Routing (MLR) to modify the Signaling Connection Control Part (SCCP) called party address (CdPA) global title (GT) selector and digits prior to routing to the specified result. MLR modifies the SCCP CdPA PC and subsystem number (SSN) using a modification profile. MLR modifies the SCCP CdPA via modify-profile for all MAP-based operations. MLR expands its SCCP calling party address (CgPA) modification to be applied to all MAP-based operations

Refer to the following document for more information about this feature:

IP Transfer Point (ITP)

Enhancing GTT Address Conversion Flexibility

Global title translation (GTT) address conversion allows the operator to specify the number of digits removed from the original address prefix when the in-address prefix is matched. GTT address-conversion supports 0 digits for the update in-address parameter. The supported range today is between 1 and 15 digits. The range of digits removed may be between 0 and 15 digits, and has no relation to the number of digits specified in the in-address parameter.

Refer to the following document for more information about this feature:

IP Transfer Point (ITP)

Extending the Application Group to 64 Entries per Group

This feature extends the limit of eight global title translation (GTT) application group members per application group to 64 application group members. The composition of the application group supports the range of 64 members with the same cost value and 64 members with unique cost values.

Refer to the following document for more information about this feature:

IP Transfer Point (ITP)

MLR Routing to M3UA AS without Modifying the DPC

This feature gives Multi Layer Routing (MLR) the ability to route a received packet to an MTP3 User Adaptation Layer (M3UA) application server (AS) without modifying the Destination Point Code (DPC). This is not a message signal unit (MSU) copy feature, but a modification to the routing of the received MSU.

Refer to the following document for more information about this feature:

IP Transfer Point (ITP)

Saving, Loading, and Non-Disruptive Replacement of a GWS Configuration or GWS Table to a Remote or Local File

In Cisco IOS Release 12.4(15)SW and later releases, you can save a Gateway Screening (GWS) table or a general GWS configuration to a local or remote file system, load the general configuration from a local or remote file system, and non-disruptively replace the running GWS configuration or GWS table on an operational 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.

Refer to the following document for more information about this feature:

IP Transfer Point (ITP)

Saving, Loading, and Non-Disruptive Replacement of an MLR Configuration to a Remote or Local File

In Cisco IOS Release 12.4(15)SW and later releases, you can save the general Multi Layer Routing (MLR) configuration to a local or remote file system, load the general configuration from a local or remote file system, and non-disruptively replace the running MLR configuration on an operational system.

The general MLR configuration file includes MLR global result groups, loading MLR address table command, MLR rulesets, MLR modify profiles, routing tables. Individual MLR address tables may still be saved to separate files, but the load statements are included in the general MLR configuration file.

Refer to the following document for more information about this feature:

IP Transfer Point (ITP)

Translation Type (TT) Modification within an Application Group

Global title translation (GTT) currently allows post-translation modification of the TT on a per-global title address (GTA) basis, unless the result type is an application group. This feature allows post-translation modification of the TT on a per application group member basis.

Refer to the following document for more information about this feature:

IP Transfer Point (ITP)

TTMAP support for xUA AS

Mapping the called party address (CdPA) TT to a configured value is supported for all message signal units (MSUs) being sent or received over a particular linkset. This feature extends configured CdPA TT modification to all MSUs being sent or received over a particular MTP3 User Adaptation Layer (M3UA) or SCCP User Adaptation (SUA) application server (AS).

Refer to the following document for more information about this feature:

IP Transfer Point (ITP)

New Hardware Features in Release 12.4(11)SW3

There are no new hardware features supported in Cisco IOS Release 12.4(11)SW3.

New Software Features in Release 12.4(11)SW3

There are no new software features supported in Cisco IOS Release 12.4(11)SW3.

New Hardware Features in Release 12.4(11)SW2

There are no new hardware features supported 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 7200 and Cisco 7301 series routers for Cisco IOS Release 12.4(11)SW2:

- Enhanced Loadsharing, page 11
- Integrated GWS and MLR Triggers, page 11

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

There are no new hardware features supported in Cisco IOS Release 12.4(11)SW1.

New Software Features in Release 12.4(11)SW1

There are no new software features supported in Cisco IOS Release 12.4(11)SW1.

New Hardware Features in Release 12.4(11)SW

There are no new hardware features supported 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 7200 and Cisco 7301 series routers for Cisco IOS Release 12.4(11)SW:

- C-Link Backup Routing of M3UA/SUA Traffic, page 12
- GWS SCCP Error Return, page 12
- MLR SCCP Error Return, page 12
- Multiple HSL PVCs per Physical ATM interface, page 12
- SCCP/MAP Address Modification for SRI-SM Messages, page 13

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 about C-link Backup Routing:

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 about the GWS SCCP error return feature:

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 about the MLR SCCP error return feature:

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 about the multiple HSL PVCs feature:

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 about SCCP and MAP address modification:

IP Transfer Point (ITP)

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

Caveats for Cisco IOS Release 12.4 SW

Caveats describe unexpected behavior in Cisco IOS software releases. Severity 1 caveats are the most serious caveats; severity 2 caveats are less serious. Severity 3 caveats are moderate caveats, and only select severity 3 caveats are included in the caveats document.

This section contains open and resolved caveats for the current Cisco IOS maintenance release.

All caveats in Cisco IOS Release 12.4(15)T that apply to the Cisco 7200 and Cisco 7301 series routers are also in Cisco IOS Release 12.4(15)SW1.

For information on caveats in Cisco IOS Release 12.4(15)T, see *Caveats for Cisco IOS Release 12.4T*, which lists severity 1 and 2 caveats and select severity 3 caveats and is located on Cisco.com.

Note If you have an account on Cisco.com, you can also use the Bug Toolkit to find select caveats of any severity. To reach the Bug Toolkit, l**og in** to Cisco.com and click **Products and Services > Cisco IOS Software > Cisco IOS Software Releases 12.2 > Troubleshooting > Bug Toolkit**. Another option is to go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl. (If the defect that you have requested cannot be displayed, this may be due to one or more of the following reasons: the defect number does not exist, the defect does not have a customer-visible description yet, or the defect has been marked Cisco Confidential.)

The *Dictionary of Internetworking Terms and Acronyms* contains definitions of acronyms that are not defined in this document:

http://www.cisco.com/univercd/cc/td/doc/cisintwk/ita/index.htm

Table 4 Caveats Reference for 12.4SW

DDTS Number	Software Release Caveat Corrected	Caveat Open
CSCec12299	12.4(11)SW1	
CSCek63758	12.4(15)SW	No
CSCsd34549	No	12.4(15)SW
CSCsd73254	No	12.4(15)SW
CSCsd85587	12.4(11)SW1	No
CSCse11887	12.4(15)SW	No
CSCsf10777	12.4(15)SW	No
CSCsg11686	12.4(11)SW2	No
CSCsg27676	12.4(11)SW2/12.4(15)SW	No
CSCsg58153	12.4(15)SW/12.4(15)SW1	No
CSCsh33248	12.4(15)SW	No
CSCsh35975	No	12.4(15)SW
CSCsh595601	12.4(11)SW2	No
CSCsh69956	12.4(11)SW2/12.4(15)SW	No
CSCsi34398	12.4(15)SW	No
CSCsi40918	12.4(15)SW	No
CSCsi60319	12.4(11)SW2/12.4(15)SW	No
CSCsi64297	12.4(15)SW	No
CSCsi68841	12.4(11)SW3	No
CSCsi68966	12.4(15)SW	No
CSCsi79035	12.4(15)SW	No
CSCsi98081	12.4(15)SW	No
CSCsj36934	12.4(15)SW	No
CSCsj44081	12.4(11)SW3	No

Table 4 Caveats Reference for 12.4SW (Continued)

DDTS Number	Software Release Caveat Corrected	Caveat Open
CSCsj53415	12.4(11)SW3	No
CSCsj60899	12.4(15)SW	No
CSCsj99422	12.4(15)SW	No
CSCsk15118	12.4(15)SW	No
CSCsk25247	12.4(15)SW	No
CSCsk50308	12.4(15)SW	No
CSCsk56500	12.4(15)SW	No
CSCsk60020	12.4(15)SW1	No
CSCsk79377	12.4(15)SW1	No
CSCsl08358	12.4(15)SW1	No
CSCsl59128	12.4(15)SW1	No
CSCsl93462	12.4(15)SW1	No
CSCsm76092	12.4(15)SW1	No
CSCso00287	No	Yes
CSCso01412	No	Yes
CSCso12698	12.4(15)SW1	No

Open Caveats—Cisco IOS Release 12.4(15)SW1

This section documents possible unexpected behavior by Cisco IOS Release 12.4(15)SW1 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCsk60020

  The Secure Shell server (SSH) implementation in Cisco IOS contains multiple vulnerabilities that allow unauthenticated users the ability to generate a spurious memory access error or, in certain cases, reload the device.

  The IOS SSH server is an optional service that is disabled by default, but its use is highly recommended as a security best practice for management of Cisco IOS devices. SSH can be configured as part of the AutoSecure feature in the initial configuration of IOS devices, AutoSecure run after initial configuration, or manually. Devices that are not configured to accept SSH connections are not affected by these vulnerabilities.

  Common Vulnerabilities and Exposures (CVE) identifier CVE-2008-1159 has been assigned to this bug.

  The Security Advisory for this issue is posted at

  http://www.cisco.com/warp/public/707/cisco-sa-20080521-ssh.shtml.

- CSCso00287

  The SUP processor on a distributed Cisco ITP platform or the Route Processor (RP) on a single processor Cisco ITP platform exceeds the normal CPU operating range even with light traffic.

  This problem occurs when the Enhanced Gateway Screening (GWS) console logging is turned on for all received/sent packets.

Workaround: Turn off GWS console logging. File logging may be used as an alternative.

- CSCso01412

  An ATM IMA port link may not activate after a reload.

```
Router#show cs7 linkset msc-server
lsn=msc-server apc=16258 state=avail avail/links=1/2
SLC Interface Service PeerState Inhib
00 ATM13/1/7 avail --------- -----
*01 ATM13/1/2 FAILED ---------
```

  This problem occurs when an ATM link does not activate after reload.

  Workaround: Execute the **shut** and **no shut** commands, or unplug and plug in the cable. The link should comes up.

Resolved Caveats—Cisco IOS Release 12.4(15)SW1

All the caveats listed in this section are resolved in Cisco IOS Release 12.4(15)SW1. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCsg58153

  The port adapter (PA) has crashed and is unresponsive

  This problem occurs because bad circuits on uplink links cause all the SS7 links to go down and flap continuously.

  Workaround: Bring the PA up after it has crashed.

- CSCsk79377

  The **remove** option specified in a global title translation (GTT) address conversion table is not applied when performing GTT address conversion.

  This problem only occurs when the GTT address conversion table is used for Signaling Connection Control Part (SCCP) conversion across instances when cs7 multi-instance is configured.

  There are no known workarounds.

- CSCsl08358

  SCCP User Adaptation (SUA) Application Server Processes (ASPs) may reject SCCP segmented messages from an ITP SUA Signaling Gateway (SG).

  This problem occurs because the segmentation parameter in SUA CLDT messages is populated incorrectly when the sequence delivery option is set to '1'b (Class 1) in the received SCCP XUDT segmentation parameter. In this case, bit 7 within the first/remain field of the SUA segmentation parameter is also set, which may cause the ASP to interpret the number of remaining segments to be greater than 15.

  There are no known workarounds.

- CSCsl59128

  Cisco ITP does not reject m3ua/sua messages without a Routing Context parameter when the ASP is active in multiple AS's.

  This problem occurs when the sending ASP is active in multiple AS's.

  There are no known workarounds.

- CSCsl93462

  No linkUp and linkDown Simple Network Management Protocol (SNMP) traps are generated when the remote end is down for the controller. No linkUp trap generated when the controller is brought up by **no shutdown** command.

  This problem is specific to the PA-MCX-8TE1-M and PA-MCX-4TE1-Q port adapters.

  There are no known workarounds.

- CSCsm76092

  If the default conversion is removed with the real and alias instance swapped in the **cs7 instance** command, then reentered, the FlexWan is not updated, and the PC is not converted.

  For example:

```
Router(config)#cs7 instance 1 pc-conversion default 0
Router(config)#no cs7 instance 0 pc-conversion default 1
Router(config)#cs7 instance 0 pc-conversion default 1
%Error: Default conversion already defined for instance 0

Roouter(config)#cs7 instance 1 pc-conversion default 0
%Error: Alias PC 0.0.0:0 already in use
```

  This problem occurs when ITP has multiple instances configured and default instance conversion configured.

  Workaround: Enter the default conversion with the **no-route** option:

```
Router(config)#cs7 instance 0 pc-conversion default 1 no-route
```

- CSCso12698

  When a set of links are quickly shut and then removed, as with a cut and paste of a prepared script into the console terminal, the ITP software can crash. The crash traceback is not predictable or fixed.

  A cut and paste of a script similar to the one below can result in a crash:

```
Router(config)#cs7 linkset linksetname
Router(config-cs7-ls)#link 1
Router(config-cs7-ls-link)#shut
Router(config-cs7-ls-link)#no link 1
Router(config-cs7-ls-link)#link 2
Router(config-cs7-ls-link)#shut
Router(config-cs7-ls-link)#no link 2
...
Router(config-cs7-ls-link)#end
```

  Workaround: Do not remove links using a cut and paste of a script. Wait 4 to 5 seconds after shutting a link before issuing the **no link** command.

Open Caveats—Cisco IOS Release 12.4(15)SW

This section documents possible unexpected behavior by Cisco IOS Release 12.4(15)SW and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCsd34549

  An unexpected config_state value is seen during reload or switchover.

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

  There are no known workarounds

- CSCsd73254

  If a specific software error on the active Route Processor (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.

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

  There are no known workarounds.

- CSCsh35975

  A Bad VCD message occurs when the following actions are performed:

  - Shut the main interface and its subinterfaces that are used in links
  - No shut the main interface, but keep the subinterfaces shut

  Traffic on the other links and subinterfaces does not seem to be affected.

  There are no known workarounds.

Resolved Caveats—Cisco IOS Release 12.4(15)SW

All the caveats listed in this section are resolved in Cisco IOS Release 12.4(15)SW. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCek63758

  Message signal unit (MSU) rates spike after clearing counters.

  This problem occurs on all ITP platforms

  There are no known workarounds.

- CSCse11887

  An IPCALLOCFAIL error occurs during online insertion and removal (OIR) of a FlexWAN. module.

  This issue occurs intermittently during FlexWAN OIR.

  There are no known workarounds.

- CSCsf10777

  An ATMPA-3-CMDFAIL can occur when you extract the FlexWAN module from the chassis.

  This issue only occurs when the FlexWAN module contains an E1 IMA PA and the FlexWAN module is extracted from the chassis. Once the FlexWAN module is reinserted, no additional symptoms occur.

  There are no known workarounds if the FlexWAN module is extracted.

- CSCsg27676

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

  This problem occurs on all ITP platforms.

  There are no known workarounds.

- CSCsg58153

  The PA crashes and is unresponsive.

  This issue occurs because bad circuits on uplink links cause all the SS7 links to go down and flap continuously.

  Workaround: Bring the PA up after it has crashed.

- CSCsh33248

  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
```

  This issue occurs in a multi-PVC configuration after a switchover, and may be caused by configuration of a non-existent subinterface.

  Workaround: Do not unconfigure a non-existent subinterface.

- CSCsh69956

  Syslog messages and Simple Network Management Protocol (SNMP) traps are not generated for clock transitions on the PA-A3-8T1IMA

  This problem occurs on all ITP platforms

  There are no known workarounds.

- CSCsi34398

  When unconfiguring and reconfiguring OC3 ATM interfaces and associated linksets with the multi-PVC feature, including a subinterface and IP protocol, the system may reload unexpectedly.

  Some conditions that can cause this problem include configuring and unconfiguring subinterfaces, the IP protocol, and ATM NNI.

  Workaround: Avoid configuring and unconfiguring the OC3 ATM interface multiple times. Once the system is configured, it remains stable.

- CSCsi40918

  The Route Switch Processor (RSP) crashes causing a switchover to the standby RSP.

  This crash occurs during normal router operations.

  There are no known workarounds.

- CSCsi60319

  The Multimedia Message Service Center (MMSC) gateway feature of the ITP is not returning the responding Home Location Register (HLR) E.164 address to the Short Message Peer-to-Peer (SMPP) client when the HLR responds with an ERROR or REJECT component.

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

  There are no known workarounds.

- CSCsi64297

  A Versatile Interface Processor (VIP) crashes while processing global title translation (GTT) traffic.

  This issue occurs when Message Transfer Part Level 3 (MTP3) offload is enabled with a VIP performing GTT on both UDT and XUDT SCCP messages.

  There are no known workarounds.

- CSCsi68966

  The Signaling Connection Control Part (SCCP) fails to route messages to XUA PCs even though they are available.

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

  Workaround: The global title address (GTA) entered in the configuration should point to application server (AS) name directly instead of a PC.

- CSCsi79035

  The MTP3 User Adaptation Layer (M3UA) Application Server Process (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 show two.

  This issue occurs when M3UA ASPs have local-ip addresses from different FlexWANs, and only one IP address is used by the Stream Control Transmission Protocol (SCTP) instance.

  Workaround: Perform a **shutdown** and **no shutdown** of the affected M3UA instance to clear the problem. The output of the **show ip sctp instanc**e command should now show two local-ip addresses.

- CSCsi98081

  A buffer leak occurs because of a large quantity of Simple Network Management Protocol (SNMP) traps.

  This problem occurs on all ITP platforms.

  There are no known workarounds.

- CSCsj36934

  The router crashes with the following bus error: `System returned to ROM by bus error at PC 0x4107D360 TLB (load or instruction fetch) exception, CPU signal 10, PC = 0x4107D36`0

  This issue occurs during normal operations.

  There are no known workarounds.

- CSCsj60899

  FlexWAN crashes while processing outbound MTP3 User Adaptation Layer (M3UA) Signaling Connection Control Part (SCCP) message signal unit (MSU) Extended Unitdata (XUDT).

  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.

  There are no known workarounds.

- CSCsj99422

  A new Application Server Process (ASP) binding during a Non-Stop Operation (NSO) bulk sync causes a SYNCERR.

  This issue occurs during an NSO switchover on an ITP running MTP3 User Adaptation Layer (M3UA)/SCCP User Adaptation (SUA) traffic.

  There are no known workarounds.

- CSCsk15118

  ITP crashes while performing Signaling Connection Control Part (SCCP) instance address conversion.

  This issue occurs when the following three conditions occur:

  – SCCP instance conversion where address conversion is used between instances

  – A message signal unit (MSU) with more than 16 digits is in the received called party address

  – 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 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 MTP2-User Peer-to-Peer Adaptation Layer (M2PA) link stops processing received messages and eventually fails after receiving a Stream Control Transmission Protocol (SCTP) DATA chunk that is 300 bytes or more.

  This issue occurs because the DATA chunk is larger than the maximum message signal unit (MSU) size allowed on the link and is discarded as an invalid message before the Forward Sequence Number (FSN) in the M2PA header is updated for the link. As a result, all subsequent messages received over the link will be dropped due to an invalid FSN. The link will eventually fail if a Signaling Link Test Message (SLTM)/Signaling Link Test Acknowledgement (SLTA) is dropped, or when the remote peer can no longer buffer forwarded messages.

  Either the **show cs7 m2pa statistics** or the **show cs7 m2pa state** command may be used to identify that this problem is occurring. The **show cs7 m2pa statistics** command will show an elevated number of Unexpected FSN_rcvd errors; the **show cs7 m2pa state** command will show that the 'bsnr' field is not incrementing despite data chunks being received over the association.

  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 action, however, will not prevent the problem from re-occurring.

- CSCsk50308

  When configuring a Message Transfer Part Level 3 (MTP3) route to an MTP3 User Adaptation Layer (M3UA)/SCCP User Adaptation (SUA) point code, the initial route status is "available" even though the M3UA/SUA point code is locally inactive.

  This issue occurs only upon initial route configuration.

  Workaround: Perform one of the following actions:

  - Bring the M3UA/SUA point code active to match the route availability.
  - Execute an MTP3 restart.

- CSCsk56500

  The removal of a card leaves the controller configuration intact.

  This issue occurs on ITPs only when the **no card type** *t1* or *e1* command is issued. The controller configuration remains in the show running-configuration output.

  Workaround: Do not issue a **no card type** command. A reload is required to change the card type on all ITP systems.

Open Caveats—Cisco IOS Release 12.4(11)SW3

This section documents possible unexpected behavior by Cisco IOS Release 12.4(11)SW3 and describes only severity 1 and 2 caveats and select severity 3 caveats.

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.

- CSCsi68841

  After configuring a cs7 group, ITP crashes during normal traffic processing.

  There are no known workarounds.

- CSCsj44081

  Improper use of data structures occurs 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.

  There are no known workarounds.

- CSCsj53415

  When traffic goes through global title translation (GTT), which results in the traffic going to an xUA application server (AS), but the traffic is blocked by outbound Gateway Screening (GWS), the buffer is lost. Eventually all buffers are exhausted, and the links fail and do not recover. The **show buffers** command displays an extremely large number of cs7 buffers and an extremely large number of misses in the global pool. The cs7 buffers keep increasing until the links fail.

  Workaround: To prevent the problem, remove the outbound GWS rule. If the links fail, you must reload the individual line card that contains the inbound links, or reload the entire router.

Open Caveats—Cisco IOS Release 12.4(11)SW2

This section documents possible unexpected behavior by Cisco IOS Release 12.4(11)SW2 and describes only severity 1 and 2 caveats and select severity 3 caveats.

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.

  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.

  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.

  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.

  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.

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

  There are no known workarounds.

Open Caveats—Cisco IOS Release 12.4(11)SW1

This section documents possible unexpected behavior by Cisco IOS Release 12.4(11)SW1 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- 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.

  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)SW1

All the caveats listed in this section are resolved in Cisco IOS Release 12.4(11)SW1. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCec12299

  Devices running Cisco IOS versions 12.0S, 12.2, 12.3 or 12.4 and configured for Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs) or VPN Routing and Forwarding Lite (VRF Lite) and using Border Gateway Protocol (BGP) between Customer Edge (CE) and Provider Edge (PE) devices may permit information to propagate between VPNs.

  Workarounds are available to help mitigate this vulnerability.

  This issue is triggered by a logic error when processing extended communities on the PE device.

  This issue cannot be deterministically exploited by an attacker.

  Cisco has released free software updates that address these vulnerabilities. Workarounds that mitigate these vulnerabilities are available.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20080924-vpn.shtml.

- 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

This section documents possible unexpected behavior by Cisco IOS Release 12.4(11)SW and describes only severity 1 and 2 caveats and select severity 3 caveats.

- 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.

  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

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

There are no known resolved caveats for Cisco IOS Release 12.4(11)SW.

Related Documentation

The following sections describe the documentation available for the Cisco 7200 and Cisco 7301 series routers. These documents consist of hardware and software installation guides, Cisco IOS configuration guides 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 and http://www.cisco.com/univercd/home/index.htm.

Use these release notes with these documents:

- Release-Specific Documents, page 26
- Platform-Specific Documents, page 26
- Cisco IOS Release 12.4T Documentation Set, page 27

Release-Specific Documents

The following documents are specific to Cisco IOS Release 12.4 T and are located on Cisco.com and http://www.cisco.com/univercd/home/index.htm:

- *Cross-Platform Release Notes for Cisco IOS Release 12.4 T*

  On Cisco.com at:

  Products and Services > Cisco IOS Software > Cisco IOS Software Releases 12.4T > General Information> Release Notes

  On http://www.cisco.com/univercd/home/index.htm at:

  Cisco IOS Software > Cisco IOS Release 12.4T > Release Notes

- Product bulletins, field notices, and other release-specific documents at http://www.cisco.com/univercd/home/index.htm

- *Caveats for Cisco IOS Release 12.4 T*

  As a supplement to the caveats listed in "Caveats for Cisco IOS Release 12.4 SW" in these release notes, see *Caveats for Cisco IOS Release 12.4 T*, which contains caveats applicable to all platforms for all maintenance releases of Cisco IOS Release 12.4 T.

  On Cisco.com at:

  Products and Services > Cisco IOS Software > Cisco IOS Software Releases 12.4T > General Information > Release Notes > Cross-Platform Release Notes for Cisco IOS Release 12.4T, Part 5: Caveats

  On http://www.cisco.com/univercd/home/index.htm at:

  Cisco IOS Software > Cisco IOS Release 12.4T > Release Notes > Cross-Platform Release Notes for Cisco IOS Release 12.4T, Part 5: Caveats

Note If you have an account on Cisco.com, you can also use the Bug Toolkit to find select caveats of any severity. To reach the Bug Toolkit, l**og in** to Cisco.com and click **Products and Services > Cisco IOS Software > Cisco IOS Software Releases 12.2 Mainline> Troubleshoot and Alerts > Bug Toolkit**. Another option is to go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl. (If the defect that you have requested cannot be displayed, this may be due to one or more of the following reasons: the defect number does not exist, the defect does not have a customer-visible description yet, or the defect has been marked Cisco Confidential.)

Platform-Specific Documents

These documents are available for the Cisco 7200 and Cisco 7301 series routers on Cisco.com:

- *Cisco 7200 VXR Installation and Configuration Guide*
- *Cisco 7200 Routers Quick Start Guide*
- *Cisco 7301 Installation and Configuration Guide*
- *Cisco 7301 Router Quick Start Guide*

On Cisco.com at:

Products and Services >Routers

On http://www.cisco.com/univercd/home/index.htm at:

Cisco Product Documentation: Routers

Cisco IOS Release 12.4T Documentation Set

Table 5 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(15)SW is based on Cisco IOS Release **12.4(15)T.** All features in Cisco IOS Release **12.4(15)T** are in Cisco IOS Release 12.4(15)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(15)SW.

Table 5 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 *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 *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 *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 *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 5 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 *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 *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 *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 *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 *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 *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 *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 5 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 *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 *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 *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 *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 *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 *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 5 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 *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 *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 *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 *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 *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 *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 5 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 *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 *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 *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 *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 *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 5 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 *Cisco IOS Bridging Command Reference*, Release 12.4T *Cisco IOS IBM Networking Command Reference*, Release 12.4T	The configuration guide is a task-oriented guide to configuring: • 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). • 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. 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 *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 *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 *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 *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 *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 6 lists the documents and resources that support the Cisco IOS Release 12.4T software configuration guides and command references.

Table 6 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: 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: http://www.cisco.com/go/mibs

Open Source License Notices

The following notices pertain to this software license.

OpenSSL/Open SSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License:

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”.
4. The names “OpenSSL Toolkit” and “OpenSSL Project” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called “OpenSSL” nor may “OpenSSL” appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

   “This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)”.

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT “AS IS”' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License:

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)".

   The word 'cryptographic' can be left out if the routines from the library being used are not cryptography-related.
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)".

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License]

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

Product Documentation DVD

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from Cisco Marketplace at this URL:

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

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.

Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

http://www.cisco.com/techsupport

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

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

Note Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

http://www.cisco.com/techsupport/servicerequest

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)
EMEA: +32 2 704 55 55
USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

http://www.cisco.com/techsupport/contacts

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

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

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

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

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

  http://www.ciscopress.com

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

  http://www.cisco.com/packet

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

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

  or view the digital edition at this URL:

  http://ciscoiq.texterity.com/ciscoiq/sample/

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/ipj

- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:

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

- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:

  http://www.cisco.com/discuss/networking

- World-class networking training is available from Cisco. You can view current offerings at this URL:

  http://www.cisco.com/en/US/learning/index.html

This document is to be used in conjunction with the documents listed in the "Related Documentation" section on page 25.