Release Notes for Cisco IOS Release 12.4(6)XT

September 24, 2008

Cisco IOS Release 12.4(6)XT2

Text Part Number OL-12451-03

Note See the "Important Notes" section on page 6 for important information for Cisco IOS Release 12.4(6)XT.

These release notes support Cisco IOS Release 12.4(6)XT. They are updated to describe new memory requirements, hardware support, software platform deferrals, and related documents.

We recommend 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/kobayashi/support/tac/fn_index.html. If you do not have a Cisco.com login account, you can find field notices at http://www.cisco.com/public/support/tac/fn_index.html.

Contents

These release notes contain the following sections:

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

Introduction

Cisco IOS Release 12.4(6)XT is the first general availability release of this software. Many of the features and the hardware supported in this software have been previously released to customers on other software releases.

For information on new features and Cisco IOS commands that are supported by Cisco IOS Release 12.4(6)XT, see the "New and Changed Information" section on page 5 and the "Caveats" section on page 7.

System Requirements

This section describes the system requirements for Cisco IOS Release 12.0(32)SY and includes the following sections:

Memory Recommendations

The memory recommendation tables have been removed from the Cisco IOS Release 12.4T release notes to improve the usability of the release notes documentation. The memory recommendations that were provided by these tables are available through Cisco Feature Navigator.

Cisco Feature Navigator is a web-based tool that enables you to determine which Cisco IOS 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:

www.cisco.com/go/fn

For frequently asked questions about Cisco Feature Navigator, see the FAQs at the following URL:

http://tools.cisco.com/ITDIT/CFN/jsp/help.jsp

Determining Memory Recommendations for Software Images (Feature Sets)

To determine memory recommendations for software images (feature sets) in Cisco IOS Release 12.4T, go to the Cisco Feature Navigator home page and perform the following steps.

Step 1 From the Cisco Feature Navigator home page, click **Search by Software/Image Name/Product Code/Platform**.

Step 2 To find the memory recommendations for the latest Cisco IOS release, click the release under the Cisco IOS Quick Pick Latest Release area. For other releases, go to Step 3.

a. Choose **All Platforms** (or a specific platform) from the Platform drop-down list.

b. Choose **All Feature Sets** from the Feature Set drop-down list.

The Search Results table will list all the software images (feature sets) that support the release that you chose, plus the DRAM and flash memory recommendations for each image.

Step 3 If the release is not listed in the Cisco IOS Quick Pick Latest Release area, choose **IOS** from the Software drop-down list, and click **Continue**.

a. Choose a release from the Major Release drop-down list, and click **Continue** again.

b. Choose a specific release from the Release drop-down list.

c. Choose **All Platforms** (or a specific platform) from the Platform drop-down list

d. Choose **All Feature Sets** from the Feature Set drop-down list.

The Search Results table will list all the software images (feature sets) that support the release that you chose, plus the DRAM and flash memory recommendations for each image.

Hardware Supported

Cisco IOS Release 12.4(6)XT supports the following Cisco hardware platforms:

- SOHO 90 series routers[1]
- Cisco VG224 analog gateways
- Cisco 800 series routers[2]
- Cisco 1700 series routers
- Cisco 1800 series routers (fixed configuration and modular)
- Cisco IAD2430 series
- Cisco 2600XM series and Cisco 2691 modular access routers
- Cisco 2800 series routers
- Cisco 3200 series mobile access routers
- Cisco 3600 series routers
- Cisco 3700 series routers
- Cisco 3800 series routers
- Cisco AS5350 and Cisco AS5350XM universal gateways
- Cisco AS5400, Cisco AS5400HPX, and Cisco AS5400XM universal gateways
- Cisco AS5850, AS5850-ERSC universal gateways
- Cisco Catalyst 6000/Cisco 7600 MWAM
- Cisco Catalyst 6500/Cisco 7600 communication media module
- Cisco 7000 series routers[3]
- Cisco IGX 8400 series URM[4]
- Cisco 8450 RPM-XF[5]
- Cisco signaling link terminals

1. The Cisco SOHO 91 and Cisco SOHO 96 series routers are not supported in Cisco IOS Release 12.4(6)T and later releases.
2. The Cisco 815 router is supported in Cisco IOS Release 12.4(11)T.
3. The Cisco 7200-NPE-G2 is supported in Cisco IOS Release 12.4(11)T.
4. The Cisco IGX 8400 series URM is not supported in Cisco IOS Release 12.4(4)T and later releases.
5. The Cisco 8450 RPM-XF images are not supported in Cisco IOS Release 12.4(11)T.

For detailed descriptions of the new hardware features, see the "New and Changed Information" section on page 5.

Determining Your Software Version

To determine the version of Cisco IOS software that is running on your Cisco network device, log in to the device and enter the **show version** EXEC command:

```
Router> show version

Cisco IOS Software, 5350 Software (C5350-IS-M), Version 12.4(6)XT, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
```

Upgrading to a New 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 documents:

- Cisco 1700 Series Routers

  http://www.cisco.com/en/US/partner/products/hw/routers/ps259/products_tech_note09186a00801fc986.shtml

- Cisco 1800 Series Routers (fixed configuration and modular)

  http://www.cisco.com/en/US/partner/products/ps5853/tsd_products_support_series_home.html

- Cisco IAD2430 Integrated Access Device

  http://www.cisco.com/en/US/products/hw/gatecont/ps887/products_configuration_guide_chapter09186a0080192882.html

- Cisco 2600 Series Multiservice Platforms

  http://www.cisco.com/en/US/partner/products/hw/routers/ps259/products_tech_note09186a00801fc986.shtml

- Cisco 3200 Series Mobile Access Routers

  http://www.cisco.com/en/US/partner/products/hw/routers/ps272/tsd_products_support_series_home.html

- Cisco 3600 Series Multiservice Platforms

  http://www.cisco.com/en/US/partner/products/hw/routers/ps259/products_tech_note09186a00801fc986.shtml

- Cisco 3700 Series Multiservice Access Routers

  http://www.cisco.com/en/US/partner/products/hw/routers/ps259/products_tech_note09186a00801fc986.shtml

- Cisco 3800 Series Integrated Services Routers

  http://www.cisco.com/en/US/partner/products/ps5855/tsd_products_support_series_home.html

- Cisco AS5350 Series Universal Gateways

  http://www.cisco.com/en/US/products/sw/accesssw/ps502/tsd_products_support_series_home.html

- Cisco AS5400 Series Universal Gateways

  http://www.cisco.com/en/US/products/hw/univgate/ps505/products_tech_note09186a00800949f4.shtml

- Cisco AS5850 Series Universal Gateways

  http://www.cisco.com/en/US/products/sw/accesssw/ps511/tsd_products_support_series_home.html

- Cisco Catalyst 6500/Cisco 7600 Communication Media Module

  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/relnotes/ol_6314.htm#wp181078

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

  http://www.cisco.com/en/US/products/hw/routers/ps341/tsd_products_support_install_and_upgrade.html

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 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/cfn

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.

New and Changed Information

This section lists the new hardware and software features that are supported in Cisco IOS Release 12.4T and contains the following sections:

Note A cumulative list of all new and existing features supported in this release, including platform and software image support, can be found in Cisco Feature Navigator at http://www.cisco.com/go/cfn.

New Hardware Features in Release 12.4(6)XT2

There are no new hardware features in Cisco IOS Release 12.4(6)XT2.

New Software Features in Release 12.4(6)XT2

There are no new software features in Cisco IOS Release 12.4(6)XT2.

New Hardware Features in Release 12.4(6)XT1

There are no new hardware features in Cisco IOS Release 12.4(6)XT1.

New Software Features in Release 12.4(6)XT1

There are no new software features in Cisco IOS Release 12.4(6)XT1.

New Hardware Features in Release 12.4(6)XT

There are no new hardware features in Cisco IOS Release 12.4(6)XT.

New Software Features in Release 12.4(6)XT

There are no new software features in Cisco IOS Release 12.4(6)XT.

Important Notes

The following sections contain important notes about Cisco IOS Release 12.4(6)XT.

Deferrals

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

Field Notices and Bulletins

For general information about the types of documents listed in this section, see the following document:

http://www.cisco.com/warp/customer/cc/general/bulletin/software/general/1654_pp.htm

- Field Notices—We recommend that you view the field notices for this release to see if your software or hardware platforms are affected. If you have an account with Cisco.com, you can find Field Notices at a http://www.cisco.com/kobayashi/support/tac/fn_index.html. If you do not have a Cisco.com login account, you can find field notices at http://www.cisco.com/public/support/tac/fn_index.html.
- Product Bulletins—If you have an account with Cisco.com, you can find product bulletins at http://www.cisco.com/warp/customer/cc/general/bulletin/index.shtml. If you do not have a Cisco.com login account, you can find product bulletins at http://www.cisco.com/warp/public/cc/general/bulletin/iosw/index.shtml.

- *What's Hot in Software Center—What's Hot in Software Center* provides information about caveats that are related to deferred software images. If you have an account on Cisco.com, you can access *What's Hot for IOS Releases* at http://www.cisco.com/kobayashi/sw-center or by logging in and choosing **Technical Support > Software Center > Cisco IOS Software > What's Hot in Software Center**.
- *What's New for IOS—What's New for IOS* lists recently posted Cisco IOS software releases and software releases that have been removed from Cisco.com. If you have an account on Cisco.com, you can access *What's New for IOS* at http://www.cisco.com/kobayashi/sw-center/sw-ios.shtml or by logging into Cisco.com and choosing **Technical Support > Software Center > Products and Downloads > Cisco IOS Software**.

Important Notes for Cisco IOS Release 12.4(6)XT

The following information applies to all releases of Cisco IOS Release 12.4(6)XT.

Cisco Unified Customer Voice Portal

Cisco IOS Release 12.4(6)XT is optimized for the Cisco Unified Customer Voice Portal (CVP) 4.0. CVP 4.0 introduces many key IVR features including a SIP interface to the Cisco IOS VoiceXML Browser.

Caveats

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.

For information on caveats in Cisco IOS Release 12.4T, refer to the *Caveats for Cisco IOS Release 12.4T* document, which lists severity 1 and 2 caveats and select severity 3 caveats for Cisco IOS Release 12.4T and is located on Cisco.com.

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

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, log in to Cisco.com and click **Products and Services > Cisco IOS Software > Cisco IOS Software Releases 12.4T > 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.)

Open Caveats—Cisco IOS Release 12.4(6)XT2

There are no open caveats in this release.

Resolved Caveats—Cisco IOS Release 12.4(6)XT2

CSCsd95616

Two crafted Protocol Independent Multicast (PIM) packet vulnerabilities exist in Cisco IOS software that may lead to a denial of service (DoS) condition. 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-multicast.shtml.

CSCsj81502 show pagp clis are not displaying the correct information

Symptom In release 12.2(33)SXH or 12.2(18)SXF10 releases, the output of 'show pagp neighbor' command may truncate the neighbor device name and port name fields by 1 character. This is just a display issue and has no functional impact on the PAGP protocol.

Conditions This issue is only seen with 12.2(33)SXH and 12.2(18)SXF10 images and affects only PAGP etherchannel member ports.

Workaround There is no workaround. If a user wants to find out the partner's correct information, he/she could use the output of "show cdp neighbor" command.

CSCsj66692 Data integrity traceback seen in voip/ccapi/ccapi_call.c

Symptom Data corruption copy error tracebacks are seen on the console or output from the show logging command:

```
%DATACORRUPTION-1-DATAINCONSISTENCY: copy error,  -PC= 0x41224EFC,  -
Traceback= 0x4153A7D0 0x4155BA0C 0x4157FAF0 0x41224EFC 0x41DDC0A8 0x41DDC198
0x41DC6D84 0x41DF3B0C 0x41DC506C 0x41DCE5A4 0x41D91AF8 0x41D90F88 0x41D9BEFC
0x41D9C0C0 0x41DAEA68
```

Conditions With the new enhancement in place, IOS will emit a %DATACORRUPTION-1-DATAINCONSISTENCY error message whenever it detects an inconsistency in its internal data structures.

Workaround There is no workaround.

CSCsj97602 Memory leak on mem_pool:: in Dead pool

Symptom A Cisco access server may run out of free processor memory. This symptom can be seen in the <CmdBld>show process memory<NoCmdBld> command. Increased memory utilization will be seen in the dead pool.

Conditions This symptom has been observed only in access servers that participate in Cisco Customer Voice Portal (CVP). When a VXML application is configured with fetchaudio, the fetchaudio playout fails after the user disconnects. The fetchaudio should have been removed from the prompt list, but it was not. This causes the session not to be freed when the application is finished.

Workaround A reload will temporarily free the leaked memory.

CSCsj86725 Running lpd with certain configurations could cause overflow

This DDTS addresses the issue in the Cisco Product Security Incident Response Team (PSIRT) response to an issue discovered and reported to Cisco regarding a stack overflow in the Cisco IOS Line Printer Daemon (LPD) Protocol feature. This security response is posted at:

http://www.cisco.com/warp/public/707/cisco-sr-20071010-lpd.shtml

CSCsg39295 Syslog Displays Password if SCP or FTP Selected in CISCO-COPY-CONFIG-MIB

Symptom Password information may be displayed in a Syslog message as follows:

```
%SYS-5-CONFIG_I: Configured from scp://userid:password@10.1.1.1/config.txt by
 console
```

Conditions When using SNMP to modify a configuration by means of the CISCO-CONFIG-COPY-MIB, selection of ConfigCopyProtocol of SCP or FTP may result in the password being exposed in a syslog message.

Workaround When using SNMP to modify a configuration by means of the CISCO-CONFIG-COPY-MIB, use the ConfigCopyProtocol of RCP to avoid exposure of the password.

CSCsh74975 udp packets to port 2517 cause memory depletion or reload on router

Symptom A router may reload or a leak memory may occur when UDP malformed packets are sent to port 2517.

Conditions This symptom is observed on a Cisco router that functions as a VoIP dial peer and that is configured for H.323.

Workaround There is no workaround.

CSCsh04686 Malformed TCP packet forces reload with x25 routing (XOT)

Symptom With X25 over TCP (XOT) enabled on a router or catalyst switch, malformed traffic sent to TCP port 1998 will cause the device to reload. This was first observed in IOS 12.2(31)SB2.

Conditions Must have "x25 routing" enabled on the device.

Workaround Use IPSEC or other tunneling mechanisms to protect XOT traffic. Also, apply ACLs on affected devices so that traffic is only accepted from trusted tunnel endpoints.

CSCsk97130 VXML tree not release when subdialog root document is shared

Symptom For a VXML application, if the calling document and called document of a subdialog shares the same root document, the tree structure used for the root document will not be released after the call session is finished. This causes memory leakage.

CSCsi67763 IPS evasion using Unicode encoding for HTTP-based attacks

The U.S. Computer Emergency Response Team (US-CERT) has reported a network evasion technique using full-width and half-width unicode characters that affects several Cisco products. The US-CERT advisory is available at the following link:

http://www.kb.cert.org/vuls/id/739224

By encoding attacks using a full-width or half-width unicode character set, an attacker can exploit this vulnerability to evade detection by an Intrusion Prevention System (IPS) or firewall. This may allow the attacker to covertly scan and attack systems normally protected by an IPS or firewall. Cisco response is posted at the following link: http://www.cisco.com/warp/public/707/cisco-sr-20070514-unicode.shtml

CSCse56800 SIP-3-BADPAIR register timer expiry causes slow memory leak

Symptom If a Cisco IOS SIP gateway receives an out-of-dialog OPTIONS request over UDP, then the gateway will respond to it with 200 OK, but the call control block used to process that request is not freed, which results in a memory leak.

Conditions This symptom has been observed with a Cisco IOS SIP gateway running Cisco IOS Release 12.4(9)T or later. This message below is what causes this behavior.

```
007042: Jun 17 15:18:45.024 EDT: %SIP-3-BADPAIR: Unexpected timer 23
(SIP_TIMER_REMOVE_TRANSACTION) in state 27 (SIP_STATE_OPTIONS_WAIT) substate 0
(SUBSTATE_NONE)
```

Workaround There is no workaround.

Open Caveats—Cisco IOS Release 12.4(6)XT1

There are no open caveats in this release.

Resolved Caveats—Cisco IOS Release 12.4(6)XT1

This section describes possible unexpected behavior by Cisco IOS Release 12.4(6)XT1. All the caveats listed in this section are resolved in Cisco IOS Release 12.4(6)XT1. This section describes 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.

CSCse56800

- CSCse56800

Multiple vulnerabilities exist in the Session Initiation Protocol (SIP) implementation in Cisco IOS that can be exploited remotely to trigger a memory leak or to cause a reload of the Cisco IOS device.

Cisco has released free software updates that address these vulnerabilities. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities addressed in this advisory.

There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself, if administrators do not require the Cisco IOS device to provide voice over IP services.

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

CSCsd81407

Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

- Session Initiation Protocol (SIP)
- Media Gateway Control Protocol (MGCP)
- Signaling protocols H.323, H.254
- Real-time Transport Protocol (RTP)
- Facsimile reception

Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself.

This advisory is posted at
http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml

CSCse40276

Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

- Session Initiation Protocol (SIP)
- Media Gateway Control Protocol (MGCP)
- Signaling protocols H.323, H.254
- Real-time Transport Protocol (RTP)
- Facsimile reception

Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself.

This advisory is posted at
http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml

- CSCse56501

A device running Cisco IOS software that has Internet Protocol version 6 (IPv6) enabled may be subject to a denial of service (DoS) attack. For the device to be affected by this vulnerability the device also has to have certain Internet Protocol version 4 (IPv4) User Datagram Protocol (UDP) services enabled. To exploit this vulnerability an offending IPv6 packet must be targeted to the device. Packets that are routed throughout the router can not trigger this vulnerability. Successful exploitation will prevent the interface from receiving any additional traffic. The only exception is Resource Reservation Protocol (RSVP) service, which if exploited, will cause the device to crash. Only the interface on which the vulnerability was exploited will be affected.

Cisco is providing fixed software to address this issue. There are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at
http://www.cisco.com/warp/public/707/cisco-sa-20080326-IPv4IPv6.shtml.

CSCsf30058

Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

- Session Initiation Protocol (SIP)
- Media Gateway Control Protocol (MGCP)
- Signaling protocols H.323, H.254
- Real-time Transport Protocol (RTP)

- Facsimile reception

Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself.

This advisory is posted at
http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml

CSCsi80749

Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

- Session Initiation Protocol (SIP)
- Media Gateway Control Protocol (MGCP)
- Signaling protocols H.323, H.254
- Real-time Transport Protocol (RTP)
- Facsimile reception

Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself.

This advisory is posted at
http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml

CSCsg70474

Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

- Session Initiation Protocol (SIP)
- Media Gateway Control Protocol (MGCP)
- Signaling protocols H.323, H.254
- Real-time Transport Protocol (RTP)
- Facsimile reception

Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself.

This advisory is posted at
http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml

CSCsi01470

A vulnerability in the Cisco implementation of Multicast Virtual Private Network (MVPN) is subject to exploitation that can allow a malicious user to create extra multicast states on the core routers or receive multicast traffic from other Multiprotocol Label Switching (MPLS) based Virtual Private Networks (VPN) by sending specially crafted messages.

Cisco has released free software updates that address this vulnerability. Workarounds that mitigate this vulnerability are available.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20080326-mvpn.shtml.

CSCsi60004

Multiple voice-related vulnerabilities are identified in Cisco IOS software, one of which is also shared with Cisco Unified Communications Manager. These vulnerabilities pertain to the following protocols or features:

- Session Initiation Protocol (SIP)
- Media Gateway Control Protocol (MGCP)
- Signaling protocols H.323, H.254
- Real-time Transport Protocol (RTP)
- Facsimile reception

Cisco has made free software available to address these vulnerabilities for affected customers. Fixed Cisco IOS software listed in the Software Versions and Fixes section contains fixes for all vulnerabilities mentioned in this advisory.

There are no workarounds available to mitigate the effects of any of the vulnerabilities apart from disabling the protocol or feature itself.

This advisory is posted at
http://www.cisco.com/warp/public/707/cisco-sa-20070808-IOS-voice.shtml

CSCsi09530

Symptom If the **authenticate register** command is configured under the **voice register global** command, then Cisco Unified CallManager Express (CME) SIP fails to register.

Conditions The **authenticate registe**r command is configured under the **voice register global** command when CME is acting as a registrar.

Workaround Disable the **authenticate register** option under the **voice register global** command.

CSCsj32707

Symptom A “SIP UPDATE” message from a Cisco Unified CallManager or SIP Proxy Server with a “Cseq” value of 0 may be rejected or considered invalid by a Cisco gateway.

Conditions This symptom is observed on a Cisco gateway that runs Cisco IOS Release 12.4(9)T4 or a later release, and that is connected to a SIP endpoint.

Workaround There is no workaround. Note that the symptom does not occur in Cisco IOS Release 12.4(9)T3.

CSCdz55178

Symptom The system reloads unexpectedly, or other serious side-affects such as memory corruption occur.

Conditions A cable qos profile with a length greater than 32 characters is configured on the system. For example: cable qos profile 12 name g711@10ms_for_any_softswitch_Traa^C 000000000111111111122222222333^ 123456789012345678901234567890l2| | PROBLEM (Variable Overflowed).

Workaround Change the qos profile name to a value less that 32 characters.

CSCsj52927

Symptom DATACORRUPTION-1-DATAINCONSISTENCY messages are seen in 'show log'

Conditions The messages are seen when the router comes up.

Workaround There is no workaround.

CSCsg92700

Symptom All GLBP IPv6 group members remain in the active state at all times, and no GLPB IPv6 protocol information is passed between group members.

Conditions This symptom is observed on a Cisco router that runs Cisco IOS interim Release 12.4(11.4)T or a later release.

Workaround There is no workaround.

CSCsi84017

Symptom When you reload a Cisco 2600 series, the router may hang.

Conditions This symptom is observed on a Cisco 2600 Series router when you attempt to run the c2600-entservices-mz image of Cisco IOS Release 12.4(9)T4. The symptom may also occur in other releases.

Workaround There is no workaround.

CSCsg96319

Symptom When a reverse SSH session is established with valid authentication credentials, anyone can obtain unprivileged Telnet access to a system without being authenticated. This situation affects only reverse SSH sessions when a connection is made with the **ssh -l** *userid* :**number** *ip-address* command.

Conditions This symptom is observed only when the Reverse SSH Enhancement is configured. This enhancement is documented at the following URL:

http://www.cisco.com/en/US/products/ps6350/products_configuration_guide_chapter09186a00804831b6.html

Workaround Configure reverse SSH by entering the ip ssh port *portnum* rotary *group* command. This configuration is explained at the following URL:

http://www.cisco.com/en/US/tech/tk583/tk617/technologies_q_and_a_item09186a0080267e0f.shtml#newq1

CSCsg40567

Symptom Malformed SSL packets may cause a router to leak multiple memory blocks.

Conditions This symptom is observed on a Cisco router that has the **ip http secure server** command enabled.

Workaround Disable the ip http secure server command.

CSCsb40304

Symptom Cisco IOS device may crash while processing malformed Secure Sockets Layer (SSL) packets. In order to trigger these vulnerabilities, a malicious client must send malformed packets during the SSL protocol exchange with the vulnerable device.

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.

Cisco IOS is affected by the following vulnerabilities:

* Processing ClientHello messages, documented as Cisco bug ID CSCsb12598

* Processing ChangeCipherSpec messages, documented as Cisco bug ID CSCsb40304

* Processing Finished messages, documented as Cisco bug ID CSCsd92405

Cisco has made free software available to address these vulnerabilities for affected customers. There are workarounds available to mitigate the effects of these vulnerabilities.

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

Note Another related advisory has been posted with this advisory. This additional advisory also describes a vulnerability related to cryptography that affects Cisco IOS. This related advisory is available at the following link:
http://www.cisco.com/warp/public/707/cisco-sa-20070522-crypto.shtml

A combined software table for Cisco IOS is available to aid customers in choosing a software releases that fixes all security vulnerabilities published as of May 22, 2007. This software table is available at the following link:
http://www.cisco.com/warp/public/707/cisco-sa-20070522-cry-bundle.shtml.

CSCse05736

Symptom A router that is running RCP can be reloaded by a specific packet.

Conditions This symptom is seen under the following conditions: - The router must have RCP enabled. - The packet must come from the source address of the designated system configured to send RCP packets to the router. - The packet must have a specific data content.

Workaround Put access lists on the edge of your network blocking RCP packets to prevent spoofed RSH packets. Use another protocol such as SCP. Use VTY ACLs.

CSCsg16908

Multiple vulnerabilities exist in the Cisco IOS File Transfer Protocol (FTP) Server feature. These vulnerabilities include Denial of Service, improper verification of user credentials and the ability to read or write any file in the device's filesystem, including the device's saved configuration, which may include passwords or other sensitive information.

The IOS FTP Server is an optional service that is disabled by default. Devices that are not specifically configured to enable the IOS FTP Server service are unaffected by these vulnerabilities.

This vulnerability does not apply to the IOS FTP Client feature.

This advisory is posted at: http://www.cisco.com/warp/public/707/cisco-sa-20070509-iosftp.shtml.

CSCsf28840

A vulnerability exists in the Data-link Switching (DLSw) feature in Cisco IOS where an invalid value in a DLSw message could result in a reload of the DLSw device. Successful exploitation of this vulnerability requires that an attacker be able to establish a DLSw connection to the device. There are workarounds available for this vulnerability. This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070110-dlsw.shtml

CSCse24889

Symptom Malformed SSH version 2 packets may cause a memory leak, causing the platform to operate under a degraded condition. Under rare circumstances, the platform may reload to recover itself.

Conditions This symptom is observed on a Cisco platform that is configured for SSH version 2 after it has received malformed SSHv2 packets.

Workaround As an interim solution until the affected platform can be upgraded to a Cisco IOS software image that contains the fix for caveat CSCse24889, configure SSH version 1 from the global configuration mode, as in the following example:

```
config t
ip ssh version 1 end
```

Alternate Workaround: Permit only known trusted hosts and/or networks to connect to the router by creating a vty access list, as in the following example:

```
10.1.1.0/24 is a trusted network that
is permitted access to the router, all
other access is denied

access-list 99 permit 10.1.1.0 0.0.0.255
access-list 99 deny any
line vty 0 4
access-class 99 in

end
```

Further Problem Description—For information about configuring vty access lists, see the Controlling Access to a Virtual Terminal Line document: http://www.cisco.com/en/US/products/ps6441/products_configuration_guide_chapter09186a0080716ec2.html

For information about SSH, see the Configuring Secure Shell on Routers and Switches Running Cisco IOS document: http://www.cisco.com/warp/public/707/ssh.shtml

CSCec12299

Symptom EIGRP-specific Extended Community 0x8800 is corrupted and shown as 0x0:0:0.

Conditions This symptom is observed when EIGRP-specific Extended Community 0x8800 is received via an IPv4 EBGP session on a CE router. This occurs typically in the following inter-autonomous system scenario:

ASBR/PE-1 <----> VRF-to-VRF <----> ASBR/PE-2

Workaround Use a configuration such as the following to remove extended communities from the CE router:

```
router bgp 1
address-family ipv4 vrf one
neighbor 1.0.0.1 remote-as 100
neighbor 1.0.0.1 activate
neighbor 1.0.0.1 route-map FILTER in
exit-address-family

! ip extcommunity-list 100 permit _RT.*_
!
!
route-map FILTER permit 10
set extcomm-list 100 delete
!
```

CSCsj16292

Symptom Following an upgrade to Cisco IOS Release 12.2(18)SXF9, the following message may be displayed:

%DATACORRUPTION-1-DATAINCONSISTENCY: copy error -Traceback=

Conditions This message may appear as a result of SNMP polling of PAgP variables, but does not appear to be service impacting.

Workaround There is no workaround.

CSCsj18014

Symptom A caller ID may be received with extra characters.

Conditions This symptom is observed when caller ID is enabled on both routers and when the station ID and station name are configured on the FXS side.

Workaround Ther is no workaround.

CSCsj13380

Symptom Data corruption messages may be displayed, and the **show isdn active** command may show incorrect information for calling number on outgoing calls.

Conditions This problem is inconsistent, and shows up most frequently with the **isdn test call** command for outgoing calls.

Workaround There is no workaround.

CSCsi40766

Symptom H.323 calls on a Cisco IOS VoIP gateway may fail after the gateway has processed about 54,500 calls.

Conditions This symptom is observed when H.323 uses TCP to transport signaling messages. When the Cisco IOS gateway must generate a unique port for the local TCP session, this port is selected from a range of open ports. When the number of times that an unique TCP session is created for the same IP address on the gateway exceeds 54,500, further attempts to create a local TCP port fail and calls are not completed. The symptom occurs for H.323 calls only when a separate TCP session is established for the H.245 session. When H.245 tunneling is enabled or no H.245 session is established, the symptom does not occur for H.323 calls. When the **debug ip tcp transaction** command is enabled on the gateway, the "TCP: Ran out of ports for network 0" debug output is generated when the symptom occurs. Enabling debugs on a Cisco IOS gateway should always be done with caution to minimize impact to the performance of the router. As a minimum, ensure that logging to the console is changed from the default behavior of the debug level to, for example, an informational level.

Workaround After the symptom has occurred, reload the Cisco IOS VoIP gateway. To prevent the symptom from occurring, ensure that for H.323 call processing all H.323 devices have H.245 tunneling enabled. This may not always be possible: for example, H.245 tunneling on Cisco Unified CallManager is not supported.

CSCsi91665

Symptom H.323 calls intermittently disconnect.

Conditions For each new call the H.323 GW will generate a TCP Port to be used for call setup. Intermittently the GW will generate a TCP Port that is being used for an established connection. When the GW initiates the three way handshake for the new call it receives a response with an unexpected ACK sequence number. The GW will then send a TCP RST causing the currently established TCP connection/call to be torn down. This problem has been seen in both 12.4(13a) and 12.4(13b).

Workaround There is no wrokaround.

CSCsh23148

Cisco devices running an affected version of Internetwork Operating System (IOS) which supports Session Initiation Protocol (SIP) are affected by a vulnerability that may lead to a reload of the device when receiving a specific series of packets destined to port 5060. This issue is compounded by a related bug which allows traffic to TCP 5060 and UDP port 5060 on devices not configured for SIP. There are no known instances of intentional exploitation of this issue. However, Cisco has observed data streams that appear to be unintentionally triggering the vulnerability. Workarounds exist to mitigate the effects of this problem on devices which do not require SIP. This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20070131-sip.shtml.

CSCsj06951

Symptom Traceback seen on terminal.

Conditions When configuring the user-locale and generating the CNF file in the telephony-service.

Workaround There is no workaround.

Open Caveats—Cisco IOS Release 12.4(6)XT

There are no open caveats in this release.

Resolved Caveats—Cisco IOS Release 12.4(6)XT

This section describes possible unexpected behavior by Cisco IOS Release 12.4(6)XT. All the caveats listed in this section are resolved in Cisco IOS Release 12.4(6)XT. This section describes severity 1 and 2 caveats and select severity 3 caveats.

The following information is provided for each caveat:

- Symptoms: A description of what is observed when the caveat occurs.
- Conditions: The conditions under which the caveat has been known to occur.
- Workaround: Solutions, if available, to counteract the caveat.

Miscellaneous

CSCek54481

Symptom HTTP query data is not cached on the HTTP Client.

Conditions This symptom has been observed when making voice calls with a VXML script accessing the HTTP Server with query data (a question mark '?' after the URL). The response data from the HTTP Server is not cached on the HTTP Client, which is the Cisco IOS voice browser.

Workaround Instead of using query (?) to retrieve a file from the HTTP Server, use a static file name with the query character (?).

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.

`CSCsg16908`

Multiple vulnerabilities exist in the Cisco IOS File Transfer Protocol (FTP) Server feature. These vulnerabilities include Denial of Service, improper verification of user credentials and the ability to read or write any file in the device's filesystem, including the device's saved configuration, which may include passwords or other sensitive information.

The Cisco IOS FTP Server is an optional service that is disabled by default. Devices that are not specifically configured to enable the Cisco IOS FTP Server service are unaffected by these vulnerabilities.

This vulnerability does not apply to the Cisco IOS FTP Client feature.

This advisory is posted at:

http://www.cisco.com/warp/public/707/cisco-sa-20070509-iosftp.shtml.

CSCsg59037

Symptom Cisco 851 and 871 routers have no way to remotely upgrade the ROMMON firmware image.

Conditions Cisco IOS versions for the Cisco 851 and 871 routers did not provide a mechanism to remotely upgrade the ROMMON firmware image.

Workaround Cisco IOS Release 12.4(11)T1 for the Cisco 851 and 871 router introduces the command upgrade rom-monitor file which allows the ROMMON firmware image to be remotely upgraded. Please consult this link for more information:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios124/124tcr/tcf_r/cf_13ht.htm#wp1032550

CSCsh22551

Symptom When VXML requests an ECMA script larger than 32K, the VXML GW displays an error similar to below:

```
//9805//AFW_:/vapp_session_exit_event_name: Exit Event vxml.session.error
//9805/7BA9641F86C2/VXML:/vxml_vapp_terminate: vapp_status=0 ref_count 0
//9805/7BA9641F86C2/VXML:/vxml_vapp_terminate:
CALL_ERROR; http://170.196.114.104:8080/osdm2-core/digits
vxml session terminating with code=ERROR
vapp status=VAPP_SUCCESS vxml async status=VXML_ERROR_NOMEM
//9805//AFW_:/vapp_terminate:
```

Conditions This symptom has been observed on a Cisco AS5400HPX running Cisco IOS Release 12.4(6)T2. In Cisco IOS, there is a file limit of 32K, in which any one file being downloaded at one time cannot exceed 32K. If the file is larger, this vapp error is generated and the call is disconnected. Also, when requesting new ECMA files, Cisco IOS does not flush the prior-requested scripts' memory allocation before requesting more memory for the new file be requested. Instead, it doubles the memory allocation of the prior script many times resulting in the above error. As an example, if a script with a file size of 20K is downloaded and executed and then within the same context/call another script of 31K is requested, rather than Cisco IOS requesting 31K for the new script, Cisco IOS doubles the 20K allocation of the prior script. This allocation equals 40K, which is more that the allowed 32k limit, and the call fails with the above error.

Workaround There is no workaround.

TCP/IP Host-Mode Services

CSCsg39837

Symptom HTTP errors occur while accessing a Win2003 Web Server.

Conditions This symptom has been observed with a Cisco IOS Voice gateway running Cisco IOS Release 12.4(6)T accessing a Win2003 HTTP web server under heavy load. Cisco IOS Voice has the **ip http client connection persistent** command disabled.

Workaround There are two possible workarounds:

1. Switch to a Win2000 HTTP web server.
2. On a Win2003 server, set "TcpTimedWaitDelay" to the minimum (30 seconds). This does not totally eliminate but will reduce the occurrences of dropped TCP SYN requests from the Cisco IOS router.

CSCsg74376

Symptom Traceback is observed at open_connection on Cisco 2600, Cisco 3631, Cisco 3660, and Cisco 3745 platforms.

Conditions This symptom has been observed with Cisco IOS interim Release 12.4 (11.3)PI6a on Cisco 2600, Cisco 3631, Cisco 3660, and Cisco 3745 platforms.

Workaround There is no workaround.

Troubleshooting

The following documents provide assistance with troubleshooting your Cisco hardware and software:

- *Hardware Troubleshooting Index Page* at:

  http://www.cisco.com/warp/public/108/index.shtml
- *Troubleshooting Bus Error Crashes* at:

  http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_tech_note09186a00800cdd51.shtml
- *Why Does My Router Lose Its Configuration During Reboot?* at:

  http://www.cisco.com/warp/public/63/lose_config_6201.html
- *Troubleshooting Router Hangs* at:

  http://www.cisco.com/warp/public/63/why_hang.html
- *Troubleshooting Memory Problems* at:

  http://www.cisco.com/warp/public/63/mallocfail.shtml

- *Troubleshooting High CPU Utilization on Cisco Routers* at:

  http://www.cisco.com/warp/public/63/highcpu.html

Related Documentation

The following sections describe the documentation available for Cisco IOS Release 12.4(6)XT. These documents consist of software installation guides, Cisco IOS configuration and command references, system error messages, feature modules, and other documents.

Use these release notes with the documents and tools described in the following sections:

- Release-Specific Documents, page 25
- Feature Modules, page 25
- Cisco Feature Navigator, page 26
- Cisco IOS Software Documentation Set, page 26

Release-Specific Documents

The following document is specific to Cisco IOS Release 12.4T and is located on Cisco.com:

- *Caveats for Cisco IOS Release 12.4T*

  Refer to *Caveats for Cisco IOS Release 12.4T* for caveats applicable to all platforms for all maintenance releases of Cisco IOS Release 12.4T.

On Cisco.com at:

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

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, log in to Cisco.com and click **Products and Solutions > Cisco IOS Software > IOS Technologies > 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.)

Feature Modules

Feature modules describe new features that are supported in Cisco IOS Release 12.4T and are updates to the Cisco IOS documentation set. A feature module consists of a brief overview of the feature, benefits, configuration tasks, and a command reference. As updates, the feature modules are available online only. Feature module information is incorporated into the next printing of the Cisco IOS documentation set.

On Cisco.com at:

Technical Documents > Cisco IOS Software > Cisco IOS Release 12.4 > New Feature Documentation > 12.4T New Features and System Messages

Cisco Feature Navigator

Cisco Feature Navigator is a web-based tool that enables you to determine which Cisco IOS 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 release. Under the release section, you can compare releases side by side to display both the features unique to each software release and the features in common.

Cisco Feature Navigator is available 24 hours a day, 7 days a week, and 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/cfn

Cisco IOS Software Documentation Set

The Cisco IOS Release 12.4 documentation set consists of the configuration guide and command reference pairs listed in Table 1 and the supporting documents listed in Table 2. The configuration guides and command references are organized by technology. For the configuration guides:

- Some technology documentation, such as that for DHCP, contains features introduced in Releases 12.2T and 12.3T and, in some cases, Release 12.2S.
- Other technology documentation, such as that for OSPF, consists of a chapter and accompanying Release 12.2T and 12.3T feature documents.

Note In some cases, information contained in Release 12.2T and 12.3T feature documents augments or supersedes content in the accompanying documentation. Therefore it is important to review all feature documents for a particular technology.

Table 1 lists the Cisco IOS Release 12.4 configuration guides and command references.

Table 1 Cisco IOS Release 12.4 Configuration Guides and Command References

Configuration Guide and Command Reference Titles	Description
IP	
Cisco IOS IP Addressing Services Configuration Guide, Release 12.4 *Cisco IOS IP Addressing Services Command Reference*, Release 12.4	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 12.4 *Cisco IOS Application Services Command Reference*, Release 12.4	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 12.4	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.

Table 1 Cisco IOS Release 12.4 Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Description
Cisco IOS IP Multicast Configuration Guide, Release 12.4 *Cisco IOS IP Multicast Command Reference*, Release 12.4	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.
Cisco IOS IP Routing Protocols Configuration Guide, Release 12.4 *Cisco IOS IP Routing Protocols Command Reference*, Release 12.4	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 12.4	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 12.4 *Cisco IOS IPv6 Command Reference*, Release 12.4	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 Optimized Edge Routing Configuration Guide, Release 12.4 *Cisco IOS Optimized Edge Routing Command Reference*, Release 12.4	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 12.4 *Cisco IOS Security Command Reference*, Release 12.4	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 12.4 *Cisco IOS Quality of Service Solutions Command Reference*, Release 12.4	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 12.4	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.
Multiprotocol Label Switching (MPLS)	

Table 1 Cisco IOS Release 12.4 Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Description
Cisco IOS Multiprotocol Label Switching Configuration Guide, Release 12.4 *Cisco IOS Multiprotocol Label Switching Command Reference*, Release 12.4	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 Monitoring Technology Command Reference*, Release 12.4	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 12.4 *Cisco IOS NetFlow Command Reference*, Release 12.4	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 12.4	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 IOS Voice Configuration Library, Release 12.4 *Cisco IOS Voice Command Reference*, Release 12.4	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 12.4	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 1 Cisco IOS Release 12.4 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 12.4	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 12.4	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 12.4	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.
Long Reach Ethernet (LRE) and Digital Subscriber Line (xDSL)	
Cisco IOS Broadband and DSL Configuration Guide, Release 12.4 *Cisco IOS Broadband Access Aggregation and DSL Command Reference*, Release 12.4	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 12.4	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 12.4	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.
Asynchronous Transfer Mode (ATM)	
Cisco IOS Asynchronous Transfer Mode Configuration Guide, Release 12.4 *Cisco IOS Asynchronous Transfer Mode Command Reference*, Release 12.4	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.

Table 1 Cisco IOS Release 12.4 Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Description
WAN	
Cisco IOS Wide-Area Networking Configuration Guide, Release 12.4 *Cisco IOS Wide-Area Networking Command Reference*, Release 12.4	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 12.4	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 12.4	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.
IBM Technologies	
Cisco IOS Bridging and IBM Networking Configuration Guide, Release 12.4 *Cisco IOS Bridging Command Reference*, Release 12.4 *Cisco IOS IBM Networking Command Reference*, Release 12.4	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 12.4	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.

Table 1 Cisco IOS Release 12.4 Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Description
Cisco IOS DECnet Configuration Guide, Release 12.4 *Cisco IOS DECnet Command Reference*, Release 12.4	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 12.4	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 12.4	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 12.4	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 2 lists the documents and resources that support the Cisco IOS Release 12.4 software configuration guides and command references.

Table 2 Cisco IOS Release 12.4 Supporting Documents and Resources

Document Title	Description
Cisco IOS Master Commands List, Release 12.4	An alphabetical listing of all the commands documented in the Cisco IOS Release 12.4 command references.
Cisco IOS New, Modified, Replaced, and Removed Commands, Release 12.4	A listing of all the new, modified, replaced and removed commands since Cisco IOS Release 12.3, grouped by Release 12.3T maintenance release and ordered alphabetically within each group.
Cisco IOS New and Modified Commands, Release 12.3	A listing of all the new, modified, and replaced commands since Cisco IOS Release 12.2, grouped by Release 12.2T maintenance release and ordered alphabetically within each group.
Cisco IOS System Messages, Volume 1 of 2 *Cisco IOS System Messages, Volume 2 of 2*	Listings and descriptions of Cisco IOS system messages. 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 12.4	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.
Release Notes, Release 12.4	A description of general release information, including information about supported platforms, feature sets, platform-specific notes, and Cisco IOS software defects.

Table 2 Cisco IOS Release 12.4 Supporting Documents and Resources (continued)

Document Title	Description
Dictionary of Internetworking Terms and Acronyms	Compilation and definitions of 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

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

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

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

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