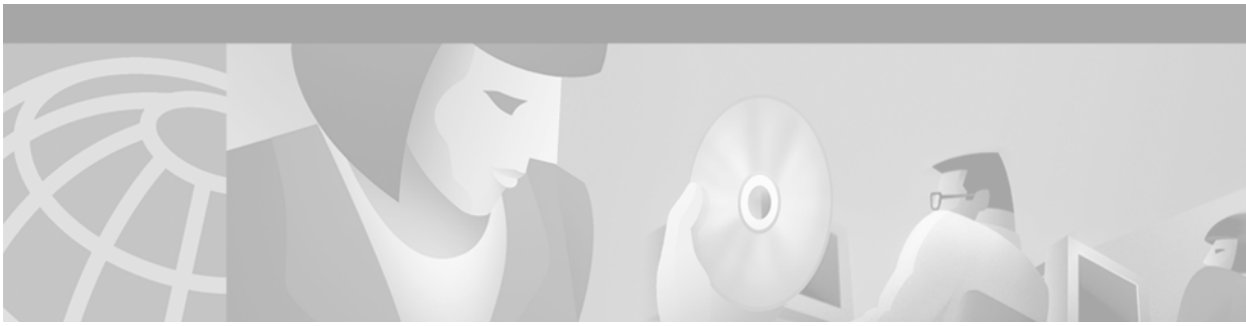

Release Notes for Cisco 7000 Family for Cisco IOS Release 12.2 YE

June 3, 2002

Cisco IOS Release 12.2(9)YE

OL-2613-01

These release notes for the Cisco 7000 family describe the enhancements provided in Cisco IOS Release 12.2(9)YE. These release notes are updated as needed.

For a list of the software caveats that apply to Cisco IOS Release 12.2(9)YE, see the "Caveats for Cisco IOS Release 12.2" section on page 7 and *Caveats for Cisco IOS Release 12.2*. The caveats document is updated for every maintenance release and is located on Cisco.com and the Documentation CD-ROM.

Use these release notes with *Cross-Platform Release Notes for Cisco IOS Release 12.2* located on Cisco.com and the Documentation CD-ROM.

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/770/index.shtml. If you do not have a Cisco.com login account, you can find field notices at http://www.cisco.com/warp/public/770/index.shtml.

Documentation Survey

Is Cisco documentation helpful? Click here to give us your feedback or go to the following URL to give us your feedback:
http://forums.cisco.com/eforum/servlet/viewsflash?cmd=showform&pollid=rtgdoc01!rtgdoc.

CISCO SYSTEMS

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

Contents

These release notes describe the following topics:

System Requirements

This section describes the system requirements for Cisco IOS Release 12.2 YE and includes the following sections:

Memory Recommendations

Table 1 Images and Memory Recommendations for Cisco IOS Release 12.2 YE

Platforms	Feature Sets	Image Name	Software Image	Flash Memory Recommended	DRAM Memory Recommended	Runs From
Cisco 7400 Series	IP Standard Feature Set	IP IPSec 3DES	c7400-ik9s-mz	16 MB	128 MB	RAM
	IP Firewall Standard Feature Set	IP/FW/IDS IPSec 3DES	c7400-ik9o3s-mz	16 MB	128 MB	RAM

Supported Hardware

Cisco IOS Release 12.2(9)YE supports the following Cisco 7000 family platforms:

- Cisco 7401 ASR routers

For detailed descriptions of the new hardware features, see the "New and Changed Information" section on page 4.

For additional information about supported hardware for this platform and release, please refer to the Hardware/Software Compatibility Matrix in the Cisco Software Advisor at the following location:

http://www.cisco.com/cgi-bin/front.x/Support/HWSWmatrix/hwswmatrix.cgi

Determining the Software Version

To determine the version of Cisco IOS software running on your Cisco 7000 family router, log in to the Cisco 7000 family router and enter the **show version** EXEC command. The following sample **show version** command output is from a router running a Cisco 7401 ASR software image with Cisco IOS Release 12.2(9)YE:

```
Router> show version
Cisco Internetwork Operating System Software
IOS (tm) 12.2 YE Software (c7400-ik9s-mz), Version 12.2(9)YE, RELEASE SOFTWARE
```

Upgrading to a New Software Release

For general information about upgrading to a new software release, refer to S*oftware Installation and Upgrade Procedures* located at the following URL:

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

Feature Set Tables

The Cisco IOS software is packaged in feature sets consisting of software images—depending on the platform. Each feature set contains a specific set of Cisco IOS features.

Cisco IOS Release 12.2(9)YE supports the same feature sets as Cisco IOS Release 12.2, but Cisco IOS Release 12.2(9)YE can include new features supported by the Cisco 7000 family.

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.

Table 2 lists the features and feature sets supported by the Cisco 7401 ASR routers in Cisco IOS Release 12.2(9)YE 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, (9)YE means a feature was introduced in 12.2(9)YE.

Table 2 Feature List by Feature Set for the Cisco 7401 ASR (continued)

Features	In	Software Images by Feature Sets			
		IP IPSec 3DES	IP/FW/IDS IPSec 3DES		
VPN Acceleration Module	(9)YE	Yes	Yes		
VDM 1.1.1	(9)YE	Yes	Yes		
IPSec VPN High Availability Enhancements	(9)YE	Yes	Yes		

New and Changed Information

The following sections list the new hardware and software features supported by the Cisco 7000 family for Cisco IOS Release 12.2(9)YE.

New Hardware Features in Cisco IOS Release 12.2(9)YE

There are no new hardware features supported by the Cisco 7000 family for Cisco IOS Release 12.2(9)YE.

New Software Features in Cisco IOS Release 12.2(9)YE

The following new software features are supported by the Cisco 7000 family for Cisco IOS Release 12.2(9)YE:

IPSec VPN High Availability Enhancements

Platforms: Cisco 7401 ASR routers

The IPSec VPN High Availability feature consists of two new features—Reverse Route Injection and Hot Standby Router Protocol and IPSec—that work together to provide users with a simplified network design for VPNs and reduced configuration complexity on remote peers with respect to defining gateway lists.

Reverse Route Injection

Reverse Route Injection (RRI) is a feature designed to simplify network design for Virtual Private Network (VPNs) in which there is a requirement for redundancy or load balancing. RRI works with both dynamic and static crypto maps.

In the dynamic case, as remote peers establish IPSec security associations (SAs) with an RRI-enabled router, a static route is created for each subnet or host protected by that remote peer. For static crypto maps, a static route is created for each destination of an extended access-list rule.

When routes are created, they are injected into any dynamic routing protocol and distributed to surrounding devices. This traffic flows, requiring IPSec to be directed to the appropriate RRI router for transport across the correct SAs to avoid IPSec policy mismatches and possible packet loss.

Hot Standby Router Protocol and IPSec

Hot Standby Router Protocol (HSRP) is designed to provide high network availability by routing IP traffic from hosts on Ethernet networks without relying on the availability of any single router. HSRP is particularly useful for hosts that do not support a router discovery protocol, such as ICMP Router Discovery Protocol (IRDP), and do not have the functionality to switch to a new router when their selected router reloads or loses power. Without this functionality, a router that loses its default gateway because of a router failure is unable to communicate with the network.

HSRP is configurable on LAN interfaces using standby command line interface (CLI) commands. It is now possible to use the standby IP address from an interface as the local IPSec identity, or local tunnel endpoint.

By using the standby IP address as the tunnel endpoint, failover can be applied to VPN routers by using HSRP. Remote VPN gateways connect to the local VPN router via the standby address that belongs to the active device in the HSRP group. In the event of failover, the standby device takes over ownership of the standby IP address and begins to service remote VPN gateways.

VDM 1.1.1

Platforms: Cisco 7401 ASR routers

VPN Device Manager (VDM) release 1.1.1 supports 7400 series routers. For more information about VDM, see *Installation and Release Notes for VPN Device Manager1.1.1*.

VPN Acceleration Module

Platforms: Cisco 7401 ASR routers

The VPN Acceleration Module (VAM) is a single-width acceleration module. It provides high-performance, hardware-assisted tunneling and encryption services suitable for virtual private network (VPN) remote access, site-to-site intranet, and extranet applications. It also provides platform scalability and security while working with all services necessary for successful VPN deployments — security, quality of service (QoS), firewall and intrusion detection, service-level validation, and management. The VAM off-loads IPSec processing from the main processor, thus freeing resources on the processor engines for other tasks.

The VAM provides hardware-accelerated support for the following multiple encryption functions:

- 56-bit Data Encryption Standard (DES) standard mode: Cipher Block Chaining (CBC)
- 3-Key Triple DES (168-bit)
- Secure Hash Algorithm (SHA)-1 and Message Digest 5 (MD5)
- Rivest, Shamir, Adelman (RSA) public-key algorithm
- Diffie-Hellman key exchange RC4-40

MIBs

Current MIBs

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB website on Cisco.com at http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml.

Deprecated and Replacement MIBs

Old Cisco MIBs will be replaced in a future release. Currently, OLD-CISCO-* MIBs are being converted into more scalable MIBs without affecting existing Cisco IOS products or network management system (NMS) applications. You can update from deprecated MIBs to the replacement MIBs as shown in Table 3.

Table 3 Deprecated and Replacement MIBs

Deprecated MIB	Replacement
OLD-CISCO-APPLETALK-MIB	RFC1243-MIB
OLD-CISCO-CHASSIS-MIB	ENTITY-MIB
OLD-CISCO-CPUK-MIB	To be determined
OLD-CISCO-DECNET-MIB	To be determined
OLD-CISCO-ENV-MIB	CISCO-ENVMON-MIB
OLD-CISCO-FLASH-MIB	CISCO-FLASH-MIB
OLD-CISCO-INTERFACES-MIB	IF-MIB CISCO-QUEUE-MIB
OLD-CISCO-IP-MIB	To be determined
OLD-CISCO-MEMORY-MIB	CISCO-MEMORY-POOL-MIB
OLD-CISCO-NOVELL-MIB	NOVELL-IPX-MIB
OLD-CISCO-SYS-MIB	(Compilation of other OLD* MIBs)
OLD-CISCO-SYSTEM-MIB	CISCO-CONFIG-COPY-MIB
OLD-CISCO-TCP-MIB	CISCO-TCP-MIB
OLD-CISCO-TS-MIB	To be determined
OLD-CISCO-VINES-MIB	CISCO-VINES-MIB
OLD-CISCO-XNS-MIB	To be determined

Important Notes

The following sections contain important notes about Cisco IOS Release 12.2 YE that can apply to the Cisco 7000 family.

Field Notices and Bulletins

- Field Notices—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/770/index.shtml. If you do not have a Cisco.com login account, you can find field notices at http://www.cisco.com/warp/public/770/index.shtml.
- Product Bulletins—If you have an account on 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 for IOS Releases: Cisco IOS 12.2—What's Hot for IOS Releases: Cisco IOS 12.2* provides information about caveats that are related to deferred software images for Cisco IOS Release 12.2. If you have an account on Cisco.com, you can access *What's Hot for IOS Releases: Cisco IOS 12.2* at http://www.cisco.com/kobayashi/sw-center/sw-ios.shtml or by logging in and selecting **Software Center: Cisco IOS Software: What's Hot for IOS Releases: Cisco IOS 12.2**.
- *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 in and selecting **Software Center: Cisco IOS Software: What's New for IOS**.

Caveats for Cisco IOS Release 12.2

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 only open and resolved caveats for the current Cisco IOS maintenance release.

All caveats in Cisco IOS Release 12.2 and Cisco IOS Release 12.2 S are also in Cisco IOS Release 12.2(9)YE.

For information on caveats in Cisco IOS Release 12.2, see *Caveats for Cisco IOS Release 12.2*.

For information on caveats in Cisco IOS Release 12.2 T, see *Caveats for Cisco IOS Release 12.2 T*, which lists severity 1 and 2 caveats and select severity 3 caveats and is located on Cisco.com and the Documentation CD-ROM.

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 **Service & Support: Software Center: Cisco IOS Software: BUG TOOLKIT**. Another option is to go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

Because Cisco IOS Release 12.2(9)YE is the initial base release, there are no resolved caveats. For a list of the resolved caveats, refer to the next set of release notes for this release version.

Table 4 Caveats Reference for Cisco IOS Release 12.2 MB

DDTS Number	Open in Release	Resolved in Release
CSCdp85074	12.2(9)YE	
CSCdu07646	12.2(9)YE	
CSCdu22576	12.2(9)YE	
CSCdv39447	12.2(9)YE	
CSCdv56287	12.2(9)YE	
CSCdw23620	12.2(9)YE	
CSCdw27097	12.2(9)YE	
CSCdw37371	12.2(9)YE	
CSCdw50463	12.2(9)YE	
CSCdw51754	12.2(9)YE	
CSCdw59016	12.2(9)YE	
CSCdw65511	12.2(9)YE	
CSCdw79279	12.2(9)YE	
CSCdw89255	12.2(9)YE	
CSCdx02106	12.2(9)YE	
CSCdx07358	12.2(9)YE	
CSCdx11848	12.2(9)YE	
CSCdx17233	12.2(9)YE	
CSCdx22158	12.2(9)YE	
CSCdx23494	12.2(9)YE	
CSCdx26656	12.2(9)YE	
CSCdx70480	12.2(9)YE	
CSCdz71127		12.2(9)YE

Open Caveats—Cisco IOS Release 12.2(9)YE

This section documents possible unexpected behavior by Cisco IOS Release 12.2(9)YE and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdp85074

  A Cisco router that is running the Resource Reservation Protocol (RSVP) may treat some conforming reserved traffic as nonconforming. This behavior may cause traffic to be improperly marked (with precedence or type of service [TOS] markings) or improperly scheduled (that is, not assigned a reserved queue/Low Latency Queueing [LLQ] or preferential Weighted Random Early Detection [WRED] precedence/Differentiated Services Code Point [DSCP]). This condition occurs if the **ip rsvp flow-assist** interface configuration command and Weighted Fair Queueing (WFQ), Class-Based Weighted Fair Queuing (CBWFQ), LLQ, or WRED precedence/DSCP are configured on an interface.

  Workaround: Remove the **ip rsvp flow-assist** interface configuration command from the configuration on the interface.

- CSCdu07646

  When TCP packets with window size 0 are continuously sent from the Multilayer Switch Feature Card (MSFC2) to the router, the router may fail to complete a configuration load. This condition occurs when an Access Control List (ACL) configuration is transferred through a cut-and-paste procedure using a Telnet relay.

  There are no known workarounds.

- CSCdu22576

  A Cisco router that is implementing the Downstream Physical Unit (DSPU) feature may reload because of a loop that is observed when the router is replying to a Simple Network Management Protocol (SNMP) request.

  Workaround: Do not query the dspuSapType fields of the Cisco DSPU MIN using SNMP.

- CSCdv39447

  The Flash MIB implementation for a High End System (HES) in Cisco IOS software does not provide correct information for the following objects:

  - ciscoFlashCode

  - ciscoFlashChipDescr

  - ciscoFlashDeviceInitTime

  There is no workaround.

- CSCdv56287

  Cisco Express Forwarding (CEF) does not work with IP Security (IPSec). Packets are fast-switched instead of being switched by Cisco Express Forwarding (CEF).

  There are no known workarounds.

- CSCdw23620

  High cpu utilisation on a 7206(NPE 200) with 12.2.(5) may be caused by a service-policy. Excessive interrupts may cause the router to reload.

- CSCdw27097

  When the router is configured for IPSec or GRE+IPSec links packet fragmentation is handled in the process path when fast switching or CEF is enabled. Similar behavior was observed on c2600 & c3600 series routers.

- CSCdw37371

  A 7400 router crashes when a service-policy with WRED is attached to the ATM PVC. However, it does not crash immediately. It happens after a lot of configuration changes, involving attachment and detachment of service policies as well as forwarding traffic. It is noticed that the crash happens indeterministically - not necessarily with RED policy alone. It is also observed with C7200 router running 12.2 (6.8)T image.

  No known workaround exists.

- CSCdw50463

  DSR drops on tty line during the set up of x28 profile

  This works in 12.1(9) but not in 12.2.1b, 12.0.7XK1, 12.1.1T or 12.2(6)

- CSCdw51754

  A Cisco router may crash while running ip nat translation processing LDAP.

- CSCdw59016

  A 7400 router reloads when a service-policy is attached to an ATM PVC and after getting out from the configuration mode.

- CSCdw65511

  squeezing a bootflash of size ~65MB might cause High CPU utilization. Will update this section with further details.

- CSCdw79279

  If a member PVC in an atm bundle is not added at the same time as bundle creation, all the members may go to state INACTIVE when the main interface is reset (shut/no shut). Problem seen only for the 7500.

  Workaround: Add all members when the bundle is first created.

- CSCdw89255

  Remote dlsw router doing sdlc/dlsw conversion with multidropped atm devices may hang. The last input/last output timers increment continually and a debug sdlc packet indicates that RR is not sent to the remote device.

  Workaround is to shur/no shut the serial interface

- CSCdx02106

  When MLPoFR/ATM is configured, interleaving functionality (LFI) may not work properly. There is no workaround.

- CSCdx07358

  Under rare circumstances, a Cisco router running IOS 12.2(7) may reload due to a bus error at an invalid address such as 0xFFDF000D:

  ```
  System returned to ROM by bus error at PC 0x611D2FAC, address 0xFFDF000D
  ```

  There is no known workaround at this time.

- CSCdx11848

  Stuck mbgp entries with no valid path may cause RPF (Reverse Path Forwarding) failures for multicast traffic.

- CSCdx17233

  There is a severe memory leak when doing SNMP V1 testing, and may cause router to reload. There is no workaround.

- CSCdx22158

  On Cisco IOS Release 12.2(S), a router with a VAM card encrypting a large amount of traffic over an extended period of time may reload.

  There is no workaround.

- CSCdx23494

  If you manually change the Message Digest 5 (MD5) keyword during a Border Gateway Protocol (BGP) session, the BGP session is reset. This behavior makes it impossible to dynamically manage security parameters in a network.

  There is no workaround.

- CSCdx26656

  In any 12.2 release L2TP Dial-out with callback cases, when the calls initiated by LNS side, Virtual interface of LNS failed to accept sent CONFACK during vpdn/ppp callback negotiating.

  There is no workaround.

- CSCdx70480

  On a Cisco 7400 series router, the monitor feature in VDM does not work properly.

  When a tunnel is created and VDM is use, it shows in the report screen IKE=0 and IPSec=1. The TopN screens are empty and have no tunnel, and all the graph that related to ipsec / ike are empty (contain no data).

  There are no known workarounds.

Resolved Caveats—Cisco IOS Release 12.2(9)YE

All the caveats listed in this section are resolved in Cisco IOS Release 12.2(9)YE. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdz71127

  Cisco routers and switches running Cisco IOS software and configured to process Internet Protocol version 4 (IPv4) packets are vulnerable to a Denial of Service (DoS) attack. A rare sequence of crafted IPv4 packets sent directly to the device may cause the input interface to stop processing traffic once the input queue is full. No authentication is required to process the inbound packet. Processing of IPv4 packets is enabled by default. Devices running only IP version 6 (IPv6) are not affected. A workaround is available.

  Cisco has made software available, free of charge, to correct the problem.

  This advisory is available at

  http://www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.shtml

Related Documentation

The following sections describe the documentation available for the Cisco 7000 family. 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 the Documentation CD-ROM.

Use these release notes with these documents:

Release-Specific Documents

The following documents are specific to Cisco IOS Release 12.2 and are located on Cisco.com and the Documentation CD-ROM:

- *Cross-Platform Release Notes for Cisco IOS Release 12.2*

  On Cisco.com at:

  Technical Documents: **Cisco IOS Software**: **Cisco IOS Release 12.2**: **Release Notes**: **Cross-Platform Release Notes**

Note *Cross-Platform Release Notes for Cisco IOS Release 12.2 T* are located on Cisco.com at: **Technical Documents**: **Cisco IOS Software**: **Cisco IOS Release 12.2**: **Release Notes**: **Cisco IOS Release 12.2 T.**

  On the Documentation CD-ROM at:

  Cisco Product Documentation: **Cisco IOS Software Configuration**: **Cisco IOS Release 12.2**: **Release Notes**: **Cross-Platform Release Notes**

- Product bulletins, field notices, and other release-specific documents on Cisco.com at:

  Technical Documents

- *Caveats for Cisco IOS Release 12.2*

  As a supplement to the caveats listed in "Caveats for Cisco IOS Release 12.2" in these release notes, see *Caveats for Cisco IOS Release 12.2* which contains caveats applicable to all platforms for all maintenance releases of Cisco IOS Release 12.2.

  On Cisco.com at:

  Technical Documents: **Cisco IOS Software Configuration**: **Cisco IOS Release 12.2**: **Release Notes**: **Caveats**

  On the Documentation CD-ROM at:

  Cisco Product Documentation: Cisco IOS Software Configuration: **Cisco IOS Release 12.2**: **Caveats**

- *Caveats for Cisco IOS Release 12.2 T*

  As a supplement to the caveats listed in "Caveats for Cisco IOS Release 12.2" in these release notes, see *Caveats for Cisco IOS Release 12.2 T* which contains caveats applicable to all platforms for all maintenance releases of Cisco IOS Release 12.2 T.

  On Cisco.com at:

  Technical Documents: **Cisco IOS Software Configuration**: **Cisco IOS Release 12.2**: **Release Notes**: **Caveats**

  On the Documentation CD-ROM at:

  Cisco Product Documentation: Cisco IOS Software Configuration: **Cisco IOS Release 12.2**: **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, log in to Cisco.com and click **Service & Support: Software Center: Cisco IOS Software: BUG TOOLKIT**. Another option is to go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

Platform-Specific Documents

These documents are available for the Cisco 7000 family of routers on Cisco.com and the Documentation CD-ROM:

- *Cisco 7000 Hardware Installation and Maintenance*
- *Cisco 7000 User Guide*
- *Cisco 7010 User Guide*
- *Cisco 7200 VXR Installation and Configuration Guide*
- Cisco 7200 VXR Quick Start Guide
- *Cisco 7202 Installation and Configuration Guide*
- *Cisco 7204 Installation and Configuration Guide*
- *Cisco 7206 Installation and Configuration Guide*
- Cisco 7206 Quick Start Guide
- Cisco 7401 ASR Installation and Configuration Guide
- Cisco 7401 ASR Quick Start Guide
- *Quick Reference for Cisco 7204 Installation*
- *Quick Start Guide Cisco 7100 Series VPN Router*

  Technical Documents: **Documentation Home Page**: **Core/High-End Routers**

  On the Documentation CD-ROM at:

  Cisco Product Documentation: **Core/High-End Routers**

Feature Modules

Feature modules describe new features supported by Cisco IOS Release 12.2(9)YE 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 in the next printing of the Cisco IOS documentation set.

On Cisco.com at:

Technical Documents: **Cisco IOS Software**: **Cisco IOS Release 12.2**: **New Feature Documentation**

On the Documentation CD-ROM at:

Cisco Product Documentation: **Cisco IOS Software Configuration**: **Cisco IOS Release 12.2**: **New Feature Documentation**

Cisco IOS Software Documentation Set

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

Documentation Modules

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

On Cisco.com at:

Technical Documents: **Cisco IOS Software**: **Cisco IOS Release 12.2**: **Configuration Guides and Command References**

On the Documentation CD-ROM at:

Cisco Product Documentation: **Cisco IOS Software Configuration**: **Cisco IOS Release 12.2**: **Configuration Guides and Command References**

Cisco IOS Release 12.2 Documentation Set Contents

Table 5 lists the contents of the Cisco IOS Release 12.2 software documentation set, which is available in electronic form and in printed form if ordered.

Note You can find the most current Cisco IOS documentation on Cisco.com and the Documentation CD-ROM.

On Cisco.com at:

Technical Documents: **Cisco IOS Software**: **Cisco IOS Release 12.2**

On the Documentation CD-ROM at:

Cisco Product Documentation: **Cisco IOS Software Configuration**: **Cisco IOS Release 12.2**

Table 5 Cisco IOS Release 12.2 Documentation Set

Books	Major Topics
• *Cisco IOS Configuration Fundamentals Configuration Guide* • *Cisco IOS Configuration Fundamentals Command Reference*	Cisco IOS User Interfaces File Management System Management
• *Cisco IOS Bridging and IBM Networking Configuration Guide* • *Cisco IOS Bridging and IBM Networking Command Reference, Volume 1 of 2* • *Cisco IOS Bridging and IBM Networking Command Reference, Volume 2 of 2*	Transparent Bridging SRB Token Ring Inter-Switch Link Token Ring Route Switch Module RSRB DLSW+ Serial Tunnel and Block Serial Tunnel LLC2 and SDLC IBM Network Media Translation SNA Frame Relay Access NCIA Client/Server Airline Product Set DSPU and SNA Service Point SNA Switching Services Cisco Transaction Connection Cisco Mainframe Channel Connection CLAW and TCP/IP Offload CSNA, CMPC, and CMPC+ TN3270 Server
• *Cisco IOS Dial Technologies Configuration Guide: Dial Access* • *Cisco IOS Dial Technologies Configuration Guide: Large-Scale Dial Applications* • *Cisco IOS Dial Technologies Command Reference, Volume 1 of 2* • *Cisco IOS Dial Technologies Command Reference, Volume 2 of 2*	Dial Access Modem and Dial Shelf Configuration and Management ISDN Configuration Signaling Configuration Point-to-Point Protocols Dial-on-Demand Routing Dial Backup Dial Related Addressing Service Network Access Solutions Large-Scale Dial Solutions Cost-Control Solutions Internetworking Dial Access Scenarios
• *Cisco IOS Interface Configuration Guide* • *Cisco IOS Interface Command Reference*	LAN Interfaces Serial Interfaces Logical Interfaces
• *Cisco IOS IP Configuration Guide* • *Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services* • *Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols* • *Cisco IOS IP Command Reference, Volume 3 of 3: Multicast*	IP Addressing IP Services IP Routing Protocols IP Multicast
• *Cisco IOS AppleTalk and Novell IPX Configuration Guide* • *Cisco IOS AppleTalk and Novell IPX Command Reference*	AppleTalk Novell IPX

Table 5 Cisco IOS Release 12.2 Documentation Set (continued)

Books	Major Topics
• *Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Configuration Guide* • *Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Command Reference*	Apollo Domain Banyan VINES DECnet ISO CLNS XNS
• *Cisco IOS Voice, Video, and Fax Configuration Guide* • *Cisco IOS Voice, Video, and Fax Command Reference*	Voice over IP Call Control Signaling Voice over Frame Relay Voice over ATM Telephony Applications Trunk Management Fax, Video, and Modem Support
• *Cisco IOS Quality of Service Solutions Configuration Guide* • *Cisco IOS Quality of Service Solutions Command Reference*	Packet Classification Congestion Management Congestion Avoidance Policing and Shaping Signaling Link Efficiency Mechanisms
• *Cisco IOS Security Configuration Guide* • *Cisco IOS Security Command Reference*	AAA Security Services Security Server Protocols Traffic Filtering and Firewalls IP Security and Encryption Passwords and Privileges Neighbor Router Authentication IP Security Options Supported AV Pairs
• *Cisco IOS Switching Services Configuration Guide* • *Cisco IOS Switching Services Command Reference*	Cisco IOS Switching Paths NetFlow Switching Multiprotocol Label Switching Multilayer Switching Multicast Distributed Switching Virtual LANs LAN Emulation
• *Cisco IOS Wide-Area Networking Configuration Guide* • *Cisco IOS Wide-Area Networking Command Reference*	ATM Frame Relay SMDS X.25 and LAPB
• *Cisco IOS Mobile Wireless Configuration Guide* • *Cisco IOS Mobile Wireless Command Reference*	General Packet Radio Service

Table 5 Cisco IOS Release 12.2 Documentation Set (continued)

Books	Major Topics
• *Cisco IOS Terminal Services Configuration Guide* • *Cisco IOS Terminal Services Command Reference*	ARA LAT NASI Telnet TN3270 XRemote X.28 PAD Protocol Translation
• *Cisco IOS Configuration Guide Master Index* • *Cisco IOS Command Reference Master Index* • *Cisco IOS Debug Command Reference* • *Cisco IOS Software System Error Messages* • *New Features in 12.2-Based Limited Lifetime Releases* • *New Features in Release 12.2 T* • *Release Notes* (Release note and caveat documentation for 12.2-based releases and various platforms)	

Obtaining Documentation

The following sections explain how to obtain documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following URL:

http://www.cisco.com

Translated documentation is available at the following URL:

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

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which is shipped with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

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

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

If you are reading Cisco product documentation on Cisco.com, you can submit technical comments electronically. Click **Leave Feedback** at the bottom of the Cisco Documentation home page. After you complete the form, print it out and fax it to Cisco at 408 527-0730.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

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

We appreciate your comments.

Obtaining Technical Assistance

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

Cisco.com

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

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

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

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

You can self-register on Cisco.com to obtain customized information and service. To access Cisco.com, go to the following URL:

http://www.cisco.com

Technical Assistance Center

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

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

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

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

Cisco TAC Web Site

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

http://www.cisco.com/tac

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

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

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

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

If you have Internet access, it is recommended that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

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

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

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

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