



Release Notes for Cisco 800 and SOHO 90 Series Routers for Cisco IOS Release 12.3(8)YA1

January 24, 2005

Contents

- [System Requirements, page 1](#)
- [New and Changed Information, page 5](#)
- [Limitations and Restrictions, page 7](#)
- [Caveats, page 8](#)
- [Related Documentation, page 10](#)
- [Obtaining Documentation, page 15](#)
- [Documentation Feedback, page 16](#)
- [Cisco Product Security Overview, page 17](#)
- [Obtaining Technical Assistance, page 18](#)
- [Obtaining Additional Publications and Information, page 19](#)

System Requirements

This section describes the system requirements for Cisco IOS Cisco IOS Release 12.3(8)YA and includes the following sections:

- [Memory Requirements, page 2](#)
- [Hardware Supported, page 2](#)
- [Determining the Software Version, page 3](#)
- [Upgrading to a New Software Release, page 3](#)
- [Feature Set Tables, page 3](#)



Memory Requirements

This section describes the memory requirements for the Cisco IOS feature sets that are supported by Cisco IOS Release 12.3(8)YA on the Cisco 831, 836, 837, SOHO 91, SOHO 96, and SOHO 97 routers.

Table 1 Recommended Memory for the Cisco 831, 836, 837, SOHO 91, SOHO 96, and SOHO 97 Routers

Platform	Image Name	Feature Set	Image	Flash Memory		DRAM	
				Minimum	Recommended ¹	Minimum	Recommended
Cisco 831	Cisco 831 Series IOS IP/FW2 IPSec 3DES	IP/FW2/IPSec 3DES	c831-k9o3y6-mz	12 MB	12 MB	48 MB	48 MB
	Cisco 831 Series IOS IP/FW2 Plus IPSec 3DES	IP Plus/FW2/IPSec 3DES	c831-k9o3sy6-mz	12 MB	12 MB	48 MB	48 MB
Cisco 836	Cisco 836 Series IOS IP/FW2 IPSec 3DES	IP/FW2/IPSec 3DES	c836-k9o3y6-mz	12 MB	12 MB	48 MB	48 MB
	Cisco 836 Series IOS IP/FW2 Plus IPSec 3DES	IP Plus/FW2/IPSec 3DES	c836-k9o3sy6-mz	12 MB	12 MB	48 MB	48 MB
	Cisco 836 Series IOS IP/FW2/Dial Backup Plus IPSec 3DES	IP Plus/FW2/Dial Backup IPSec 3DES	c836-k9o3s8y6-mz	12 MB	12 MB	48 MB	48 MB
Cisco 837	Cisco 837 Series IOS IP/FW2 IPSec 3DES	IP/FW2/IPSec 3DES	c837-k9o3y6-mz	12 MB	12 MB	48 MB	48 MB
	Cisco 837 Series IOS IP/FW2 Plus IPSec 3DES	IP Plus/FW2/IPSec 3DES	c837-k9o3sy6-mz	12 MB	12 MB	48 MB	48 MB
Cisco SOHO 91	Cisco SOHO 91 Series IOS IP/FW/3DES	IP/FW 3DES	soho91-k9oy6-mz	8 MB	8 MB	32 MB	32 MB
Cisco SOHO 96	Cisco SOHO 96 Series IOS IP/FW/3DES	IP/FW 3DES	soho96-k9oy1-mz	8 MB	8 MB	32 MB	32 MB
Cisco SOHO 97	Cisco SOHO 97 Series IOS IP/FW 3DES	IP/FW 3DES	soho97-k9oy1-mz	8 MB	8 MB	32 MB	32 MB

1. Recommended memory is the memory required for potential future expansions.

Hardware Supported

Cisco IOS Release 12.3(8)YA supports the following routers:

- Cisco 831 router
- Cisco 836 router
- Cisco 837 router

- Cisco SOHO 91 router
- Cisco SOHO 96 router
- Cisco SOHO 97 router

For detailed descriptions of new hardware features and which features are supported on each router, see the “[New and Changed Information](#)” section on page 5. For descriptions of existing hardware features and supported modules, see the hardware installation guides, configuration and command reference guides, and additional documents specific to the Cisco 831, 836, 837, SOHO 91, SOHO 96, and SOHO 97 routers, which are available on [Cisco.com](#) at the following location:

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

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

Technical Documentation: Routers: Fixed Config. Access Routers: <platform_name>

Determining the Software Version

To determine which version of the Cisco IOS software is currently running on your Cisco 831, 836, 837, SOHO 91, SOHO 96, or SOHO 97 router, log in to the router, and enter the **show version** command. The following sample output from the **show version** command indicates the version number on the second output line.

```
router> show version
Cisco Internetwork Operating System Software
IOS (tm) C836 Software (C836-K9O3SY6-M), Version 12.4(11)XJ, EARLY DEPLOYMENT RELEASE
SOFTWARE (fc1) Synchronized to technology version 12.3(9.6)T
```

Upgrading to a New Software Release

For general information about upgrading to a new software release, see the *Software Installation and Upgrade Procedures* located at

<http://www.cisco.com/cgi-bin/Support/browse/index.pl?i=Hardware&f=742>.

Feature Set Tables

The Cisco IOS software is packaged in feature sets consisting of software images, depending on the platform. Each feature set contains a specific set of Cisco IOS features. Release 12.3(8)YA1 includes the same feature sets supported by the Cisco 800 and SOHO 90 series routers as Releases 12.3, 12.3(8)T, and 12.3(8)YA. There are no new features in Release 12.3(8)YA1



Caution

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

Table 2 through Table 7 list the features and feature sets that are supported in Cisco IOS Cisco IOS Release 12.3(8)YA.

The tables use the following conventions:

- In—The number in the “In” column indicates the Cisco IOS release in which the feature was introduced. For example, “12.4(11)XJ” indicates that the feature was introduced in Release 12.4(11)XJ. If a cell in this column is empty, the feature was included in a previous release or in the initial base release.
- Yes—The feature is supported in the software image.
- No—The feature is not supported in the software image.



Note

These feature set tables contain only a list of selected features, which are cumulative for Release 12.3(8)*nn* early deployment releases only (*nn* identifies each early deployment release). The tables do not list all the features in each image; additional features are listed in [Cross-Platform Release Notes for Cisco IOS Release 12.3\(8\)T](#) and in Release 12.3(8)T Cisco IOS documentation.

Table 2 Feature Set Table for the Cisco 831 Router

Feature	In	Feature Set	
		IP/FW2 3DES	IP/FW2 Plus 3DES
Dynamic DNS Support for Cisco IOS	12.4(11)XJ	Yes	Yes
No Service Password Recovery	12.4(11)XJ	Yes	Yes
Bridge MIB	12.4(11)XJ	Yes	Yes

Table 3 Feature Set Table for the Cisco 836 Router

Feature	In	Feature Set		
		IP/FW2 3DES	IP/FW2 Plus 3DES	IP Plus/FW2/Dial Backup IPSec 3DES
Dynamic DNS Support for Cisco IOS	12.4(11)XJ	Yes	Yes	Yes
No Service Password Recovery	12.4(11)XJ	Yes	Yes	Yes
Bridge MIB	12.4(11)XJ	Yes	Yes	Yes

Table 4 Feature Set Table for the Cisco 837 Router

Feature	In	Feature Set	
		IP/FW2 3DES	IP/FW2 Plus 3DES
Dynamic DNS Support for Cisco IOS	12.4(11)XJ	Yes	Yes
No Service Password Recovery	12.4(11)XJ	Yes	Yes
Bridge MIB	12.4(11)XJ	Yes	Yes

Table 5 *Feature Set Table for the Cisco SOHO91 Router*

Feature	In	Feature Set
		IP/FW 3DES
Dynamic DNS Support for Cisco IOS	12.4(11)XJ	Yes
No Service Password Recovery	12.4(11)XJ	Yes
Bridge MIB	12.4(11)XJ	No

Table 6 *Feature Set Table for the Cisco SOHO 96 Router*

Feature	In	Feature Set
		IP/FW 3DES
Dynamic DNS Support for Cisco IOS	12.4(11)XJ	Yes
No Service Password Recovery	12.4(11)XJ	Yes
Bridge MIB	12.4(11)XJ	No

Table 7 *Feature Set Table for the Cisco SOHO 97 Router*

Feature	In	Feature Set
		IP/FW 3DES
Dynamic DNS Support for Cisco IOS	12.4(11)XJ	Yes
No Service Password Recovery	12.4(11)XJ	Yes
Bridge MIB	12.4(11)XJ	No

New and Changed Information

The following sections list the new software features supported by the Cisco 831, 836, 837, SOHO 91, SOHO 96, and SOHO 97 routers for Cisco IOS Release 12.3(8)YA.

New Software Features in Cisco IOS Release 12.3(8)YA

There are no new software features in Cisco IOS Release 12.3(8)YA.

New Software Features in Release 12.3(8)YA

The following sections describe the new software features supported by the Cisco 800 and SOHO 90 series routers for Release 12.3(8)YA.

Dynamic DNS Support for Cisco IOS

The Dynamic DNS Support for Cisco IOS feature enables Cisco IOS devices to perform Dynamic Domain Name System (DDNS) updates to ensure that an IP host DNS name is correctly associated with its IP address.

It provides two mechanisms to generate or perform DDNS: the IETF standard as defined by RFC 2136, and a generic HTTP using various DNS services. With this feature, you can define a list of host names and IP addresses that will receive updates, specify an update method, and specify a configuration for DHCP triggered updates.

With the Dynamic DNS Support feature, you can define a list of hostnames and/or IP addresses that will receive updates, can specify an update method, and can specify a configuration for DHCP-triggered updates.

For more details about the Dynamic DNS Support for Cisco IOS feature, see the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123limit/123y/123ya8/gt_ddns.htm

No Service Password Recovery

The No Service Password-Recovery feature is a security enhancement that prevents anyone with access to a console from accessing the router configuration and clearing the password. It also prevents anyone from changing the configuration register values and accessing non-volatile RAM (NVRAM).

The No Service Password Recovery feature is enabled using the **no service password-recovery** hidden command. When this hidden command is used, a warning and a confirmation prompt appear on your router.

To disable the feature, use the **service password-recovery** command.

The No Service Password Recovery feature also recovers the forgotten passwords. When this feature is enabled, the router accepts the break signal within 5 seconds, just after the Cisco IOS software is decompressed during booting. The user is then prompted to confirm the action. After confirmation, the startup configuration is erased, the password recovery procedure is enabled, and the router boots with the factory default configuration. When the user enters “no”, the router boots normally and with the No Service Password Recovery feature enabled.

For more details about the No Service Password Recovery feature, see the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123limit/123y/123ya8/ftn_svpwd.htm

The No Service Password Recovery feature requires use of ROMMON version 12.2(11r)YV1. The procedure for upgrading the ROMMON image from ROMMON mode is given at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_fix/827/820rmup.htm#54965

Bridge MIB

The Bridge MIB feature, extracted from RFC 1493, defines objects for managing MAC bridges between LAN segments. The Bridge MIB feature provides information regarding various ports of the bridge, Spanning Tree Protocol (STP), and transparent bridging, and supports dot1dBase, dot1dStp, and dot1dTp standards.

New Software Features in Release 12.3(8)T

For information regarding the features supported in the Cisco IOS Release 12.3(8)T, see the Cross-Platform Release Notes and New Feature Documentation links at the following location on [Cisco.com](http://www.cisco.com):

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123relnt/xprn123/index.htm>

This URL is subject to change without notice. If it changes, point your web browser to [Cisco.com](http://www.cisco.com), and click the following path:

Service & Support: Technical Documents: Cisco IOS Software: Release 12.3: Release Notes: Cross-Platform Release Notes (Cisco IOS Release 12.3(8)T)

Limitations and Restrictions

The following sections describe limitations concerning the new hardware and software features supported by the Cisco 800 series routers for Cisco IOS Release 12.3(8)YA and 12.3(8)YA.

No Service Password Recovery

The following limitations apply for the No Service Password Recovery feature:

- After the feature is configured, it remains configured even after router reload (the command will be listed in running configuration). It is not necessary to write this configuration into NVRAM to keep the feature enabled between reloads.
- To enable the feature, disable the break bit and the bit to ignore the startup configuration. Set the boot bits value in the configuration register.
- If you want to change configuration register value after the No Service Password Recovery feature is enabled, the above restrictions still apply.

[Table 8](#) lists the meanings of the software configuration memory bits.

Table 8 Software Configuration Memory Bits

Bit Number	Hexadecimal	Meaning
00 to 03	0x0000 to 0x000F	Boot field
06	0x0040	Causes system software to ignore NVRAM contents
07	0x0080	OEM bit enabled
08	0x0100	Break disabled
09	0x0200	Use secondary bootstrap
10	0x0400	IP broadcast with all zeros
11 to 12	0x0800 to 0x1000	Console line speed (default is 9600 baud)
13	0x2000	Boot default Flash software if network boot fails

Table 8 **Software Configuration Memory Bits (continued)**

Bit Number	Hexadecimal	Meaning
14	0x4000	IP broadcasts do not have network numbers
15	0x8000	Enable diagnostic messages and ignore NVRAM contents

- When the feature is enabled, do not reload or powercycle the router without a valid image in the boot device. The router will not go into the ROMMON mode because of the No Service Password Recovery feature and since there is no IOS to boot with, the ROMMON continuously reloads. The only workaround to recover from this setup is to request a Cisco Systems return materials authorization (RMA).
- Before you downgrade the image in the router, disable the feature. It will not be possible to reset the feature with a downgraded image.
- Reload the router so that any changes to the configuration register value will take effect.

Caveats

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

Caveats in Cisco IOS Release 12.3(8)T are also in Cisco IOS Release 12.3(8)YA. For information on caveats in Cisco IOS Release 12.3(8)T, see the [Caveats for Cisco IOS Release 12.3\(8\)T](#) document. This document lists severity 1 and 2 caveats; the documents are located on [Cisco.com](#).



Note

If you have an account with [Cisco.com](#), you can also use the Bug Toolkit to find select caveats of any severity. To reach the Bug Toolkit, log in to [Cisco.com](#) and click **Service & Support: Technical Assistance Center: Tool Index: Bug Toolkit**. Another option is to go to http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl.

Resolved Caveats - Cisco IOS Release 12.3(8)YA

This section documents possible unexpected behavior by Cisco IOS Release 12.4(11)XJ1 and describes only severity 1 and 2 caveats and select severity 3 caveats.

-
- CSCef83876
DHCP Client could not renew the IP address using the ATM unnumbered interface, after changing the configuration on the bridge.
- CSCef95695
When configuring ezvpn using nat-t on a Cisco 831 router, the IPSec SA's are created but only encaps packets are shown in the byte counts. The esp frames are sent with protocol 50 instead of 4500 for nat-t.
- CSCeg44078 c836

- DMZ - Huge delay transmitting traffic on Eth0 and Eth2.
- CSCeg47738
Incorrect count loaded into Timer3 that handles ISDN layer1.
- CSCef46191
Unable to telnet.
- CSCef12235
ISDN TEI negotiation fails when Layer 2 is not activated. ISDN TEI negotiation on Layer 2 (and consequently ISDN calls on Layer 3) may fail on a Cisco 836 router when Layer 1 is active and Layer 2 is not activated.
- CSCin77315—EZVPN: crash in map_db_check_acl.
Easy Virtual Private Network (EZVPN) crashes while reconnecting.
- CSCee66832—The **show ip access-list** command does not show configured extended access-list.
The output of the **show ip access-list command** does not show extended access lists.
- CSCin77426—Crypto map entries not cleared for dialer, EZVPN halts at SS_OPEN.
- CSCee01865—BADSHARE tracebacks seen when packet errors occur in hardware crypto.
- CSCin82407

Cisco Internetwork Operating System (IOS) Software release trains 12.2T, 12.3 and 12.3T may contain vulnerabilities in processing certain Internet Key Exchange (IKE) Xauth messages when configured to be an Easy VPN Server.

Successful exploitation of these vulnerabilities may permit an unauthorized user to complete authentication and potentially access network resources.

This advisory will be posted to

<http://www.cisco.com/warp/public/707/cisco-sa-20050406-xauth.shtml>

- CSCef43691
A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled “ICMP Attacks Against TCP” (draft-gont-tcpm-icmp-attacks-03.txt).

These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

1. Attacks that use ICMP “hard” error messages
2. Attacks that use ICMP “fragmentation needed and Don’t Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
3. Attacks that use ICMP “source quench” messages

Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

Multiple Cisco products are affected by the attacks described in this Internet draft.

Cisco has made free software available to address these vulnerabilities. In some cases 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-20050412-icmp.shtml>.

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: <http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en>.

- CSCef44225

A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled “ICMP Attacks Against TCP” (draft-gont-tcpm-icmp-attacks-03.txt).

These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

1. Attacks that use ICMP “hard” error messages
2. Attacks that use ICMP “fragmentation needed and Don’t Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
3. Attacks that use ICMP “source quench” messages

Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

Multiple Cisco products are affected by the attacks described in this Internet draft.

Cisco has made free software available to address these vulnerabilities. In some cases 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-20050412-icmp.shtml>.

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: <http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en>.

Open Caveats - Cisco IOS Release 12.3(8)YA

This section documents possible unexpected behavior by Cisco IOS Release 12.4(11)XJ1 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCee73477—Spurious access at show_ip2access.

Traceback may be seen when **show ip access-list** command is given, when named access lists are configured.

Workaround

Use numbered access lists.

- CSCee83305—Spurious access @dialer_redial_initiate found when configured as BRI.

Related Documentation

The following sections describe the documentation available for the Cisco 800 and SOHO 90 series routers. These documents consist of hardware and software installation guides, Cisco IOS configuration guides and command references, system error messages, feature modules, and other documents.

Documentation is available as printed manuals or electronic documents, except for feature modules, which are available online on [Cisco.com](http://www.cisco.com) and <http://www.cisco.com/univercd/home/index.htm>.

Use these release notes with these documents:

- [Release-Specific Documents](#)
- [Platform-Specific Documents](#)
- [Cisco Feature Navigator](#)

Release-Specific Documents

The following documents are specific to Cisco IOS Release 12.3 and are located on [Cisco.com](http://www.cisco.com) and <http://www.cisco.com/univercd/home/index.htm>:

- *Cross-Platform Release Notes for Cisco IOS Release 12.3(8)T*

On [Cisco.com](http://www.cisco.com) at:

Products and Solutions: Cisco IOS Software: Cisco IOS Software Releases 12.3: Instructions and Guides: Release Notes

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

Cisco IOS Software: Cisco IOS Release 12.3: Release Notes: Cross-Platform Release Notes



Note *Cross-Platform Release Notes for Cisco IOS Release 12.3T* are located on [Cisco.com](http://www.cisco.com) at or on <http://www.cisco.com/univercd/home/index.htm> at **Cisco IOS Software: Cisco IOS Release 12.3: Release Notes: Cisco IOS Release 12.3T**.

- Product bulletins, field notices, and other release-specific documents at <http://www.cisco.com/univercd/home/index.htm>
- *Caveats for Cisco IOS Release 12.3*

As a supplement to the caveats listed in these release notes, see *Caveats for Cisco IOS Release 12.3* and *Caveats for Cisco IOS Release 12.3T*, which contains caveats applicable to all platforms for all maintenance releases of Cisco IOS Release 12.3 and Cisco IOS Release 12.3T.

On [Cisco.com](http://www.cisco.com) at:

Products & Solutions: IOS Software: Cisco IOS Software Releases 12.3: Instructions and Guides: Release Notes: Release Notes for Cisco IOS Release 12.3, Part 5: Caveats

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

Cisco IOS Software: Cisco IOS Release 12.3: Release Notes: Caveats

- If you have an account on [Cisco.com](http://www.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](http://www.cisco.com) and click **Products and Solutions: Cisco IOS Software: Cisco IOS Software Releases 12.3: Troubleshooting: 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 800 and SOHO 90 series routers:

On [Cisco.com](http://www.cisco.com) at:

Technical Documentation: Routers: Fixed Config. Access Routers: <platform_name>

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

Product Documentation: Routers: Fixed Config. Access Routers: <platform_name>

Cisco Feature Navigator

Cisco IOS software is packaged in feature sets that are supported on specific platforms. To obtain updated information regarding platform support for this feature, access Cisco Feature Navigator. Cisco Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Cisco Feature Navigator is a web-based tool that enables you to quickly 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.

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

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

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://tools.cisco.com/ITDIT/CFN/jsp/index.jsp>

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.

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](http://www.cisco.com) at:

Products and Solutions: Cisco IOS Software: Cisco IOS Releases 12.3: Instructions and Guides

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

Cisco IOS Software: Cisco IOS Release 12.3: Configuration Guides and Command References

Cisco IOS Release 12.3 Documentation Set Contents

Table 9 lists the contents of the Cisco IOS Release 12.3 software documentation set, which is available in electronic form and in printed form if ordered.

On [Cisco.com](http://www.cisco.com) at:

Products and Solutions: Cisco IOS Software: Cisco IOS Releases 12.3: Instructions and Guides

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

Cisco IOS Software: Cisco IOS Release 12.3

Table 9 Cisco IOS Release 12.3 Documentation Set

Books	Major Topics
<ul style="list-style-type: none"> <i>Cisco IOS Configuration Fundamentals and Network Management Configuration Guide</i> <i>Cisco IOS Configuration Fundamentals and Network Management Command Reference</i> 	Configuration Fundamentals Overview Cisco IOS User Interfaces File Management System Management
<ul style="list-style-type: none"> <i>Cisco IOS Bridging and IBM Networking Configuration Guide</i> <i>Cisco IOS Bridging and IBM Networking Command Reference, Volume 1 of 2: Bridging</i> <i>Cisco IOS Bridging and IBM Networking Command Reference, Volume 2 of 2: IBM Networking</i> 	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

Table 9 Cisco IOS Release 12.3 Documentation Set (continued)

Books	Major Topics
<ul style="list-style-type: none"> • <i>Cisco IOS Dial Technologies Configuration Guide</i> • <i>Cisco IOS Dial Technologies Command Reference</i> 	Preparing for Dial Access Modem and Dial Shelf Configuration and Management ISDN Configuration Signaling Configuration Dial-on-Demand Routing Configuration Dial Backup Configuration Dial Related Addressing Service Virtual Templates, Profiles, and Networks PPP Configuration Callback and Bandwidth Allocation Configuration Dial Access Specialized Features Dial Access Scenarios
<ul style="list-style-type: none"> • <i>Cisco IOS Interface and Hardware Component Configuration Guide</i> • <i>Cisco IOS Interface and Hardware Component Command Reference</i> 	LAN Interfaces Serial Interfaces Logical Interfaces
<ul style="list-style-type: none"> • <i>Cisco IOS IP Configuration Guide</i> • <i>Cisco IOS IP Command Reference, Volume 1 of 4: Addressing and Services</i> • <i>Cisco IOS IP Command Reference, Volume 2 of 4: Routing Protocols</i> • <i>Cisco IOS IP Command Reference, Volume 3 of 4: Multicast</i> • <i>Cisco IOS IP Command Reference, Volume 4 of 4: IP Mobility</i> 	IP Addressing and Services IP Routing Protocols IP Multicast
<ul style="list-style-type: none"> • <i>Cisco IOS AppleTalk and Novell IPX Configuration Guide</i> • <i>Cisco IOS AppleTalk and Novell IPX Command Reference</i> 	AppleTalk Novell IPX
<ul style="list-style-type: none"> • <i>Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Configuration Guide</i> • <i>Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Command Reference</i> 	Apollo Domain Banyan VINES DECnet ISO CLNS XNS
<ul style="list-style-type: none"> • <i>Cisco IOS Voice Configuration Library</i> • <i>Cisco IOS Voice Command Reference</i> 	Voice over IP Call Control Signaling Voice over Frame Relay Voice over ATM Telephony Applications Trunk Management Fax, Video, and Modem Support
<ul style="list-style-type: none"> • <i>Cisco IOS Quality of Service Solutions Configuration Guide</i> • <i>Cisco IOS Quality of Service Solutions Command Reference</i> 	Packet Classification Congestion Management Congestion Avoidance Policing and Shaping Signaling Link Efficiency Mechanisms

Table 9 Cisco IOS Release 12.3 Documentation Set (continued)

Books	Major Topics
<ul style="list-style-type: none"> • <i>Cisco IOS Security Configuration Guide</i> • <i>Cisco IOS Security Command Reference</i> 	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
<ul style="list-style-type: none"> • <i>Cisco IOS Switching Services Configuration Guide</i> • <i>Cisco IOS Switching Services Command Reference</i> 	Cisco IOS Switching Paths NetFlow Switching Multiprotocol Label Switching Multilayer Switching Multicast Distributed Switching Virtual LANs LAN Emulation
<ul style="list-style-type: none"> • <i>Cisco IOS Wide-Area Networking Configuration Guide</i> • <i>Cisco IOS Wide-Area Networking Command Reference</i> 	ATM Broadband Access Frame Relay SMDS X.25 and LAPB
<ul style="list-style-type: none"> • <i>Cisco IOS Mobile Wireless Configuration Guide</i> • <i>Cisco IOS Mobile Wireless Command Reference</i> 	General Packet Radio Service
<ul style="list-style-type: none"> • <i>Cisco IOS Terminal Services Configuration Guide</i> • <i>Cisco IOS Terminal Services Command Reference</i> 	ARA LAT NASI Telnet TN3270 XRemote X.28 PAD Protocol Translation
<ul style="list-style-type: none"> • <i>Cisco IOS Configuration Guide Master Index</i> • <i>Cisco IOS Command Reference Master Index</i> • <i>Cisco IOS Debug Command Reference</i> • <i>Cisco IOS Software System Messages</i> 	

Obtaining Documentation

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

Cisco.com

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

<http://www.cisco.com/univercd/home/home.htm>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

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

Documentation DVD

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

Registered Cisco.com users (Cisco direct customers) can order a Cisco Documentation DVD (product number DOC-DOCDVD=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

<http://www.cisco.com/en/US/partner/ordering/>

Cisco Marketplace:

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:
<http://www.cisco.com/en/US/partner/ordering/>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 1 800 553-NETS (6387).

Documentation Feedback

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

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

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

We appreciate your comments.

Cisco Product Security Overview

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

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

From this site, you can perform these tasks:

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

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

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

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

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

Reporting Security Problems in Cisco Products

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

- Emergencies—security-alert@cisco.com
- Nonemergencies—psirt@cisco.com



Tip

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

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one that has the most recent creation date in this public key server list:

<http://pgp.mit.edu:11371/pks/lookup?search=psirt%40cisco.com&op=index&exact=on>

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

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

Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

The Cisco Technical Support Website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, 365 days a year, at this URL:

<http://www.cisco.com/techsupport>

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

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



Note

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

Submitting a Service Request

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

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

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

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

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

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

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

Definitions of Service Request Severity

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

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

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

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

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

Obtaining Additional Publications and Information

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

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:
<http://www.cisco.com/go/marketplace/>
- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:
<http://www.ciscopress.com>
- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:
<http://www.cisco.com/packet>
- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:
<http://www.cisco.com/go/iqmagazine>
- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:
<http://www.cisco.com/ipj>

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

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

This document is to be used in conjunction with the documents listed in the “[Related Documentation](#)” section.

CCSP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0411R)

Copyright © 2005 Cisco Systems, Inc. All rights reserved.