



Release Notes for the Cisco 1800 Series Fixed Configuration Routers for Cisco IOS Release 12.3(8)YI

August 8, 2007

Cisco IOS Release 12.3(8)YI3

OL-8341-02 Fourth Release

These release notes describe new features and significant software components for the Cisco 1801, 1801W, 1802, 1802W, 1803, 1803W, 1811, 1811W, 1812, and 1812W series routers that support Cisco IOS Release 12.3(8)T, up to and including Release 12.3(8)YI3. These release notes are updated as needed to describe new memory requirements, new features, new hardware support, software platform deferrals, microcode or modem code changes, related document changes, and any other important changes. Use these release notes with the [Cross-Platform Release Notes for Cisco IOS Release 12.3 T](#) for Cisco IOS Release 12.3 T located on [Cisco.com](#).

For a list of the software caveats that apply to Release 12.3(8)YI3, refer to the Caveats section below and to the online [Caveats for Cisco IOS Release 12.3 T](#) document. The caveats document is updated for every 12.3 T maintenance release and is located on [Cisco.com](#).

Contents

- [System Requirements, page 2](#)
- [New and Changed Information, page 5](#)
- [Limitations and Restrictions, page 7](#)
- [Caveats, page 8](#)
- [Additional References, page 15](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines, page 16](#)



Americas Headquarters:

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

© 2007 Cisco Systems, Inc. All rights reserved.

System Requirements

This section describes the system requirements for Cisco IOS Release 12.3(8)YI3.

Memory Requirements

[Table 1](#) lists the memory requirements for Cisco IOS Release 12.3(8)YI3.


Note

Recommended memory is the memory required for potential future expansions.

Table 1 *Memory Requirements for the Cisco 1800 Series Fixed Configuration Routers*

Platform	Software Product Description	Feature Set	Image	Flash	DRAM
Cisco 1801 Cisco 1802 Cisco 1803	Cisco 180X IP Broadband	Cisco 180X IP Broadband	c180x-broadband-mz	32MB	128MB
Cisco 1801 Cisco 1801W Cisco 1802 Cisco 1802W Cisco 1803 Cisco 1803W	Cisco 180X Advanced IP Services	Cisco 180X Advanced IP Services	c180x-advipservicesk9-mz	32MB	128MB
Cisco 1801 Cisco 1801W Cisco 1802 Cisco 1802W Cisco 1803 Cisco 1803W	Cisco 180X Advanced Enterprise Services	Cisco 180X Advanced Enterprise Services	c180x-adventerprisek9-mz	32MB	128MB
Cisco 1811 Cisco 1811W Cisco 1812 Cisco 1812W	Cisco 181X Advanced IP Services	Cisco 181X Advanced IP Services	c181x-advipservicesk9-mz	32MB	128MB
Cisco 1811 Cisco 1811W Cisco 1812 Cisco 1812W	Cisco 181X Advanced Enterprise Services	Cisco 181X Advanced Enterprise Services	c181x-adventerprisek9-mz	32MB	128MB

Hardware Supported

Cisco IOS Release 12.3(8)YI3 supports the following Cisco 1800 series routers:

- Cisco 1801 - One Fast Ethernet port, one ADSL over POTS port, one ISDN-BRI S/T port, and eight Fast Ethernet Switch ports
- Cisco 1801W - One Fast Ethernet port, one ADSL over POTS port, one ISDN-BRI S/T port, eight Fast Ethernet Switch ports, and IEEE 802.11a & 802.11b/g
- Cisco 1802 - One Fast Ethernet port, one ADSL over ISDN port, one ISDN-BRI S/T port, and eight Fast Ethernet Switch ports
- Cisco 1802W - One Fast Ethernet port, one ADSL over ISDN port, one ISDN-BRI S/T port, eight Fast Ethernet Switch ports, and IEEE 802.11a & 802.11b/g
- Cisco 1803 - One Fast Ethernet port, one G.SDHDSL (4 wire) port, one ISDN-BRI S/T port, and eight Fast Ethernet Switch ports
- Cisco 1803W - One Fast Ethernet port, one G.SDHDSL (4 wire) port, one ISDN-BRI S/T port, eight Fast Ethernet Switch ports, and IEEE 802.11a & 802.11b/g
- Cisco 1811 - Two Fast Ethernet ports, one V.92 Modem port, eight Fast Ethernet Switch ports, and two USB connectors
- Cisco 1811W - Two Fast Ethernet ports, one V.92 Modem port, eight Fast Ethernet Switch ports, two USB connectors, and IEEE 802.11a & 802.11b/g
- Cisco 1812 - Two Fast Ethernet ports, one ISDN-BRI S/T port, eight Fast Ethernet Switch ports, and two USB connectors
- Cisco 1812W - Two Fast Ethernet ports, one ISDN-BRI S/T port, eight Fast Ethernet Switch ports, two USB connectors, and IEEE 802.11a & 802.11b/g

Determining the Software Version

To determine the version of Cisco IOS software running on your Cisco router, log in to the router and enter the **show version** EXEC command. The following sample displays command output from a Cisco 1811 router running Cisco IOS Release 12.3(8)YI3:

```
Router>show version
```

```
Cisco IOS Software, C181X Software (C181X-ADVENTERPRISEK9-M), Version 12.3(8)YI3, RELEASE SOFTWARE (fc1)
Synched to technology version 12.3(10.3)T
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Mon 07-Feb-05 02:22 by ealyon

ROM: System Bootstrap, Version 12.3(8r)YH3, RELEASE SOFTWARE (fc1)
```

Upgrading to a New Software Release

For general information about upgrading to a new software release, see Cisco IOS Software Release 12.3 T Installation and Upgrade Procedures located on Cisco.com.

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)YI3 supports the same feature sets as Cisco IOS Release 12.3(8)YI1, and Cisco IOS Release 12.3(8)YI2.

Table 2 shows the feature set table for Cisco IOS Release 12.3(8)YI3.

Table 2 Feature Set Table

Product	IP Base	IP Voice	IP Broad-band	Enterprise Base	Advanced Security	Service Provider Services	Advanced IP Services	Enterprise Services	Advanced Enterprise Services
Cisco 1801	Not supported	Not supported	Supported	Not supported	Not supported	Not supported	Supported	Not supported	Supported
Cisco 1801W	Not supported	Not supported	Not supported	Not supported	Not supported	Not supported	Supported	Not supported	Supported
Cisco 1802	Not supported	Not supported	Supported	Not supported	Not supported	Not supported	Supported	Not supported	Supported
Cisco 1802W	Not supported	Not supported	Not supported	Not supported	Not supported	Not supported	Supported	Not supported	Supported
Cisco 1803	Not supported	Not supported	Supported	Not supported	Not supported	Not supported	Supported	Not supported	Supported
Cisco 1803W	Not supported	Not supported	Not supported	Not supported	Not supported	Not supported	Supported	Not supported	Supported
Cisco 1811	Not supported	Not supported	Not supported	Not supported	Not supported	Not supported	Supported	Not supported	Supported
Cisco 1811W	Not supported	Not supported	Not supported	Not supported	Not supported	Not supported	Supported	Not supported	Supported
Cisco 1812	Not supported	Not supported	Not supported	Not supported	Not supported	Not supported	Supported	Not supported	Supported
Cisco 1812W	Not supported	Not supported	Not supported	Not supported	Not supported	Not supported	Supported	Not supported	Supported

New and Changed Information

Cisco IOS Release 12.3(8)YI3 supports the features listed in this section.

New Hardware Features in Cisco IOS Release 12.3(8)YI3

The Cisco IOS Release 12.3(8)YI3 supports the same hardware features as Cisco IOS Release 12.3(8)YI2.

New Hardware Features in Cisco IOS Release 12.3(8)YI2

The following features are supported by Cisco IOS Release 12.3(8)YI2.

Cisco 1801 Routers

- One Fast Ethernet port
- One ADSL over POTS port
- One ISDN-BRI S/T port
- Eight Fast Ethernet Switch ports

Cisco 1801W Routers

- One Fast Ethernet port
- One ADSL over POTS port
- One ISDN-BRI S/T port
- Eight Fast Ethernet Switch ports
- IEEE 802.11a and 802.11b/g wireless

Cisco 1802 Routers

- One Fast Ethernet port
- One ADSL over ISDN port
- One ISDN-BRI S/T port
- Eight Fast Ethernet Switch port

Cisco 1802W Routers

- One Fast Ethernet port
- One ADSL over ISDN port
- One ISDN-BRI S/T port
- Eight Fast Ethernet Switch port
- IEEE 802.11a and 802.11b/g wireless

Cisco 1803 Routers

- One Fast Ethernet port
- One G.SHDSL port
- One ISDN-BRI S/T port
- Eight Fast Ethernet Switch ports

Cisco 1803W Routers

- One Fast Ethernet port
- One G.SHDSL port
- One ISDN-BRI S/T port
- Eight Fast Ethernet Switch ports
- IEEE 802.11a and 802.11b/g wireless

Cisco 1811 Routers

- Two Fast Ethernet ports
- One V.92 Modem port
- Eight Fast Ethernet Switch ports
- Two USB connectors

Cisco 1811W Routers

- Two Fast Ethernet ports
- One V.92 Modem port
- Eight Fast Ethernet Switch ports
- Two USB connectors
- IEEE 802.11a and 802.11b/g wireless

Cisco 1812 Routers

- Two Fast Ethernet ports
- One ISDN-BRI S/T port
- Eight Fast Ethernet Switch ports
- Two USB connectors

Cisco 1812W Routers

- Two Fast Ethernet ports
- One ISDN-BRI S/T port
- Eight Fast Ethernet Switch ports
- Two USB connectors
- IEEE 802.11a and 802.11b/g wireless

New Software Features in Cisco IOS Release 12.3(8)YI3

The Cisco IOS Release 12.3(8)YI3 supports the same software features that are supported in the Cisco IOS Release 12.3(8)YI2.

New Software Features in Cisco IOS Release 12.3(8)YI2

The following sections describe the new software features supported by the Cisco IOS Release 12.3(8)YI2.

Inline Power Auto Negotiation

Inline power auto negotiation is supported.

Easy VPN Remote Web Based Activation

This feature provides user-friendly Web based entry of username/password via client web browser (IE or Netscape). A bypass mode is provided for Internet access without requiring VPN tunnel activation. One-time passwords are supported using RADIUS.

Limitations and Restrictions

Inline Power

The Cisco 1811, 1812, and 1812-J routers are able to deliver up to 80 W of power through Fast Ethernet switch ports if the routers are equipped with field-upgradable inline power daughter card and an external power supply. Up to eight IP phones may be powered by inline power.

USB

USB ports should not be connected to laptops or other hosts using Type A to Type A cables or connectors.

IPSec Tunnels

50 simultaneous IPSec tunnels are supported. A tunnel is defined as five SAs: one IKE, two AH and two ESPs. A data plane consists of ESP encapsulated in AH, encapsulated in IP.

Firewall

At least 4000 concurrent sessions are supported through the Cisco IOS firewall.

VLANs

A total of 8 VLANs can be configured on the 10/100BaseT ports.

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 of all three levels are listed below.

Resolved Caveats - Cisco IOS Release 12.3(8)YI3

- CSCsb24007

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>

- CSCeh60551

Symptom: Certain malformed client certificates may cause an AP running 12.3.2.JA2 or 12.3.4.JA to crash when EAP-TLS is used.

Workaround: Issue a new client certificate.

- CSCei61732
Cisco IOS may permit arbitrary code execution after exploitation of a heap-based buffer overflow vulnerability. Cisco has included additional integrity checks in its software, as further described below, that are intended to reduce the likelihood of arbitrary code execution.
Cisco has made free software available that includes the additional integrity checks for affected customers.
This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20051102-timers.shtml>.
- CSCsa54608
The Cisco IOS Firewall Authentication Proxy for FTP and/or Telnet Sessions feature in specific versions of Cisco IOS software is vulnerable to a remotely-exploitable buffer overflow condition.
Devices that do not support, or are not configured for Firewall Authentication Proxy for FTP and/or Telnet Services are not affected.
Devices configured with only Authentication Proxy for HTTP and/or HTTPS are not affected.
Only devices running certain versions of Cisco IOS are affected.
Cisco has made free software available to address this vulnerability. There are workarounds available to mitigate the effects of the vulnerability.
This advisory will be posted at http://www.cisco.com/warp/public/707/cisco-sa-20050907-auth_proxy.shtml
- CSCef10564
Radio systems messages show up with no radio present on reload.
- CSCei19059
tracebacks for dot11 card while querying the ENTITY-MIB.
- CSCei22782
Symptom: Power value advertised is in mW instead of dBm.
Conditions: Beacon and probe packet that publish power values.
Workaround: Use legacy, instead of 802.11d.
- CSCeg51272
Symptoms: Router reloads while executing the show ip nbar protocol-discovery command.
Conditions: NBAR protocol-discovery is enabled on the Virtual-Template interface.
Workaround: There is no workaround.
- CSCeh23780
Symptoms: Router fails to boot.
Conditions: This symptom occurs when you change the Cisco IOS image from an image that does not include the fix for caveat CSCsa50959, to an image that does include the fix for caveat CSCsa50959.
Workaround: There is no workaround.
- CSCeh92096
Bridge MIB not Populated.
- CSCei16040
VendorType and ParentRelPos of ENTITY-MIB displays incorrect values.

- CSCei16679
Symptoms: Clients behind AP cannot ping clients behind repeater/WGB.
Conditions: With fragmentation threshold set on both airlink and repeater to 256, cln1 and cln2 cannot be pinged when the packet size is above the fragmentation threshold, but it can be pinged when the packet is not fragmented.
Workaround: There is no workaround.
- CSCsa82225
Symptom: It takes over five minutes for the adsl line to be trained. If you perform the 'no shutdown' command at the adsl/atm interface, wait for the line to come up and then remove the cable, it will take approximately 15 minutes for the %LINEPROTO-5-UPDOWN message to be printed on the console.
Condition: This occurs when the CLI 'dsl enable-training-log' under 'int atm 0' is active.
Workaround: Enter 'no dsl enable-training-log.'
- CSCsb19208
Symptom: CISCO-DSL-CPE-MIB: some values are not initialized, including cdcAssetVendorType.
Conditions: A Cisco 1800 router with CISCO-DSL-CPE-MIB support.
Workaround: There is no workaround.

- CSCsb43655

Symptom: Incoming packets (larger than 1400 bytes) are counted as "input errors" for the ATM interface. The ATM error debug reports "ATM0: AAL5 rx errors (status = 0C100000)" which suggests a CNG is experienced during cells traversing. During testing, a consistent pattern of lost packets was not found.

Conditions: A router configured as PPPoE client or pure RFC1483 bridging.

Workaround: There is no workaround.
- CSCeg15044

Symptoms: Although there are free tty lines, you cannot make a Telnet connection and a "No Free TTYs error" message is generated.

Conditions: This symptom is observed when there are simultaneous Telnet requests.

Workaround: There is no workaround.
- CSCeg12134

Symptoms: When sending multicast traffic over an IPsec tunnel, a memory leak occurs.

Conditions: This symptom is observed on a Cisco router running Cisco IOS Release 12.3T when both IP CEF and hardware encryption are configured.

Workaround: Switch to software encryption for a while, and then switch back to hardware encryption.

Alternate Workaround: Disable IP CEF.
- CSCeg68557

Symptoms: When there is a failure between two IPsec peers, DPD can detect that the communication fails. When there are multiple phase 2 SAs and DPD failures, phase 1 SAs are deleted, but only one phase 2 SA is deleted.

Further Problem Description: If Reverse Route Injection is also configured, the corresponding route is not deleted.

Conditions: This is observed on a Cisco router that is configured for IPsec ISAKMP when there are multiple ACEs in a dynamic crypto ACL, causing multiple phase 2 SAs to be generated.

Workaround: Enter the **clear crypto sa** command.
- CSCeh35823

Symptoms: When the router detects "invalid identity" failures while decrypting IPsec packets, a memory leak occurs for the packet memory that is associated with these failed packets.

Conditions: This symptom is observed only when an "invalid identity" error occurs, which is an uncommon error that indicates that the originating router does not send packets according to what was originally negotiated. However, if there is another error that causes a "bad" decryption, the packet could be invalid and may also cause the symptom to occur.

Workaround: There is no workaround.
- CSCeh46867

Unmatched SSID probe request response causes TX stuck.
- CSCeh61857

Symptom: Unable to configure anything under non-dot11 subinterface, including IP address.

Workaround: None before code change.

- CSCei27330
Symptoms: A router that is configured for Dynamic Multipoint VPN (DMVPN) may frequently generate the following error message:
%SYS-2-BADSHARE: Bad refcount in datagram_done
Conditions: This symptom is observed on the routers that function as a DMVPN spoke.
Workaround: There is no workaround.
- CSCin96534
Symptoms: Routers crash while enabling dot1x
Conditions: The crash is seen only when enabling dot1x on onboard FE interface, not on the switchports.
Workaround: There is no workaround.
- CSCsb13034
IPv6 multicast traffics does not get fast-switched.
- CSCsb56224
Symptom: Buffering problem on aux line on the Cisco 871 and Cisco 851 series routers. The last character of AT commands from the router AUX line (line 1) is displayed only after first "RETURN" character. After the second "RETURN" character, the AT command is executed by the analog modem. This behaviour is causing problems with chat scripts and sending AT commands to the analog modem (impossible to dialout using chat scripts). It is possible to send AT commands to the modem using reverse telnet (AUX port), but after each command, hit the Enter key twice. Entering command characters (like AT), the letter A is echoed after pressing T, the letter T is echoed after next character and so on.
Conditions: This problem is observed in the Cisco 871 and Cisco 851 series router.
Workaround: There is no workaround.
- CSCsa48125
Symptoms: Outgoing calls fail on ISDN Non-Facility Associated Signaling (NFAS) group members that do not have a D-channel.
Conditions: The symptom is observed when outgoing calls are made via NFAS group members that have the **nfas_d none** keyword configured.
Workaround: There is no workaround.
- CSCee68153
Show wlccp ap mob forwarding, show dot asso mission from show tech.
- CSCsb70282
1812 router should close 2887 wlccp port.
- CSCei30235
EAP user-name field length restricted to 64 bytes.

Open Caveats - Cisco IOS Release 12.3(8)YI2

- CSCeg04695
Previously associated clients intermittently cannot reassociate upon reload.

- CSCeh85556
LEAP intermittent failure when dot1x reauth-period config;reboot req.
- CSCeh90412
WPA-PSK intermittently fails.
- CSCei06052
Applying “IP unnumbered vlan1” on dot11 sub-interface doesn't work.

Resolved Caveats - Cisco IOS Release 12.3(8)YI2

- CSCeh82849
Not all wireless clients are shown under dot11 network-map.
- CSCef69209
Traceback generated on SNMP query of CISCO-IETF-DOT11-QOS-EXT-MIB
- CSCsa85925
NAS-Port-Type needs to be consistent with WNBUS AP.
- CSCeh86927
FW broken on dot11 with VLAN.
- CSCin90771
Airlink IF-MIB - ifInUcastPkts Counter32 value decreasing.
- CSCeh83208
Router crashes with Airlink during client LEAP authentication.
- CSCeh80851
Remove ipv6 commands under dot11 interface.
- CSCeh80843
Can configure aes-ccm encryption mode, clients will be disassociated.
- CSCeh76767
PSP client may stuck in dead lock, keep associated, but no traffic.
- CSCeh73210
When booting with no startup configuration, the line “station-role root” is missing from Dot11Radio0 interface.
- CSCeh72067
Shared/static wep function broken in latest.
- CSCeh51374
loss of range with latest image.
- CSCeg03958
Router crash at k_cvdpnBundleEntry_get while doing SNMP walk.

- CSCsa40962
Memory leak in Crypto IKMP process on IOS EzVPN server.
- CSCeh80746
See ASSERTION FAILED: when trying to associate more than 25 clients.

Open Caveats - Cisco IOS Release 12.3(8)Y11

- CSCef14879
rtsp_smi test intermittently fails; some rtsp-data may be missing.
- CSCeg79282
Policy may not classify packets with subprotocols.
- CSCeh72067
Static wep fails if transmit-keys between router and client are different.
- CSCeg04695
Previously associated clients are sometimes not reassociated upon router reload.
- CSCeh69802
Tx side of 802.11g radio fluctuates during stress testing.
- CSCeh80843
Unsupported wireless encryption mode “aes-ccm” displays error message, but results in a partial “encryption mode ciphers” configuration that can disassociate clients.
- CSCeh74272
show dot11 association sometimes shows incorrect IP address.
- CSCeh80851
IPv6 commands under dot11 interface to be removed.

Resolved Caveats - Cisco IOS Release 12.3(8)Y11

- CSCeg39083
Traceback messages are generated with the dial string rotation feature.
- CSCef63944
Alignment/spurious errors occur while testing IPsec-realtime DNS.
- CSCeh06336
WPA-PSK and WPA 802.1x authentication, such as network-eap or open eap, can be configured simultaneously on the same SSID.

Workaround: While the GUI prevents this invalid configuration, CLI users need to make sure that both WPA-PSK and WPA 802.1x authentication are not configured on the same SSID.

Additional References

The following sections describe the documentation available for the Cisco 1801, 1801W, 1802, 1802W, 1803, 1803W, 1811, 1811W, 1812, and 1812W series routers. Typically, these documents consist of hardware and software installation guides, Cisco IOS configuration and command references, system error messages, feature modules, and other documents. Documentation is available as printed manuals or electronic documents, except for feature modules, which are available online on Cisco.com in pdf or html form.

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

- [Release-Specific Documents, page 15](#)
- [Platform-Specific Documents, page 15](#)

Release-Specific Documents

The following documents are specific to Release 12.3 and apply to Cisco IOS Release 12.3(8)YI. They are located on [Cisco.com](#):

- *Cross-Platform Release Notes for Cisco IOS Release 12.3T*
- *Field Notices:* http://www.cisco.com/warp/public/tech_tips/index/fn.html.
- *Caveats for Cisco IOS Release 12.3 and Caveats for Cisco IOS Release 12.3(11)T*

Platform-Specific Documents

Hardware installation guides, configuration and command reference guides, and additional documents specific to the Cisco 1801, 1801W, 1802, 1802W, 1803, 1803W, 1811, 1811W, 1812, and 1812W series routers are available on [Cisco.com](#) at the following location:

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

Feature Modules

Feature modules describe new features supported by Cisco IOS Release 12.3 and Cisco IOS Release 12.4(6)XE, 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.

Cisco Feature Navigator

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

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

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

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

Cisco IOS Software Documentation Set

The Cisco IOS software documentation set consists of the Cisco IOS configuration guides, Cisco IOS command references, and several other supporting documents.

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. *Cisco IOS Software Documentation* is available in html or pdf form.

Select your release and click the command references, configuration guides, or any other Cisco IOS documentation you need

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feed-back, security guidelines, and also recommended aliases and general Cisco documents, 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>

Use this document in conjunction with the documents listed in the “Additional References” section.

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, *Packet*, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath 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. (0705R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007, Cisco Systems, Inc. All rights reserved

