Release Notes for the Cisco 1800 Series Fixed Routers for Cisco IOS Release 12.4(2)XA

April 24, 2006
Cisco IOS Release 12.4(2)XA
OL-9451-01Rev A3

These release notes describe new features and significant software components for the Cisco 1800 series fixed routers that support the Cisco IOS Cisco IOS Release 12.4(2)XA releases. 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 12.4T* located on Cisco.com and the Documentation CD.

For a list of the software caveats that apply to Cisco IOS Release 12.4(2)XA, see the "Caveats" section on page 8 and *Caveats for Cisco IOS Release 12.4(2)T*. The online caveats document is updated for every maintenance release and is located on Cisco.com and the Documentation CD.

Contents

System Requirements

This section describes the system requirements for Cisco IOS Release 12.4(2)XA and includes the following sections:

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

Memory Requirements

Table 1 describes the memory requirements for the Cisco IOS feature sets supported by Cisco IOS Cisco IOS Release 12.4(2)XA on the Cisco 1800 series routers.

Table 1 Recommended Memory for the Cisco 1800 Series Routers with Cisco IOS Release 12.4(2)XA

Platform	Image Name	Feature Set	Image	Flash Memory	DRAM
1801 1802 1803	Cisco 180x Series IOS ADV. ENTERPRISE SERVICES	IOS ADV. ENTERPRISE SERVICES	c180x-adventerprisek9-mz	32	128
	Cisco 180x Series IOS ADV. IP SERVICES	IOS ADV. IP SERVICES	c180x-advipservicesk9-mz	32	128
	Cisco 180x Series IOS IP BROADBAND	IOS IP BROADBAND	c180x-broadband-mz	32	128
1811 1812	Cisco 181x Series IOS ADV. ENTERPRISE SERVICES	IOS ADV. ENTERPRISE SERVICES	c181x-adventerprisek9-mz	32	128
	Cisco 181x Series IOS ADV. IP SERVICES	IOS ADV. IP SERVICES	c181x-advipservicesk9-mz	20	128
1841	Cisco 1841 IOS AISK9-AESK9 FEAT SET FACTORY UPG FOR BUNDLES Cisco 1841 IOS ASK9-AESK9 FEAT SET FACTORY UPG FOR BUNDLES Cisco 1841 IOS BB-AESK9 FEAT SET FACTORY UPG FOR BUNDLES	IOS AISK9-AESK9 FEAT SET FACTORY UPG FOR BUNDLES IOS ASK9-AESK9 FEAT SET FACTORY UPG FOR BUNDLES IOS BB-AESK9 FEAT SET FACTORY UPG FOR BUNDLES	c181x-adventerprisek9-mz	32	128

Table 1 Recommended Memory for the Cisco 1800 Series Routers with Cisco IOS Release 12.4(2)XA (continued)

Platform	Image Name	Feature Set	Image	Flash Memory	DRAM
1841	Cisco 1841 IOS ASK9-AISK9 FEAT SET FACTORY UPG FOR BUNDLES Cisco 1841 IOS BB-AISK9 FEAT SET FACTORY UPG FOR BUNDLES	IOS ASK9-AISK9 FEAT SET FACTORY UPG FOR BUNDLES IOS BB-AISK9 FEAT SET FACTORY UPG FOR BUNDLES	c181x-advipservicesk9-mz	20	128
	Cisco 1841 IOS BB-ASK9 FEAT SET FACTORY UPG FOR BUNDLES	IOS BB-ASK9 FEAT SET FACTORY UPG FOR BUNDLES	c1841-advsecurityk9-mz	32	128
	Cisco 1841 IOS BB-SPSK9 FEAT SET FACTORY UPG FOR BUNDLES	IOS BB-SPSK9 FEAT SET FACTORY UPG FOR BUNDLES	c1841-spservicesk9-mz	32	128
	IOS 1841 ENTERPRISE BASE	ENTERPRISE BASE	c1841-entbasek9-mz	32	128
	IOS 1841 ENTERPRISE SERVICES W/O CRYPTO	ENTERPRISE SERVICES W/O CRYPTO	c1841-entservices-mz	64	192
	IOS 1841 ENTERPRISE SERVICES	ENTERPRISE SERVICES	c1841-entservicesk9-mz	64	192
	IOS 1841 IP BASE W/O CRYPTO	IP BASE W/O CRYPTO	c1841-ipbase-mz	32	128
	IOS 1841IP BASE	IP BASE	c1841-ipbasek9-mz	32	128
	IOS 1841 SP SERVICES	SP SERVICES	c1841-spservicesk9-mz	64	128

Hardware Supported

Cisco IOS Cisco IOS Release 12.4(2)XA supports the following Cisco 1800 series routers:

- Cisco 1801
- Cisco 1802
- Cisco 1803
- Cisco 1811
- Cisco 1812
- Cisco 1841

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 1800 series routers, which are available on Cisco.com and the Documentation CD at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/1800/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:

Cisco Product Documentation: **Access Servers and Access Routers**: **Modular Access Routers**: **Cisco 1800 Series Routers**: **<platform_name>**

Determining the Software Version

To determine which version of Cisco IOS software is currently running on your Cisco 1800 series router, log in to the router and enter the **show version** EXEC command. The following sample output from the **show version** command indicates the version number.

```
router> show version
Cisco Internetwork Operating System Software
IOS (tm) C1800 Software (C1800-Y7-MZ), Version 12.4(2)XA, EARLY DEPLOYMENT RELEASE
SOFTWARE (fc1)
Synched to technology version 12.4(2)T
```

Upgrading to a New Software Release

For general information about upgrading to a new software release, refer to the *Software Installation and Upgrade Procedures* located at 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 12.4(2)XA supports the same feature sets as Releases 12.4 and 12.4(2)T, but Cisco IOS Release 12.4(2)XA includes new features supported by the Cisco 1800 series routers.

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 lists the feature and feature sets supported in the Cisco IOS Cisco IOS Release 12.4(2)XA.

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(2)XA” indicates that the feature was introduced in 12.4(2)XA. 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 selected list of features, which are cumulative for Release 12.4(2)*nn* early deployment releases only (*nn* identifies each early deployment release). The tables do not list all features in each image—additional features are listed in *Cross-Platform Release Notes for Cisco IOS Release 12.4(2)T* and Release 12.4(2)T Cisco IOS documentation.

Table 2 Cisco IOS Release 12.4(2)XA Feature List for Cisco 1800 Routers

Feature	In	Image
ATM Oversubscription for DSL	Yes	All. See Table 1 for image names.
Multiqueue Command	Yes	All. See Table 1 for image names.
Protected Port	Yes	All. See Table 1 for image names.
Transmit Power Control (TPC)	Yes	All. See Table 1 for image names.
Wi-Fi 80211h and Dynamic Frequency Selection (DFS)	Yes	All. See Table 1 for image names.

New and Changed Information

This section contains the following information:

New Hardware Features in Release 12.4(2)XA and 12.4(2)XA1

Single Port G.SHDSL WAN Interface Card (WIC-1SHDSL-V3)

A single port multi line G.SHDSL WAN interface card (WIC), or WIC-1SHDSL-V3, provides Multirate Symmetrical High-Speed Digital Subscriber Line (G.SHDSL) feature support for Two-Wire Mode and Four-Wire Mode for SHDSL on the Cisco 1700 series, Cisco 1800 series, Cisco 26xxXM, Cisco 2691, Cisco 2800, Cisco 3700 series, and Cisco 3800 series modular access routers. The WIC-1SHDSL-V3 incorporates the latest firmware and the latest circuitry. For more information about this feature, see the following document:

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_7/gt4wire.htm

New Software Features in Cisco IOS Release 12.4(2)XA and 12.4(2)XA1

The following sections describe the new software features supported by the Cisco 1800 series routers for Cisco IOS Release 12.4(2)XA and 12.4(2)XA1.

ATM Oversubscription for DSL

The ATM Oversubscription for DSL feature lets you configure bandwidth oversubscription on Cisco xDSL interfaces up to a defined bandwidth. You can configure variable bit rate (VBR) and unspecified bit rate plus (UBR+) service classes for permanent virtual circuit (PVC) connections with a sum of sustainable cell rates (SCRs) greater than the line rate, which means you can configure an infinite oversubscription amount of bandwidth. Each PVC receives up to its configured SCR value of traffic, and PVCs with higher SCR values receive more bandwidth.

To enable ATM oversubscription for DSL, use the ATM oversubscribe factor command in ATM configuration mode. To disable ATM oversubscription for DSL, use the no form of this command.

atm oversubscribe factor *factor*
no atm oversubscribe factor *factor*

To configure unspecified bit rate (UBR) quality of service (QoS) and specify the output peak cell rate and output minimum guaranteed cell rate for an ATM PVC, PVC range, switched virtual circuit (SVC), virtual circuit (VC) class, or VC bundle member, use the **ubr+** command in the appropriate command mode. To remove the UBR+ parameters, use the **no** form of this command.

ubr+ *output-pcr output-mcr* [*input-pcr*] [*input-mcr*]
no ubr+ *output-pcr output-mcr* [*input-pcr*] [*input-mcr*]

Multiqueue Command

The **multiqueue** command enables a priority and a regular (nonpriority) queue for traffic streams. When the command is enabled and there are multiple classes of packet streams over the same PVC, packets coming from the streams that have priority values configured in a policy map are sent to the high priority queue. Packets from all other streams will be sent over the low priority queue. Multiqueue is intended for configuring DSL lines and permits configuring one data flow in a priority queue. If you have configured more than one flow in a priority queue, the latency for delay-sensitive traffic flow may not be guaranteed.

The multiqueue approach does not work well with applications such as MLPPP with interleave and Crypto. This is because MLPPP uses the same sequence numbering scheme for interleaved packets as the multiqueue approach. For example, if there are a voice and two data packets interleaved, the MLPPP sequence numbers for these packets could be 1 for the first data packet, 2 for the voice packet, and 3 for a second data packet. In the multiqueue approach, the voice packet with MLPPP sequence number 2 would go out before the data packet with MLPPP sequence number 1. This would result in out-of-order sequencing of packets as far as MLPPP is concerned, and result in unexpected behavior. The same problems apply to the Crypto application. The multiqueue approach is disabled by default so that when MLPPP and the Crypto applications are used with DSL the network will not be disrupted by upgrading to an image with multiqueue support.

To enable two queues to prioritize multiple classes of packet streams over the same PVC, use the **multiqueue** command in either the PVC- or VC-class configuration modes. To return to a single queue, use the **no** form of this command.

multiqueue
no multiqueue

Protected Port

The PVLAN edge (protected port) is a feature that has only local significance to the switch (unlike private VLANs), and there is no isolation provided between two protected ports located on different switches. A protected port does not forward any traffic to any other port that is also protected in the same switch. Traffic cannot be forwarded between protected ports at Layer 2, all traffic passing between protected ports must be forwarded through a Layer 3 device.

Transmit Power Control (TPC)

Transmit Power Control (TPC) for Cisco Aironet access points is used by Cisco Aironet access points to relay transmit power information to Cisco and Cisco-compatible wireless client devices. Client devices use the TPC information in conjunction with the access point's signal strength to calculate path loss and the transmit power necessary for the client to reach the Cisco Aironet access point. This feature extends client device battery life.

The following link provides instructions on controlling TPC:

http://www.cisco.com/univercd/cc/td/doc/product/wireless/airo1100/accsspts/i1234ja/i1234sc/s34rf.htm#wp1017196

Wi-Fi 80211h and Dynamic Frequency Selection (DFS)

Dynamic Frequency Selection (DFS) for Cisco Aironet access points is configured at the factory for use in Europe and Singapore to detect radar signals such as military and weather sources and switch channels on the access points.

The following link provides information to configure DFS:

http://www.cisco.com/univercd/cc/td/doc/product/wireless/airo1100/accsspts/i1234ja/i1234sc/s34rf.htm#wp1088457

Changed Software Features in Cisco IOS Release 12.4(2)XA and 12.4(2)XA1

Table 3 lists the feature history for ATM Mode for Two-Wire or Four-Wire SHDSL

Table 3 Feature History for ATM Mode for Two-Wire or Four-Wire SHDSL

Release	Modification
12.3(4)XD	This feature (WIC-1SHDSL-V2) was introduced on the Cisco 2600 series and Cisco 3700 series routers to add 4-wire support. 2-wire support was previously available in Cisco IOS Release 12.2(8)T. For more information, see the document 1-Port G.SHDSL WAN Interface Card for Cisco 2600 Series and Cisco 3600 Series Routers.
12.3(4)XG	This feature (WIC-1SHDSL-V2) was integrated into Cisco IOS Release 12.3(4)XG on the Cisco 1700 series routers.
12.3(7)T	This feature (WIC-1SHDSL-V2) was integrated into the Cisco IOS Release 12.3(7)T on the Cisco 2600 series, Cisco 3631, and Cisco 3700 series routers. Cisco 1700 series routers do not support the WIC-1SHDSL-V2 in this release.
12.3(4)XG1	Support for the auto line-mode feature was added.

Table 3 Feature History for ATM Mode for Two-Wire or Four-Wire SHDSL (continued)

Release	Modification
12.3(11)T	Support for the following was added: additional annex parameters for Cisco 1700, Cisco 2600, Cisco 2800, Cisco 3631, Cisco 3700, and Cisco 3800 series routers; the HDSL2-SHDSL-LINE-MIB (RFC3276); and support for the ATM Mode for SHDSL feature was added for Cisco 2800 series and Cisco 3800 series routers.
12.3(14)T	Support was added for Cisco 1800 series routers and the Cisco 2801 integrated services router.
12.4(2)XA and 12.4(2)XA1	Support was added for the WIC-1SHDSL-V3 interface card.

Limitations and Restrictions

There are no known limitations or restrictions.

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 12.4(2)T are also in Cisco IOS Release 12.4(2)XA. For information on caveats in Cisco IOS Release 12.4(2)T, refer to the *Caveats for Cisco IOS Release 12.4(2)T* document. This document lists severity 1 and 2 caveats; the documents are located on Cisco.com and the Documentation CD.

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.

This section contains the following caveat information:

Resolved Caveats - Release 12.4(2)XA2

- CSCsc36096: 1812 FE flap after plugging out/in cable or reload

Symptoms: On the Cisco1812 , FastEthernet interface(FastEthernet0 or FastEthernet1) might randomly go down and back up in some situation.

Conditions: This symptom occurs when you plug out and back in, or when you do a shut/no shut. or after a reload.

This symptom depends on the timing: Sometimes it cannot be seen in these situation above. Under the situation using RIP, it could be that flapping interface does not appear on RIP database and accordingly Cisco 1812 does not send rip update packets.

Workaround: Use the **damping** command in interface configuration mode.

- CSCsc36118: The default route is removed if the one of multiple PPPoE session down

  Symptoms: The default route is removed if the one of multiple PPPoE session down.

  Conditions: This problem occurs when you configure multiple PPPoE which connect to the same BRAS or same LNS if using L2TP and **ppp ipcp route default** is configured using Cisco IOS Software Release 12.4(2)T1.

  Workaround: There is no workaround. However, you can still turn routing on. For example, configure the multiple default routes pointing to the dialer interface(s) as the next hop.

- CSCsd50841: IPsec VPN Traffic from c800/c1800 stops after several rekeys

  Symptoms: When running an 800 router as an EzVPN client CPU over 50%, traffic may stop being passed after one or more IPSEC re-keys. When this happens, "PacketsDropped" and "Invalid Flow Error" counters begin incrementing in the cryptoaccelerator stats. This also affects 1800 routers.

  Conditions: This problem occurs on Cisco 870 and Cisco 1800 routers when the IPSec flow ID reaches value 300 (1800) or 40 (870). Workaround is to clear the SA to go to next value.

  Workaround: Clear the IPSEC SAs to restart traffic, or set a longer IPSEC rekey interval.

Open Caveats - Release 12.4(2)XA2

There are no known open caveats in this release.

Resolved Caveats - Release 12.4(2)XA1

- CSCsb76796: Seconds granularity support for X.25 encapsulation VC idle timeout

  Symptoms: This caveat fix enhances the **x25 idle** and **x25 map** interface configuration mode commands to support seconds granularity for X.25 idle VC timeout for X.25 encapsulation VCs.

  Workaround: Use the enhanced **x25 idle** command with seconds option:

```
Router(config-if)#x25 idle ?
  <0-255>  Minutes; 0 to never clear

tinaturner(config-if)#x25 idle 0 ?
  <1-59>  Seconds; valid for encapsulation VCs only
  <cr>

tinaturner(config-if)#x25 idle 0 10 ?
  <cr>
```

  Use the enhanced **x25 map** command with seconds option:

```
Router(config-if)#x25 map ip 2.132.0.9 200910 idle ?
  <0-255>  Idle time (minutes)
```

```
tinaturner(config-if)#x25 map ip 2.132.0.9 200910 idle 0 ?
  <1-59>          Idle time (seconds)
  accept-reverse  Accepting incoming reverse-charged calls
  broadcast       Send broadcasts to this host
  compress        Use payload Compression
  cug             Specify a Closed User Group number
  method          Specify encapsulation method
  no-incoming     Do not use map for incoming Calls
  no-outgoing     Do not use map for outgoing Calls
  nudata          Specify user formatted network user ID
  nuid            Specify Cisco formatted network user ID
  nvc             Set number of virtual circuits for this map
  packetsize      Request data packet sizes for originated calls
  reverse         Use reverse charging on originated calls
  roa             Specify ROA
  throughput      Request bandwidth in X.25 network
  transit-delay   Specify transit delay (msec)
  windowsize      Request window sizes for originated calls
  <cr>

Router(config-if)#x25 map ip 2.132.0.9 200910 idle 0 10 ?
  accept-reverse  Accepting incoming reverse-charged calls
  broadcast       Send broadcasts to this host
  compress        Use payload Compression
  cug             Specify a Closed User Group number
  method          Specify encapsulation method
  no-incoming     Do not use map for incoming Calls
  no-outgoing     Do not use map for outgoing Calls
  nudata          Specify user formatted network user ID
  nuid            Specify Cisco formatted network user ID
  nvc             Set number of virtual circuits for this map
  packetsize      Request data packet sizes for originated calls
  reverse         Use reverse charging on originated calls
  roa             Specify ROA
  throughput      Request bandwidth in X.25 network
  transit-delay   Specify transit delay (msec)
  windowsize      Request window sizes for originated calls
  <cr>
```

- CSCsb90481: Bad enque and traceback when ping with packets > 1445 bytes

  Symptoms: The following error and traceback messages are shown on the console:

  ```
  *Sep 19 15:04:17.027: %SYS-2-LINKED: Bad enqueue of 46ECBC6C in queue 4678EF4C
  -Process= "<interrupt level>", ipl= 4
  -Traceback= 0x414C292C 0x400AF600 0x4277FB60 0x4036E0EC 0x41A8CE98 0x400E0BD0
  0x40067050 0x42C555B0 0x42C559CC 0x42B06718 0x430B4AA8 0x4312FEB4 0x4313882C
  0x4313AF2C 0x43124AFC 0x43124FA4
  ```

  Conditions: This occurs when you ping with packets > 1445 bytes

  Workaround: There is no workaround.

- CSCsc22408: Radio interface stops functioning w/ 40+ client after some time

  Symptoms: A Cisco 1811 with Cisco IOS Release 12.4(2)T is seeing disassocation on all clients after a random period of time (~1hour or 2). Entering the **show tech** command shows a high drop on both input and output queues as well as an indication of queue1 stuck: Dot11Radio0 is up, line protocol is up.

  Workaround: Enter the **shut/no shut** command on the radio interface to bring the association back up.

- CSCsc25724: Slow switching performance with PPPoE encap'd traffic

Symptoms: The maximum cef or fast switching capacity of PPPoE encapsulated packets on the Cisco 181x platform can be significantly lower than for other encapsulations. This issue is typically only noticed however under fairly extreme test conditions.

Conditions: This problem occurs when the following symptoms are present:

- High traffic rate cef or fast switching on Cisco 181x platform
- PPPoE encapsulation

Workaround: There is no workaround.

- CSCsc25964: PPPoE dialer CEF VAI adjacency does not honor dialer **ip mtu**

  Symptoms: A PPPoE client router does not honor the **ip mtu** command settings whey they are configured on the PPPoE dialer interface when the IP MTU is different from the interface MTU.

  Fragmentation of IP packets larger than the configured IP MTU will not happen, which can create problems in a PPPoE environment.

  Conditions: This symptom occurs whenever a v-access is cloned from the dialer interface and could be PPPoE, multilink or PPPoA.

  Workaround: Configure the **interface mtu** command to the required value.

Open Caveats - Cisco IOS Release 12.4(2)XA1

There are no open caveats in this release.

Resolved Caveats - Cisco IOS Release 12.4(2)XA

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

- CSCed27956: TCP checks should verify ack sequence number.

  A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

  All Cisco products which contain TCP stack are susceptible to this vulnerability.

  This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS® software.

  A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml.

Open Caveats - Release 12.4(2)XA

- CSCeh97137: newRoot & topologyChange Traps are not generated for Bridge Mib

  Symptoms: The topology change trap is not generated while state from listening to learning & learning to forwarding is getting change on an interface. The new root trap is not generated while bridging is enabled & disabled on interfaces and while changing the mac address to make a new root.

  Workaround: There is no workaround.

Related Documentation

The following sections describe the documentation available for the Cisco 1800 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 and the Documentation CD.

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

- Release-Specific Documents
- Platform-Specific Documents

Release-Specific Documents

The following documents are specific to Release 12.4 and apply to Cisco IOS Release 12.4(2)XA. They are located on Cisco.com and the Documentation CD (under the heading Service & Support):

- To reach the *Cross-Platform Release Notes for Cisco IOS Release 12.4(2)T*, click this path:

  Technical Documents: **Cisco IOS Software**: **Release 12.4**: **Release Notes**: **Cisco IOS Release 12.4(2)T**

- To reach product bulletins, field notices, and other release-specific documents, click this path:

  Technical Documents: **Product Bulletins**

- To reach the *Caveats for Cisco IOS Release 12.4* and *Caveats for Cisco IOS Release 12.4(2)T* documents, which contain caveats applicable to all platforms for all maintenance releases of Release 12.4, click this path:

  Technical Documents: **Cisco IOS Software**: **Release 12.4**: **Caveats**

Note If you have an account with Cisco.com, you can also use the Bug Toolkit to find selected 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.

Platform-Specific Documents

Hardware installation guides, configuration and command reference guides, and additional documents specific to the Cisco 1800 series routers are available on Cisco.com and the Documentation CD at the following location:

http://www.cisco.com/univercd/cc/td/doc/product/access/acs_mod/1800/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:

Cisco Product Documentation: **Access Servers and Access Routers**: **Modular Access Routers**: Series Integrated Services Routers: **<platform_name>**

Feature Navigator

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. Feature Navigator is available 24 hours a day, 7 days a week.

To access Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, e-mail the Contact Database Administration group at cdbadmin@cisco.com. If you do not have an account on Cisco.com, go to http://www.cisco.com/register and follow the directions to set up an account.

To use 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.

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/fn

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 that are shipped with your order in electronic form on the Documentation CD-ROM—unless you specifically ordered 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. The Cisco IOS software documentation set is available on Cisco.com and on the Documentation CD-ROM.

On Cisco.com:

Products & Services: IOS Software: Cisco IOS Software Releases 12.4 Mainline: Technical Documentation: Master Indices

On the Documentation CD-ROM at:

Product Documentation: Cisco IOS Software: **Cisco IOS Release 12.4: Configuration Guides and Command References**

Release 12.4 Documentation Set

Table 4 describes the contents of the Cisco IOS Release 12.4 software documentation set, which is available in both electronic and printed form.

Note You can find the most current Cisco IOS documentation on Cisco.com and the Documentation CD-ROM. These electronic documents may contain updates and modifications made after the hard-copy documents were printed.

Note Some aspects of the complete Cisco IOS Release 12.4 software documentation set might not apply to the Cisco 1800 router.

Table 4 Cisco IOS Release 12.4 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

Table 4 Cisco IOS Release 12.4 Documentation Set (continued)

Books	Major Topics
• 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
• 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

Table 4 Cisco IOS Release 12.4 Documentation Set (continued)

Books	Major Topics
• 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
• 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 12.4-Based Limited Lifetime Releases • New Features in Release 12.4T • Release Notes (Release note and caveat documentation for 12.4-based releases and various platforms)	

Service and Support

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain online 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 with these tasks:

- 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

If you want to obtain customized information and service, you can self-register on Cisco.com. To access Cisco.com, go to this URL:

http://www.cisco.com

Technical Assistance Center

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

Cisco TAC inquiries 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.

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

Cisco TAC Web Site

You can use the Cisco TAC Web Site 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 this URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco service 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 this URL to register:

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

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

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

If you have Internet access, we recommend that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. 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 automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this 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). When you call the center, please have available your service agreement number and your product serial number.

Open Source License Acknowledgements

The following notices pertain to this software license.

OpenSSL/Open SSL Project

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

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

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

License Issues

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

OpenSSL License:

Copyright © 1998-2007 The OpenSSL Project. All rights reserved.

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

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

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

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

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

Original SSLeay License:

Copyright © 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

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

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

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

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

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

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

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

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

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

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

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