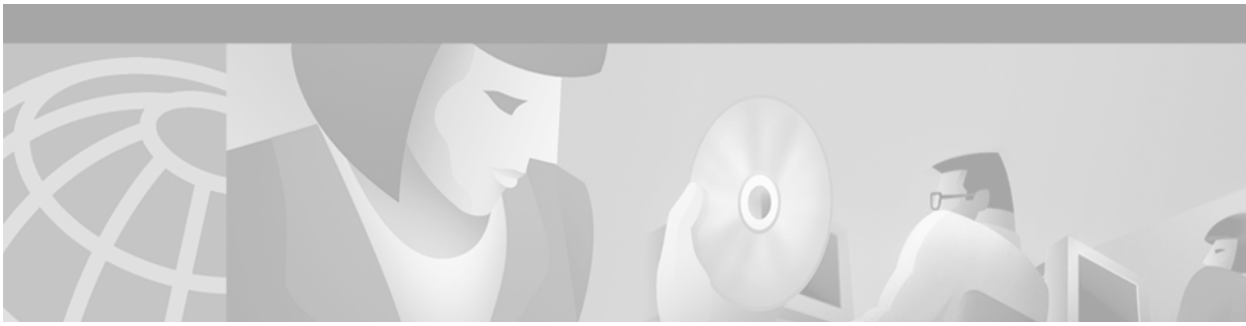

Release Notes for Cisco IOS Release 12.1(6)E Software Feature Packs for the Cisco 7100 Series

June 25, 2001

Note You can find the most current Cisco IOS documentation on Cisco.com. This set of electronic documents may contain updates and modifications made after CD-ROM documents are created.

These release notes for the Cisco 7100 series describe the enhancements provided in Cisco IOS Release 12.1(6)E2. These release notes are updated as needed.

For a list of the software caveats that apply to Cisco IOS Release 12.1(6)E2, see the "Caveats" section on page 8, the *Caveats for Cisco IOS Release 12.1* document, and the *Release Notes for Cisco 7000 Family for Cisco IOS Releases 12.0(5)XE through 12.0(7)XE1*. All caveats in Cisco IOS Release 12.1(2) and Cisco IOS Release 12.0(7)XE1 are also in Cisco IOS Release 12.1(6)E2.

Use these release notes with the *Cross-Platform Release Notes for Cisco IOS Release 12.1* and the *Release Notes for Cisco 7000 Family for Cisco IOS Release 12.0(5)XE Through 12.0(7)XE1* located on Cisco.com and on the Documentation CD-ROM.

Contents

These release notes describe the following topics:

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

Introduction

List of Terms

The following terms are used throughout this document:

Feature—Networking functionality that supports network technology and hardware. For example: Double Authentication, IP Multicast over Token Ring, Voice Over IP, PPP over ATM, and so forth.

Feature Set—A group of features. For example: IP, IP Plus, Enterprise Plus, IP IPSec 56, and so forth.

Image—Software code containing a Cisco IOS feature set. The image file nomenclature, such as c800-y6-mw, c1000-bnsy40-mz, and c2500-g-l, specifies a platform, feature set, and file compression method. For example, c4500-is56i-mz indicates:

- Cisco 4500 platform: c4500.
- IP Plus IPSec 56 feature set: is56i.
- RAM compression method: mz.

Feature Pack—A folder containing installation documentation and CDs that contain software images, applications and electronic documentation. Feature packs provide software upgrades for many of the Cisco hardware platforms.

Feature Pack Contents

Your feature pack contains:

- A Software Feature Pack CD-ROM with the following software:
  - Cisco IOS feature set software images that can include bundled modem firmware
  - Trivial File Transfer Protocol (TFTP) server application (for Windows 95 only)
  - These release notes
- Documentation CD-ROM that contains all Cisco documentation
- *Getting Started Fast*
- *Loading the Software Feature Pack* instruction booklet
- Cisco Connection Online wallet card and sticker with service contact information
- Software license for using Cisco software in object code form on a single access server or router.

System Requirements

This section describes the system requirements for Cisco IOS Release 12.1(6)E2:

Hardware Supported

Cisco IOS Release 12.1(6)E2 supports the Cisco 7100 series routers (including the Cisco 7120 and Cisco 7140).

A hardware-software compatibility matrix is available on Cisco.com for users with Cisco.com login accounts. Using this matrix, you can search for supported hardware components by entering a Cisco platform and an IOS release number. The hardware-software compatibility matrix tool is available at the following URL:

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

Determining the Software Version

To determine the version of Cisco IOS software running on your Cisco 7100 series router, log in to the Cisco 7100 series router and enter the **show version** EXEC command. The following sample **show version** command output is from a router running a Cisco 7100 series software image with Cisco IOS Release 12.1(6)E2:

```
Router> show version
Cisco Internetwork Operating System Software
IOS (tm) 7100 Software (C7100-JS56I-MZ), Version 12.1(6)E2, RELEASE SOFTWARE
```

Feature Pack Table

Table 1 Cisco uBR7100 Series Feature Packs

Product Number	CD-ROM Title	Image Name(s)		Recommended Memory	
		UNIX	DOS	Flash	Main
CD71-C-12.1.6E=	Cisco 7100 Series IP Feature Pack Release 12.1(6)E	c7100-is-mz.121-6.E	aaa1501	16 MB	64 MB
		c7100-boot-mz.121-6.E	aaa1502	16 MB	64 MB
CD71-CL-12.1.6E=	Cisco 7100 Series IP IPSEC 56 Feature Pack Release 12.1(6)E	c7100-is56i-mz.121-6.E2	aaa1503	16 MB	64 MB
		c7100-boot-mz.121-6.E	aaa1502	16 MB	64 MB
CD71-CK2-12.1.6E=	Cisco 7100 Series IP IPSEC 3DES Feature Pack Release 12.1(6)E	c7100-ik2s-mz.121-6.E2	aaa1504	16 MB	64 MB
		c7100-boot-mz.121-6.E	aaa1502	16 MB	64 MB
CD71-CH-12.1.6E=	Cisco 7100 Series IP/FW/IDS Feature Pack Release 12.1(6)E	c7100-io3s-mz.121-6.E	aaa1505	16 MB	64 MB
		c7100-boot-mz.121-6.E	aaa1502	16 MB	64 MB
CD71-CHL-12.1.6E=	Cisco 7100 Series IP/FW/IDS IPSEC 56 Feature Pack Release 12.1(6)E	c7100-ik2o3s-mz.121-6.E2	aaa1506	16 MB	64 MB
		c7100-boot-mz.121-6.E	aaa1502	16 MB	64 MB
CD71-CHK2-12.1.6E=	Cisco 7100 Series IP/FW/IDS IPSEC 3DES Feature Pack Release 12.1(6)E	c7100-ik2o3s-mz.121-6.E2	aaa1507	16 MB	64 MB
		c7100-boot-mz.121-6.E	aaa1502	16 MB	64 MB

Table 1 Cisco uBR7100 Series Feature Packs (continued)

Product Number	CD-ROM Title	Image Name(s)		Recommended Memory	
		UNIX	DOS	Flash	Main
CD71-A-12.1.6E=	Cisco 7100 Series Enterprise Feature Pack Release 12.1(6)E	c7100-js-mz.121-6.E	aaa1508	16 MB	64 MB
		c7100-boot-mz.121-6.E	aaa1502	16 MB	64 MB
CD71-AL-12.1.6E=	Cisco 7100 Series Enterprise IPSEC 56 Feature Pack Release 12.1(6)E	c7100-js56i-mz.121-6.E2	aaa1509	16 MB	64 MB
		c7100-boot-mz.121-6.E	aaa1502	16 MB	64 MB
CD71-AK2-12.1.6E=	Cisco 7100 Series Enterprise IPSEC 3DES Feature Pack Release 12.1(6)E	c7100-jk2s-mz.121-6.E2	aaa1510	16 MB	64 MB
		c7100-boot-mz.121-6.E	aaa1502	16 MB	64 MB
CD71-AH-12.1.6E=	Cisco 7100 Series Enterprise/FW/IDS Feature Pack Release 12.1(6)E	c7100-jo3s-mz.121-6.E	aaa1511	16 MB	64 MB
		c7100-boot-mz.121-6.E	aaa1502	16 MB	64 MB
CD71-AHL-12.1.6E=	Cisco 7100 Series Enterprise/FW/IDS IPSEC 56 Feature Pack Release 12.1(6)E	c7100-jo3s56i-mz.121-6.E2	aaa1512	16 MB	64 MB
		c7100-boot-mz.121-6.E	aaa1502	16 MB	64 MB
CD71-AHK2-12.1.6E=	Cisco 7100 Series Enterprise/FW/IDS IPSEC 3DES Feature Pack Release 12.1(6)E	c7100-jk2o3s-mz.121-6.E2	aaa1513	16 MB	64 MB
		c7100-boot-mz.121-6.E	aaa1502	16 MB	64 MB

Feature Set Table

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 12.1(6)E2 supports the same feature sets as Cisco IOS Release 12.1(5)T, but Cisco IOS Release 12.1(6)E2 can include new features supported by the Cisco 7100 series.

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

Table 2 through Table 4 list the feature sets for Cisco 7100 series routers. The tables use the following conventions:

- Yes—The feature is supported in the software image.
- No—The feature is not supported in software image.
- In—The number in the In column indicates the Cisco IOS release in which the feature was introduced. For example, (1) means a feature was introduced in Cisco IOS Release 12.1(1)E. If a cell in this column is empty, the feature was included in the initial base release.

Note These tables might not be cumulative or list all the features in each image. You can find the most current Cisco IOS documentation on Cisco.com. These electronic documents may contain updates and modifications made after the hard-copy documents were printed. If you have a Cisco.com login account, you can find image and release information regarding features prior to Cisco IOS Release 12.1(6)E2 by using the Feature Navigator tool at: http://www.cisco.com/go/fn.

Table 2 Feature List by Feature Set for the Cisco 7100 Series, Part 1

Features	In	Software Images by Feature Sets			
		IP	IP IPSec 56	IP IPSec 3DES	IP/FW/IDS
IP Addressing and Services					
Express RTP Header Compression	(4)	Yes	Yes	Yes	Yes
IP Routing					
IOS SLB Enhancements	(1)	Yes	Yes	Yes	Yes
Load Balancing					
Transparent Webcache Load Balancing	(5a)	Yes	Yes	Yes	Yes
Management					
Turbo Access Control Lists	(4)	Yes	Yes	Yes	Yes
Miscellaneous					
Multi-ISA	(5a)	No	Yes	Yes	No
Quality of Service					
NBAR Enhancements	(1)	Yes	Yes	Yes	Yes
NBAR Enhancements	(2)	Yes	Yes	Yes	Yes
QDM 1.0 Support	(1)	Yes	Yes	Yes	Yes
QDM 1.1 Support	(2)	Yes	Yes	Yes	Yes
QDM 1.2 Support	(3a)	Yes	Yes	Yes	Yes
Security					
IPSec MIB	(4)	No	Yes	Yes	No
VPN Device Manager	(6)	No	Yes	Yes	No

Table 3 Feature List by Feature Set for the Cisco 7100 Series, Part 2

Features	In	Software Images by Feature Sets			
		IP/FW/IDS IPSec 56	IP/FW/IDS IPSec 3DES	Enterprise	Enterprise IPSec 56
IP Addressing and Services					
Express RTP Header Compression	(4)	Yes	Yes	Yes	Yes
IP Routing					
IOS SLB Enhancements	(1)	Yes	Yes	Yes	Yes
Load Balancing					

Table 3 Feature List by Feature Set for the Cisco 7100 Series, Part 2 (continued)

Features	In	Software Images by Feature Sets			
		IP/FW/IDS IPSec 56	IP/FW/IDS IPSec 3DES	Enterprise	Enterprise IPSec 56
Transparent Webcache Load Balancing	(5a)	Yes	Yes	Yes	Yes
Management					
Turbo Access Control Lists	(4)	Yes	Yes	Yes	Yes
Miscellaneous					
Multi-ISA	(5a)	Yes	Yes	No	Yes
Quality of Service					
NBAR Enhancements	(1)	Yes	Yes	Yes	Yes
NBAR Enhancements	(2)	Yes	Yes	Yes	Yes
QDM 1.0 Support	(1)	Yes	Yes	Yes	Yes
QDM 1.1 Support	(2)	Yes	Yes	Yes	Yes
QDM 1.2 Support	(3a)	Yes	Yes	Yes	Yes
Security					
IPSec MIB	(4)	Yes	Yes	No	Yes
VPN Device Manager	(6)	Yes	Yes	No	Yes

Table 4 Feature List by Feature Set for the Cisco 7100 Series, Part 3

Features	In	Software Images by Feature Sets			
		Enterprise IPSec 3DES	Enterprise/ FW/IDS	Enterprise/ FW/IDS IPSec 56	Enterprise/ FW/IDS IPSec 3DES
IP Addressing and Services					
Express RTP Header Compression	(4)	Yes	Yes	Yes	Yes
IP Routing					
IOS SLB Enhancements	(1)	Yes	Yes	Yes	Yes
Load Balancing					
Transparent Webcache Load Balancing	(5a)	Yes	Yes	Yes	Yes
Management					
Turbo Access Control Lists	(4)	Yes	Yes	Yes	Yes
Miscellaneous					
Multi-ISA	(5a)	Yes	No	Yes	Yes
Quality of Service					
NBAR Enhancements	(1)	Yes	Yes	Yes	Yes
NBAR Enhancements	(2)	Yes	Yes	Yes	Yes
QDM 1.0 Support	(1)	Yes	Yes	Yes	Yes
QDM 1.1 Support	(2)	Yes	Yes	Yes	Yes

Table 4 Feature List by Feature Set for the Cisco 7100 Series, Part 3 (continued)

Features	In	Software Images by Feature Sets			
		Enterprise IPSec 3DES	Enterprise/ FW/IDS	Enterprise/ FW/IDS IPSec 56	Enterprise/ FW/IDS IPSec 3DES
QDM 1.2 Support	(3a)	Yes	Yes	Yes	Yes
Security					
IPSec MIB	(4)	Yes	No	Yes	Yes
VPN Device Manager	(6)	Yes	No	Yes	Yes

New and Changed Information

The following sections list the new hardware and software features supported by the Cisco 7100 series routers for Cisco IOS Release 12.1(6)E2.

All features in Cisco IOS Release 12.0(7)XE1 are also in Cisco IOS Release 12.1 E.

For a list of features for Cisco IOS Release 12.0(7)XE1, see the *Release Notes for Cisco 7000 Family for Cisco IOS Releases 12.0(5)XE through 12.0(7)XE1*.

All features in Cisco IOS Release 12.1(1) are also in Cisco IOS Release 12.1(2)E. For a list of features for Cisco IOS Release 12.1(1), see the *Cross-Platform Release Notes for Cisco IOS Release 12.1*.

New Software Features in Cisco IOS Release 12.1(6)E

The following new software feature was introduced in Cisco IOS Release 12.1(6)E.

VPN Device Manager

VPN Device Manager (VDM) software is installed directly onto Cisco VPN routers. It allows network administrators to use a web browser to manage and configure site-to-site VPNs on a single router. VDM implements a wizard-based graphical user interface (GUI) that allows simplified VPN configuration of the router on which it resides and peer-to-peer interfaces from that router to remote devices. VDM requires configuration of some Cisco IOS commands before it can be fully operational.

Note In addition to having the relevant Cisco IOS image installed on your router, you must make sure the VDM client software has been preinstalled in the router Flash memory. If not, you must download it from Cisco.com. See *Installation and Release Notes for VPN Device Manager 1.0* for details on completing this task. See the VPN Device Manager index (http://www.cisco.com/warp/public/cc/pd/nemnsw/vpdvmn/) for further information.

VDM also monitors general system statistics and router health information such as tunnel throughput and errors. The graphing capability allows comparison of such parameters as traffic volume, tunnel counts, and system utilization.VDM supports site-to-site VPNs. Its step-by-step wizards simplify the configuration of common VPN setups, interfaces, and policies, including:

- IPSec tunnels
- Preshared keys and Internet Key Exchange (IKE) policies

MIBs

Current MIBs

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

Deprecated and Replacement MIBs

MIBs will be replaced in a future release. Currently, OLD-CISCO-* MIBs are being converted into more scalable MIBs without affecting existing Cisco IOS products or network management system (NMS) applications. You can update from deprecated MIBs to the replacement MIBs as shown in Table 5.

Table 5 Deprecated and Replacement MIBs

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

Caveats

Resolved Caveats—Cisco IOS Release 12.1(6)E2

This section documents possible behavior by Cisco IOS Release 12.1(6)E2 and describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdt60803

  A Cisco router configured for tag distribution protocol (TDP) and operating with very little free memory may reload.

  There are no known workarounds.

- CSCdt76083

  A Cisco7100 series or Cisco 7200 series VPN router running CiscoIOS Release 12.1(6)E with ISA enabled may drop packets by the decrypting router due to a faulty switch decision after ISA decryption. This particularly occurs when process switching in involved.

  Workaround:Disable the ISA card.

  Alternative workaround:Use an earlier version of Cisco IOS (such as 12.1(5a)E2) instead of 12.1(6)E.

  Alternative workaround:Use a version of Cisco IOS from the T-train or an IOS from the mainline instead of 12.1(6)E.

- CSCdt85382

  A Cisco router running Cisco Express Forwarding (CEF) and IP Security (IPSEC) through a GRE tunnel and using the SA-ISA hardware encryption engine may cause memory allocation problems across the tunnel interface for multicast packets. The resulting SYS-3-INVMEMINT error message below indicates that multicast packets were not processed by the router:

  ```
  002441 %SYS-3-INVMEMINT Invalid memory action (malloc) at interrupt level
  ```

  There are no known workarounds.

Resolved Caveats—Cisco IOS Release 12.1(5c)E11

All the caveats listed in this section are resolved in Cisco IOS Release 12.1(5c)E11. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdt10256

  A Cisco 7000 series router with an Automatic Protection System (APS) switch will generate the following error message:

  ```
  %SYS-3-INVMEMINT: Invalid memory action (malloc)
  ```

  There are no known workarounds.

- CSCdt51478

  On a Cisco router, deleted subinterfaces may retain their settings and these settings may reappear when the same subinterface is created again.

  Workaround: Cleanup all settings on a subinterface before deleteing it.

  Alternative workaround: Delete all subinterface before deleting the main interface.

- CSCdt60803

  A Cisco router configured for Tag Distribution Protocol (TDP) and operating with very little free memory may reload.

  There are no known workarounds.

Resolved Caveats—Cisco IOS Release 12.1(5a)E4

All the caveats listed in this section are resolved in Cisco IOS Release 12.1(5c)E4. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCds70641

  With multicast routing enabled, one may get %ALIGN-3-SPURIOUS at or near the following location:

  ```
  ip_age_one_mroute(0x607c5d50)+0xc3c
  ```

  The spurious interrupt would show a NULL pointer dereference with address at or near 0x558.

  More detail:

  In this particular case, the ALIGN-3-SPURIOUS syslog is harmless.The code was reading a boolean flag based on a pointer, and it didn't check whether the pointer was NULL or not. When the pointer was NULL, the code ended up reading a non-existing memory location and triggered the ALIGN-3-SPURIOUS syslog. On the MIPS based platform, such a read got a value of zero (i.e. FALSE for a boolean flag).

  Since the same path would be taken either if the pointer is NULL, or the boolean flag is FLASE, the syslog in this case indicated a harmless event.

- CSCds87131

  When "priority" is configured in a class that matches on an access-list, and the priority kbps parameter is greater than 1/2 of the interface bandwidth, the feature does not function after router reloads.

  An error message is displayed:

  ```
  bandwidth of <x> kbps is not available (y).
  ```

  The workaround is to remove and re-attach the service-policy.

- CSCdt11369

  After removing and reconfiguring a FR subinterface (or creating a new subinterfaces in some cases), the pings will succeed only 50%% and there will be cef drops. The workaround is to do a shut/no shut on the main interface or to remove and -quickly@ reconfigure- the dlci.

- CSCdt11656

  The '**fair-queue queue-limit** #packets command is not working and thus the per-flow queue-limit values cannot be tuned away from the default values. There is no workaround.

- CSCdt20222

  Packet classification does not happen for router-originated packets when a distributed traffic-shaping (dTS) service policy is applied to a FR PVC. All router-originated packets are put in class-default queue and the class-map counter does not count those packets. The "packets output" counter for class-default is incremented normally, however.

  The problem configuration is:

  ```
  policy-map vc-cbwfq
    ...

   policy-map vc-shape
    class class-default
     shape average <cir>
     service-policy vc-cbwfq
  ```

```
map-class frame-relay foo
  service-policy output vc-shape
```

There is no workaround.

- CSCdt25060

  Removing "match access-group" criteria from class which has only that match criteria left can cause router crash for certain type of policy like policy with llq in one of classes.

  Workaround: First add another match criteria with which "match access-group" criteria will be replaced and then remove "match access-group" criteria.

Resolved Caveats—Cisco IOS Release 12.1(4)E

All the caveats listed in this section are resolved in Cisco IOS Release 12.1(4)E. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdr38962

  The bugID CSCdk52846 causes a router to advertise all areas and all nodes within its own area reachable via itself, with a cost of 704 and hop count of 29. The fix for bugID CSCdp25634 aids routing by having the router ignore these special updates. However, any other devices on that segment will still get the routing updates. This bug is filed to disable this feature or add a knob to disable the special updates.

  Resolution:

  A new CLI command 'decnet cluster-alias update' has been introduced. By default this command is enabled, and all cluster-alias updates will be propagated. However, if a user wishes to prevent these updates from propagating, he can configure 'no decnet cluster-alias update'.'no decnet cluster-alias update' will block all special updates, with a cost of 704 and hop count of 29.

- CSCdr49641

  A Cisco router that receives a large packet that was fragmented before receipt may display the following error message at the rendezvous point of a multicast network that is running Protocol Independent Multicast (PIM) sparse mode:

  ```
  %PIM-5-REG_ENCAP_INVALID: Bad register from <IP-address> for (<IP-address>,
  <Class-D-IP-address>). Trace = ....
  ```

  Workaround: Send a mix of large and small packets from the source, so that the source tree is set up correctly by the small packets between the first hop and the Route Processor (RP). If the multicast data is forwarded correctly, then this situation may not cause any real harm.

  Alternate workaround: Reduce the packet size from the source, so that fragmentation does not occur between the first hop and the RP.

- CSCdr74413

  WRED will classify all MPLS packets as precedence 0 in the MPLS->MPLS and MPLS->IP paths, regarless of their actual MPLS Experimental field value.

- CSCds24749

  A Cisco 7100 series router running Cisco IOS Release 12.1 E may reload with a bus error in crypto_classify_packet. There is no workaround.

- CSCds43345

  ISA firmware errors in malloc handling result in a possible crash, ISA lockup or 1cxx errors.

- CSCds56733

  When Server Load Balancing is configured, fragmented ICMP ping responses from the virtual ip address may be corrupted.

  The last 14 bytes of the ping response are corrupted. Note that this only affects ICMP packets, not TCP or UDP packets. Typically, this only occurs if a large ping packet is sent to an SLB vserver.

  One workaround is to deny fragmented ICMP packets with a destination ip address of a virtual server using an input Access Control List on the interfaces. This prevents Server Load Balancing from generating the corrupted response to the ping.

- CSCds04548

  After CSCdr76238 OSPF does not work on unnumbered interfaces.

  Workaround is to configure IP address on the interface.

- CSCds07275

  When you use Multilink PPP over virtual private dial-up network (VPDN), the links fail to come up.

  Workaround: Disable Multilink PPP over those links.

Resolved Caveats—Cisco IOS Release 12.1(3a)E4

All the caveats listed in this section are resolved in Cisco IOS Release 12.1(3a)E4. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdr91706

Resolved Caveats—Cisco IOS Release 12.1(1)E3

All the caveats listed in this section are resolved in Cisco IOS Release 12.1(1)E3. This section describes only severity 1 and 2 caveats and select severity 3 caveats.

- CSCdp69004

  A Gigabit Ethernet Interface Processor (GEIP) that is configured for Cisco Encryption Technology (CET) decrypts packets correctly but fails to encrypt packets that match the crypto policy and should be encrypted. In this situation, the GEIP forwards the packets unencrypted.

  Workaround: When network topology permits, use the VIP2-40 or VIP2-50 with one or two PA-FE port adapters.

- CSCdr01079

  The VIP in the highest slot may not boot properly after a router reload.

  There are no known workarounds.

- CSCdr05739

  During the startup, default bandwidth was not being properly set up for ATM Dlx card. The default visible_bandwidth was set to BANDWIDTH_SCALE by the common interface initialization routine, which is 10000000. Now, the code has been changed to set up the default interface bandwidth and delay during startup config setup for ATM Dlx.

  There are no known workarounds.

- CSCdr18877

In some configurations, if a policy-map is configured to use class-maps based on access lists, after bootup the classification does not occur properly (for example, packets that should match the class are not considered to match).

Workaround: Remove and redefine the class after bootup.

- CSCdr24768

  CEF may not process an interface up event, resulting in a **show interface** command displaying the interface as up while the **show cef interface** command displays the same interface as down. This may result in missing prefixes in the CEF table.

  Workaround: Repeat the **no shutdown** command on the interface. It is not necessary to first issue a **shutdown** command on the interface.

Note For a list of open and resolved caveats for QDM 1.0 Support for Cisco IOS Release 12.1(1)E3, see the "Caveats" section of the *Release and Installation Notes for Cisco Quality of Service Device Manager 1.0* on Cisco.com and on the Documentation CD-ROM.

Related Documentation

The following sections describe the documentation available for the Cisco 7100 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 and the Documentation CD-ROM.

Use these release notes with these documents:

- Release-Specific Documents, page 13
- Platform-Specific Documents, page 14
- Feature Modules, page 15
- Cisco IOS Software Documentation Set, page 15

Release-Specific Documents

The following documents are specific to Release 12.1 and are located on Cisco.com and on the Documentation CD-ROM:

- *Cross-Platform Release Notes for Cisco IOS Release 12.1*

  On Cisco.com at:

  Technical Documents: **Documentation Home Page**: **Cisco IOS Software Configuration**: **Cisco IOS Release 12.1**: **Release Notes**: **Cross-Platform Release Notes**

  On the Documentation CD-ROM at:

  Cisco Product Documentation: **Cisco IOS Software Configuration**: **Cisco IOS Release 12.1**: **Release Notes**: **Cross-Platform Release Notes**

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

  Technical Documents

- *Caveats for Cisco IOS Release 12.1*

  As a supplement to the caveats listed in "Caveats" in these release notes, see the *Caveats for Cisco IOS Release 12.1* document.

  On Cisco.com at:

  Technical Documents: **Documentation Home Page**: **Cisco IOS Software Configuration**: **Cisco IOS Release 12.1**: **Release Notes**: **Caveats**

  On the Documentation CD-ROM at:

  Cisco Product Documentation: **Cisco IOS Software Configuration**: **Cisco IOS Release 12.1**: **Release Notes**: **Caveats**

  Note If you have an account with Cisco.com, you can use Bug Navigator II to find caveats of any severity for any release. To reach Bug Navigator II, log in to Cisco.com and click **Software Center**: **Cisco IOS Software**: **Cisco IOS Bug Navigator II**. Another option is to go to http://www.cisco.com/support/bugtools.

- *Release Notes for Cisco 7000 Family for Cisco IOS Releases 12.0(5)XE through 12.0(7)XE1*

  On Cisco.com at:

  Technical Documents: **Documentation Home Page**: **Cisco IOS Software Configuration**: **Cisco IOS Release 12.0**: **Release Notes: Cisco 7000 Family Routers**: **Cisco 7000 Family—Release Notes for Release 12.0 XE**: **Release Notes for Cisco 7000 Family for Cisco Releases 12.0(5)XE through 12.0(7)XE1**

  On the Documentation CD-ROM at:

  Cisco Product Documentation: **Cisco IOS Software Configuration**: **Cisco IOS Release 12.0**: **Release Notes**: **Cisco 7000 Family Routers**: **Cisco 7000 Family—Release Notes for Release 12.0 XE**: **Release Notes for Cisco 7000 Family for Cisco IOS Releases 12.0(5)XE through 12.0(7)XE1**

Platform-Specific Documents

These documents are available for the Cisco 7100 series routers on Cisco.com and on the Documentation CD-ROM:

- *Quick Start Guide Cisco 7100 Series VPN Router*
- *Cisco 7000 User Guide*
- *Cisco 7000 Hardware Installation and Maintenance*

On Cisco.com at:

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

On the Documentation CD-ROM at:

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

Feature Modules

Feature modules describe new features supported by Release 12.1 E and are updates to the Cisco IOS documentation set. A feature module consists of a brief overview of the feature, benefits, configuration tasks, and a command reference. As updates, the feature modules are available online only. Feature module information is incorporated in the next printing of the Cisco IOS documentation set.

On Cisco.com at:

Technical Documents: **Documentation Home Page**: **Cisco IOS Software Configuration**: **Cisco IOS Release 12.1**: **New Feature Documentation**: **New Features in 12.1-Based Limited Lifetime Releases**: **Cisco IOS Release 12.1 E**

On the Documentation CD-ROM at:

Cisco Product Documentation: **Cisco IOS Software Configuration**: **Cisco IOS Release 12.1**: **New Feature Documentation**: **New Features in 12.1-Based Limited Lifetime Releases**: **Cisco IOS Release 12.1 E**

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 establish 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 Java Script 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. The Cisco IOS software documentation set is shipped with your order in electronic form on the Documentation CD-ROM—unless you specifically ordered the printed versions.

Documentation Modules

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

On Cisco.com at:

Technical Documents: **Documentation Home Page**: **Cisco IOS Software Configuration**: **Cisco IOS Release 12.1**: **Configuration Guides and Command References**

On the Documentation CD-ROM at:

Cisco Product Documentation: **Cisco IOS Software Configuration**: **Cisco IOS Release 12.1**: **Configuration Guides and Command References**

Cisco IOS Release 12.1 Documentation Set Contents

Table 6 lists the contents of the Cisco IOS Release 12.1 software documentation set, which is available in electronic form and in printed form if ordered.

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

On Cisco.com at:

Technical Documents: **Documentation Home Page**: **Cisco IOS Software Configuration**: **Cisco IOS Release 12.1**

On the Documentation CD-ROM at:

Cisco Product Documentation: **Cisco IOS Software Configuration**: **Cisco IOS Release 12.1**

Table 6 Cisco IOS Release 12.1 Documentation Set

Books	Major Topics
• *Cisco IOS Configuration Fundamentals Configuration Guide* • *Cisco IOS Configuration Fundamentals Command Reference*	Configuration Fundamentals Overview Cisco IOS User Interfaces Cisco IOS File Management Cisco IOS System Management Cisco IOS User Interfaces Commands Cisco IOS File Management Commands Cisco IOS System Management Commands
• *Cisco IOS Bridging and IBM Networking Configuration Guide* • *Cisco IOS Bridging and IBM Networking Command Reference, Volume I* • *Cisco IOS Bridging and IBM Networking Command Reference, Volume II*	Using Cisco IOS Software Overview of SNA Internetworking Bridging IBM Networking

Table 6 Cisco IOS Release 12.1 Documentation Set (continued)

• *Cisco IOS Dial Services Configuration Guide: Terminal Services* • *Cisco IOS Dial Services Configuration Guide: Network Services* • *Cisco IOS Dial Services Command Reference*	Preparing for Dial Access Modem Configuration and Management ISDN and Signaling Configuration PPP Configuration Dial-on-Demand Routing Configuration Dial-Backup Configuration Terminal Service Configuration Large-Scale Dial Solutions Cost-Control Solutions Virtual Private Networks X.25 on ISDN Solutions Telco Solutions Dial-Related Addressing Services Interworking Dial Access Scenarios
• *Cisco IOS Interface Configuration Guide* • *Cisco IOS Interface Command Reference*	Interface Configuration Overview Configuring LAN Interfaces Configuring Serial Interfaces Configuring Logical Interfaces
• *Cisco IOS IP and IP Routing Configuration Guide* • *Cisco IOS IP and IP Routing Command Reference*	IP Addressing and Services IP Routing Protocols IP Multicast
• *Cisco IOS AppleTalk and Novell IPX Configuration Guide* • *Cisco IOS AppleTalk and Novell IPX Command Reference*	AppleTalk and Novell IPX Overview Configuring AppleTalk Configuring 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, and XNS Overview Configuring Apollo Domain Configuring Banyan VINES Configuring DECnet Configuring ISO CLNS Configuring XNS
• *Cisco IOS Multiservice Applications Configuration Guide* • *Cisco IOS Multiservice Applications Command Reference*	Multiservice Applications Overview Voice Video Broadband
• *Cisco IOS Quality of Service Solutions Configuration Guide* • *Cisco IOS Quality of Service Solutions Command Reference*	Quality of Service Overview Classification Congestion Management Congestion Avoidance Policing and Shaping Signaling Link Efficiency Mechanisms Quality of Service Solutions

Table 6 Cisco IOS Release 12.1 Documentation Set (continued)

• *Cisco IOS Security Configuration Guide* • *Cisco IOS Security Command Reference*	Security Overview Authentication, Authorization, and Accounting (AAA) Security Server Protocols Traffic Filtering and Firewalls IP Security and Encryption Other Security Features
• *Cisco IOS Switching Services Configuration Guide* • *Cisco IOS Switching Services Command Reference*	Cisco IOS Switching Services Overview Cisco IOS Switching Paths Cisco Express Forwarding 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*	Wide-Area Networking Overview Configuring ATM Configuring Frame Relay Configuring Frame Relay-ATM Interworking Configuring SMDS Configuring X.25 and LAPB
• *Cisco IOS Configuration Guide Master Index* • *Cisco IOS Command Reference Master Index* • *Cisco IOS Debug Command Reference* • *Cisco IOS Dial Services Quick Configuration Guide* • *Cisco IOS Software System Error Messages* • New Features in 12.1-Based Limited Lifetime Releases • New Features in Release 12.1 T • Release Notes (Release note and caveat documentation for 12.1-based releases and various platforms)	

Obtaining Documentation

The following sections provide sources for obtaining documentation from Cisco Systems.

World Wide Web

The most current Cisco documentation is available on the World Wide Web at http://www.cisco.com. Translated documentation can be accessed at http://www.cisco.com/public/countries_languages.shtml.

Documentation CD-ROM

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

Ordering Documentation

Cisco documentation is available in the following ways:

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

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

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

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

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

Documentation Feedback

If you are reading Cisco products documentation on the World Wide Web, you can submit technical comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco.

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

For your convenience, many documents contain a response card behind the front cover for submitting your comments by mail. Otherwise, you can mail your comments to the following address:

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

We appreciate your comments.

Obtaining Technical Assistance

The following sections provide sources for obtaining technical assistance from Cisco Systems.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

http://www.cisco.com

Technical Assistance Center

The Cisco TAC website is available to all customers who need technical assistance with a Cisco product or technology that is under warranty or covered by a maintenance contract.

Contacting TAC by Using the Cisco TAC Website

If you have a priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC website:

http://www.cisco.com/tac

P3 and P4 level problems are defined as follows:

- P3—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- P4—You need information or assistance on Cisco product capabilities, product installation, or basic product configuration.

In each of the above cases, use the Cisco TAC website to quickly find answers to your questions.

To register for Cisco.com, go to the following website:

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

Cisco.com registered users who cannot resolve a technical issue by using the TAC online resource can open a case online by using the TAC Case Open tool at the following website:

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

Contacting TAC by Telephone

If you have a priority level 1(P1) or priority level 2 (P2) problem, contact TAC by telephone and immediately open a case. To obtain a directory of toll-free numbers for your country, go to the following website:

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

P1 and P2 level problems are defined as follows:

- P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.
- P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section on page 13.