



Release Notes for the Cisco 10000 Series Internet Router for Cisco IOS Release 12.0(17)SL9

July 21, 2003

These release notes provide information about Cisco IOS Release 12.0(17)SL9 running on the Cisco 10000 Series Internet Router. These release notes include fixes for caveats discovered and resolved since Cisco IOS Release 12.0(17)SL8.

These release notes are updated as needed to describe new features, memory requirements, hardware support, software platform deferrals, and changes to the microcode and related documents.

Cisco IOS Release 12.0(17)SL9 is based on the following previous releases:

- Cisco IOS Release 12.0(17)SL8
- Cisco IOS Release 12.0(17)SL7
- Cisco IOS Release 12.0(17)SL6
- Cisco IOS Release 12.0(17)SL5
- Cisco IOS Release 12.0(17)SL4
- Cisco IOS Release 12.0(17)SL3
- Cisco IOS Release 12.0(17)SL2
- Cisco IOS Release 12.0(17)SL1
- Cisco 12.0ST features synchronized with Cisco IOS Release 12.0S

For a list of the software caveats that apply to previous Cisco IOS Release 12.0(17)SL releases, refer to the appropriate Release Note document located at the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/aggr/10000/10krn/index.htm>

Use these release notes in conjunction with the *Release Notes for Cisco IOS Release 12.0(S)* and the cross-platform *Release Notes for Cisco IOS Release 12.0*.

To review the release notes for Cisco IOS Release 12.0S, go to www.cisco.com and click **Technical Documents**. Select **Release 12.0** from the Cisco IOS Software drop-down menu. Then click **Release Notes > Cisco 12000 Series Routers > Cisco 7000 Family and 12000 Series—Release Notes for Release 12.0 S**.



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

Copyright © 2002. Cisco Systems, Inc. All rights reserved.

To review the cross-platform *Release Notes for Cisco IOS Release 12.0*, go to www.cisco.com and click **Technical Documents**. Select **Release 12.0** from the Cisco IOS Software drop-down menu. Then click **Release Notes > Cross-Platform Release Notes**.

Contents

This document contains the following sections:

- [Cisco Security Advisory, page 2](#)
- [System Requirements, page 2](#)
- [New Features—Cisco IOS Release 12.0\(17\)SL, page 3](#)
- [Cisco 10000 Series Internet Router Software Features, page 4](#)
- [Limitations and Restrictions, page 5](#)
- [Important Notes, page 6](#)
- [Open Caveats—Cisco IOS Release 12.0\(17\)SL, page 7](#)
- [Resolved Caveats—Cisco IOS Release 12.0\(17\)SL9, page 15](#)
- [Other Resolved Caveats, page 15](#)
- [Obtaining Documentation, page 17](#)
- [Obtaining Technical Assistance, page 18](#)
- [Obtaining Additional Publications and Information, page 20](#)

Cisco Security Advisory

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

Cisco has made software available, free of charge, to correct the problem. For more information, refer to the *Cisco Security Advisory: Cisco IOS Interface Blocked by IPv4 Packet*, located at the following URL:

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

System Requirements

We recommend that you use 512 MB of memory on the Performance Routing Engine (PRE). New PREs are shipped with 512 MB of memory. In a redundant setup, both PREs should have the same amount of memory.

Upgrading to a New Software Release

For specific information about upgrading your Cisco 10000 series router to a new software release, refer to the *Cisco 10000 Series Internet Router Software Configuration Guide*.

For general information about upgrading to a new software release, refer to the product bulletin *Cisco IOS Upgrade Ordering Instructions* located at:

http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/957_pp.htm

For additional information about ordering Cisco IOS software, refer to the Cisco IOS Software Releases URL:

<http://www.cisco.com/warp/public/cc/pd/iosw/iore/index.shtml>

Upgrading Cisco IOS Software from Earlier Cisco IOS Releases



Caution

If you are upgrading your Cisco 10000 series router from Cisco IOS Release 12.(14)SL or from earlier 12.0(x)SL-based releases, read this section.

Before you upgrade to Cisco IOS Release 12.0(17)SL9, save your current configuration file. If you decide to re-install Release 12.0(14)SL, or an earlier release, you must also re-install the configuration file associated with that release. This is because some BGP configuration file entries in Cisco IOS Release 12.0(17)SL9 are not compatible with Release 12.0(14)SL or earlier releases.

New Features—Cisco IOS Release 12.0(17)SL

The following new features and improvements are supported in Cisco IOS Release 12.0(17)SL:

- **Multiple Quality-of-Service (QoS) matches per phase**—QoS matching logic was optimized to handle multiple non-ACL matches, with up to four matches in a single pass when the matches are in separate class maps.
- **QoS classification for voice traffic**—Support was added for Real Time Protocol (RTP) to provide high priority classification for voice traffic.
- **QoS Priority Queueing (PQ)**—Ensures minimum latency for delay-sensitive traffic.
- **QoS Class-Based Weighted Fair Queueing (CBWFQ)**—Allows you to configure a portion of interface bandwidth for several different classes of traffic.
- **Frame Relay Traffic Shaping (FRTS)**—A method of limiting excess traffic on a Frame Relay interface at the PVC level.
- **Generic Traffic Shaping**—A method of limiting excess traffic at the interface level.
- **802.1q PXF switching for ARPA encapsulation**—Supports the ability to link individual VLANs to MPLS VPNs.
- **Per-Packet Load Balancing (PPLB)**—Ensures load balancing over multiple links by allowing the router to send successive data packets over paths, without regard to individual hosts or user sessions. PPLB uses a round-robin method to determine which path each packet takes to arrive at the destination.
- **ATM PVCs**—The Cisco 10000 series router now supports 4000 ATM PVCs.

Cisco 10000 Series Internet Router Software Features

Table 1 lists the features supported in the Cisco 10000 series Internet router.

Table 1 *Principal Software Features*

Administration	Cisco Discovery Protocol (CDP) Simple Network Management Protocol (SNMP)
Availability	SONET 1+1 Automatic Protection Switching (APS) Route Processing Redundancy Plus (RPR+)
Encapsulations	Ethernet High-Level Data Link Control (HDLC) Frame Relay Point-to-Point (PPP) Multilink Point-to-Point (MLP)
Multiprotocol Label Switching	Multiprotocol Label Switching Virtual Private Network (MPLS/VPN) edge services 802.1q PXF switching for ARPA encapsulation
Multicast Features	Multicast Static Routes Multicast Routing Monitor (MRM)
Multicast Services	Internet Group Management Protocol (IGMP) Protocol-Independent Multicast (PIM) Distance Vector Multicast Routing Protocol (DVMRP) Cisco Group Management Protocol (CGMP) Unidirectional Link Routing (UDLR) Session Directory Protocol (SDP) Multicast Source Discovery Protocol (MSDP) Border Gateway Protocol (BGP)
Quality of Service	Committed Access Rate (CAR) Class-Based Weighted Random Early Detection (CBWRED) QoS Policy Propagation on BGP (QPPB) Priority Queueing (PQ) Class-Based Weighted Fair Queueing (CBWFQ) Frame Relay Traffic Shaping (FRTS) Generic Traffic Shaping (GTS)

Table 1 *Principal Software Features (continued)*

Routing Protocols	Border Gateway Protocol (BGP) Intermediate System-to-Intermediate System (IS-IS) Open Shortest Path First (OSPF) Interior Gateway Routing Protocol (IGRP) Enhanced Interior Gateway Routing Protocol (EIGRP) Routing Information Protocol (RIP)
Security Features	Standard and extended access lists Authentication, Authorization, and Accounting (AAA) Kerberos authentication and client support on Telnet Radius authentication Terminal Access Controller Access Control System Plus (TACACS+)

Limitations and Restrictions

This section describes any limitations and restrictions that you should review before you use the Cisco 10000 series router.

Automatic Protection Switching Support

Automatic protection switching (APS) is supported on the OC-12 Packet Over SONET (POS) and Channelized OC-12 (ChOC-12) line cards. However, certain limitations apply if the PRE installed in your system is the PRE, Part Number ESR-PRE. These limitations do not apply to the PRE, Part Number ESR-PRE1. You can use the **show version** command to verify which PRE is installed in the router.

For APS to work properly with the PRE, Part Number ESR-PRE, you must ensure that the OC-12 POS or ChOC-12 line card is installed in the lower-numbered (odd) slot.

The system receives clocking information from the line card in the odd slot. If you remove the odd-numbered card (or if the clocking mechanism on that card fails), the clocking is lost and the data path is shut down (Caveat CSCdr81416).

As a workaround, we recommend the following:

1. For the card pair, fully configure the lower-numbered card, and leave the higher-numbered card set to its default configuration.
2. Before you remove a card from the odd slot, run the **no associate** command and shut down the card. The following is an example of how to disable APS for cards in slots 3 and 4:

```
Router(config)# redundancy
Router(config-r)# no associate 3 4
Router(config-r-a-sl)# exit
Router(config)# interface pos 3/0/0
Router(config-if)# shutdown
```

You can now remove the card in slot 3.

3. Move the card located in the even slot to the odd slot and enter the **no shutdown** command. Traffic flow resumes. Insert a new card into the even slot and reconfigure the pair for redundancy.

Testing Performance of High-Speed Interfaces

Cisco IOS Release 12.0(17)SL is enhanced with multiple queues for all classes of traffic over high-speed interfaces. The software selects a queue based on the source and destination address for the packet. This ensures that a traffic flow always uses the same queue and the packets are transmitted in order.

When the Cisco 10000 series router is installed in a real network, the high-speed interfaces work efficiently to spread traffic flows equally over the queues. However, using single traffic streams in a laboratory environment might result in less-than-expected performance.

Therefore, to ensure accurate test results, you should test the throughput of the gigabit Ethernet, POS, or ATM uplink with multiple source or destination addresses.

**Tip**

To determine if traffic is being properly distributed, use the **show hardware pxf cpu queue** command.

Important Notes

This section contains issues that you should be aware of with Cisco IOS Release 12.0(17)SL.

Inserting a New Line Card

If you insert a new line card into the Cisco 10000 series router chassis, the line card initially reports that the line is up.

Frame Relay and PPP Sessions

You can run up to 4200 Frame Relay sessions or 1300 PPP sessions, and you can configure up to 800 BGP peers on the Cisco 10000 series router. The router also supports up to 512 Multilink Point-to-Point (MLP) protocol sessions.

**Note**

Each T1 interface in an MLP bundle represents a single PPP session. Thus, if you configure 130 MLP bundles of 10 T1 interfaces, each results in 1300 PPP sessions (which is the maximum number of PPP sessions that are supported on the Cisco 10000 series router).

Cisco Discovery Protocol

Beginning in Cisco IOS Release 12.0(15)SL, the Cisco Discovery Protocol (CDP) is disabled by default. To enable CDP on an interface, use the **cdp enable** command.

Open Caveats—Cisco IOS Release 12.0(17)SL

Table 2 describes the caveats for the Cisco 10000 series router running Cisco IOS Release 12.0(17)SL.

Table 2 Cisco IOS Release 12.0(17)SL Open Caveats

Caveat	Description
CSCdp96265	<p>If you configure a DS3 BERT pattern 2^20-O153 on any unchannelized DS3 (by using the bert pattern 2^20-O153 interval 1-14400 command), and you then connect the line card to T-Bird 310 test set, the pattern does not synchronize with T-Bird 310.</p> <p>Workaround: Use a different BERT pattern.</p>
CSCdr25441	<p>The router sends DHCP INFORM and DISCOVER messages containing an incorrect Ethernet address.</p> <p>Workaround: No workaround is necessary. This caveat is harmless because these DHCP messages are not used to acquire IP addresses. They are used to gather environmental data such as the domain name server address.</p>
CSCdr36564	<p>When you use the Frame Relay autosense feature, the Cisco 10000 series router sends all three LMI status message types immediately after the interface starts responding. However, sometimes the switch at the other end is not ready to receive messages and as a result, misses one or two messages that were sent. LMI autosense waits until the next scheduled interval (default is 1 minute) to send the messages again.</p> <p>This problem primarily affects clear channel CT3 interfaces.</p> <p>Workaround: There is currently no workaround.</p>
CSCdr37991	<p>If you configure an STS-1 on a ChOC-12 line card as unchannelized and then configure the remote side to send idle-character marks (namely, 0xFF), the T3 line stops responding and transmits a Remote Alarm Indication (RAI).</p> <p>Workaround: When you use unchannelized T3 mode, configure the remote side to send idle-character flags (0x7E). To set this value, use the interface configuration mode idle-character command.</p>
CSCdr43835	<p>When you send large numbers of packets from the Gigabit Ethernet line card to the PRE in the Cisco 10000 series router, you might lose a small number of packets. This only occurs for some packet sizes at very high bandwidths, with loss rates of a few parts per million.</p> <p>Workaround: There is currently no workaround.</p>
CSCdr62013	<p>If large MLP configurations are in use, and you attempt to copy the configuration from a TFTP server directly into the running config, the copy might fail. Failures might include interfaces not appearing, or IPCP or LCP states not opening correctly.</p> <p>Workaround: These failures are far less likely to occur if the configuration is copied to bootflash, and then from bootflash to the running config. Copy the configuration file to the startup config and then reload the router.</p>
CSCdr81416	<p>Limited support exists for APS. For detailed information, refer to the “Automatic Protection Switching Support” section on page 5.</p>
CSCdr81671	<p>On rare occasions, the system cannot retrieve remote performance data if you are using a ChOC-12 line card that has its T1s configured with ANSI FDL enabled.</p> <p>Workaround: There is currently no workaround.</p>

Table 2 Cisco IOS Release 12.0(17)SL Open Caveats (continued)

Caveat	Description
CSCdr84775	<p>WRED does not drop outbound packets correctly on the Channelized T3 line card (CT3) in the default WRED configuration.</p> <p>Workaround: Change the WRED policy to a non-default value.</p>
CSCdr98341	<p>The Flash disk can fall into the chassis when you insert the disk into the empty space to the right of the slot B in the PRE flash assembly.</p> <p>Workaround: Pay extra attention when inserting a flash disk into the PRE flash assembly. Do not insert the disk in the empty space to the right of the slot B—<i>if you insert a card in that space, it will fall into the chassis.</i></p>
CSCds06423	<p>Some MPLS packets are CEF switched when they should be label switched. This condition occurs if the Cisco 10000 series router has two interfaces configured for label switching.</p> <p>Workaround: Configure only one interface for label switching.</p>
CSCds25069	<p>The default logging parameter (logging rate-limit console all 10 except critical) sets console logging to disabled.</p> <p>Workaround: Enter the logging console critical command to view the most important events such as card up/down and toaster failure events.</p>
CSCds36324	<p>Mass configuration (which occurs during boot/reload and can occur during link state changes) takes a long period of time (for example, more than 40 minutes for 2000 VCs associated with a main interface) with large numbers of PVCs (100s to 1000s). This problem occurs when you attempt to configure large numbers of PVCs on the main interface (or multipoint subinterfaces) with static maps on each PVC.</p> <p>Workaround: Do not configure more than 500 PVCs on a single OC-12 ATM line card or more than 900 PVCs on a Cisco 10000 series router.</p>
CSCds40839	<p>After you enter the show controller command, occasionally an alarm LED appears as active even though no alarms are indicated.</p> <p>Workaround: Perform a shut/no shut configuration on the SONET controller. For example:</p> <pre data-bbox="537 1325 821 1453"> conf t controller sonet 7/0/0 shut no shut end </pre>

Table 2 Cisco IOS Release 12.0(17)SL Open Caveats (continued)

Caveat	Description
CSCds41791	<p>If you reload a Cisco 10000 series router, some initialization messages are logged to the console before the startup-config is loaded. These initialization messages are transitional and might report an incorrect state, especially for the FastEthernet interface.</p> <pre>00:00:15: Downloading Microcode: file=system:pxf/ucode_file, version=2.0(21.4), description=Nightly Build Software created Wed 13-Sep-00 00:38 00:00:21: %LINK-3-UPDOWN: Interface Ethernet0/0/0, changed state to up 00:00:21: %LINK-5-CHANGED: Interface FastEthernet0/0/0, changed state to reset 00:00:23: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0/0, changed state to up 00:00:23: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0/0, changed state to down</pre> <p>These messages do not appear in the buffered log.</p> <p>Workaround: Ignore these messages.</p>
CSCds43837	<p>The show atm pvc command displays "Unexpected QoS type" for its traffic parameters. This occurs when a PVC was previously configured with only an ATM vc-class, and then the vc-class was subsequently deleted.</p> <p>For example:</p> <pre>sw-apollo-3(config)# vc-class atm test sw-apollo-3(config-vc-class)# vbr-nrt 1000 1000 10 sw-apollo-3(config-vc-class)# exit sw-apollo-3(config)# int atm 3/0/0 sw-apollo-3(config-if)# pvc 200 sw-apollo-3(config-if-atm-vc)# class-vc test sw-apollo-3(config-if-atm-vc)# end sw-apollo-3#sh atm vc VCD / Peak Avg/Min Burst Interface Name VPI VCI Type Encaps Kbps Kbps Cells Sts 3/0/0 1 0 200 PVC SNAP 1000 1000 10 UP sw-apollo-3#</pre> <p>Now delete the vc-class:</p> <pre>sw-apollo-3#conf t sw-apollo-3(config)#no vc-class atm test sw-apollo-3(config)#end sw-apollo-3#sh atm vc VCD / Peak Avg/Min Burst Interface Name VPI VCI Type Encaps Kbps Kbps Cells Sts 3/0/0 1 0 200 PVC SNAP %Unexpected qos type UP</pre> <p>Workaround: Configure the vc directly using conventional means (non ATM vc-classes), or remove the vc and re-create it with a new ATM vc-class.</p>
CSCds48362	<p>The show interface output occasionally displays an extremely large number of configured VCs which do not really exist.</p> <p>Workaround: There is currently no workaround.</p>

Table 2 Cisco IOS Release 12.0(17)SL Open Caveats (continued)

Caveat	Description
CSCds49222	<p>When a segment on a MPLS traffic engineered path is disabled, the PXF engine reloads, temporarily causing all forwarding to stop.</p> <p>Workaround: There is currently no workaround.</p>
CSCds49948	<p>With multiple PVP tunnels, if the aggregate traffic received by one or more of the PVPs is heavily oversubscribed (starting at about 110% of the tunnel's PCR rate), the traffic on companion PVP tunnels on that interface might experience throughput that is lower than expected.</p> <p>Workaround: There is currently no workaround.</p>
CSCds49957	<p>When you boot the Cisco 10000 series router, the system might display the following messages:</p> <pre data-bbox="537 695 1430 800">*Oct 17 12:32:48.287: %SNMP-3-TRAPBLOCK: Attempt to generate SNMP trap from a process with blocking disabled -Traceback= 60565064 606A6B34 60678238 60678438 6067AD88 6067AF30 602FCBDC 6024817C 60248168</pre> <p>Workaround: Ignore the messages.</p>
CSCds50249	<p>If incoming multicast packets match an input access list that has the log option enabled, the output of the show log command and show access-list commands display double the number of matches.</p> <p>Workaround: There is currently no workaround.</p>
CSCds63025	<p>Line Protocol on one or two T1s might not come up when you perform a reload with a large configuration (for example, 1008 T1s with PPP encap or 504 MLPPPs).</p> <p>Workaround: Reload the line card using the command hw slot slot_number reset.</p>
CSCds63387	<p>When a redundant power supply is removed or a line card is OIRed, SNMP traps are generated by the syslog mib. There is a request to generate these traps using the env, mon, and entity MIBs respectively.</p> <p>Workaround: Filter the SNMP traps using the syslog MIB.</p>
CSCds67459	<p>When a serial interface is configured to be part of a MPLS/VPN, if you enter the no channelized command on the T3 controller, this clears the interface. However, the show ip vrf vrf_name command continues to show the interface as part of the VRF.</p> <p>Workaround: The only way to eliminate unwanted interfaces in the VRF table is to reload the box.</p>
CSCds68294	<p>In the unlikely event of a total failure of the cooling fan tray, or any other scenario resulting in high-temperature operation, the Cisco 10000 series router continues running, and does not power off.</p> <p>Workaround: If you observe fan failure or over-temperature alarms or log messages, immediately power off the chassis until the problem is corrected.</p>
CSCds69465	<p>Ping traffic does not resume after you switch from an explicit path to a dynamic path.</p> <p>Workaround: There is currently no workaround.</p>

Table 2 Cisco IOS Release 12.0(17)SL Open Caveats (continued)

Caveat	Description
CSCds74846	<p>When MPLS TE is configured and the logging console is turned on, the following error message appears repeatedly in the window:</p> <pre>"00:58:10: %TFIB-7-SCANSABORTED: TFIB scan not completing. MAC string updated."</pre> <p>Workaround: Leave the logging console turned off.</p>
CSCds86646	<p>ISIS adjacencies become recalculated with 65 to 85 MB of TCP traffic to the router.</p> <p>Workaround: Because this problem is caused by hackers, we recommend that you use access lists to block out hackers. Access lists prevent packets from punting to the RP and taking down the router.</p>
CSCds86767	<p>A Cisco 10000 series router running Cisco IOS Release 12.0(10)SL might experience a buffer leak when interfaces are down (but not administratively down).</p> <p>Workaround: Administratively shut down the interfaces.</p>
CSCdt00312	<p>If you request deletion of a file from flash storage, the flash file delete function might choose an incorrect default device. The incorrect default used is slot0:.</p> <p>Workaround: When you specify the filename, prefix the filename with disk0:.</p>
CSCdt04686	<p>During the reloading process, the match input-interface Serial3/0/0/1:0 configuration statement is not recognized and disappears from the configuration files after the Cisco 10000 series router is reloaded.</p> <p>Workaround: Reenter the match input-interface Serial3/0/0/1:0 command.</p>
CSCdt08501	<p>PVCs in the down state can still pass traffic. When a PVP is created with associated F4 OAM VCs, and those F4 OAM VCs do not appear (for instance, because there is no VP at the far end or the VP at the far end did not create F4 OAM VCs), traffic can still be passed on the PVCs associated with the PVP in question. When the F4 OAM loopback cells are not returned, Cisco IOS software declares all PVP associated PVCs to be down. IOS does not, however, notify the forwarding engine or the line card. This allows traffic routed over the PVCs in question to pass.</p> <p>Workaround: There is currently no workaround.</p>
CSCdt21254	<p>When the ACL is downloaded from the tftp server, the CPU advances to 100% utilization and several line cards lost IPC with the PRE and are reset.</p> <p>Workaround: Do not configure all 8000 lines of ACL. Split the ACL into several smaller ACLs and download them separately.</p>
CSCdt28444	<p>In a chassis using TACACS security and running redundant PREs, you can access the console while the secondary PRE is cutting over to primary PRE. If no action is taken on the console for the length of the session timeout period, TACACS engages on the console. If the user does access the console during the cutover, the user enters exec mode (not enable mode).</p> <p>Workaround: To help control security, set a short session timeout on the console port, and keep tight control of the enable password.</p>
CSCdt38819	<p>MALLOCFAIL with multicast traffic if a high rate of multicast traffic is sent out before multicast routing entries are updated.</p> <p>Workaround: There is currently no workaround. After the routing entries are updated, this problem disappears.</p>

Table 2 Cisco IOS Release 12.0(17)SL Open Caveats (continued)

Caveat	Description
CSCdt47342	TFIB table failure. Workaround: There is currently no workaround. However, the table eventually updates.
CSCdt50540	Sometimes a traceback message is generated during an RPR+ switch over to the new primary PRE. A message similar to the following appears: 00:03:07: %IPC-5-INVALID: Sequence Structure port index=0x3 -Traceback= 60321EC0 60322868 60806A54 603348C8 60359924 60025B94 602828CC 602828B8 Workaround: This message is harmless. Ignore the message.
CSCdt54684	On rare occasions, if a large number of ds0 interfaces are configured on a CT3 line card, spurious memory error messages might appear. Workaround: There is currently no workaround.
CSCdt55873	On rare occasions in which relatively high rates of traffic bursts are received on the OC-12 ATM line card, some packets might be dropped but not counted by the software. Workaround: There is currently no workaround.
CSCdt57432	If you use snmpwalk or other similar tool to display the value of different objects associated with a Cisco 10000 series router, you can see that when an unchannelized DS3 controller has been created in a ChOC-12 line card, the configuration values of the DS3 MIB are not correct. If subsequent configuration commands are issued, the values displayed are correct. This problem probably exists in a channelized STM-1 line card as well, when in unchannelized DS3 mode. Workaround: Rely on the outcome of the show controller t3 and show interface serial commands.
CSCdt57555	Verilink-hibit mode does not work on the Cisco 10000 series router with ChOC-12 line cards whose paths are configured in unchannelized DS3 mode. When the Verilink-hibit mode is chosen by the network administrator, Verilink-lowbit mode is programmed in the hardware instead. Workaround: There is currently no workaround. You must use Verilink-lowbit mode.
CSCdt63838	The message Bad file magic number – cannot load bootflash appears. Workaround: Perform the following: a. copy bootflash:<file> to disk0:<file> b. delete bootflash:<file> and squeeze bootflash: c. copy disk0:<file> bootflash:<file>
CSCdt64787	At the end of the line in the show run command output, 0.0.0.0 is appended randomly. Workaround: Make sure that 0.0.0.0 is not in the running-config when saving it and then reusing it.

Table 2 Cisco IOS Release 12.0(17)SL Open Caveats (continued)

Caveat	Description
CSCdt65387	<p>ChOC-12 DS3 subrate does not work in Kentrox mode at full bandwidth.</p> <p>Workaround: Set the ChOC-12 interface to Digital Link mode and full bandwidth (no dsu bandwidth). This works the same as the Kentrox CSU/DSU when set to full bandwidth, and will work with scrambling enabled or disabled (set the same value at both ends).</p>
CSCdt70049	<p>With 500 Frame Relay interfaces on CT3 running IP Multicast, multicast packets get punted to the RP causing IPC OIR on the CT3. This causes the line protocol on the router connected to the Cisco 10000 series router to go down (and remain down) on some interfaces. The interface stats show no traffic over the affected interface. On the Cisco 10000 series router, the Frame Relay PVC corresponding to it shows as Deleted.</p> <p>Workaround: Perform a shut/no shut on the affected interface, or a hw-module slot reset on the line card to bring the line protocol back up.</p>
CSCdt76746	<p>In some cases, ATM counters display incorrect packet input values after receiving packets from several locations (for example, the line card, IOS, and the PXF forwarding engine).</p> <p>Workaround: There is currently no workaround.</p>
CSCdu10065	<p>If you reload microcode, and you have changed IP addresses on interfaces just before the reload, traffic might be forwarded to an incorrect interface.</p> <p>Workaround: Use the shutdown command to shut down the interface experiencing the problem, and then reactivate it by using the no shutdown command.</p>
CSCdu22374	<p>When the Cisco 10000 series router is configured for 802.1q VLANs, the output of the show vlans command reports values that are higher than they should be, for the following parameters:</p> <ul style="list-style-type: none"> • gigabit Ethernet received packets • gigabit Ethernet received bytes • VLAN received packets <p>Workaround: There is currently no workaround.</p>
CSCdu22652	<p>If you perform a reload, the values for the transmitted and received output of the show vlans command indicates, incorrectly, that those values incremented.</p> <p>Workaround: There is currently no workaround.</p>

Table 2 Cisco IOS Release 12.0(17)SL Open Caveats (continued)

Caveat	Description
CSCdu25589	<p>When the destination IP address of an incoming 802.1q packet matches one of the IP addresses of the router, the output of the show vlans command for 802.1q packets increments two times. Ping request packets, however, are always counted correctly regardless of destination.</p> <p>Workaround: There is currently no workaround.</p>
CSCdu25747	<p>If you configure fair queueing on a Frame Relay interface with a large number of PVCs, and the traffic exceeds the link rate, several PVCs might experience a greater number of drops than other PVCs on that interface.</p> <p>Workaround: There is currently no workaround.</p>
CSCdu28935	<p>When the interface on the remote end is set to be administratively down, and you are attempting to bring up the PPP protocol, the status of the interface alternate between down and up until the PPP protocol is up.</p> <p>Workaround: There is currently no workaround.</p>
CSCdu32435	<p>If you configure 998 VPNs over VLAN, and you configure over 146 BGP routes per VPN, the BGP neighbor might start flapping.</p> <p>Workaround: There is no workaround, but the problem is less likely to occur if you configure fewer than 146 BGP routes per VPN.</p>
CSCdu34349	<p>If you configure more than 100 BGP routes per VPN, and there are more than 200 VPNs configured on the system, CEF might not function properly after redistributing.</p> <p>Workaround: Reduce the number of BGP routes per VPN to 100 or less.</p>
CSCdu40483	<p>If you enable multicast replication with an MLP bundle as the source, and the MLP broadcaster might exhibit behavior that is not compliant with MLP standards, then replication might not occur for all interfaces.</p> <p>Workaround: If replication does not occur on all interfaces, reload the microcode.</p>

Resolved Caveats—Cisco IOS Release 12.0(17)SL9

This section lists problems that were found since the release of Cisco IOS Release 12.0(17)SL8, and are resolved in Cisco IOS Release 12.0(17)SL9.

For information about problems resolved in previous releases, refer to the appropriate Release Note document located at the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/aggr/10000/10krn/index.htm>

CSCea02355

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

Cisco has made software available, free of charge, to correct the problem. For more information, refer to the *Cisco Security Advisory: Cisco IOS Interface Blocked by IPv4 Packet*, located at the following URL:

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

Other Resolved Caveats

This section includes caveats listed in previous release notes that are listed as resolved because they are unreproducible or do not affect the behavior of the Cisco 10000 series router. In the event a caveat listed in this section causes problems, contact Cisco customer service.

For a list of unreproducible caveats in previous Cisco IOS Releases, refer to the release notes for those particular releases.

CSCdr47500

During periods of heavy traffic (approaching interface line rate), some interfaces experienced inconsistent performance between interfaces of the same type.

CSCdr72007

The number of VPNs that could be created on gigabit Ethernet subinterfaces was limited to under 100.

CSCdr82363

When the encapsulation mode was changed from PPP to HDLC or vice-versa, the system dropped about 3 of the next 10 packets transmitted. After that, the packets were transmitted normally.

CSCdr82579

When a ChOC-12 line card was reconfigured from a channelized T3 configuration to an unchannelized T3 configuration or vice-versa, the initial packets were not forwarded.

CSCds01233

If you sent a large number of small packets in large multicast groups, this could cause certain debug messages to appear on the console.

CSCds64134

Occasionally, after you reloaded routers (with background traffic load equal to no_drop rate), the throughput was 3 to 400 pps below the expected rate.

CSCds65431

On rare occasions, after a single reload while under load, the Gigabit Ethernet line card was up, but dropped nearly all packets on the output queue.

CSCdt12602

If some interfaces flapped continuously in a Frame-Relay environment, the interface statistics reported input errors (overruns) on the flapping interfaces.

CSCdt19582

Following a reload of the Cisco IOS software, the Gigabit Ethernet interface did not always come back up. The interface remained in the "GigabitEthernet1/0/0 is down, line protocol is down" state.

CSCdt25901

During a reload, if the router continuously received IP packets, CPUHOG messages might have appeared in the log, and the router might have taken longer to come up.

CSCdt28191

After you reloaded line cards under background traffic load, one or more interfaces would not come up.

CSCdt33623

If you issued a **write erase** command on the primary PRE followed by an **erase sec-nvram:** command, and then reloaded both PREs simultaneously, some line cards would not be recognized correctly on reboot.

CSCdt40511

The router stopped responding after several hours of receiving multicast traffic over 500 CT3 ds0 Frame Relay interfaces, at a rate of 10 pps of 260-byte packets.

CSCdt41680

The **ip address negotiate** command sent dynamic host configuration protocol (DHCP) requests out to all serial line interfaces.

CSCdt50591

In some test instances, Frame Relay interfaces did not correctly join a multicast group when it should have. The result is that multicast packets destined for those interfaces will be punted to the route processor. If enough packets were received, the CPU usages on the route processor to run at a high usage.

CSCdt53363

On rare occasions, when a large number of ds0 interfaces was configured on a CT3 line card, buffer with corrupt pool pointer error messages would appear.

CSCdt63854

Under rare conditions in which scripts of VC creates and VC deletes were executed in turn, some VBR-nrt VCs were not created.

Obtaining Documentation

Cisco provides several ways to obtain documentation, technical assistance, and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

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

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

You can access the Cisco website at this URL:

<http://www.cisco.com>

International Cisco web sites can be accessed from this URL:

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

Documentation CD-ROM

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

Registered Cisco.com users can order a single Documentation CD-ROM (product number DOC-CONDOCCD=) through the Cisco Ordering tool:

http://www.cisco.com/en/US/partner/ordering/ordering_place_order_ordering_tool_launch.html

All users can order monthly or quarterly subscriptions through the online Subscription Store:

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

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

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

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

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. On the Cisco Documentation home page, click **Feedback** at the top of the page.

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

You can submit your comments by writing to the following address:

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

We appreciate your comments.

Obtaining Technical Assistance

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

Cisco.com

Cisco.com offers a suite of interactive, networked services that let you access Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com 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

To obtain customized information and service, you can self-register on Cisco.com at this URL:

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

Technical Assistance Center

The Cisco 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 website and the Cisco TAC Escalation Center. The avenue of support that you choose depends on the priority of the problem and the conditions stated in service contracts, when applicable.

- We categorize Cisco TAC inquiries according to urgency:
- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration. There is little or no impact to your business operations.

- Priority level 3 (P3)—Operational performance of the network is impaired, but most business operations remain functional. You and Cisco are willing to commit resources during normal business hours to restore service to satisfactory levels.
- Priority level 2 (P2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively impacted by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.
- Priority level 1 (P1)—An existing network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Cisco TAC Website

The Cisco TAC website provides online documents and tools to help troubleshoot and resolve technical issues with Cisco products and technologies. To access the Cisco TAC website, 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 website. Some services on the Cisco TAC website require 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://tools.cisco.com/RPF/register/register.do>

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

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

If you have Internet access, we recommend that you open P3 and P4 cases through the Cisco TAC website so that you can describe the situation in your own words and attach any necessary files.

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 you call, 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, have your service agreement number and your product serial number available.

Obtaining Additional Publications and Information

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

- The *Cisco Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the *Cisco Product Catalog* at this URL:
http://www.cisco.com/en/US/products/products_catalog_links_launch.html
- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: *Internetworking Terms and Acronyms Dictionary*, *Internetworking Technology Handbook*, *Internetworking Troubleshooting Guide*, and the *Internetworking Design Guide*. For current Cisco Press titles and other information, go to Cisco Press online at this URL:
<http://www.ciscopress.com>
- *Packet* magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access *Packet* magazine at this URL:
<http://www.cisco.com/go/packet>
- iQ Magazine is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. You can access iQ Magazine at this URL:
<http://www.cisco.com/go/iqmagazine>
- Internet Protocol Journal is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:
http://www.cisco.com/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html
- Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:
http://www.cisco.com/en/US/learning/le31/learning_recommended_training_list.html

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

All other trademarks mentioned in this document or Web site 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. (0304R)

Copyright © 2003, Cisco Systems, Inc.
All rights reserved.