



# Release Notes for the Cisco 10000 Series Internet Router for Cisco IOS Release 12.0(23)SX5

---

**September 22, 2003**

These release notes provide information about Cisco IOS software Release 12.0(23)SX5 for the Cisco 10000 series Internet router. These release notes describe new features, memory requirements, hardware support, software platform deferrals, and changes to the microcode and related documents.

Cisco IOS Release 12.0(23)SX5 is based on previous 12.0(23)SX releases, which include all of the new features introduced in Cisco IOS Release 12.0(23)S. You can review the release notes for Cisco IOS Release 12.0(23)S at the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/relnote/7000fam/rn120s.htm>

## Contents

These release notes contain the following sections:

- [Cisco Security Advisory, page 2](#)
- [System Requirements, page 2](#)
- [New Features in Cisco IOS Release 12.0\(23\)SX5, page 3](#)
- [New Features in Cisco IOS Release 12.0\(23\)SX, page 4](#)
- [Limitations and Restrictions, page 6](#)
- [Important Notes, page 7](#)
- [Resolved Caveats in Cisco IOS Release 12.0\(23\)SX5, page 8](#)
- [Open Caveats in Cisco IOS Release 12.0\(23\)SX5, page 9](#)
- [Obtaining Documentation, page 12](#)
- [Obtaining Technical Assistance, page 13](#)
- [Obtaining Additional Publications and Information, page 15](#)



---

**Corporate Headquarters:**

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

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

## 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.

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

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

## System Requirements

This release requires that you have the performance routing engine (PRE, Part Number ESR-PRE1) installed in the Cisco 10000 series router chassis. To verify which PRE is installed in the router, use the **show version** command.

## Memory Requirements

The following table lists memory requirements for the Cisco 10000 series router.

Feature Set by Router	Image Name	Flash Memory	DRAM Memory	Runs From
Edge Services Router	c10k-p10-mz	40 MB	512 MB	RAM
Service Provider/ Secured Shell 3DES	c10k-k4p10-mz	40 MB	512 MB	RAM

## 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* at the following URL:

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

For general information about how to upgrade to a new software release, refer to the product bulletin *Cisco IOS Upgrade Ordering Instructions* at the following URL:

[http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/957\\_pp.htm](http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/957_pp.htm)

## Upgrading Software from Earlier Cisco IOS Releases

### Upgrading from Cisco IOS Release 12.0(21)SX or Release 12.0(21)SX1

If you are upgrading your software from Cisco IOS Release 12.0(21)SX or Release 12.0(21)SX1 to Cisco IOS Release 12.0(23)SX5, you must upgrade the eboot image on the Cisco 10000 series router. If you fail to upgrade the eboot image, the router configuration may not load properly, and a checksum error appears on the console. If you are upgrading the software from an earlier Cisco IOS release, you do not need to upgrade the eboot image.

### Upgrading from Cisco IOS Release 12.0(14)SL or from Earlier 12.0(x)SL-based Releases

If you are upgrading your software from Cisco IOS Release 12.0(14)SL or from earlier 12.0(x)SL-based releases to Cisco IOS Release 12.0(23)SX5, save your current configuration file. If you decide to reinstall Release 12.0(14)SL or an earlier release, you must also reinstall the configuration file associated with that release. This is because some Border Gateway Protocol (BGP) configuration-file entries in Release 12.0(23)SX5 are not compatible with Release 12.0(14)SL or earlier releases.

## Upgrading Software on Redundant PREs

When you upgrade software on redundant Cisco 10000 series performance routing engines (PREs), be sure to download the software to both the active PRE and the standby PRE before you reload both PREs. For more information, see “Upgrading Software on Redundant PREs” under “Cisco 10000 Series ESR Basic Management” at the following URL:

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

**Note**

In the procedure at the above URL, specify **c10k-p10-mz** instead of c10k-p6-mz for the image name.

## New Features in Cisco IOS Release 12.0(23)SX5

Cisco IOS Release 12.0(23)SX5 contains no new features. Several known problems are fixed in this release (see the “[Resolved Caveats in Cisco IOS Release 12.0\(23\)SX5](#)” section on page 8).

Cisco IOS Release 12.0(23)SX5 includes all of the new features introduced in Release 12.0(23)SX, and all of the problem fixes in subsequent 12.0(23)SX releases. See the following section (“[New Features in Cisco IOS Release 12.0\(23\)SX](#)”) for a brief overview of new features in that release, and refer to the appropriate Release Notes document at the following URL for information about a particular release:

<http://www.cisco.com/univercd/cc/td/doc/product/aggr/10000/10krn/120sx/index.htm>

# New Features in Cisco IOS Release 12.0(23)SX

Following is a list of the new features and improvements in Cisco IOS Release 12.0(23)SX on which Cisco IOS Release 12.0(23)SX5 is based. For more information, see the *Release Notes for the Cisco 10000 Series Internet Router for Cisco IOS Release 12.0(23)SX* at the URL above.

## Multirouter–Automatic Protection Switching

The multirouter–automatic protection switching (MR–APS) feature allows switchover of SONET connections in the event of circuit failure. MR–APS is often required when connecting SONET equipment to telco equipment. APS refers to the mechanism of using a "protect" SONET interface in the SONET network as the backup for a working SONET interface. When the working interface fails, the protect interface quickly assumes its traffic load. For more information on this feature, refer to the following URL. Note that the documentation includes **aps** commands for POS interfaces. However, the same commands also apply for ATM interfaces.

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios112/ios112p/gsr/posapsgs.htm>

## Multicast for MPLS VPN

The Multicast for Multiprotocol Label-Switching (MPLS) Virtual Private Network (VPN) feature allows service providers to offer multicast services over their MPLS core network. Multicast for MPLS VPN allows end-user customers to improve productivity and communication flow for applications such as corporate communication, e-learning, data warehousing, content synchronization, trading stocks and commodities (stock quotes and ticker information), and emergency messaging services.

## DiffServe Aware Traffic Engineering for MPLS

The DiffServer Aware Traffic Engineering feature extends DiffServe quality of service (QoS) over an MPLS backbone that uses traffic engineering. Bandwidth pools assigned to tunnel interfaces ensure that critical data is associated with a tunnel that has enough bandwidth to transport data over the MPLS network. For more information about this feature, refer to the following URL:

[http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120st/120st14/ds\\_te.htm](http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120st/120st14/ds_te.htm)

## MPLS Traffic Engineering Fast Reroute

The Fast Reroute (FRR) link protection feature of MPLS traffic engineering provides link protection to label-switched paths (LSPs). MPLS traffic engineering automatically establishes and maintains LSPs across the backbone using Resource ReSerVation Protocol (RSVP). Paths for LSPs are calculated at the headend, based on the LSP resource requirements and available network resources such as bandwidth. Under failure conditions, the headend determines a new route for the LSP. This provides for the optimal use of resources. However, due to messaging delays, recovery at the headend is not as quick as recovery at the point of failure. For more information about this feature, refer to the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/120newft/120limit/120st/120st10/fastrout.htm>

## eiBGP Multipath Load-Sharing

The Border Gateway Protocol (BGP) Multipath Load-Sharing for external BGP (eBGP) and internal BGP (iBGP) in a Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) feature allows you to configure multihomed autonomous systems and provider edge (PE) routers to:

- Distribute traffic across eBGP and iBGP paths in BGP networks
- Import eBGP and iBGP paths from multihomed and stub networks

The eiBGP Multipath Load Sharing feature performs unequal cost load balancing by default by selecting BGP paths that do not have an equal cost of the Interior Gateway Protocol (IGP).

For more information about this feature, see the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t4/fteibmpl.htm>

### Link Fragmentation and Interleaving

Interactive traffic (Telnet, voice over IP) is susceptible to increased latency and jitter when the network processes large packets (for example, LAN-to-LAN FTP transfers traversing a WAN link), especially as they are queued on slower links. The Link Fragmentation and Interleaving (LFI) feature reduces delay and jitter on slower-speed links by breaking up large datagrams and interleaving low-delay traffic packets (such as voice) with the smaller packets resulting from the fragmented datagram. LFI was designed especially for lower-speed links where serialization delay is significant.

### Single Rate 3-Color Marker for Traffic Policing

The single rate 3-Color Marker feature meters an IP packet stream and marks its packets different colors, based on the Committed Information Rate (CIR) and two associated burst sizes: Committed Burst Size (CBS) and Excess Burst Size (EBS). CIR is measured in bytes of IP packets per second (and it includes the IP header, but not link specific headers). CBS and EBS are measured in bytes.

The single rate 3-color marker uses the following colors to classify packets:

- Green (conforming)—Packet size is at most Bc or CBS and within the CIR allowance.
- Yellow (exceeding)—Packet size is greater than the CIR allowance but is at most Be or EBS bytes and within the available surplus.
- Red (violating)—Packet size is greater than both the CIR allowance and the available surplus. This is because either the packet's size exceeds Be or EBS or because a previous packet used some of the surplus and the traffic since then has not slowed sufficiently to acquire the surplus needed for the current packet.

The marker starts with a surplus equal to Be or EBS, and replenishes the surplus by the amount of unused CIR allowance until the surplus reaches Be or EBS.

### Cisco 10000 Series Router MIB Enhancements

MIB capabilities on the Cisco 10000 series router have been enhanced as follows:

- The CISCO-ENTITY-EXT-MIB and CISCO-OAM-MIB were added.
- Support was verified for the following MIBs: ATM-MIB, CISCO-AAL5-MIB, CISCO-ATM-EXT-MIB, SONET-MIB, RFC1315-MIB, CISCO-FRAME-RELAY-MIB, and CISCO-RF-MIB.
- Support was added for MPLS-LSR-MIB mplsInSegmentOctets and mplsInSegmentOctets.
- The IF-MIB was enhanced to support MPLS.
- MIBs were enhanced to support the Cisco 10000 series router high-availability feature.

For more information about the MIB capabilities for this release, refer to Tables 3-1 and 3-2 in the “MIB Specifications” chapter of the *Cisco 10000 Series Internet Router Leased Line MIB Specifications Guide* (Version 3) at the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/aggr/10000/10kmibs/llguides/llgdv3/mib3.htm>

### SNMP Trap Filtering

Use the SNMP trap filtering feature to filter linkDown traps so that SNMP only sends a linkDown trap if the main interface goes down. If a Cisco 10000 series Internet router interfaces goes down, all of its subinterfaces go down, which results in numerous linkDown traps for each subinterface. This feature filters out those subinterface traps. This feature is turned off by default.

To enable the SNMP trap filtering feature, issue the following CLI command. Use the no form of the command to disable the feature.

```
[no] snmp ifmib trap throttle
```

## Limitations and Restrictions

### PRE Network Management Ethernet Port

Ensure that the Fast Ethernet NME port on the PRE is configured for Auto-Negotiation mode, which is the system default. Duplex mode can cause problems, such as flapping. If the port is experiencing such problems and has been configured for Duplex mode, use the **no half-duplex** or **no full-duplex** command to disable Duplex mode.

### Controlling the Rate of Logging Messages

It is important that you limit the rate that system messages are logged by the Cisco 10000 series router. This helps to avoid a situation in which the router becomes unstable and the CPU is overloaded. To control the output of messages from the system, use the **logging rate-limit** command.

We recommend that you configure the **logging rate-limit** command as follows. This rate-limits all messages to the console to 10 per second, except for messages with critical priority (level 3) or greater.

```
Router(config)# logging rate-limit console all 10 except critical
```

For more information on the **logging rate-limit command**, refer to the *Cisco IOS Configuration Fundamentals Command Reference*.

### Frame Relay

The following limitations apply to the Cisco 10000 series router implementation of Frame Relay:

- The **ip rtp reserve** command is not supported.
- Only one priority queue per VC is allowed.

### Nested Policy Feature

The following limitations and restrictions apply to the Cisco 10000 series router nested policy feature:

- Nested policies support no more than two hierarchy levels.
- For additional restrictions and limitations on creating nested policies, refer to the “Configuring Nested Policies on the Cisco 10000 Series Router” section of the Cisco document at the following location:  
[http://www.cisco.com/univercd/cc/td/doc/product/aggr/10000/10kfm/nest\\_pol.htm](http://www.cisco.com/univercd/cc/td/doc/product/aggr/10000/10kfm/nest_pol.htm)
- The nested-policy shape rate is reserved for nested-policy traffic only. Excess bandwidth is not used for other traffic.
- DotP marking is not supported, nor is 802.1P (including matching and marking the 802.1P header).



**Note** The actual shape rate applied to nested-policy traffic might differ from that specified in the policy. For example, a specified shape rate of 10.5 Mbps might be mapped to 11 Mbps. Use the command **show policy-map interface** to determine the actual shape rate.

### Testing Performance of High-Speed Interfaces

Cisco IOS software running on the Cisco 10000 series router has 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 proper order.

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

### Cisco Discovery Protocol

Unlike other Cisco routers, on the Cisco 10000 series Internet router, the Cisco Discovery Protocol (CDP) is disabled by default. You can enable CDP on an interface using the **cdp enable** command.

### Frame Relay and PPP Sessions

You can run up to 4000 Frame Relay sessions or 4000 PPP sessions, and you can configure up to 800 Border Gateway Protocol (BGP) peers on the Cisco 10000 series Internet router. The router also supports up to 512 Multilink Point-to-Point (MLP) protocol sessions and up to 1024 MLP bundles.

### Performance Routing Engine 1 on the Cisco 10000 Series Edge Services Router

To run Cisco IOS Release 12.0(22)S and later releases on the Cisco 10000 series router, the performance routing engine (PRE) installed in the chassis must be the PRE (Part Number ESR-PRE1). You can verify which PRE is installed in the chassis by using the **show version** command.



Note

---

The Cisco 10000 series router does not support mixing two different PRE revisions in the same chassis. Do not install a PRE (Part Number ESR-PRE) and PRE (Part Number ESR-PRE1) in the same chassis.

---

### VLAN Session Support

The Cisco 10000 series router provides session support for 4000 802.1Q VLANs.

### Inserting a New Line Card

Unlike other Cisco routers, if you insert a new or different line card into a Cisco 10000 series router chassis slot that previously had a line card installed, the line card initially reports that it is administratively up.

### RBE Subinterfaces

To ensure that the performance routing engine (PRE) microcode has adequate IP address space, use IP addresses in a contiguous address space. Also, use the **ip unnumbered** command on the RBE subinterface.

# Resolved Caveats in Cisco IOS Release 12.0(23)SX5

The following problems have been fixed in Cisco IOS Release 12.0(23)SX5. For information about problems fixed in earlier releases, refer to the appropriate Release Notes at the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/aggr/10000/10krm/120sx/index.htm>

## **CSCdy89195**

The router correctly handles stateful switchover (SSO) in configurations in which ATM and Multiprotocol Label Switching (MPLS) are both used. Previously, MPLS label-controlled virtual circuits (LVCs) failed to come back up after an SSO.

## **CSCdz63644**

A PRE-1 cutover in Route Processor Redundancy Plus (RPR+) mode no longer causes VCs to be lost. Previously, VCs were lost when the default SSO mode was changed to RPR+ mode and a cutover was performed.

## **CSCea08828**

When SNMP trap filtering is enabled on a Cisco 1-port channelized OC-12 line card, the T3 layer no longer generates a linkDown trap when the SONET layer is shut down. Previously, a trap was generated although it should not have been.

## **CSCea66250**

The Parallel Express Forwarding (PXF) network processor no longer fails when an ICMP echo request (ping) packet is received on an interface that has access control list (ACL) logging enabled.

## **CSCeb21537**

Multicast Virtual Private Network (VPN) now works correctly over Fast Ethernet (FE) egress interfaces. Previously, when configured for multicast VPN, an FE egress interface sometimes failed to forward multicast packets.

## **CSCeb30183**

When policy-based routing (PBR) is configured on the router, PXF no longer stops processing when you issue the commands **shutdown** followed by **no shutdown** on an egress interface.

## **CSCeb57074**

When Reverse Path Forwarding (RPF) Strict-Checking mode is configured on a serial interface, the interface now allows pings to local IP addresses. Previously, these pings failed. In addition, the allow-self-ping option of the **ip verify unicast source** command also works correctly.

## **CSCeb60371**

The router no longer experiences memory leaks and memory fragmentation when syslog traps are enabled. Previously, these leaks and fragmentation eventually caused the router to fail.

## **CSCeb65653**

When configured for multicast VPN, label-controlled ATM (LC-ATM) interfaces now forward multicast traffic correctly. Previously, the interfaces dropped all multicast traffic.

**CSCeb78329**

The router no longer experiences problems when PVCs or PVPs are deleted after a switchover is performed in RPR+ mode. Previously, after you deleted a PVC or PVP, you could not re-create it.

**CSCeb81033**

When an output service policy is applied to an interface, the router no longer experiences random early detection (RED) packet drops while the average queue size is below the minimum RED threshold. Previously, the router dropped packets before the threshold was reached, although it should not have.

**CSCec02970**

The default settings for temperature alarm thresholds have been increased. Previously, the default settings were too low, which sometimes caused the router to display minor temperature warnings even though nothing was wrong. The new default settings for temperature alarm thresholds are:

Alarm Type	Inlet Temp	Outlet Temp
Minor	45°C	50°C
Major	54°C	58°C
Critical <sup>1</sup>	67°C	85°C

1. On the PRE-1, the default setting for the critical alarm temperature threshold is 72°C.

**CSCec14259**

The router now processes multicast packets correctly during QoS processing. Previously, the precedence and differentiated services codepoint (DSCP) bits were ignored and packets were misclassified.

## Open Caveats in Cisco IOS Release 12.0(23)SX5

Table 1 describes the open caveats in Cisco IOS Release 12.0(23)SX5.

**Table 1** Open Caveats in Cisco IOS Release 12.0(23)SX5

Caveat	Description
<b>General</b>	
<b>CSCdz02942</b>	<p>After a stateful switchover (SSO) in a redundant PRE system, the MIB objects ifLastChange (IF-MIB) and atmVclLastChange (ATM-MIB) might not match sysUpTime.0 (MIB-2), although they should. This problem can occur:</p> <ul style="list-style-type: none"> <li>• After a second switchover</li> <li>• When the standby PRE is reset, followed by a switchover</li> <li>• When the standby PRE is inserted in the chassis later, after insertion of the primary PRE</li> </ul> <p><b>Workaround:</b> None.</p>
<b>CSCdz26218</b>	<p>PXF diversion statistics do not clear when you issue the <b>microcode reload all</b> command, although they should.</p> <p><b>Workaround:</b> Reload the Cisco IOS software.</p>

Table 1 Open Caveats in Cisco IOS Release 12.0(23)SX5 (continued)

Caveat	Description
<b>General (continued)</b>	
<b>CSCdz29077</b>	<p>After you issue the <b>shutdown</b> and <b>no shutdown</b> commands on a Cisco channelized OC-12 line card, the <b>show controller t3</b> command incorrectly displays the T3 controller as Down. The controller is really Up.</p> <p><b>Workaround:</b> Issue the <b>shutdown</b> command, wait several seconds, and then issue the <b>no shutdown</b> command on the SONET interface. This sets the T3 interface to Up in the <b>show controller t3</b> command.</p>
<b>CSCdz32795</b>	<p>A routing policy does not count packets of 65 bytes or larger. The packets are transported, but not counted.</p> <p><b>Workaround:</b> None.</p>
<b>CSCdz35018</b>	<p>A traceback message appears during testing of IP multicast.</p> <p><b>Workaround:</b> None.</p>
<b>CSCdz54597</b>	<p>The Cisco 4-port channelized OC-3 line card experiences low throughput and packet loss when configured with 252 SONET interfaces (VT E1 unframed).</p> <p><b>Workaround:</b> None.</p>
<b>CSCdz56101</b>	<p>On a Cisco channelized 4-port STM-1 line card with 756 interfaces, each at 512 Kbps with SDH framing and AU-4-TUG-3 controllers, the line protocol fails to initialize for several interfaces.</p> <p><b>Workaround:</b> None.</p>
<b>CSCea74742</b>	<p>When the traffic policing max burst size is set to a small value, the policing exceed function does not work correctly.</p> <p><b>Workaround:</b> None.</p>
<b>CSCec32648</b>	<p>If a policy map containing the <b>priority</b> keyword is applied to a Frame Relay interface with 512 Kbps bandwidth or less, the interface fails after being congested for more than 30 seconds or when packets are larger than 512 bytes. (The <b>service-policy output</b> command assigns the policy map to an interface.)</p> <p><b>Workaround:</b> None.</p>
<b>eiBGP Multipath Load Sharing</b>	
<b>CSCdy88837</b>	<p>If eiBGP multipath is configured in an MPLS network and one of the links is configured as eBGP, traffic may not be distributed through all links. This problem occurs when MAX Paths EIBGP is enabled under the address family. In this case, the IP BGP table indicates multiple routes to a destination network (eBGP and iBGP paths), but the IP Route VPN table only shows iBGP paths.</p> <p><b>Workaround:</b> Disable eiBGP and use the <b>weight</b> command to forward traffic through eBGP or iBGP paths.</p>
<b>CSCdz10264</b>	<p>When the router is configured as a provider edge (PE) router with 100 VPNs, the number of packets reported at an ingress port might not reflect the actual number of packets forwarded by the router. This problem occurs on gigabit Ethernet (gigE) line cards when a gigE port is configured as a subinterface on a VLAN, and traffic is sent to each VLAN ID from another router.</p> <p><b>Workaround:</b> None.</p>

Table 1 Open Caveats in Cisco IOS Release 12.0(23)SX5 (continued)

Caveat	Description
<b>eiBGP Multipath Load Sharing (continued)</b>	
<b>CSCdz26257</b>	<p>Traffic might not be load-balanced through iBGP paths when MPLS eiBGP or iBGP max-paths is configured. For example, two iBGP paths might exist to the next hop but the PXF only forwards traffic through one of them. This means one of the links is not being used.</p> <p><b>Workaround:</b> If the router is forwarding traffic through the slower link, you can shut down the slower link to allow the faster link to forward traffic.</p>
<b>Link Fragmentation and Interleaving</b>	
<b>CSCdy75500</b>	<p>The <b>show frame-relay fragment</b> command truncates the Frame Relay interface name for Cisco channelized 4-port STM-1 line cards.</p> <p><b>Workaround:</b> None.</p>
<b>CSCdz27628</b>	<p>When class-based weighted fair queuing (CBWFQ) is used with LFI enabled and multiple queues are configured for a link, packets are dropped from underloaded queues rather than overloaded (congested) queues. This problem occurs when traffic with different packet sizes is sent to different queues, which causes fragmentation on some queues but not others.</p> <p><b>Workaround:</b> Be sure to use a priority queue when you enable LFI.</p>
<b>CSCdz42829</b>	<p>When LFI is enabled, the <b>show frame pvc</b> command sometimes shows invalid counts for input and output packets and bytes.</p> <p><b>Workaround:</b> None.</p>
<b>SNMP and MIBs (see also General)</b>	
<b>CSCdz50531</b>	<p>The SONET-MIB does not update the intervals in the sonetVTIntervalTable or sonetVTFarEndIntervalTable for channelized STM and channelized OC-12 AU-3 TU controllers.</p> <p><b>Workaround:</b> None.</p>
<b>CSCdz65705</b>	<p>When SNMP trap filtering is enabled (<b>snmp ifmib trap throttle</b>), SNMP does not generate a notification when a subinterface is shut down, although it should.</p> <p><b>Workaround:</b> None.</p>
<b>Stateful Switchover</b>	
<b>CSCdy66774</b>	<p>After a stateful switchover (SSO), the first packet sent through UDP is lost.</p> <p><b>Workaround:</b> Configure the router to check that the first IP packet has an ARP entry defined for its destination (which must be connected through a fast Ethernet interface). To do this, issue the following CLI command (where <i>A.B.C.D</i> is the destination IP address and <i>H.H.H</i> is the 48-bit hardware address):</p> <pre>conf t arp A.B.C.D H.H.H</pre>

# 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](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](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\\_inpk/pdi.htm](http://www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm)

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the 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](mailto: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](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](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](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.