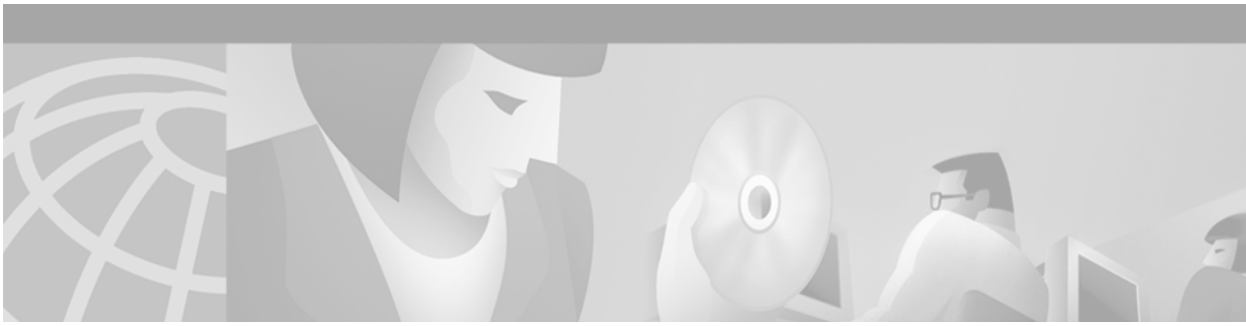

Release Notes for the Cisco 10000 Series ESR for Cisco IOS Release 12.0(19)SL

October 8, 2001

These release notes provide information about Cisco IOS Release 12.0(19)SL running on the Cisco 10000 series edge services router (ESR). 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(19)SL is based on these previous releases:

- Cisco IOS Release 12.0(17)SL2
- Cisco IOS Release 12.0(17)SL1
- Cisco IOS Release 12.0(17)SL
- Cisco 12.0ST features synchronized with Cisco IOS Release 12.0S

For a list of the software caveats that apply to Cisco IOS Release 12.0(19)SL, see the "Caveats in Cisco IOS Release 12.0(19)SL" section on page 7 and the *Release Notes for Cisco IOS Release 12.0(S)*.

To review the release notes for Cisco IOS Release 12.0S, go to www.cisco.com and click Technical Documents > Cisco Product Documentation > Cisco IOS Software Configuration > Cisco IOS Release 12.0 > Release Notes > Cisco 12000 Series Router > *Cisco 7000 Family and 12000 Series – Release Notes for Release 12.0(S)*.

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

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

Contents

This document contains the following sections:

Upgrading to a New Software Release

For specific information about upgrading your Cisco 10000 series ESR to a new software release, see the *Cisco 10000 Series ESR Software Configuration Guide*.

For general information about upgrading to a new software release, see 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 ESR 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(19)SL, 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 BGP configuration-file entries in Release 12.0(19)SL are not compatible with Release 12.0(14)SL or earlier releases.

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.

New Features in Cisco IOS Release 12.0(19)SL

The following new features and improvements are supported in Cisco IOS Release 12.0(19)SL:

NetFlow Accounting—Supports gathering and exporting Version 5 and Version 8 record types to NetFlow FlowCollectors, and provides basic metering for a key set of applications, including network traffic accounting, usage-based network billing, network planning, and network monitoring capabilities.

GRE Tunneling—Supports GRE IP and DVMRP multicast tunnel modes to transport otherwise unroutable packets across the IP network and provide data separation for VPN services. GRE tunnels make it possible to have multiprotocol local networks running over a single-protocol backbone. They also provide workarounds for networks containing protocols that have limited hop counts, connectivity for discontinuous subnetworks, and allow VPNs to connect across wide-area networks. DVMRP multicast tunnel modes are only supported between the Cisco 10000 series ESR and a Sun SPARCstation running DVMRP version 3.8 or higher.

Policy-Based Routing (PBR)—Provides a tool for expressing and implementing the forwarding or routing of data packets, based on the policies defined by network administrators. PBR is a way to have policy override on routing protocol decisions by selectively applying policies based on access list and/or packet size. Network administrators can also use PBR to selectively change the IP ToS, IP precedence, and IP QoS Group fields for matching incoming packets on an interface.

The Cisco 10000 series ESR supports a maximum of 255 PBR policies, and 32 route maps within each policy. The following subset of Policy-Based routing commands are supported in this release of IOS software:

- **[no] ip policy route-map** *map-tag*
- **[no] route-map** *map-tag* **[{permit|deny}]** *sequence-number*
- **[no] match ip address** {*ACL-number* | *ACL-name*} [*ACL-number* | *ACL-name* ...]
- **[no] match length** *min max*
- **[no] set [default] interface** *type number* **[*type number* ...]**
- **[no] set ip [default] next-hop** *ip-address* **[*ip-address* ...]**
- **[no] set ip precedence** *value*
- **[no] set ip qos-group** *value*
- **[no] set ip tos** *value*
- **show route-map [** *map-tag* **]**

Turbo QoS—Provides more efficient handling of QoS policy maps for quicker packet classification and a QoS solution that scales.

Subinterface Policy Maps—Allows you to use the service-policy command to configure QoS features at the subinterface level in addition to configuring it on main interfaces. The types of subinterfaces supported include Frame Relay, ATM (both UBR and VBR), and 802.1Q VLAN. ATM VBR

subinterfaces support all QoS features including queueing. On all other subinterface types, any queueing-related commands in the service-policy, such as bandwidth, priority, shape, queue-limit and random-detect, are ignored.

Diffserv WRED—Extends the functionality of WRED to enable support for Differentiated Services (DiffServ) and Assured Forwarding (AF) Per Hop Behavior (PHB). DiffServ WRED enables customers to implement AF PHB by coloring packets according to DSCP values and then assigning preferential drop probabilities to those packets.

PQ/CBWFQ on ATM PVCs—Allows a service policy, including class queue policy statements, to be attached to ATM VBR VCs. This feature is enabled using the Modular Quality of Service Command-Line Interface (MQC) syntax.

Cisco 10000 Series ESR Software Features

Table 1 lists the features supported in the Cisco 10000 series ESR.

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)

Table 1 Principal Software Features (continued)

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)
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 ESR.

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 with this release. However, certain limitations apply if the PRE installed in your system is the ESR-PRE. These limitations do not apply to the ESR-PRE1. You can verify which PRE is installed in the ESR by using the **show version** command.

For APS to work properly with the 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 disabling 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.

Controlling the Rate of Logging Messages

It is important that you limit the rate that system messages are logged by the Cisco 10000 series ESR. This avoids a situation where the router becomes unstable and the CPU is overloaded. Use the **logging rate-limit** command to control the output of messages from the system.

We recommend that you configure the **logging rate-limit** command as follows:

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

This command rate-limits all messages to the console to 10 per second, except for messages with critical priority (level 3) or greater.

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

Testing Performance of High-Speed Interfaces

Since Cisco IOS Release 12.0(17)SL, the software has been 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 ESR 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 may 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 important issues that you should be aware of with Cisco IOS Release 12.0(19)SL and previous releases.

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 ESR. 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 ESR).

Cisco Discovery Protocol

Starting with Cisco IOS Release 12.0(15)SL, the Cisco Discovery Protocol (CDP) is disabled by default. You can enable CDP on an interface using the **cdp enable** command.

Caveats in Cisco IOS Release 12.0(19)SL

Table 2 describes the caveats for the Cisco 10000 series ESR running Cisco IOS Release 12.0(19)SL.

Table 2 Caveats in Cisco IOS Release 12.0(19)SL

Caveat	Description
CSCdr37991	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). **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.
CSCdr43835	When you send large numbers of packets from the Gigabit Ethernet line card to the PRE in the Cisco 10000 series ESR, you may 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. **Workaround:** There is currently no workaround.
CSCdr81671	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. **Workaround:** There is currently no workaround.
CSCdr84775	WRED does not drop outbound packets correctly on the Channelized T3 line card (CT3) in the default WRED configuration. **Workaround:** Change the WRED policy to a non-default value.

Table 2 Caveats in Cisco IOS Release 12.0(19)SL (continued)

Caveat	Description
CSCds06423	Some MPLS packets are CEF switched when they should be label switched. This condition occurs if the Cisco 10000 ESR has two interfaces configured for label switching. **Workaround:** Configure only one interface for label switching.

CSCds40839	After you enter the **show controller** command, occasionally an alarm LED appears as active even though no alarms are indicated.
	
	Workaround: Perform a **shut/no shut** configuration on the SONET controller. For example:
	
	`conf t`
	`controller sonet 7/0/0`
	`shut`
	`no shut`
	`end`

CSCds49948	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 may experience throughput that is lower than expected. **Workaround:** There is currently no workaround.
CSCds63025	Line Protocol on one or two T1s may not come up when you perform a reload with a large configuration (for example, 1008 T1s with PPP encap or 504 MLPPPs). **Workaround:** Reload the line card using the command **hw slot slot_number reset**.
CSCds63387	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. **Workaround:** Filter the SNMP traps using the syslog MIB.
CSCds68294	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 continues running, and does not power off. **Workaround:** If you observe fan failure or over-temperature alarms or log messages, immediately power off the chassis until the problem is corrected.
CSCdt04686	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 is reloaded. **Workaround:** Reenter the **match input-interface Serial3/0/0/1:0** command.

Table 2 Caveats in Cisco IOS Release 12.0(19)SL (continued)

Caveat	Description
CSCdt08501	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 come up (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 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. **Workaround:** There is currently no workaround.
CSCdt38819	MALLOCFAIL with multicast traffic if a high rate of multicast traffic is sent out before multicast routing entries are updated. **Workaround:** None. After the routing entries are updated, this problem disappears.
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.
CSCdt57432	If you use snmpwalk or other similar tool to display the value of the different objects associated with a Cisco 10000, 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 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 for this problem. You must use Verilink-lowbit mode.
CSCdt65387	ChOC-12 DS3 subrate does not work in Kentrox mode at full bandwidth. **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).

Table 2 Caveats in Cisco IOS Release 12.0(19)SL (continued)

Caveat	Description
CSCdu08173	If you use the **set interface** command or the **set default interface** command to configure a point-to-multipoint interface as a PBR route-map routing destination, packets that match the PBR route-map may not get routed to the proper next-hop on that point-to-multipoint interface. **Workaround:** Use the **set ip next-hop** command when you configure PBR routing on a point-to-multipoint interface. This may require the definition of separate route-maps to steer traffic to each of the desired next-hops.
CSCdu10065	If you reload microcode, and you have changed IP addresses on interfaces just before you reload, traffic may be forwarded to an incorrect interface. **Workaround:** Use the **shutdown** command to shutdown the interface experiencing the problem, and then reactivate it by using the **no shutdown** command.
CSCdu25747	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 may experience a greater number of drops than other PVCs on that interface. **Workaround:** There is currently no workaround.
CSCdu32435	If you configure 998 VPNs over VLAN, and you configure over 146 BGP routes per VPN, the BGP neighbor may start flapping. **Workaround:** There is no workaround, but the problem is less likely to occur if you configure fewer than 146 BGP routes per VPN.
CSCdu34349	If you configure more than 100 BGP routes per VPN, and there are more than 200 VPNs configured on the system, CEF may not function properly after redistributing. **Workaround:** Reduce the number of BGP routes per VPN to 100 or less.
CSCdu39975	If you configure the router with Policy Based Routing (PBR) policies which use a large number of total ACLs as part of IP address-matching criteria, the router may run out of stack space for some processes. This is because some PBR route-maps use a very large total number of ACLs as part of IP address-matching criteria. **Workaround:** To avoid this problem, limit the total number of ACEs included in the ACLs used by each PBR route-map policy. For each PBR policy, the maximum allowable number of ACEs (totaled across all ACLs used by that policy) depends on the number of route-maps defined in the policy. To determine the maximum total number of ACEs used by a PBR policy, divide 10500 by the number of route-maps in that policy. For example, if the number of route-maps defined in a PBR policy is 8, then the maximum total number of ACEs used by that policy would be 1312.
CSCdu40483	If you enable multicast replication with an MLP bundle as the source, and the MLP broadcaster may exhibit behavior that is not compliant with MLP standards, then replication may not occur for all interfaces. **Workaround:** If replication does not occur on all interfaces, reload the microcode.

Table 2 Caveats in Cisco IOS Release 12.0(19)SL (continued)

Caveat	Description
CSCdu57769	If you remove the second configured interface from load balancing Policy Based Routing configuration, forwarding does not resume. **Workaround:** Use the **set next-hop** command instead of the **set interface** command when you configure the PBR route-map.
CSCdu67461	GRE and DVMRP tunnels are not supported over MLPPP bundles. Sending data over this configuration will cause the router to crash. **Workaround:** There is currently no workaround.
CSCdu73079	If you configure the router with many IP Multicast groups, you see CPU Hog messages when you issue the **clear ip mroute *** command, or if the mroute table is cleared and rebuilt from scratch. This happens when the router is configured with approximately 100 groups and 1000 interfaces, with each interface joining the 100 groups, and multicast traffic is passing through all these groups to all interfaces. The CPU hogs seem to happen in "Exec", "IP Input" and "PIM Process" processes. Sometimes the CPU hog is accompanied by IPC timeouts when the table is built from scratch. **Workaround:** There is currently no workaround.
CSCdu77099	If the router receives a PIM Join/Prune packet, in which group1 and group2 are pruned and both are Multicast group addesses, the router interprets that as an instruction to prune group1 and join and prune group2 instead of just prune group2. This behavior can be seen in the mroute table output when you use the **sh ip mroute summary** command. The group1 entry appears as pruned and will eventually time out, whereas the group2 entry does not time out and continually refreshes because of the joins in between the prunes. **Workaround:** If supported, configure the remote connecting device to send prunes in two separate packets instead of one.
CSCdv05164	Large numbers of group joins/leaves over a DVMRP tunnel may cause Traceback messages in the log. However, this will not affect the DVMRP tunnel performance and does not require that you reload. **Workaround:** There is currently no workaround.
CSCdv27957	If you use the **access-list 101 deny ipinip any any** command with an ACL to control traffic, and it is the first line in the ACL, it will prohibit all ip traffic. If the ACL is not entered first, the problem does not occur. **Workaround:** We recommend that you be explicit when using ipinip ACL, for example: `access-list 101 deny ipinip host 2.1.1.1 host 1.1.1.1`

Table 2 Caveats in Cisco IOS Release 12.0(19)SL (continued)

Caveat	Description
CSCdv39768	If you configure the router with Policy Based Routing (PBR) route-maps, including setting default next-hop and/or default interface using the **set ip default next-hop** command and/or the **set default interface** command, then those routing destinations are not used as defaults. The current precedences for packet routing destinations are: 1. PBR set ip next-hop routes 2. PBR set interface routes 3. PBR set ip default next-hop routes 4. PBR set default interface routes 5. Normal (i.e., non-PBR) explicit routes The precedences should be as follows: 1. BBR set ip next-hop routes 2. PBR set interface routes 3. Normal (i.e., non-PBR) explicit routes 4. PBR set ip default next-hop routes 5. PBR set default interface routes
CSCdv49324	If labels are applied to Netflow export records before they are sent, the router will reload unexpectedly. **Workaround:** Only specify export destinations not requiring tagging.
CSCdv50572	If you enable Netflow accounting on an interface that imposes labels on arriving packets, the packets will not be forwarded properly. The label stack may become corrupt, and the downstream neighbor may drop the packets. **Workaround:** Turn off Netflow accounting on interfaces where incoming traffic is likely to have labels imposed, or disable MPLS.

Resolved Problems in Cisco IOS Release 12.0(19)SL

This section lists problems that were found and resolved in Cisco IOS Release 12.0(19)SL.

CSCdr98341

The Flash disk can fall into the chassis when you insert the disk into the empty space to the right of slot B in the PRE flash assembly.

CSCds48362

The **show interface** output occasionally displays an extremely large number of configured VCs which do not exist.

CSCds50249

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.

CSCds69465

Ping traffic does not resume after switching from an explicit path to a dynamic path.

CSCdt00312

The flash file delete function may choose the wrong default device when you request deletion of a file from flash storage. The incorrect default used is slot0:.

CSCdt21254

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.

CSCdt28444

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).

CSCdt47342

TFIB table failure.

CSCdt76746

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).

CSCdu28935

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.

CSCdu61078

Cannot ping Cisco 10000 over PPLB group.

Resolved Problems in Cisco IOS Release 12.0(17)SL2

This section lists problems that were found and resolved in Cisco IOS Release 12.0(17)SL2.

CSCdr19206

PRE performance is no longer affected when preconfiguring a line card using the **card** command.

CSCdt93862

The access level issue that occurred when using the Web interface has been corrected.

CSCdt96234

Router no longer crashes after `wr mem` command.

CSCdu31306

There is no longer a PFX stall error with 126 Multi-Link PPPs in a QoS configuration.

CSCdu58727

Priority queues no longer experience tail drops when line card is under heavy load.

CSCdu65451

Duplicate caveat which was resolved (see CSCdu73749).

CSCdu87866

When you unconfigure and configure the router using the **copy tftp run** command, this no longer causes the router to hang.

CSCdv04992

A large increase in latency for Multi-Link PPP bundles combined with an increase in the number of packet tail drops no longer causes a dramatic decrease in performance.

CSCdv05972

Duplicate caveat which was resolved (see CSCdv12192).

CSCdv07513

The PXF stall error no longer occurs in column 6 during low traffic.

CSCdv08702

There is no longer a slow buffer leak when running multicast input on MLP.

CSCdv12192

There is no longer a buffer leak in Multi-Link PPP column 7.

Resolved Problems in Cisco IOS Release 12.0(17)SL1

This section lists problems that are resolved in Cisco IOS Release 12.0(17)SL1.

CSCdt11794

If you enter the **dir disk0/1** command at the rommon prompt, a TLB (Store) Exception error message no longer appears.

CSCdu71387

If the router receives an IP packet with Ethernet padding over the MLP bundle, it now properly passes the packet to the line card.

CSCdu73749

When the router was configured with large numbers of routes, clearing the entire routing table caused high CPU use. In rare cases, the line cards or Cisco IOS software reboot. This problem no longer occurs.

Resolved Problems in Cisco IOS Release 12.0(17)SL

This section lists problems that are resolved in Cisco IOS Release 12.0(17)SL. For a list of problems that were resolved in previous Cisco IOS Releases, refer to the release notes for those particular versions.

CSCdr32279

When you enter the **hw-module** *slot_number* **reset** command, the event sequence appears in a different order than that shown by the **reload** command if the logging console is configured to informational.

CSCdr52081 and CSCdj94209

The PRE may crash if you repeatedly change a port back and forth from channelized to unchannelized.

Repeated conversions of a T3 port from channelized mode to unchannelized mode and back, with intervening assignments of IP addresses to the interfaces and ping testing, may cause the PRE crash.

CSCdr92058

Large multicast groups may cause CPU hog issues with PIM.

CSCds04367

When older CT3 line cards are powered on with live DS3 signals present at the receive BNC connector, the receive line interface device on the board may lock up, preventing the controller from running.

CSCds18665

If the interface between a PE (PE1) and CE router goes down, MPLS labels disappear at the far end provider edge peer (PE2) MPLS interface.

CSCds36117

If you enter the **clear ip mroute** command on a system with large multicast groups, CPU hog issues may arise that cause problems of moderate severity (such as losing keepalives).

CSCds51102

If you perform an SNMP walk or view entries in the if table, cef-layer internal interfaces appear in the interface table.

CSCds55667

Kentrox DS3 subrate mode does not work when you set it to full bandwidth (45.2 Mbps on Kentrox CSU, 44210 kbps on a Cisco 10000 Series ESR).

CSCds86293

If you issue the **dir** or **show slot0:** or **show slot1:** command, the router reports Open device slot0 failed (Device not ready).

CSCds89640

If large OIDs (1024.1 fields) are sent to the router, the Cisco 10000 stops responding.

CSCds91966

If you delete a T1/E1, IP routes associated with subinterfaces are not removed.

CSCdt11390

On a Cisco 10000 system with channelized OC-12 line cards, the output of the **show controllers** command is incomplete and incorrect.

CSCdt31691

When a large number of VBR-nrt VCs are configured (200 and above) and the link transitions DOWN the host software running on the OC-12 ATM line card may take a SW Watchdog timeout, forcing the line card firmware to reload.

CSCdt34428

If you perform OIR on a line card configured for 768 PPP sessions with traffic running on all interfaces, some interfaces fail to come up. The **show interface** command displays the IPCP state as "Listen".

CSCdt42890

On rare occasions, line cards may not be recognized when you perform an OIR of multiple cards on a new system, or in a system in which the configuration was erased (for example, using **write erase**).

CSCdt63446

If an access-list with logging option enabled is attached to an interface, and you send traffic through the interface, this brings down all of the interfaces.

CSCdt67315

Under circumstances where ATM VCs are created and deleted on a regular basis, the OC-12 ATM segmenter firmware can transition to a state in which it drops some packets without counting them in a data stream where packet sizes alternate from small to large. This manifests itself in lower throughput.

CSCdt74932

When a TU-AIS is received at a particular TU in TUG3#3, the next TU at the T1 or E1 level contains data corruption as well.

CSCdt76739

If you remove an APS configuration for a ChOC-12 line card, followed by the **show controllers sonet** <high slot number, for example 2/0/0> or the **show controllers sonet** command, the Cisco 10000 crashes.

Other Resolved Caveats

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

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

CSCdp96265

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.

CSCdr25441

The router sends out DHCP INFORM and DISCOVER messages containing an incorrect Ethernet address.

CSCdr36564

When you use the Frame Relay autosense feature, the Cisco 10000 Series ESR 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.

This problem primarily affects clear channel CT3 interfaces.

CSCdr47500

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

CSCdr62013

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 may fail. Failures may include interfaces not appearing, or IPCP or LCP states not opening correctly.

CSCdr72007

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

CSCdr82579

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

CSCdr82363

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

CSCds01233

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

CSCds25069

The default logging parameter (logging rate-limit console all 10 except critical) sets console logging to disabled.

CSCds36324

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.

CSCds41791

If you reload a Cisco 10000, some initialization messages are logged to the console before the startup-config is loaded. These initialization messages are transitional and may report an incorrect state, especially for the FastEthernet interface.

CSCds43837

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.

CSCds49222

When a segment on an MPLS traffic engineered path is disabled, the PXF engine reloads, temporarily causing all forwarding to stop.

CSCds49957

Note This problem was fixed in Cisco IOS Release 12.0(17)SL, but was reported in error as an open caveat in 12.0(17)SL, 12.0(17)SL1, and 12.0(17)SL2.

When you boot the Cisco 10000, the system may display the following messages:

```
*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
```

CSCds64134

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

CSCds65431

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

CSCds67459

When a serial interface is configured to be part of an MPLS/VPN, if you enter the **no channelized** command on the T3 controller, this clears the interface. However, the **sh ip vrf** *vrf_name* continues to show the interface as part of the vrf.

CSCds74846

When MPLS TE is configured and the logging console is turned on, the following error message appears repeatedly:

```
"00:58:10: %TFIB-7-SCANSABORTED:  TFIB scan not completing. MAC string updated."
```

CSCds86646

ISIS adjacencies recalculated with 65-85MB of tcp traffic to rtr.

CSCds86767

A Cisco 10000 router running Release 12.0(10)SL may experience a buffer leak when interfaces are down but not administratively down.

CSCdt12602

If in a Frame-Relay environment a handful of interfaces are flapping continuously, the interface statistics report input errors (overruns) on the flapping interfaces.

CSCdt19582

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

CSCdt25901

During a reload, if the router continuously receives IP packets, CPUHOG messages may appear in the log, and the router may take longer to come up.

CSCdt28191

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

CSCdt33623

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

CSCdt40511

The Cisco 10000 crashed after several hours of testing with 500 CT3 ds0 interfaces configured for Frame Relay that were receiving multicast traffic at a rate of 10 pps of 260-byte packets.

CSCdt41680

ip address negotiate sends dhcp requests out 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. Enough packets cause the CPU usages on the route processor to run at a high usage.

CSCdt53363

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

CSCdt54684

On rare occasions, if a large number of ds0 interfaces are configured on a CT3 line card, spurious memory error messages may appear.

CSCdt55873

On rare occasions in which relatively high rates of bursty traffic are received on the OC-12 ATM line card, some packets may be dropped but not counted by the software.

CSCdt63838

Bad file magic number - cannot load bootflash.

CSCdt63854

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

CSCdt64787

At the end of the line in the **show run** command output, 0.0.0.0 is appended randomly.

CSCdt70049

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 to go down (and remain down) on some interfaces. The interface stats show no traffic over the affected interface. On the Cisco 10000 the Frame Relay PVC corresponding to it shows as Deleted.

CSCdu22374

When the Cisco 10000 series ESR is configured for 802.1q VLANs, the output of the **show vlans** command reports values for gigabit Ethernet received packets, gigabit Ethernet received bytes, and VLAN received packets to be higher than they should be.

CSCdu22652

If you perform a reload, the values for the transmitted and received output of the **show vlans** command indicates, incorrectly, that those values incremented.

CSCdu25589

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.

Obtaining Documentation

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

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following sites:

- http://www.cisco.com
- http://www-china.cisco.com
- http://www-europe.cisco.com

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 product 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.

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

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

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

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/

If you cannot resolve your technical issue by using the TAC online resources, Cisco.com registered users 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.