



Release Notes for the Cisco 10000 Series Internet Router for Cisco IOS Release 12.0(25)SX

June 17, 2004

These release notes provide information about Cisco IOS software Release 12.0(25)SX for the Cisco 10000 series Internet router. 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(25)SX is based on Cisco IOS Release 12.0(25)S. The Cisco 10000 Internet router supports a subset of the new features in Cisco IOS Release 12.0(25)S. For more information, see the “[New Features in Cisco IOS Release 12.0\(25\)S](#)” section on page 7. This section lists the features supported on the Cisco 10000 Internet router.

To view the release notes for the Cisco IOS 12.0 SX Releases, go to the following URL:

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

To view the release notes for the Cisco IOS 12.0 S Releases, go to the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/relnote/xprn120s/index.htm>



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

Copyright © 2003–2004. Cisco Systems, Inc. All rights reserved.

Contents

These release notes contain the following sections:

- [System Requirements, page 2](#)
- [New Features in Cisco IOS Release 12.0\(25\)SX, page 4](#)
- [New Features in Cisco IOS Release 12.0\(25\)S, page 7](#)
- [Limitations and Restrictions, page 8](#)
- [Open Caveats—Cisco IOS Release 12.0\(25\)SX, page 9](#)
- [Resolved Caveats—Cisco IOS Release 12.0\(25\)SX, page 10](#)
- [Obtaining Documentation, page 13](#)
- [Obtaining Technical Assistance, page 15](#)
- [Obtaining Additional Publications and Information, page 16](#)

System Requirements

This release requires that you have the performance routing engine (PRE), part number ESR-PRE1 installed in the Cisco 10000 series Internet 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
Internet 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 Internet router to a new software release, refer to the *Cisco 10000 Series Internet Router Software Configuration Guide* located at the following URL:

http://www.cisco.com/en/US/products/hw/routers/ps133/products_configuration_guide_book09186a00804cd88e.html

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

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

For information about how to order Cisco IOS software, refer to the *Cisco IOS Software Releases* located at the following URL:

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

Upgrading from Earlier Cisco IOS Releases

Upgrading from Cisco IOS Release 12.(14)SL or from Earlier Releases Based on Cisco IOS Release 12.0(x)SL

If you are upgrading your software from Cisco IOS Release 12.0(14)SL or from earlier releases based on Cisco IOS Release 12.0(x)SL to Cisco IOS Release 12.0(25)SX, save your current configuration file. If you decide to reinstall Cisco IOS Release 12.0(14)SL or an earlier release, you must also reinstall the configuration file associated with that release because some Border Gateway Protocol (BGP) configuration file entries in Cisco IOS Release 12.0(25)SX are not compatible with Cisco IOS Release 12.0(14)SL or earlier releases.

Upgrading Software on Redundant PREs

When you upgrade software on redundant Cisco 10000 series router 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, refer to the “Upgrading Software on Redundant PREs” section at the following URL. This section is in the “System Startup and Basic Configuration Tasks” chapter of the *Cisco 10000 Series Internet Router Software Configuration Guide*.

The procedure included in the “Upgrading Software on Redundant PREs” section instructs you to tell the Cisco 10000 series router the location in which the new boot image resides. Be sure to specify **c10k-p10-mz** instead of the c10k-p6-mz image name indicated in the documentation.

New Features in Cisco IOS Release 12.0(25)SX

Cisco IOS Release 12.0(25)SX introduces support on the Cisco 10000 series Internet router for the following features, which are described in the sections that follow:

- [Policy-Map Scaling, page 4](#)
- [Percent-Based Policing, page 4](#)
- [Random Early Detection with Queue-Limit, page 4](#)
- [Enhanced RED Statistics, page 5](#)
- [3-Level Policies, page 5](#)
- [Virtual Circuit Oversubscription, page 5](#)
- [External Border Gateway Protocol Label Distribution, page 6](#)
- [QA Error Recovery, page 6](#)

Policy-Map Scaling

The Policy-Map Scaling feature increases the system-wide number of quality of service (QoS) policy maps that you can configure. In Cisco IOS Release 12.0(25)SX, the Cisco 10000 Internet router supports up to 4,096 policy maps. Each **policy-map** command counts as one policy map. The **policy-map** command syntax is unchanged. The maximum number of classes that you can configure in a policy is 32 classes.

Percent-Based Policing

The Percent-Based Policing feature enables you to specify the police rate as a percentage of the bandwidth of the network interface on which policing is applied. To specify the police rate as a percentage, use the **percent percent** option of the **police** command:

```
police [cir] percent {percent} [normal-burst-in-ms ms [max-burst-in-ms ms [conform-action
{action} [exceed-action {action} [violate-action {action}]]]]]]
```

The *percent* argument is a value from 1 to 100 and is required when you use the **percent** keyword.

When you use a percent-based **police** command within a nested policy, the police percent is based on the policy's topmost, class-default, shape rate. Otherwise, the police percent is based on the bandwidth of the network interface on which the **police** command is applied.

For more information, refer to the "Defining QoS Policies" section of the "Creating Service Policies" chapter in the *Cisco 10000 Series Internet Router Quality of Service Configuration Guide*.

Random Early Detection with Queue-Limit

The Random Early Detection (RED) with Queue-Limit feature expands your ability to customize the size of a RED queue. In Cisco IOS Release 12.0(25)SX, you can simultaneously use the **queue-limit** and **random-detect** commands in the same class of a policy.

For more information, refer to the "Defining QoS Policies" section of the "Creating Service Policies" chapter in the *Cisco 10000 Series Internet Router Quality of Service Configuration Guide*.

Enhanced RED Statistics

The Enhanced RED Statistics feature maintains RED drop statistics for each IP precedence or differentiated services code point (DSCP) value.



Note

In releases prior to Cisco 12.0(25)SX, RED drop counts were maintained only for each class.

For more information, refer to the “Displaying Enhanced RED Statistics” section of the “Monitoring and Maintaining Quality of Service” chapter in the *Cisco 10000 Series Internet Router Quality of Service Configuration Guide*.

3-Level Policies

The 3-Level Policies feature increases the hierarchical levels of a nested QoS policy from two to three levels. A 3-level policy is typically used to define the transmission capacity of a virtual circuit in the top level, class-based queuing at the middle level, and marking or metering in the bottom level.

The **service-policy** command configured inside a policy map is used to define a hierarchical policy. The syntax of the command is unchanged. You can use the **service-policy** command in the top and middle levels of a 3-level policy.

For more information, refer to the “Defining QoS Policies” section of the “Creating Service Policies” chapter in the *Cisco 10000 Series Internet Router Quality of Service Configuration Guide*.

Virtual Circuit Oversubscription

The Virtual Circuit (VC) Oversubscription feature enables service providers to improve network utilization of otherwise underutilized shared networks by leveraging statistical multiplexing on ATM, Frame Relay, and IEEE 802.1Q networks. Instead of supporting only unconditional reservation of network bandwidth to VCs, the Cisco 10000 series router offers VC oversubscription to statistically guarantee bandwidth to VCs.

To configure VC oversubscription for Frame Relay and IEEE 802.1Q, use the **service-policy** command. You can optionally use the **service-policy** class configuration command, creating a nested policy to manage traffic within a virtual circuit. For this reason, the term Nested Policy-Map Oversubscription is sometimes used to refer to VC Oversubscription.

To enable oversubscription of ATM VCs, you must configure the following interface configuration command in service-internal mode:

```
atm over-subscription-factor {1-10}
```



Note

You do not need to use the **service-policy** command to specify the ATM VC oversubscription, because a variable bit rate (VBR) ATM VC uses sustained cell rate (SCR) to define the VC’s average transmission rate.

For more information, refer to the “Defining QoS Policies” section of the “Creating Service Policies” chapter in the *Cisco 10000 Series Internet Router Quality of Service Configuration Guide*.

External Border Gateway Protocol Label Distribution

The External Border Gateway Protocol (EBGP) Label Distribution feature enables you to configure a carrier supporting carrier network that uses BGP to distribute routes and MPLS labels between the provider edge (PE) and customer edge (CE) routers of a backbone carrier and a customer carrier. The backbone carrier offers BGP and MPLS VPN services. The customer carrier can be one of the following:

- An Internet service provider (ISP) with an IP core
- An MPLS service provider with or without VPN services

For information on how to use BGP to distribute MPLS labels and routes for both types of customer carrier, refer to the [MPLS VPN Carrier Supporting Carrier—IPv4 BGP Label Distribution, Release 12.0\(21\)ST feature module](#) and the [Inter-Autonomous Systems for MPLS VPNs, Release 12.1\(5\)T feature module](#).

QA Error Recovery

The QA Error Recovery feature enables the router to recover quickly from problems known as QAERRORs, which can be caused by hardware or software issues. When a QAERROR occurs, the router might stop responding while it tries to recover from the problem. QA error recovery reduces the router down time to as little as one second. Previously, a fully loaded router might be down for up to five minutes (300 seconds).

The QA error recovery feature is enabled by default. To disable the feature, issue the following command:

```
no hw-module main-cpu qaerror-recovery-enable
```

When QA error recovery is successful, the router displays a console message indicating success. In addition, the **show controllers cbus** command indicates the number of QAERROR recoveries.

The following sample console messages show an occurrence of a QAERROR and the router's recovery from the error. The router might display additional messages during error recovery (which can help service technicians diagnose the cause of the problem).

```
%QA-3-DIAG:Trying to recover from QA ERROR.
%QA-3-DIAG:Removing buffer header 0xE360 from all queues
%QA-3-DIAG:Buffer 0xE360 is element 155 on queue 0x2E
%QA-3-DIAG:Queue 0x2E (48000170) has 154 elements
%QA-3-DIAG:Buffer 0xE360 is element 1 on queue 0x340
%QA-3-DIAG:Queue 0x340 (48001A00) has 0 elements
%QA-3-DIAG:At least one QA queue is broken
%QA-3-DIAG:Recovered from QA ERROR
```

The following example shows QA error recovery information in **show controllers cbus** command output:

```
Router# sh controllers cbus
MEMD at E0000000, 8388608 bytes (unused 1565056, recarves 5, lost/qaerror recoveries 0/0)
.
.
.
Router#
```

New Features in Cisco IOS Release 12.0(25)S

The following is a brief list of the new features in Cisco IOS Release 12.0(25)S on which Cisco IOS Release 12.0(25)SX is based. Only new features that are supported by the Cisco 10000 series Internet router are listed here. New features for other platforms (such as the Cisco 12000 series Internet router) are not listed.

Link Fragmentation and Interleaving

Introduced on the Cisco 10000 series router in Cisco IOS Release 12.0(23)SX, 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. The feature supports Frame Relay (FRF.12) end-to-end and Multilink PPP (MLPPP).

Single Rate 3-Color Marker for Traffic Policing

Introduced on the Cisco 10000 series router in Cisco IOS Release 12.0(23)SX, 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). This feature is useful, for example, for ingress policing of a service, where service eligibility is determined only by the burst's length, and not its peak rate.

Multicast VPN

The Multicast for Multiprotocol Label-Switching (MPLS)/Virtual Private Network (VPN) feature enables service providers to offer multicast services over their MPLS core network. This feature was introduced on the Cisco 10000 series router in Cisco IOS Release 12.0(23)SX.

OSPF Support for a Redistribution Limit of Maximum-Prefixes Imported

This feature enables you to limit the number of routes that can be redistributed into the Open Shortest Path First (OSPF) protocol. The feature helps to eliminate the potential for flooding that might occur when a large number of routes are accidentally redistributed into OSPF.

ISIS Route Redistribution Limit

This feature enables you to limit the number of routes that can be redistributed into the Intermediate System-to-Intermediate System (IS-IS) protocol. This feature helps to eliminate the potential for flooding that might occur when a large number of routes are accidentally redistributed into IS-IS.

OSPF Support for Link State Advertisement Throttling

This feature enables you to slow down the rate at which the Open Shortest Path First (OSPF) protocol sends Link State Advertisement (LSA) updates during periods of network instability. This feature uses a back-off algorithm to perform the LSA throttling.

Limitations and Restrictions

3-Level Policies

The following limitations and restrictions apply to the Cisco 10000 series router 3-Level Policies feature:

- A top-level policy must specify only the class named *class-default* with only the **shape** command specified before the **service-policy** command attaches an inner policy.
- In an inner policy, to attach a **service-policy** command to a class's bottommost policy, do not configure the **police** and **set** commands for the class. Classes without a **service-policy** command configured are not restricted from using the **police** and **set** commands.
- In a bottommost policy, configure only the **police** and **set** commands for a class.
- Define each bottommost class map to match only those packets that also match its parent class map. For example, the union of the set of packets of a bottommost class and that of its parent class must be equal to the set of packets that match the parent class.
- The nested-policy shape rate is reserved for nested-policy traffic only. Excess bandwidth is not used for other traffic.



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.

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.

Cisco recommends that you configure the **logging rate-limit** command as follows. This limits the rate of 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, refer to the **logging rate-limit command** in the [Cisco IOS Configuration Fundamentals and Network Management Command Reference, Release 12.3](#).

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.

Testing Performance of High-Speed Interfaces

Cisco IOS software running on the Cisco 10000 series Internet 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 Cisco 10000 series Internet 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.

Therefore, to ensure accurate test results, you should test the throughput of the gigabit Ethernet, Packet over SONET (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.

Open Caveats—Cisco IOS Release 12.0(25)SX

Table 1 describes the caveats that are open in Cisco IOS Release 12.0(25)SX.

Table 1 Open Caveats

Caveat	Description
CSCea38453	<p>(Duplicate of CSCea34851) If you delete an ATM PVC bundle, the router sometimes displays the following error and traceback message (the hex values in your message may differ):</p> <pre>GENERAL-3-EREVENT: HWCEF: Failed to add adjacency callback Traceback= 600B6338 600B63A8 602B7DC0 602B8E30 602C7980 602CC4CC 60224710 601E3A80 602228A4 60225710 6037B620 6018F0D8 6038D6DC 603E5884 603E5870</pre> <p>Workaround: None. The router continues to function normally after the message appears.</p>
CSCea42432	<p>(Duplicate of CSCea52307) If you delete a service policy from an ATM interface, a traceback or error can occur.</p> <p>Workaround: None.</p>
CSCea74742	<p>Policing conformed packets might be less than expected when the normal burst size is set to less than two times the packet size.</p> <p>Workaround: Change the normal burst size to a value larger than 2 times the police frame size.</p>

Table 1 Open Caveats (continued)

Caveat	Description
CSCea93642	<p>When a large number of policy maps are configured on the Cisco 10000 router, it could take more time than expected before all the policy maps activate. Before an interface's policy map activates, the traffic on the interface receives default treatment.</p> <p>The router compiles a super access control list (ACL) for each policy map configured. On an average, the compilation of one super ACL takes approximately one-half second. When a large number of policy maps are configured, the router requires more time to compile all of the super ACLs.</p> <p>Workaround: Wait approximately 0.65 seconds for each policy-map to become operational. For more than one policy map, wait (N * 0.65) seconds for all the policy maps to become operational (where N is the number of policy maps).</p>
CSCeb02953	<p>When traffic is sent through an ATM subinterface to which a QoS service policy is attached, the packet count of the output queue obtained by using the show policy-map interface command does not match the packet output count obtained by using the show interface atm-subinterface command.</p> <p>Workaround: To obtain the correct packet output count, use the show policy-map interface command. Do not use the show interface atm-subinterface command to obtain packet output counts for ATM subinterfaces.</p>
CSCeb27728	<p>When microcode is reloading and traffic is running over the interface, the interface output packet and byte counters display incorrect values.</p> <p>Workaround: Clear the counters.</p>
CSCeb38728	<p>When removing a 3-level policy map attached to 4,000 VLAN interfaces, the Cisco 10000 series router stops responding.</p> <p>Workaround: None.</p>
CSCeb39589	<p>The output rate is incorrect when the Cisco 10000 series router applies the policy-map on ATM and Frame Relay interfaces.</p> <p>Workaround: None.</p>

Resolved Caveats—Cisco IOS Release 12.0(25)SX

This section describes caveats that were fixed in Cisco IOS Release 12.0(25)SX.

For information about caveats fixed in other Cisco IOS releases, refer to the appropriate Release Note document at the following URL:

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

CSCea28131

A Cisco device running IOS and enabled for the Border Gateway Protocol (BGP) is vulnerable to a Denial of Service (DOS) attack from a malformed BGP packet. The BGP protocol is not enabled by default, and must be configured in order to accept traffic from an explicitly defined peer. Unless the malicious traffic appears to be sourced from a configured, trusted peer, it would be difficult to inject a malformed packet. BGP MD5 is a valid workaround for this problem.

Cisco has made free software available to address this problem. For more details, please refer to this advisory, available at <http://www.cisco.com/warp/public/707/cisco-sa-20040616-bgp.shtml>.

CSCea55878

When you attach a policy map with policing configured to a Frame Relay main interface with one subinterface configured, the Cisco 10000 router classifies all of the traffic with the first class configured and policing works as expected for the first class. When you attach a policy map to a Frame Relay main interface with no subinterfaces configured, the router classifies all of the traffic with the first class configured, but policing fails for the first class. This has been fixed.

CSCea62765

When you configure policing on a high speed interface such as a gigabit Ethernet or VLAN interface with a 1 Gbps shape rate, if you set the normal and maximum burst sizes too small (for example, 2375 and 4750 respectively), policing fails. This has been fixed.

CSCea66266

When you attach a policy map with policing and 30 class maps configured to 4,000 VLAN interfaces, and you enter the **show class-map** command, policing statistics do not display for all of the VLAN interfaces configured. This has been fixed.

CSCea70491

The maximum number of class maps that you can configure for the Cisco 10000 series router is limited to 32 instead of 256. This has been fixed.

CSCea74836

When you configure and attach 4,000 policy maps to 4,000 virtual circuits (VCs), CPUHOG messages such as the following appear:

```
01:00:52: %SYS-3-CPUHOG: Task ran for 3812 msec (0/0), process = Exec,
PC = 604AA76C.
-Traceback= 604AA774 604AAA98 604651D0 60465880 604669A4 60178E20
60020808 600988C8 60179038 600AB10C 600B0038 600B0070 6013D720 6037B6A0
6018FD28 6038D75C
```

This has been fixed.

CSCea75008

When you configure and attach 4,000 policy maps, policy ACLs fail and traceback messages such as the following appear:

```
01:10:40: %GENERAL-3-EREVENT: can't create any more policy acl
-Traceback= 6011F9EC 60120204 601203A4 603E5DF4 603E5DE0
c10k_sys_4b#
```

This has been fixed.

CSCea75766

When you attach a nested policy map with a shape rate of 875kbps to a T1 Frame Relay interface with percent-based policing configured, policing no longer fails.

CSCea77129

The class map drop rate counter sets to a large value (for example, 937877248 bps) when you change the policing configuration while traffic is running. This has been fixed.

CSCea77454

When you change the shape rate in a top-level nested policy map, the shape rate change correctly replicates in the bottom-level policy map as expected; however, the policing function for the bottom-level uses the original shape rate. This has been fixed.

CSCea89069

After you enter the **micro reload pxf** command to reload the Cisco IOS microcode image on the performance routing engine (PRE), the default class for both the 2-level and 3-level policy maps indicate the same number of packets dropped (4294967280) when you enter the **show policy interface** command. This has been fixed.

CSCea93446

When you start a secondary performance routing engine (PRE) from the ROM monitor while 4,000 policies are running on a primary PRE and the policies are attached to 4,000 ATM virtual circuits (VCs), the secondary PRE enters a COLD-BULK SYNC state and fails. This has been fixed.

CSCeb01520

When you attach a policy map with weighted random early detection (WRED) configured to a gigabit Ethernet interface, the Cisco 10000 series router sets the queue size to 64. This has been fixed.

CSCeb02093

When you delete a class in a 3-level policy map and then reconfigure the class again, the following assertion error appears when you enter the **show policy-map interface** command:

```
Assertion failure in ../toaster/c10k_rp/c10k_police.c (642) <*****
ip dscp 0 1 2 3 (1065)
```

When you enter the **show log** command, the following traceback message appears:

```
-Traceback= 60104920 60435108 60435204 60435204 60434D00 6010B82C 60436AE8
             60436BCC 6037B8A0 6018FF40 6038D95C 603E5AF4 603E5AE0
```

This has been fixed.

CSCeb04974

When you attach a 3-level policy map with more than 32 classes configured, the following assertion error appears:

```
Assertion failure in ../toaster/c10k_rp/c10k_qos.c (3391)
Too many classes (36) specified in nested policy-map
Assertion failure in ../toaster/c10k_rp/c10k_qos.c (569)
Single-level transformation failed
```

When you enter the **show log** command, traceback messages such as the following appear:

```
00:32:54: -Traceback= 600FB7D8 600FBD60 60431AB8 60433820 604338CC 604335D8
60438C28 60438DEC 6037B8A0 6018FF40 6038D95C 603E5AF4 603E5AE0
```

This has been fixed.

CSCeb07784

When you change the shape rate in a top-level policy attached to a Frame Relay or gigabit Ethernet VLAN subinterface, the shape rate is incorrect when you enter the **show policy-map interface** command. This has been fixed.

CSCeb07983

When you enter the **show policy-map interface** command to display policy map statistics for each interface, the Cisco 10000 series router no longer displays a traceback message.

CSCeb20630

When you ran 15 negative configuration test on a 3-level policy map and attached the policy map to a gigabit Ethernet interface, the Cisco 10000 series router was left in a state to fail after the last configuration completed. Previously, when you logged in to the router and entered the **no policy-map** command to delete the policy map, the router failed with the following traceback message. This has been fixed.

```
-Traceback= 603F78F0 603F8080 600F25D8 600F2654 600F2BDC 600F4CE8 600EB5F0
            600F0DF4 600FCCA8 600FCD80 60433638 604352D0 6043544C 6043569C
```

CSCeb24061

When you attach a 2-level nested policy map to a gigabit Ethernet interface, the Cisco 10000 series router incorrectly sets percentage-based policing. This has been fixed.

CSCeb36978

During the configuration of 12,000 DLCIs, a memory out-of-range error occurs, which causes the Cisco 10000 series router to reset. This has been fixed.

CSCeb46300

When you configure a policy map with weighted random early detection (WRED) and all eight of the precedence values configured, and you attach it to a Frame Relay main interface, the Cisco 10000 series router classifies all of the traffic with precedence 0. This has been fixed.

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 the Documentation CD-ROM (product number DOC-CONDOCCD=) 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

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>

- Registered Cisco.com users can order the Documentation CD-ROM (Customer Order Number DOC-CONDOCCD=) 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 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://www.cisco.com>

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.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

Cisco TAC Website

You can use the Cisco TAC website to resolve P3 and P4 issues yourself, saving cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software:

<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, EtherFast, EtherSwitch, Fast Step, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, 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 United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0403R)

Copyright © 2003–2004 Cisco Systems, Inc.
All rights reserved.