



Release Notes for the Cisco 10000 Series Router for Cisco IOS Release 12.0(25)SX7

May 7, 2004

These release notes provide information about Cisco IOS software Release 12.0(25)SX7 for the Cisco 10000 series 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)SX7 is based on Cisco IOS Release 12.0(25)S. The Cisco 10000 router supports a subset of the new features in Cisco IOS Release 12.0(25)S. For more information, see the “[New Features—Cisco IOS Release 12.0\(25\)S](#)” section on page 7. This section lists the features supported on the Cisco 10000 router.

To view the release notes for the following Cisco IOS software releases, go to the following URLs:

- Cisco IOS Release 12.0 SX:

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

- Cisco IOS Release 12.0 S:

<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 © 2004 Cisco Systems, Inc. All rights reserved.

Contents

These release notes contain the following sections:

- [System Requirements](#), page 2
- [New Features—Cisco IOS Release 12.0\(25\)SX7](#), page 3
- [New Features—Cisco IOS Release 12.0\(25\)SX1](#), page 4
- [New Features—Cisco IOS Release 12.0\(25\)SX](#), page 5
- [New Features—Cisco IOS Release 12.0\(25\)S](#), page 7
- [Limitations and Restrictions](#), page 8
- [Open Caveats—Cisco IOS Release 12.0\(25\)SX7](#), page 8
- [Resolved Caveats—Cisco IOS Release 12.0\(25\)SX7](#), page 9
- [Obtaining Documentation](#), page 11
- [Documentation Feedback](#), page 12
- [Obtaining Technical Assistance](#), page 12
- [Obtaining Additional Publications and Information](#), page 14

System Requirements

This release requires that you have the performance routing engine (PRE), part number ESR-PRE1 installed in the Cisco 10000 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
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 Router Software Configuration Guide* located 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* 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 12.0(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)SX7, 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)SX7 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 Router Software Configuration Guide*.

<http://www.cisco.com/univercd/cc/td/doc/product/aggr/10000/config/10ksw/startos.htm#1035847>

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—Cisco IOS Release 12.0(25)SX7

Cisco IOS Release 12.0(25)SX7 contains no new features, but includes all of the new features and performance enhancements introduced in Cisco IOS Release 12.0(25)SX1 and Cisco IOS Release 12.0(25)SX, which is based on Cisco IOS Release 12.0(25)S.

For more information, see the following sections in this document:

- [New Features—Cisco IOS Release 12.0\(25\)SX1, page 4](#)
- [New Features—Cisco IOS Release 12.0\(25\)SX, page 5](#)
- [New Features—Cisco IOS Release 12.0\(25\)S, page 7](#)

New Features—Cisco IOS Release 12.0(25)SX1

Cisco IOS Release 12.0(25)SX1 provides the following performance enhancements, but contains no new features.

VTMS Link Utilization

This release improves the performance of the VTMS Link Utilization feature. The default queue size is based on link bandwidth instead of queue bandwidth as in previous releases.

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

New Features—Cisco IOS Release 12.0(25)SX

Cisco IOS Release 12.0(25)SX introduces support on the Cisco 10000 series router for the following features:

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 series 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 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 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 earlier than 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 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 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 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 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*.

New Features—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 Cisco 10000 series router are listed here. New features for other platforms (such as the Cisco 12000 series router) are not listed.

Link Fragmentation and Interleaving

Introduced on the Cisco 10000 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 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 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.

Open Caveats—Cisco IOS Release 12.0(25)SX7

Table 1 describes the caveats that are open in Cisco IOS Release 12.0(25)SX7.

Table 1 Open Caveats in Cisco IOS Release 12.0(25)SX7

Caveat	Description
CSCea42432	(Duplicate of CSCea52307) If you delete a service policy from an ATM interface, a traceback message or error message may appear. Workaround: None.
CSCea74742	Policing conformed packets might be less than expected when the normal burst size is set to less than two times the packet size. Workaround: Change the normal burst size to a value larger than 2 times the police frame size.

Table 1 Open Caveats in Cisco IOS Release 12.0(25)SX7

Caveat	Description
CSCea93642	<p>When a large number of policy maps are configured on the Cisco 10000 Cisco 10000 series 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>Under extremely rare circumstances, when you remove a 3-level policy map attached to 4,000 VLAN interfaces, the Cisco 10000 series router stops responding.</p> <p>Workaround: None.</p>

Resolved Caveats—Cisco IOS Release 12.0(25)SX7

This section describes caveats that were fixed in Cisco IOS Release 12.0(25)SX7.

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>

CSCdw33267

Previously, when a Multiprotocol Label Switching (MPLS) edge router performed hardware-assisted forwarding, the hardware and software MPLS forwarding tables might be inconsistent. An example of an MPLS edge router is a provider edge (PE) router in an MPLS virtual private network (VPN).

This problem occurred when you executed either of the following command sequences on the MPLS edge router:

- The **shutdown** command followed by the **no shutdown** command on one of the outgoing interfaces enabled for MPLS.
- The **no mpls ldp** command followed by the **mpls ldp** command on one of the outgoing interfaces enabled for MPLS.

CSCed41422

Previously, when you changed the type of service (TOS) on packets encapsulated in a Multiprotocol Label Switching (MPLS) virtual private network (VPN) tunnel, the TOS of the interior (encapsulated) packet did not change appropriately and was classified incorrectly at the de-encapsulating router.

This problem occurred when you applied input policing to an interface, associated a virtual routing and forwarding (VRF) instance with the interface, the interface was receiving multicast traffic from the customer edge (CE) router, and the router was configured for MPLS VPN.

CSCed49302

Previously, under a specific configuration using multiple E1 (framed or unframed) interfaces and 1500-byte IP packets, the maximum priority queue (PQ) latency was greater than 2 times the specified maximum transmission unit (MTU) plus 6 milliseconds. The following describes the conditions under which this problem occurred.

Seven queues were configured on each (1984k) E1 interface with the following bandwidths: PQ - 98k, C1 - 256k, C2 - 256k, C3 - 256k, C4 - 256k, CD - 98k, and MGMT - 20k.

The high latency was observed with 20 interfaces configured and bidirectional traffic was being sent at the following (per interface) pps rates to each queue, respectively:

1984k: PQ - 1733, C1 - 8, C2 - 21, C3 - 21, C4 - 21, CD - 8, MGMT - 2

2048k: PQ - 1789, C1 - 9, C2 - 21, C3 - 21, C4 - 21, CD - 9, MGMT - 2

CSCed50382

Previously, when you configured class-based weighted fair queuing (CBWFQ) on a Frame Relay permanent virtual circuit (PVC), queues could drop packets even if there was no traffic on other queues on the same link and the input traffic was less than the link bandwidth. This occurred when queue bandwidth was configured as a small percentage of link bandwidth.

CSCed72686

Previously, an ACL applied to an ATM subinterface might not function correctly after a PRE switchover. This problem occurred in a Cisco 10008 router that was configured with a PRE2.

CSCed80196

Previously, when you configured Multiprotocol Label Switching (MPLS) over Multilink PPP (MLPPP), the parallel express forwarding (PXF) microcode reloaded. After the PXF microcode reloaded, packet forwarding resumed.

CSCed86431

Previously, the parallel express forwarding (PXF) processor could drop ATM adaptation layer 5 (AAL5) Connectionless Network Service (CLNS) Intermediate System-to-Intermediate System (IS-IS) packets when the path from the PXF processor to the route processor (RP) was congested. This could occur when the RP was very busy.

CSCed87455

Previously, when you deleted an access control list (ACL) used in many route maps, SuperACL process memory usage increased significantly.

CSCed88967

Previously, when redundant Performance Routing Engines (PREs) were configured, the **write memory** command was in progress on the active PRE, an application on the standby PRE accessed standby NVRAM, and then there was a switchover to the standby PRE, an error message appeared similar to:

```
startup-config file open failed (Device or resource busy)
```

CSCed90701

Previously, when you attached a policy map to a Multilink PPP (MLPPP) interface or when links were added to an MLPPP interface and then the Cisco 10000 series router reloaded, the packet queue size on an MLPPP bundle could be larger than necessary. This could reduce scalability during the configuration of multiple MLPPP interfaces, because the system could run out of resources to allocate the packet queues. There could be substantial traffic congestion, because traffic that should have been dropped due to queue overflow was not dropped.

CSCed90731

Previously, when new links were added to a Multilink PPP (MLPPP) interface that already had a policy map with priority class attached, the priority traffic on the MLPPP interface could exceed the configured bandwidth limits. Links could be added as result of a system reload or bootup, the link going up or down, or the user configuring more links on the bundle.

CSCed90846

Previously, when network interfaces were operating at or above OC-3 speeds and a policy map class containing the **priority percent** *percentage* command was loaded at or greater than the specified rate, other classes were left with less than their fair share of the bandwidth and their bandwidth ratio was adversely affected.

CSCee04454

Previously, the router reloaded unexpectedly as ATM VCs came up. This problem occurred when ACLs were applied on ATM interfaces, and only rarely then, on images that contain the fix for CSCed72686.

CSCee22454

Previously, the router dropped packets when Unicast Reverse Path Forwarding (URPF) was configured on an interface. This problem occurred when the router had 2 paths (outgoing interfaces) to a destination in the FIB table and URPF was enabled on one of the outgoing interfaces.

CSCee34520

Previously, the router stopped forwarding traffic for some load balanced recursive prefixes, such as a BGP route with equal cost IGP paths to the BGP next hop. If any Multiprotocol Label Switching (MPLS) Label Distribution Protocol (LDP) adjacency on the router flapped or the router itself flapped, the hardware loadshare pointers for the recursive prefixes could point to old information because Cisco Express Forwarding (CEF) did not send updates to the Parallel Express Forwarding (PXF) processor with new label information.

CSCin74347

Previously, outbound security ACLs were not applied properly on Cisco 10000 Series routers. This problem occurred on all 12.0S images that contain the fix for CSCed72686.

CSCuk44928

Previously, when you configured redundant Performance Routing Engines (PREs) and saved the configuration first to the standby PRE and then to the active PRE, the configuration might not be saved. Additionally, an error message appeared similar to the following:

```
startup-config file open failed (Device or resource busy)
```

Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain 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 at this URL:

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

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

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

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 Ordering tool:
<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, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can send comments about technical documentation to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or 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

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

Cisco Technical Support Website

The Cisco Technical Support Website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, 365 days a year at this URL:

<http://www.cisco.com/techsupport>

Access to all tools on the Cisco Technical Support Website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

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

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool automatically provides recommended solutions. If your issue is not resolved using the recommended resources, your service request will be assigned to a Cisco TAC engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco TAC engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553 2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your 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.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

Obtaining Additional Publications and Information

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

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

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

- 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://cisco.com/univercd/cc/td/doc/pcat/>

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

<http://www.ciscopress.com>

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

<http://www.cisco.com/packet>

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. 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/ipj>

- World-class networking training is available from Cisco. You can view current offerings at this URL:

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

DVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, Home, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath 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. (0709R)

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

♻️ Printed in the USA on recycled paper containing 10% postconsumer waste.