Release Notes for Cisco uMG9850 QAM Module, Cisco IOS Release 12.2(20)EU1

May 12, 2005

These release notes describe the features, memory requirements, and hardware and software requirements in Cisco IOS release 12.2(20)EU1 to support the Cisco uMG9850 QAM Module. The Cisco uMG9850 supports the ITU-T J.83 Annex B standard for the delivery of digital video and audio signals.

Note This document supersedes and replaces *Release Notes for Cisco uMG9850 QAM Module, Cisco IOS Release 12.2(20)EU*. That software release is no longer available. For more information, see Introduction, page 2.

Note Use these release notes with *Release Notes for Cisco Catalyst 4500 Series Switch, Cisco IOS Release 12.2(20)EWA*, located on Cisco.com. Refer to Obtaining Documentation, page 10.

These release notes discuss the following topics:

CISCO SYSTEMS

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

Document History

Document Version	Date	Notes
1	05/12/2005	This document was first published for Cisco IOS Release 12.2(20)EU1. For more information, see Introduction, below.

Introduction

Cisco IOS Release 12.2(20)EU1 is an Early Deployment (ED) release based on Cisco IOS Release 12.2(20)EWA.

This document supersedes and replaces *Release Notes for the Cisco uMG9850 QAM Module, Cisco IOS Release 12.2(20)EU*.

Although Cisco IOS Release 12.2(20)EU has been removed from CCO, no catastrophic or deferring defect exists. You do not need to upgrade your images. A legacy feature has been removed, and images with that feature are no longer available on CCO. You may continue to operate with existing copies of Cisco IOS Release 12.2(20)EU in your network.

For more information, see Resolved Caveats—Release 12.2(20)EU1, page 8.

Note Cisco IOS Release 12.2(20)EU1 is compatible with Cisco IOS Release 12.2(20)EWA. Cisco IOS Release 12.2(20)EU1 is designed, however, to support the functionality of the Cisco uMG9850 in VoD and digital broadcast applications. Not all features applicable to traditional switching apply to the Cisco uMG9850. For configuration instructions and the command reference for the Cisco uMG9850, refer to *Configuring the Cisco uMG9850 QAM Module* in Obtaining Documentation, page 10.

The Cisco uMG9850, designed for the Cisco Catalyst 4500 series switches, provides video-on-demand (VoD) and digital broadcast services for a hybrid fiber-coaxial (HFC) cable network. It accepts Moving Pictures Expert Group-2 (MPEG-2) digital video from an IP network, and outputs the video as a quadrature amplitude modulated (QAM) RF stream that can be received by digital set-top boxes (STBs) over the cable network.

System Requirements

This section describes the system requirements for Cisco IOS Release 12.2(20)EU1:

- Memory
- Supported hardware
- Supported features
- Unsupported features

Memory Requirements

Minimum memory and flash configurations on the Cisco Catalyst 4500 series switch are sufficient to support the Cisco uMG9850 QAM Module.

Hardware Compatibility

Table 1 on page 3 lists hardware that is compatible with the Cisco uMG9850 QAM Module when used with Cisco IOS Release 12.2(20)EU1.

Table 1 Hardware Compatibility

	Product Number	Description	Notes
Cisco Catalyst Switches	WS-C4503	Cisco Catalyst 4503 switch chassis	
	WS-C4506	Cisco Catalyst 4506 switch chassis	
	WS-C4507R	Cisco Catalyst 4507R switch chassis	
Memory	MEM-C4K-FLD64M=	Cisco Catalyst 4500 Series Compact Flash, 64-MB option	
	MEM-C4K-FLD128M=	Cisco Catalyst 4500 Series Compact Flash, 128-MB option	
Supervisor Engine	WS-X4013+	Cisco Catalyst 4500 Series Supervisor Engine II-Plus	
	WS-X4013+/2	Cisco Catalyst 4507R Redundant Supervisor Engine II-Plus	
	WS-X4515	Cisco Catalyst Supervisor Engine IV	
	WS-X4515/2	Cisco Catalyst 4507R Redundant Supervisor Engine IV	

Table 1 Hardware Compatibility (Continued)

	Product Number	Description	Notes
Power Supplies	PWR-C45-1000AC	1000 W AC power supply	For the Cisco Catalyst 4506 or Cisco Catalyst 4507R switch chassis, can be configured with up to three Cisco uMG9850 QAM Modules. With four or five modules inserted in the Cisco Catalyst 4506 or 4507R switch chassis, the 1400W (AC or DC) power supply must be used. Can be configured with the maximum number of Cisco uMG9850 QAM Modules in the Cisco Catalyst 4503 switch chassis.
	PWR-C45-1000AC/2	Redundant power supply	Can be configured along with the 1000 W AC power supply.
	PWR-C45-1400DC-P	1400 W DC power supply with integrated power entry module (PEM)	For either switch chassis, can be configured with up to five Cisco uMG9850 QAM Modules.
	PWR-C45-1400DC-P/2	Redundant power supply	Can be configured along with the 1400 W DC power supply.
	PWR-C45-1400AC	1400 W AC power supply	Can be configured with the maximum number of Cisco uMG9850 QAM Modules in the Cisco Catalyst 4506 or 4507R switch chassis.
	PWR-C45-1400AC/2	Redundant power supply	Can be configured along with the 1400 W AC power supply.
Switching Modules	WS-X4148-RJ=	48-port 10/100 Fast Ethernet RJ-45 switching module	
	WS-X4306-GB=	6-port 1000BASE-X (GBIC) Gigabit Ethernet switching module	
	WS-X4712-UMG9850	Cisco Catalyst 4500 QAM Module, 12 RF ports, 24 QAM channels, ITU-T J.83 Annex B	
SFPs	GLC-SX-MM=	1000BASE-SX SFP	
	GLC-LX-SM=	1000BASE-LX SFP	
	CWDM-SFP-XXXX=	Cisco CWDM SFP	XXXX=wavelength

Table 1 Hardware Compatibility (Continued)

	Product Number	Description	Notes
GBICs	WS-G5483=	1000BASE-T GBIC	
	WS-G5484=	1000BASE-SX short-wavelength GBIC (multimode only)	
	WS-G5486=	1000BASE-LX/LH long-haul GBIC (single-mode or multimode)	
	WS-G5487=	1000BASE-ZX extended-reach GBIC (single-mode)	
	CWDM-GBIC-xxxx	Cisco 1000BASE-CWDM xxxx nm GBIC, where xxxx is the number 1470, 1490, 1510, 1530,1550, 1570, 1590, or 1610	
	DWDM-GBIC-xx.yy	Cisco 1000BASE-DWDM ITU 100-GHz grid 15xx.yy nm GBIC	
	WDM-GBIC-REC=	Cisco receive-only 1000BASE-WDM GBIC	

Software Compatibility

The Cisco uMG9850 QAM Module is supported in Cisco IOS Release 12.1(20)EU, Cisco IOS Release 12.1(20)EU1, and Cisco IOS Release 12.2(20)EU1 (this release). Images for Cisco IOS Release 12.2(20)EU1 are listed in Table 2 and are available from Cisco.com at this URL:

http://www.cisco.com/cgi-bin/Software/Iosplanner/Planner-tool/iosplanner.cgi?get_crypto=&data_from=&hardware_name=&software_name=&release_name=12.2.20-EU1&majorRel=12.2&state=:RL&type=Early%20Deployment

Table 2 Cisco IOS Software Release 12.2(20)EU1 Images and Features

Image	Description
cat4000-i9su3-mz	Cisco IOS software for the Cisco uMG9850 QAM Module—Basic MPEG-2 digital video gateway software image, including Routing Information Protocol (RIP) v1 and v2, and static routes.
cat4000-i5su3-mz	Cisco IOS software for the Cisco uMG9850 QAM Module—Enhanced MPEG-2 digital video gateway plus routing software image, including Open Shortest Path First (OSPF), Intermediate System to Intermediate System (IS-IS), Interior Gateway Routing Protocol (IGRP), and Enhanced IGRP (EIGRP).

Determining the Software Version

To determine the version of Cisco IOS software running on a Cisco Catalyst 4500 series switch, log in to the switch and enter the **show version** EXEC command:

```
Switch> show version

Cisco Internetwork Operating System Software
```

```
IOS (tm) Catalyst 4000 L3 Switch Software (cat4000-cat4000-i9su3-mz), Version
12.2(20)EU1, EARLY DEPLOYMENT RELEASE SOFTWARE (fc1)
```

Upgrading from a Previous Software Release

Updating the Switch Software

For information on upgrading software in your Cisco Catalyst 4500 series switch, refer to *Release Notes for the Catalyst 4500 Series Switch, Cisco IOS Release 12.2(20)EWA on Cisco.com* at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat4000/relnotes/ol_5184.htm

Updating the Video Routing Configuration

The configuration of video routing has changed with Cisco IOS Release 12.2(20)EU1. If video routing was configured using the Cisco IOS Release 12.1(20)EU1, the video routing command must be changed to the new syntax.

If all the Cisco uMG9850 QAM modules in a chassis are currently configured into the same subnet, either the traffic has to be combined so that it flows to one single IP address in the subnet, or multiple subnets should be used. If separate subnets were used for each Cisco uMG9850, then only the video routing command and VLAN change are needed. (See Video Routing on VLAN Interfaces, page 7.)

For detailed information, refer to “Configuring Video Routing” under “How to Configure the Cisco uMG9850 QAM Module” in *Configuring the Cisco uMG9850 QAM Module* on Cisco.com at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/cable/vod/umg9850/9850cfg.htm

New and Changed Information

This section describes new or changed information in Cisco IOS Release 12.2(20)EU1.

Digital Broadcast

Digital broadcast service provides the cable subscriber with a large selection of programs and a high-quality picture. The digital video content is typically received from a satellite broadcasting to a receiver at the headend, from where it is delivered in real time to all subscribers in the cable system. A statistical multiplexer is often used in the headend to combine broadcast programs from multiple sources and generate a multiple program transport stream (MPTS) for delivery to the STBs. Program data is also sent to the STB client application, to enable the cable subscriber to browse and select a broadcast program for viewing.

The Cisco uMG9850 supports the following key features for delivering digital broadcast services:

- Multicast Sessions

  This feature enables the Cisco uMG9850 to receive video streams via IP multicast.

  Each digital broadcast program is typically delivered to all STBs in a cable system. Multiple QAM channels are allocated for digital broadcast programs, and each QAM channel is electrically split for delivery to each service group. In order to use the IP network most efficiently, digital broadcast programs are multicast by the statistical multiplexer (or other video source) to the Cisco uMG9850.

The Cisco uMG9850 uses the multicast group address, and source address of each multicast session to route each incoming program to the correct QAM channels. The relationship between the multicast group address and QAM channel is predetermined by user commands on the Cisco uMG9850 Module.

- MPTS Pass-Through

  This feature causes an MPTS session to be passed through to the selected QAM channel.

  Digital broadcast services are typically delivered in an MPTS from a statistical multiplexer (or other video source) to the Cisco uMG9850. The Cisco uMG9850 passes the MPTS through to the STBs without multiplexing the video streams. The Cisco uMG9850 may update the PCR or TSID information in the MPTS as necessary to output a valid transport stream. The Cisco uMG9850 outputs the MPTS on one or more QAM channels based on the UDP port map (for unicast sessions) or multicast group address (for multicast sessions) of the incoming stream.

- Stream Cloning

  This feature provides a way to clone (map) a video stream to several or all QAM channels on a Cisco uMG9850. Cloning is useful for digital broadcast services when the QAM channels are not electrically split for delivery to all service groups.

  Multicast streams can be cloned to QAM channels on multiple Cisco uMG9850s, while unicast streams can be cloned to QAM channels on a single Cisco uMG9850.

Video Routing on VLAN Interfaces

With this release, each Cisco uMG9850 module no longer functions as an IP host. The supervisor engine in the Cisco Catalyst 4500 series switch plays that role, allowing for the aggregation of video traffic. This requires fewer IP addresses and simplifies IP network designs.

The **video** *slot* **route** command sets up the routing of UDP/IP (video) packets to the Cisco uMG9850. Acting as the IP host, the supervisor engine generally receives video traffic on the IP address configured on a VLAN. When the IP address of the selected VLAN is configured as the destination IP address of the video packets, any video packet destined to this IP address—and whose destination port matches the UDP range specified for video by this command—is routed to the selected Cisco uMG9850.

New MIBs

This release supports the following new MIB:

CISCO-VIDEO-NETWORK-EXT-MIB

Limitations and Restrictions

This section lists limitations or restrictions of the functionality of this release.

Interleaver Settings and MPEG Analyzers

The default interleaver setting (128,4) may not work with some MPEG analyzers, such as the Tektronix MTM400 MPEG Transport Stream Monitor. Other interleaver settings should be used.

Caveats

Caveats describe unexpected behavior in Cisco IOS Release 12.2(20)EU1 specific to the Cisco uMG9850 QAM Module. Workarounds are provided where available.

Open Caveats—Release 12.2(20)EU1

This section lists the open caveats for Cisco IOS Release 12.2(20)EU1.

- CSCeg43631

  Simultaneous changes to both PAT and PMT data in unicast session causes an "Invalid PSI" error message to display.

Resolved Caveats—Release 12.2(20)EU1

This section lists caveats resolved in Cisco IOS Release 12.2(20)EU1.

- CSCsa81379

  NetFlow Feature Acceleration has been deprecated and removed from Cisco IOS. The global command **ip flow-cache feature-accelerate** will no longer be recognized in any IOS configuration.

  If your router configuration does not currently contain the command **ip flow-cache feature-accelerate**, this change does not affect you.

  This removal does not require an upgrade of your existing installation.

  The removal of NetFlow Feature Acceleration does not affect any other aspects of Netflow operation, for example, access list processing. The features are separate and distinct.

  Cisco Express Forwarding (CEF) supersedes the deprecated NetFlow Feature Acceleration.

  Additionally, the following MIB objects and OIDs have been deprecated and removed from the NetFlow MIB (CISCO-NETFLOW-MIB):

cnfFeatureAcceleration	1.3.6.1.4.1.9.9.99999.1.3
cnfFeatureAccelerationEnable	1.3.6.1.4.1.9.9.99999.1.3.1
cnfFeatureAvailableSlot	1.3.6.1.4.1.9.9.99999.1.3.2
cnfFeatureActiveSlot	1.3.6.1.4.1.9.9.99999.1.3.3
cnfFeatureTable	1.3.6.1.4.1.9.9.99999.1.3.4
cnfFeatureEntry	1.3.6.1.4.1.9.9.99999.1.3.4.1
cnfFeatureType	1.3.6.1.4.1.9.9.99999.1.3.4.1.1
cnfFeatureSlot	1.3.6.1.4.1.9.9.99999.1.3.4.1.2
cnfFeatureActive	1.3.6.1.4.1.9.9.99999.1.3.4.1.3
cnfFeatureAttaches	1.3.6.1.4.1.9.9.99999.1.3.4.1.4
cnfFeatureDetaches	1.3.6.1.4.1.9.9.99999.1.3.4.1.5
cnfFeatureConfigChanges	1.3.6.1.4.1.9.9.99999.1.3.4.1.6

- CSCef22680

The MIB values for dvnOutQamPmtInterval and cvnOutPatInterval are incorrect. If the PSI interval is set at the chassis level, then the QAM level should be set with the same value.

- CSCeg03471

  The wrong destination source address is displayed if the same UDP source and destination are entered from two different servers.

Note Caveats CSCef44699 and CSCef60659 are identical.

- CSCef44699

  A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled “ICMP Attacks Against TCP” (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP “hard” error messages
  2. Attacks that use ICMP “fragmentation needed and Don’t Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
  3. Attacks that use ICMP “source quench” messages

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

  Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

  This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml.

  The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en.

- CSCef6059

  A document that describes how the Internet Control Message Protocol (ICMP) could be used to perform a number of Denial of Service (DoS) attacks against the Transmission Control Protocol (TCP) has been made publicly available. This document has been published through the Internet Engineering Task Force (IETF) Internet Draft process, and is entitled “ICMP Attacks Against TCP” (draft-gont-tcpm-icmp-attacks-03.txt).

  These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:

  1. Attacks that use ICMP “hard” error messages
  2. Attacks that use ICMP “fragmentation needed and Don’t Fragment (DF) bit set” messages, also known as Path Maximum Transmission Unit Discovery (PMTUD) attacks
  3. Attacks that use ICMP “source quench” messages

  Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.

  Multiple Cisco products are affected by the attacks described in this Internet draft.

Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.

This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml.

The disclosure of these vulnerabilities is being coordinated by the National Infrastructure Security Coordination Centre (NISCC), based in the United Kingdom. NISCC is working with multiple vendors whose products are potentially affected. Its posting can be found at: http://www.niscc.gov.uk/niscc/docs/re-20050412-00303.pdf?lang=en.

Related Documentation

Platform-Specific Documents

For a list of documents for the Cisco Catalyst 4500 series switch, refer to the *Release Notes for the Catalyst 4500 Switch, Cisco IOS Release 12.2(20)EWA* on Cisco.com at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat4000/relnotes/ol_5184.htm

Hardware Documents

For instructions for installing the Cisco uMG9850 QAM Module in a Cisco Catalyst 4500 series switch, refer to *Quick Start Guide—Installing the Cisco uMG9850 QAM Module* on Cisco.com at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/cable/vod/umg9850/9850qsg.htm

Software Documents

For configuration information specific to the Cisco uMG9850 QAM Module, refer to *Configuring the Cisco uMG9850 QAM Module* on Cisco.com at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/cable/vod/umg9850/9850cfg.htm

Cisco IOS Software Documentation Set

For a list of Cisco IOS software documents, refer to *Release Notes for the Catalyst 4500 Switch, Cisco IOS Release 12.2(20)EWA* on Cisco.com at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat4000/relnotes/ol_5184.htm

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

Documentation DVD

Cisco documentation and additional literature are available in a Documentation DVD package, which may have shipped with your product. The Documentation DVD is updated regularly and may be more current than printed documentation. The Documentation DVD package is available as a single unit.

Registered Cisco.com users (Cisco direct customers) can order a Cisco Documentation DVD (product number DOC-DOCDVD=) from the Ordering tool or Cisco Marketplace.

Cisco Ordering tool:

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

Cisco Marketplace:

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

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

You can order Cisco documentation in these ways:

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

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

- 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 1 800 553-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.

Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

http://www.cisco.com/go/psirt

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com
- Nonemergencies—psirt@cisco.com

Tip We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.*x* through 8.*x*.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one that has the most recent creation date in this public key server list:

http://pgp.mit.edu:11371/pks/lookup?search=psirt%40cisco.com&op=index&exact=on

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532

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

Note Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support Website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

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 provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is 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/

- *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

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.