



Release Notes for Cisco uMG9850 QAM Module, Cisco IOS Release 12.1(20)EU

April 22, 2004

These release notes describe the features, memory requirements, and hardware and software requirements in Cisco IOS release 12.1(20)EU to support the Cisco uMG9850 QAM Module on Cisco Catalyst 4500 series switches.



Note

Use these release notes with *Release Notes for Cisco Catalyst 4500 Series Switch, Cisco IOS Release 12.1(20)EW* located on Cisco.com. Refer to [Related Documentation, page 6](#).

These release notes discuss the following topics:

- [Introduction, page 2](#)
- [System Requirements, page 2](#)
- [New and Changed Information, page 4](#)
- [Limitations and Restrictions, page 5](#)
- [Caveats, page 5](#)
- [Related Documentation, page 6](#)
- [Obtaining Documentation, page 7](#)
- [Documentation Feedback, page 8](#)
- [Obtaining Technical Assistance, page 8](#)
- [Obtaining Additional Publications and Information, page 9](#)



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

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

Introduction

Cisco IOS Release 12.1(20)EU is an Early Deployment (ED) release based on Cisco IOS Release 12.1(20)EW.

**Note**

Although Cisco IOS Release 12.1(20)EU is compatible with Cisco IOS Release 12.1(20) EW, it is designed to support the functionality of the Cisco uMG9850 in VoD 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 [Related Documentation, page 6](#)

The Cisco uMG9850, designed for the Cisco Catalyst 4500 series switches, provides Video-on-Demand (VoD) 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 12.1(20)EU:

- Memory
- supported hardware
- supported features
- unsupported features

Memory Requirements

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

Hardware Compatibility

Table 1 lists hardware that is compatible with the Cisco uMG9850 QAM Module when used with Cisco IOS Release 12.1(20)EU.

Table 1 Hardware Compatibility

	Product Number	Description	Notes
Cisco Catalyst Switches	WS-C4506	Cisco Catalyst 4506 switch chassis	
	WS-C4507R	Cisco Catalyst 4507R switch chassis	
Supervisor Engine	WS-X4515	Cisco Catalyst Supervisor Engine IV	
Power Supplies	PWR-C45-1000AC	1000 W AC power supply	For either switch chassis, can be configured with up to three Cisco uMG9850 QAM Modules. With four or five modules inserted, the 1400W (AC or DC) power supply must be used.
	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	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	For either switch chassis, can be configured with up to five Cisco uMG9850 QAM Modules.
	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	
SFPs	GLC-SX-MM=	1000BASE-SX SFP	
	GLC-LX-SM=	1000BASE-LX SFP	
	CWDM-SFP-XXXX=	Cisco CWDM SFP	XXXX=wavelength

Software Compatibility

The Cisco uMG9850 QAM Module is only currently supported in Cisco IOS Release 12.1(20)EU. Images for this release are listed in Table 2 on page 4 and are available from Cisco.com at the following URL:

http://www.cisco.com/cgi-bin/Software/Iosplanner/Planner-tool/iosplanner.cgi?get_crypto=&data_from=&hardware_name=&software_name=&release_name=12.1.20-EU&majorRel=12.1&state=:RL&type=Early%20Deployment

Table 2 Cisco IOS Software Release 12.1(20)EU Images and Features

Image	Description
cat4000-i9su3-mz	Cisco IOS Software for the Cisco uMG98250 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 uMG98250 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-I9SU3-MZ), Version 12.1(20)EU, EARLY
DEPLOYMENT RELEASE SOFTWARE (fc1)
```

Upgrading to a New Software Release

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 12.1(20)EW*.

New and Changed Information

This is the initial release of support for the Cisco uMG9850 QAM module on the Cisco Catalyst 4500 series switch.

New MIBs

The following new MIB is supported:

CISCO-VIDEO-NETWORK-MIB

To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:

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

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 software release 12.1(20)EU specific to the Cisco uMG9850 QAM Module. Workarounds are provided where available.

Open Caveats—Release 12.1(20)EU

This section lists the open caveats for Cisco IOS Release 12.1(20)EU.

- CSCed63714, CSCed74155

Under some conditions, when a VoD source sends non-compliant MPEG packets, there is a potential for the Cisco uMG9850 to reset.

Resolution: (1) Check your VoD source to be sure it is not sending non-compliant MPEG packets. (2) Reload the Cisco Catalyst 4500 series switch.

- CSCed67746

Removing user-defined UDP sessions for a QAM interface does not revert to default mapping.

Workaround: Enter the **no video session** command for the QAM interface.

- CSCed69522

The maximum and average jitter measurements may not be calculated correctly for active sessions.

Use the **show video slot session active** to determine the active ports, then issue the command again on a port-by-port basis (**show video slot session UDP-port-number**) to determine the measurements.

Fixed Caveats—Release 12.1(20)EU

This section lists the caveats fixed in Cisco IOS Release 12.1(20)EU.

- CSCed27956

A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly. Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the

sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

All Cisco products which contain TCP stack are susceptible to this vulnerability.

This advisory is available at

<http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml>, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS® software.

A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at

<http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml>.

- CSCed38527

A vulnerability in the Transmission Control Protocol (TCP) specification (RFC793) has been discovered by an external researcher. The successful exploitation enables an adversary to reset any established TCP connection in a much shorter time than was previously discussed publicly.

Depending on the application, the connection may get automatically re-established. In other cases, a user will have to repeat the action (for example, open a new Telnet or SSH session). Depending upon the attacked protocol, a successful attack may have additional consequences beyond terminated connection which must be considered. This attack vector is only applicable to the sessions which are terminating on a device (such as a router, switch, or computer) and not to the sessions that are only passing through the device (for example, transit traffic that is being routed by a router). In addition, this attack vector does not directly compromise data integrity or confidentiality.

All Cisco products which contain TCP stack are susceptible to this vulnerability.

This advisory is available at

<http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-ios.shtml>, and it describes this vulnerability as it applies to Cisco products that run Cisco IOS® software.

A companion advisory that describes this vulnerability for products that do not run Cisco IOS software is available at

<http://www.cisco.com/warp/public/707/cisco-sa-20040420-tcp-nonios.shtml>.

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 12.1(20)EW* on Cisco.com at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat4000/relnotes/ol_2170.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/index.htm>

Software Documents

For configuration information specific to the 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/index.htm>

Cisco IOS Software Documentation Set

For a list of Cisco IOS software documents, refer *Release Notes for the Catalyst 4500 Switch, Cisco IOS Release 12.1(20)EW* on Cisco.com at this URL:

http://www.cisco.com/univercd/cc/td/doc/product/lan/cat4000/relnotes/ol_2170.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 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 websites can be accessed from 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_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/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 submit e-mail 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, the Cisco Technical Assistance Center (TAC) provides 24-hour-a-day, award-winning technical support services, online and over the phone. Cisco.com features the Cisco TAC website as an online starting point for technical assistance. If you do not hold a valid Cisco service contract, please contact your reseller.

Cisco TAC Website

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

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

Accessing all the tools on the Cisco TAC website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a login ID or password, register at this URL:

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

Opening a TAC Case

Using the online TAC Case Open Tool is the fastest way to open P3 and P4 cases. (P3 and P4 cases are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Case Open Tool automatically recommends resources for an immediate solution. If your issue is not resolved using the recommended resources, your case will be assigned to a Cisco TAC engineer. The online TAC Case Open Tool is located at this URL:

<http://www.cisco.com/tac/caseopen>

For P1 or P2 cases (P1 and P2 cases are those in which your production network is down or severely degraded) or if you do not have Internet access, contact Cisco TAC by telephone. Cisco TAC engineers are assigned immediately to P1 and P2 cases to help keep your business operations running smoothly.

To open a case 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 listing of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>

TAC Case Priority Definitions

To ensure that all cases are reported in a standard format, Cisco has established case priority definitions.

Priority 1 (P1)—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.

Priority 2 (P2)—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.

Priority 3 (P3)—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.

Priority 4 (P4)—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. Go to this URL to visit the company store:
<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 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/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/ipj>
- Training—Cisco offers world-class networking training. Current offerings in network training are listed 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.

CCSP, the Cisco Square Bridge logo, 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, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, 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. (0406R)

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

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