



Release Notes for Cisco CVA120 Series Cable Voice Adapter for Cisco IOS Release 12.2 CZ

December 5, 2005
Cisco IOS Release 12.2(15)CZ3
OL-6094-04



Note

You can find the most current Cisco IOS documentation on Cisco.com. This set of electronic documents may contain updates and modifications made after this document was published.

These release notes describe the enhancements provided in Cisco IOS Release 12.2(15)CZ for the Cisco CVA120 series of cable voice adapters (CVA), which includes the Cisco CVA122 Cable Voice Adapter and the Cisco CVA122E Cable Voice Adapter. These release notes are updated as needed to describe new features, memory requirements, hardware support, software platform deferrals, and related documents.



Note

Unless otherwise indicated, the terms Cisco CVA120 Series Cable Voice Adapter and cable voice adapter refer to both the Cisco CVA122 Cable Voice Adapter and Cisco CVA122E Cable Voice Adapter.

For a list of software caveats that apply to Release Number_xa4, see the [“Caveats” section on page 29](#) and *Caveats for Cisco IOS Release 12.2 T*. The caveats document is updated for every maintenance release and is located on Cisco.com and the Documentation CD-ROM.

Use these release notes with *Cross-Platform Release Notes for Cisco IOS Release 12.2* located on Cisco.com and the Documentation CD-ROM. For complete documentation on the Cisco CVA120 Series Cable Voice Adapter, see the documentation listed in the [“Related Documentation” section on page 38](#).

Contents

These release notes describe the following topics:

- [Introduction, page 2](#)
- [System Requirements, page 3](#)
- [System Requirements, page 3](#)
- [New and Changed Information, page 8](#)
- [MIBs, page 24](#)
- [Related Documentation, page 38](#)
- [Caveats, page 29](#)
- [Related Documentation, page 38](#)
- [Obtaining Documentation, page 44](#)
- [Obtaining Technical Assistance, page 45](#)

Introduction

For information on new features and Cisco IOS commands supported by Cisco IOS Release 12.2(15)CZ3, see the [“New and Changed Information” section on page 8](#) and the [“Related Documentation” section on page 38](#).

The Cisco CVA120 Series Cable Voice Adapter gives residential subscribers high-speed Internet access. The cable voice adapter supports data traffic via a shared two-way cable system and Internet Protocol (IP) backbone network. The cable voice adapter connects computers and other customer premises devices at a subscriber site to the service provider’s cable, hybrid-fiber coax (HFC), and IP backbone network.

The Cisco CVA120 series of cable voice adapters are based on Data-over-Cable Service Interface Specifications (DOCSIS) and European DOCSIS (EuroDOCSIS) standards. Depending on the model, they interoperate with any bidirectional, DOCSIS-qualified or EuroDOCSIS-qualified Cable Modem Termination System (CMTS). The cable voice adapter ships from the Cisco factory with a Cisco IOS software image stored in nonvolatile Flash memory that supports DOCSIS-compliant and EuroDOCSIS-compliant bridging operations.

The cable voice adapter uses its cable interface to connect to the CMTS over the HFC cable system. A personal computer (PC) connects to the cable voice adapter through either the Ethernet or Universal Serial Bus (USB) interface. The cable voice adapter then provides Internet access by forwarding traffic between the PC and the CMTS, creating a high-speed, permanent access to the Internet.

If supported by the service provider, the cable voice adapter can connect to multiple PCs by attaching a PC to each interface (Ethernet and USB). In addition, the cable voice adapter’s Ethernet interface can connect to an Ethernet hub, and multiple computers can then be connected to the hub.



Note

The cable voice adapter does not support networking multiple PCs using a USB bridging hub.

In addition to providing DOCSIS/EuroDOCSIS connectivity, the cable voice adapter can optionally provide Voice over IP (VoIP) services, allowing subscribers to make telephone, modem, and fax calls over Transmission Control Protocol (TCP)/IP networks such as the Internet. These calls can be made to other VoIP devices, or to telephone, modem, or fax devices on the regular telephone network (the Public Switched Telephone Network, commonly known as PSTN).

The cable voice adapter can also function as an advanced router, providing wide area network (WAN) data connectivity in a variety of configurations.

Cisco CVA122 Cable Voice Adapter

The Cisco CVA122 Cable Voice Adapter features one F-connector interface to the cable system, one RJ-45 (10BASE-T Ethernet) hub port, one USB device port, and two RJ-11 analog voice ports. The USB interface enables the cable voice adapter to connect to a PC with a USB interface, without having the user to open the unit and install an Ethernet network interface card (NIC). If supported by the PC and service provider, PCs can be connected to the cable voice adapter using both the Ethernet and USB interfaces.

The Cisco CVA122 Cable Voice Adapter supports the DOCSIS standard, which was developed with service providers to ensure that any DOCSIS-certified cable modem can interoperate with any bidirectional, DOCSIS-qualified CMTS. The DOCSIS standard supports the North American National Television Systems Committee (NTSC) channel plan, with 6 MHz channel widths, a downstream range of 88 to 860MHz, and an upstream range of 5 to 42 MHz.

Cisco CVA122E Cable Voice Adapter

The Cisco CVA122E Cable Voice Adapter features one F-connector interface to the cable system, one RJ-45 (10BASE-T Ethernet) hub port, one USB device port, and two RJ-11 analog voice ports. The USB interface enables the cable voice adapter to connect to a PC with a USB interface, without having the user to open the unit and install an Ethernet network interface card (NIC). If supported by the PC and service provider, PCs can be connected to the cable voice adapter using both the Ethernet and USB interfaces.

The Cisco CVA122E Cable Voice Adapter supports the EuroDOCSIS standard, which is almost identical to the DOCSIS standard, except that it supports the European Phase Alternating Line (PAL) and Systeme Electronique Couleur Avec Memoire (SECAM) channel plans, with 8 MHz channel widths, a downstream range of 88 to 860MHz, and an upstream range of 5 to 65 MHz.

System Requirements

This section describes the system requirements for Cisco IOS Release 12.2(15)CZ3 and includes the following sections:

- [Memory Recommendations, page 3](#)
- [Headend Interoperability, page 4](#)
- [Supported Hardware, page 4](#)
- [Determining the Software Version, page 5](#)
- [Upgrading to a New Software Release, page 5](#)
- [Feature Support, page 6](#)

Memory Recommendations

Table 1 lists the memory recommendations for each of the feature sets available for the cable voice adapter in Cisco IOS Release 12.2 CZ.

Table 1 Memory Recommendations for the Cisco CVA122 Cable Voice Adapter and Cisco CVA122E Cable Voice Adapter, Release 12.2 CZ Feature Sets

Feature Set Matrix Term	Image Name	Minimum Flash Memory	Minimum DRAM Memory	Runs From
Base IP Routing + Voice	cva120-k8o3v9y5-mz	8 MB Flash	32 MB DRAM	RAM
	cva120cvc-k8o3v9y5-mz	8 MB Flash	32 MB DRAM	RAM



Note

All software images with “cvc” forms can only be loaded if the cable modem is already running DOCSIS 1.1 software.

Headend Interoperability

DOCSIS Concatenation

If using DOCSIS concatenation with a 16-QAM ((quadrature amplitude modulation) symbol rate, the CMTS must be configured for Unique Word 16 in the preamble for both short and long data burst profiles. On the Cisco uBR7200 series universal broadband routers, use the **cable modulation-profile** global configuration command and specify “uw16” for both the long and short modulation profiles.

DOCSIS 1.0+ Extensions

The cable voice adapter supports the Cisco DOCSIS 1.0+ Extensions, which include dynamic multi-Service ID (multi-SID) assignment and concatenation. The CMTS must also support the dynamic multi-SID and concatenation features. If you are using the Cisco uBR7200 series headend equipment as the CMTS router, Cisco IOS Release 12.1(1)T or greater is required on the CMTS router to ensure that these features are activated.

To configure the cable voice adapter to support multiple classes of service, use either the Cisco Subscriber Registration Center (CSRC) tool or the configuration file editor of your choice. DOCSIS configuration files can contain multiple classes of service (CoS) to support voice and other real-time traffic. The first CoS is used for data (and voice if no other CoS is defined), and additional classes of service can be defined to give higher priority for voice and other real-time traffic.

Supported Hardware

The Cisco CVA122 Cable Voice Adapter and Cisco CVA122E Cable Voice Adapter contain the following interfaces:

- One F-connector interface to the cable system.
- One 10BASE-T Ethernet RJ-45 port that can be connected to a single computer with an Ethernet network interface card (NIC). If supported by the service provider, the Ethernet interface can also be connected to an Ethernet hub, which then can be connected to additional computers or devices at the site.
- One USB device port to connect a single computer.
- Two RJ-11 voice ports that connect to analog telephones, modems, and fax devices.

Determining the Software Version

To determine the version of Cisco IOS software running on your cable voice adapter, log into the cable voice adapter and enter the **show version EXEC** command:

For the cable voice adapter:

```
cva122# show version
Cisco Internetwork Operating System Software
IOS (tm) 120 Software (cva120-k8o3v9y5-mz), Version 12.2(15)CZ3, RELEASE SOFTWARE
```

Upgrading to a New Software Release

For technical information about upgrading to a new software release, see *Cisco IOS Upgrade Ordering Instructions* on Cisco.com located at:

<http://tools.cisco.com/Support/Fusion/index.do>

For other information about upgrading to Cisco IOS Release 12.2 T, see the product bulletin *Cisco IOS Software Release 12.2 T Ordering Procedures and Platform Support* on Cisco.com at:

Service & Support: Software Center: Cisco IOS Software: Product Bulletins: Software

Under Cisco IOS 12.2, click on Cisco IOS Software Release 12.2 T Ordering Procedures and Platform Support

Feature Support

Cisco IOS software is packaged in feature sets that consist of software images that support specific platforms. The feature sets available for a specific platform depend on which Cisco IOS software images are included in a release. Each feature set contains a specific set of Cisco IOS features.

**Caution**

Cisco IOS images with strong encryption (including, but not limited to 168-bit (3DES) data encryption feature sets) are subject to U.S. government export controls and have limited distribution. Strong encryption images to be installed outside the United States are likely to require an export license. Customer orders may be denied or subject to delay because of U.S. government regulations. When applicable, the purchaser/user must obtain local import and use authorizations for all encryption strengths. Please contact your sales representative or distributor for more information, or send an e-mail to export@cisco.com.

The feature set tables have been removed from the Cisco IOS Release 12.3 release notes to improve the usability of the release notes documentation. The feature-to-image mapping that was provided by the feature set tables is available through Cisco Feature Navigator.

Cisco Feature Navigator is a web-based tool that enables you to determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or by feature set (software image). Under the release section, you can compare Cisco IOS software releases side by side to display both the features unique to each software release and the features that the releases have in common.

To access Cisco Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

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

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

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

For frequently asked questions about Cisco Feature Navigator, see the FAQs at the following URL:

<http://www.cisco.com/support/FeatureNav/FNFAQ.html>

Determining Which Software Images (Feature Sets) Support a Specific Feature

To determine which software images (feature sets) in Cisco IOS Release 12.3 support a specific feature, go to the Cisco Feature Navigator home page, enter your Cisco.com login, and perform the following steps:

-
- Step 1** From the Cisco Feature Navigator home page, click **Feature**.
 - Step 2** To find a feature, use either “Search by full or partial feature name” or “Browse features in alphabetical order.” Either a list of features that match the search criteria or a list of features that begin with the number or letter selected from the ordered list will be displayed in the text box on the left side of the web page.
 - Step 3** Select a feature from the left text box, and click the **Add** button to add a feature to the Selected Features text box on the right side of the web page.



Note To learn more about a feature in the list, click the **Description** button below the left box.

Repeat this step to add additional features. A maximum of 20 features can be chosen for a single search.

- Step 4** Click **Continue** when you are finished selecting features.
 - Step 5** From the Major Release drop-down menu, choose **12.3**.
 - Step 6** From the Release drop-down menu, choose the appropriate maintenance release.
 - Step 7** From the Platform Family drop-down menu, select the appropriate hardware platform. The “Your selections are supported by the following:” table will list all the software images (feature sets) that support the feature(s) that you selected.
-

Determining Which Features Are Supported in a Specific Software Image (Feature Set)

To determine which features are supported in a specific software image (feature set) in Cisco IOS Release 12.3, go to the Cisco Feature Navigator home page, enter your Cisco.com login, and perform the following steps:

-
- Step 1** From the Cisco Feature Navigator home page, click **Compare/Release**.
 - Step 2** In the “Find the features in a specific Cisco IOS release, using one of the following methods:” box, choose **12.3** from the Cisco IOS Major Release drop-down menu.
 - Step 3** Click **Continue**.
 - Step 4** From the Release drop-down menu, choose the appropriate maintenance release.
 - Step 5** From the Platform Family drop-down menu, choose the appropriate hardware platform.
 - Step 6** From the Feature Set drop-down menu, choose the appropriate feature set. The “Your selections are supported by the following:” table will list all the features that are supported by the feature set (software image) that you selected.

New and Changed Information

The following sections list the new hardware and software features supported by the cable voice adapter.

New Software Features in Cisco IOS Release 12.2(15)CZ3

There are no new software features supported in Cisco IOS Release 12.2(15)CZ3.

New Hardware Features in Cisco IOS Release 12.2(15)CZ3

There are no new hardware features supported in Cisco IOS Release 12.2(15)CZ3.

New Software Features in Cisco IOS Release 12.2(15)CZ2

There are no new software features supported in Cisco IOS Release 12.2(15)CZ2.

New Hardware Features in Cisco IOS Release 12.2(15)CZ2

There are no new hardware features supported in Cisco IOS Release 12.2(15)CZ2.

New Software Features in Cisco IOS Release 12.2(15)CZ1

There are no new software features supported in Cisco IOS Release 12.2(15)CZ1.

New Hardware Features in Cisco IOS Release 12.2(15)CZ1

There are no new hardware features supported in Cisco IOS Release 12.2(15)CZ1.

No New Hardware Features in Release 12.2(15)CZ

Cisco IOS Release 12.2(15)CZ does not support any new hardware features.

New Software Features in Release 12.2(15)CZ

The following new software feature is supported in Cisco IOS Release 12.2(15)CZ.

DOCSIS 1.1 for Cisco uBR905 and Cisco uBR925 Cable Access Routers and Cisco CVA122 Cable Voice Adapters

DOCSIS 1.1 is the first major revision of the initial DOCSIS 1.0 standard for cable networks. Although the initial standard provided quality data traffic over the coaxial cable network, the demands of real-time traffic such as voice and video required many changes to the DOCSIS specification. DOCSIS 1.1 also includes support for the Baseline Privacy Interface Plus (BPI+) features, which improves and enhances the DOCSIS 1.0 BPI security and authorization mechanisms.



Note

At the time of publication, the DOCSIS 1.1 and BPI+ specifications are still being finalized. See the [CableLabs](#) specifications web site for the current status on these specifications.

The following sections describe the DOCSIS 1.1 features in more detail:

- [DOCSIS 1.1 Overview, page 9](#)
- [Baseline Privacy Interface Plus, page 12](#)
- [DOCSIS 1.1 Quality-of-Service, page 15](#)
- [Quality-of-Service Comparison, page 19](#)
- [SNMPv3 Support, page 20](#)
- [Additional DOCSIS 1.1 Features in Cisco IOS Release 12.2\(15\)CZ, page 21](#)
- [Migrating from Earlier Versions of DOCSIS, page 23](#)

DOCSIS 1.1 Overview

The DOCSIS 1.1 specification provides the following functional enhancements over DOCSIS 1.0 coaxial cable networks:

- Enhanced quality-of-service (QoS) to give priority for real-time traffic such as voice and video:
 - The DOCSIS 1.0 QoS model (a service ID [SID] associated with a QoS profile) has been replaced with a service flow model that allows greater flexibility in assigning QoS parameters to different types of traffic and in responding to changing bandwidth conditions.
 - Support for multiple service flows per cable modem allows a single cable modem to support a combination of data, voice, and video traffic.
 - Greater granularity in QoS per cable modem in either direction, using unidirectional service flows.
 - Dynamic MAC messages create, modify, and delete traffic service flows to support on demand traffic requests. The CMTS can also dynamically change the upstream and downstream channels that the cable modem is using to proactively deal with potential congestion or noise problems.
- Supported QoS models for the upstream are:
 - Best-effort—Data traffic sent on a nonguaranteed best-effort basis.
 - Committed information rate (CIR)—Guaranteed minimum bandwidth for data traffic.
 - Real-time polling (RTPS)—Real-time service flows, such as video, that produce unicast, variable-size packets at fixed intervals.

- Unsolicited grants (UGS)—Constant bit rate (CBR) traffic, such as voice, that is characterized by fixed-size packets at fixed intervals.
- Unsolicited grants with activity detection (USG-AD)—Combination of UGS and RTPS, to accommodate real-time traffic that might have periods of inactivity (such as voice using silence suppression). The service flow uses UGS fixed grants while active, but switches to RTPS polling during periods of inactivity to avoid wasting unused bandwidth.

- Service flows for Voice-over-IP (VoIP) calls can be flexibly created using the following methods:
 - Dynamic quality-of-service (DQoS)—The router is initialized with a primary upstream service flow and a primary downstream service flow. When a VoIP call is made, the router sends a request for a UGS service flow with a Dynamic Service Addition Request (DSA-REQ) message. After the call, the router deletes the service flow using a Dynamic Service Deletion Request message (DSD-REQ) message.
 - Provisioned quality-of-service (PQoS)—The router is initialized with a primary upstream service flow, a primary downstream service flow, and two secondary upstream service flows that are reserved for VoIP calls. The router keeps the secondary flows in the admitted state until a VoIP call is made. The router then activates the appropriate flow with a Dynamic Service Change Request (DSC-REQ) message with a classifier for UGS service that specifies the IP parameters needed for the voice call. After the call, the router deletes the classifier and deactivates the service flow by sending another DSC-REQ message.



Note If the CMTS does not support DOCSIS 1.1 dynamic services, the router can also use the previous DOCSIS 1.0+ mechanisms to create VoIP calls.

- Enhanced time-slot scheduling mechanisms to support guaranteed delay and jitter-sensitive traffic on the shared multiple access upstream link.
- Payload header suppression (PHS) conserves link-layer bandwidth by suppressing unnecessary packet headers on both upstream and downstream traffic flows.
- Layer 2 fragmentation on the upstream prevents large data packets from affecting real-time traffic, such as voice and video. Large data packets are fragmented and then transmitted in the time slots that are available between the time slots used for the real-time traffic.
- Concatenation allows a cable modem to send multiple MAC frames in the same time slot, as opposed to making an individual grant request for each frame. This avoids wasting upstream bandwidth when sending a number of very small packets, such as TCP acknowledgement packets.
- Advanced authentication and security through X.509 digital certificates and Triple Data Encryption Standard (3DES) dual public key encryption.
- Support for IP multicast encryption and for Internet Group Management Protocol (IGMP) groups.
- Secure software download allows a service provider to remotely upgrade a cable modem's software, without risk of interception or alteration.
- SNMPv3 Support, which includes:
 - DES 56-bit encryption.
 - Authentication based on the HMAC-MD5 or HMAC-SHA algorithms that ensures that each packet is from a valid source.
 - An improved security model that provides for a larger number of security levels, with a greater granularity in determining per-user access.
 - MIBs are updated as required for DOCSIS 1.1 support.
- DOCSIS 1.1 cable modems can coexist with DOCSIS 1.0 and 1.0+ cable modems in the same network—a DOCSIS 1.1 CMTS provides the levels of service that are appropriate for each cable modem.

Baseline Privacy Interface Plus

DOCSIS 1.0 included a Baseline Privacy Interface (BPI) to protect user data privacy across the shared-medium cable network and to prevent unauthorized access to DOCSIS-based data transport services across the cable network. BPI encrypts traffic across the RF interface between the cable modem and CMTS, and also includes authentication, authorization, and accounting (AAA) features.

BPI supports access control lists (ACLs), tunnels, filtering, protection against spoofing, and commands to configure source IP filtering on RF subnets to prevent subscribers from using source IP addresses that are not valid. These lists can be implemented either through CLI commands or by setting SNMP attributes through the DOCSIS configuration file.

DOCSIS 1.1 enhances these security features with Baseline Privacy Interface Plus (BPI+), which includes the following enhancements:

- X.509 digital certificates provide secure user identification and authentication. Each DOCSIS 1.1 cable modem contains a certificate that uniquely identifies it to the CMTS. This certificate is chained to the manufacturer's digital certificate, which securely authenticates the cable modem. The manufacturer's certificate in turn is chained to and verified by the DOCSIS certificate authority (CA) root certificate.
- Key encryption uses 168-bit Triple DES (3DES) encryption that is suitable for the most sensitive applications.
- 1024-bit public key exchange Pkcs#1 Version 2.0 encryption to ensure the secure generation and transmission of the public encryption keys between the CMTS and CM.
- Encryption of multicast broadcasts allows users to receive only those broadcasts they are authorized to use.
- Secure software download, using a Pkcs#7 digital signature, allows a service provider to upgrade a cable modem's software remotely, without the threat of interception, interference, or alteration.



Note

BPI+ is described in the Baseline Privacy Interface Plus Specification (SP-BPI+-I08-020301), available from CableLabs (<http://www.cablelabs.com>).

X.509 Digital Certificates

BPI+ uses digital certificates and a public key infrastructure (PKI) that are based on the International Telecommunications Union (ITU) X.509 Version 3.0 standard. The key components of the X.509 standard are the following:

- Digital certificate—Uniquely identifies the cable modem. The digital certificate contains the following information:
 - User name and organization—Identify the product and its manufacturer.
 - Certificate effective date and expiration Date—Give the range of dates for which the certificate is valid.
 - User public key—Allows other entities, such as the CMTS, to verify the certificate.
 - Issuer certificate authority (CA) name and signature—Provide a way of verifying that the certificate and keys have not been altered.

A DOCSIS 1.1 cable modem contains two digital certificates programmed into it at the factory: a cable modem certificate that uniquely identifies it, and a manufacturing certificate that identifies the cable modem's manufacturer (in this case, Cisco Systems).

- **Public and private keys**—Keys used to sign and verify the certificate. The cable modem uses its private key to sign its digital certificate to create an unforgeable digital signature that identifies the signer. Other entities, such as the CMTS, use the public key to unsign and verify the certificate. For security, the cable modem never transmits or displays its private key, but the public key is included as part of the certificate to allow for its verification.



Note The cable modem's private and public keys are never changed after being programmed at the factory.

- **Digital signature**—Created when a private key signs a digital certificate. The digital signature becomes part of the certificate, allowing the CMTS to verify that the certificate came from the cable modem claiming to have issued it.
- **Certificate authority (CA)**—To prevent users from creating their own certificates and private key and public key pairs, each certificate is also signed by an issuing CA. After the CMTS verifies a digital certificate with the cable modem's public key, it then verifies that the certificate has been properly signed by the issuing CA. This process continues until the CMTS can verify the certificate against a known and trusted CA (typically the root CA).
- **Root CA**—A known and trusted CA that serves as the ultimate verification for a digital certificate. For DOCSIS 1.1 cable modems, the root CA is the DOCSIS Root CA certificate, which is available from Verisign at <http://www.verisign.com/products/cable/root.html>. The root CA is self-signed, which does not present a security problem because it is originating at a known and trusted source.
- **DOCSIS root code signing CA**—Similar to the Root CA but used to verify the digital certificates that are used whenever a DOCSIS 1.1 cable modem downloads new software code.

During BPI+ initialization, the cable modem sends both of its signed digital certificates, the cable modem certificate (CMC) and the manufacturer's certificate (MC), to the CMTS. The CMTS verifies the cable modem certificate against the manufacturer's certificate, and then verifies the manufacturer's certificate against the DOCSIS Root CA certificate. This chain of verifications ensures that the CMTS can securely identify and authenticate each cable modem.

In addition, the CMTS can check the certificates against a Hot List of invalid certificates. The Hot List, which can be maintained by trusted authorities, such as a service provider or CA, can list certificates for individual cable modems that might have been stolen, hacked, or otherwise compromised. The list can also contain manufacturer's certificates for models of cable modems that the service provider does not support.

If all certificate verifications are successful, the CMTS begins the public key exchange process, which allows data encryption and decryption to begin.

Public Key Exchange

The secure use of X.509 digital certificates depends on both the cable modem and the CMTS possessing the proper encryption and decryption keys. For security and flexibility, DOCSIS 1.1 uses a dual-key public key exchange: the first set of keys, key encryption key (KEK), are used to encrypt and transmit the second set of keys, traffic encryption key (TEK), which are then used to encrypt and decrypt data.

Both sets of keys have a limited lifetime and must be renewed periodically. When a key reaches approximately half its lifespan, the cable modem begins the process to request a new set of keys. While the new set of keys is being exchanged, the cable modem can continue to use the old set to encrypt and decrypt data. The KEK keys have a longer lifetime than the TEK keys to ensure that the cable modem and CMTS will always be able to obtain new TEK keys, allowing data transmissions to continue without interruptions.

Secure Software Download

DOCSIS 1.1 supports secure software download to allow a service provider to remotely upgrade a cable modem's software without risk of interception or alteration. Secure software download also prevents users from upgrading the cable modem to unauthorized software images.

The manufacturer digitally signs the software image using a Pkcs#7 digital signature that is encrypted using the Rivest-Shamir-Adleman (RSA) algorithm and secure hash algorithm-1 (SHA-1). This digital signature is chained to the DOCSIS root code signing certificate so that it can be easily verified.

The cable operator can optionally also digitally sign the software image in a similar manner, using another digital signature that is chained to the DOCSIS root code signing certificate. This allows cable operators greater control over which software images are used on the cable network.

The cable operator initiates the software download by filling in the software filename and TFTP server fields (TLVs 9 and 21) in the DOCSIS configuration file that it sends to the cable modem during registration. You can also initiate a software download by using SNMP commands. In either case, the cable modem then requests the specified file and downloads it from the specified TFTP server.

The cable modem verifies the manufacturer's digital signature and, if present, the cable operator's digital signature, using the code verification certificates (CVCs) provided in the DOCSIS configuration file. If the signatures are valid, the cable modem loads and runs the software.

When a cable modem is running DOCSIS 1.1 software, it must use the secure software download feature to download a software image through the DOCSIS configuration file or through SNMP commands. Even if you disable BPI+, a DOCSIS 1.1 cable modem still accepts only digitally signed software images that can be verified through the secure software download process.



Note

The secure software download feature does not prevent a user with console or Telnet access, and who knows the proper passwords, from loading an unsigned software image directly into the cable modem's Flash memory by using the **copy tftp** command.

The secure software download feature requires the following prerequisites:

- The Cisco uBR905, Cisco uBR925, or Cisco CVA122 must be running a DOCSIS 1.1 software image.

If the cable modem is currently running a DOCSIS 1.0 software image, you cannot use the secure software download to upgrade to a DOCSIS 1.1 image. Instead, you must use the DOCSIS 1.0 software upgrade process to load an unsigned DOCSIS 1.1 software image. Then you will be able to use the secure software download process to load a digitally signed DOCSIS 1.1 software image.

- The desired software image must be digitally signed by the manufacturer. The cable operator can also optionally digitally sign the image. Unsigned images cannot be loaded using the secure software download process.



Note

You cannot use the **copy tftp** command to load digitally signed images into the Flash memory on the cable modem.

- You must load at least one CVC into the cable modem through the DOCSIS configuration file. The cable modem uses the CVC to verify that a downloaded software image is from the proper manufacturer and has not been altered during transmission. You can load two types of CVCs into the cable modem:
 - Manufacturer’s CVC (M-CVC)—Verifies that the downloaded software image has been digitally signed by the manufacturer (Cisco Systems). The M-CVC is loaded into the cable modem by specifying TLV 32 (MFG CVC) in the DOCSIS configuration file.
 - Cosigner’s CVC (C-CVC)—Verifies that the downloaded software image has been digitally signed by both the manufacturer (Cisco Systems) and the cable operator. The C-CVC is loaded into the cable modem by specifying TLV 33 (MSO CVC) in the DOCSIS configuration file.

If you load the M-CVC into the cable modem, you can download only those software images that Cisco Systems has digitally signed. If you load the C-CVC into the cable modem, you can download only those software images that Cisco Systems and the cable operator have digitally signed.

**Note**

A DOCSIS 1.1 cable modem must use the secure software download feature when upgrading its software image through the DOCSIS configuration file or through SNMP commands. However, users can still use CLI commands to copy an unsigned software image from a TFTP server, if they know the enable password and are allowed console or Telnet access.

After the cable modem loads and runs the DOCSIS 1.1 image, the cable modem must use the secure software download process for all future upgrades. In particular, this means that the cable modem cannot be downgraded to a DOCSIS 1.0 software image unless the manufacturer provides a digitally signed DOCSIS 1.0 image. After downgrading to a DOCSIS 1.0 image, you cannot use the secure software download process again until you have upgraded the cable modem to a new DOCSIS 1.1 image.

**Tip**

Cisco IOS software images that include “cvc” as part of the software image filename (ubr925cvc-k9o3sv9y5-mz) are digitally signed. Unsigned software images do not have “cvc” as part of the filename (ubr925-k9o3sv9y5-mz). If you are using secure software download, you *must* use a digitally signed image (includes “cvc”). If you are not using secure software download, you *must* use an unsigned image (does not include “cvc”).

DOCSIS 1.1 Quality-of-Service

DOCSIS 1.1 implemented a number of changes to allow great flexibility in the ability of a cable modem and service provider to transmit almost any combination of data traffic and real-time traffic, such as voice and video. These changes required a fundamental shift in how a cable modem requests service and how traffic can be transmitted across the cable network.

Overview

The DOCSIS 1.1 QoS framework is based on the following objects:

- Service class—A collection of settings maintained by the CMTS that provide a specific QoS service tier to a cable modem that has been assigned a service flow within a particular service class.
- Service flow—A MAC-layer transport service that provides unidirectional transport of packets to upstream packets transmitted by the cable modem or to downstream packets transmitted by the CMTS. A service flow is characterized by a set of QoS parameters such as latency, jitter, and throughput assurances.

- Packet classifier—A set of packet header fields used to classify packets onto a service flow to which the classifier belongs. When a packet is presented to the DOCSIS MAC layer at the CMTS or cable modem, it is compared to a set of packet classifiers until a matching classifier is found. The SFID from this classifier is used to identify the service flow on which the packet will be sent.
- PHS rule—A set of packet header fields that are suppressed by the sending entity before transmitting on the link, and are restored by the receiving entity after receiving a header-suppressed frame transmission. Payload header suppression increases the bandwidth efficiency by removing repeated packet headers before transmission.

In the upstream direction, the output queues at the cable modem get remotely served by the CMTS MAC scheduler, based on DOCSIS 1.1 slot scheduling constraints such as grant-interval and grant-jitter. In the downstream direction, the CMTS packet scheduler serves the flow queues depending on the flow attributes like traffic priority, guaranteed rate, and delay bound.

DOCSIS 1.1 adds several new MAC scheduling disciplines to provide guaranteed QoS for real-time service flows on the multiple access upstream channel. Multiple grants per interval helps in supporting multiple subflows (such as voice calls) on the same SID. Multiple subflows per SID reduces the minimum SID requirement in cable modem hardware.

The CMTS is responsible for supporting QoS for all cable modems in its control. The traffic in the downstream is assumed to be a combination of voice, committed information rate (CIR) data, and excess burst best-effort data. To provide QoS support, the following functions must be performed:

- Packet classification—Mapping packets to service flows based on header information
- Policing (rate limiting) the individual flows
- Queuing packets into appropriate output queues based on the type of service
- Serving the output queues to meet delay and rate guarantees

The admission control block helps the overall downstream QoS block to track the current bandwidth reservation state on a per-downstream basis. Decisions can be made whether to admit or reject a request for a new service flow on that DS channel, based on this reservation state and the QoS guarantees requested by the new service-flow.

IP packet classifiers help in filtering out unique service flows on an interface for differential QoS treatment. Rather than doing per-cable modem downstream rate shaping, DOCSIS 1.1 software provides rate shaping at a much more granular level of individual service flows of the cable modem.



Note

Cisco uBR905 and uBR925 cable access routers and Cisco CVA122 cable voice adapters running Cisco IOS Release 12.2(15)CZ can transparently interoperate with CMTS routers running DOCSIS 1.0, DOCSIS 1.0+ extensions, or DOCSIS 1.1.

Service Flows and Packet Classifiers

Every cable modem establishes a primary service flow in both the upstream and downstream directions. The primary flows maintain connectivity between the cable modem and the CMTS at all times.

In addition, a DOCSIS 1.1 cable modem can establish multiple secondary service flows. The secondary service flows either can be permanently created (they persist until the cable modem is reset or powered off) or can be created dynamically to meet the needs of the on-demand traffic being transmitted.

A service flow gets created at the time of cable modem registration (a static service flow) or as a result of a dynamic MAC message handshake between the cable modem and the CMTS (a dynamic service flow). At any given time, a service flow might be in one of three states (provisioned, admitted, or active). Only active flows are allowed to pass traffic on the DOCSIS link.

Each service flow has a set of QoS attributes associated with it. These QoS attributes define a particular class of service and determine characteristics such as the maximum bandwidth for the service flow and the priority of its traffic. The class of service attributes can be inherited from a preconfigured CMTS local service class (class-based flows), or they can be individually specified at the time of the creation of the service flow.

Every service flow also has a unique (unique per DOCSIS MAC domain) identifier called the service flow identifier (SFID). The upstream flows in the admitted and active state have an extra Layer 2 SID associated with them. The SID is the identifier used by the MAC scheduler when specifying time-slot scheduling for different service flows.

Each service flow has multiple packet classifiers associated with it, which determine the type of application traffic allowed to be sent on that service flow. Each service flow can also have a payload header suppression (PHS) rule associated with it to determine which portion of the packet header will be suppressed when packets are transmitted on the flow.

Dynamic Channel Change

DOCSIS 1.1 supports Dynamic Channel Change (DCC) requests, which allow the CMTS to change the upstream or downstream frequency that the cable modem is using. This allows the CMTS to move cable modems to another channel when the current one is either becoming congested or is encountering growing noise problems that could eventually force the cable modems offline.

The Cisco uBR905 and Cisco uBR925 cable access routers and the Cisco CVA122 Cable Voice Adapter automatically support DCC requests when running Cisco IOS Release 12.2(15)CZ.

Dynamic Quality-of-Service

DOCSIS 1.1 adds support Dynamic Services MAC-layer messages that provide for Dynamic QoS (DQoS) between the cable modem and the CMTS. These messages are DOCSIS link-layer equivalents of the higher-layer messages that create, tear down, and modify a service flow. These messages are collectively known as DSX messages to represent the three types of dynamic service messages:

- Dynamic Service Add (DSA)—Creates a new service flow.
- Dynamic Service Change (DSC)—Changes the attributes of an existing service flow. These changes can include the following:
 - Adding, replacing, or deleting a classifier from the service flow.
 - Changing the flow’s Admitted and Active QoS parameter sets.
 - Adding, setting, or deleting payload header suppression (PHS) rules for the service flow.
- Dynamic Service Deletion (DSD)—Deletes an existing service flow.

The DSX state machine module on the cable modem manages the several concurrent dynamic service transactions between cable modems and the CMTS. The DSX state machine supports all three DOCSIS 1.1 DSX MAC messages (DSA, DSC, DSD).

Provisioned QoS

Provisioned QoS (PQoS) allows the cable modem to create the service flows it needs for voice calls and other real-time traffic at the time it registers with the CMTS, without actually using the bandwidth for those flows. The service flow is kept in the admitted state and is activated only when the cable modem signals a voice call using the DOCSIS 1.1 Dynamic Service Request (DSC-REQ) message. Bandwidth is used only when the voice call is actually in progress.

To use PQoS services, you must configure the cable modem with secondary service flows for VoIP calls. (If you do not define any secondary service flows, DQoS is used instead of PQoS). You can use any voice signaling that is supported by the cable modem for VoIP traffic.

[Table 2](#) compares how the router sets up and tears down VoIP calls when using DQoS and PQoS:

Table 2 *Comparison of DQoS and PQoS Call Setup and Teardown Operation*

Quality-of-Service Type	VoIP Signaling Type	Call Setup Description
Dynamic QoS	H.323	Sends DSA at off-hook and DSD at on-hook.
	SGCP/MGCP/SIP	Sends DSA at off-hook, DSC when the call setup parameters are received from the gateway, and DSD at on-hook.
Provisioned QoS	H.323	Sends DSC at off-hook to activate the provisioned service flows and DSD at on-hook.
	SGCP/MGCP/SIP	Sends DSC at off-hook to activate the provisioned service flows, a second DSC when the call setup parameters are received from the gateway, and DSD at on-hook.

Service Flow Manager

The Service Flow Manager is a new module that manages different activities related to service flows on a cable interface. Typical events include the creation of new DOCSIS service flows, modification of the attributes of existing service flows, and the deletion of service flows.

Quality-of-Service Comparison

Quality-of-service (QoS) is a measure of performance for a transmission system that reflects its transmission quality and service availability. This section describes the differences in QoS between DOCSIS 1.1 and DOCSIS 1.0 and 1.0+.

DOCSIS 1.0

DOCSIS 1.0 uses a static QoS model that is based on a class of service (CoS) that is preprovisioned in the TFTP configuration file for the cable modem. The CoS is a bidirectional QoS profile that has limited control, such as peak rate limits in either direction and relative priority on the upstream.

DOCSIS 1.0 defines the concept of a service identifier (SID), which specifies the devices allowed to transmit and which provides device identification and CoS. In DOCSIS 1.0, each cable modem is assigned only one SID, creating a one-to-one correspondence between a cable modem and the SID. All traffic originating from, or destined for, a cable modem is mapped to that cable modem's SID.

Typically, a DOCSIS 1.0 cable modem has one CoS and treats all traffic the same, which means that data traffic on a cable modem can interfere with the quality of a voice call in progress. The CMTS, however, can prioritize downstream traffic based on IP precedence type-of-service (ToS) bits. For example, voice calls using higher IP precedence bits receive a higher queueing priority (but without a guaranteed bandwidth or rate of service). A DOCSIS 1.0 cable modem could increase voice call quality by permanently reserving bandwidth for voice calls, but then that bandwidth would be wasted whenever a voice call is not in progress.

DOCSIS 1.0+ Extensions

In response to the limitations of DOCSIS 1.0 in handling real-time traffic, such as voice calls, Cisco created the DOCSIS 1.0+ extensions to provide the more important QoS enhancements that were expected in DOCSIS 1.1. In particular, the DOCSIS 1.0+ enhancements provide basic Voice-over-IP (VoIP) service over the DOCSIS link.

Cisco DOCSIS 1.0+ extensions include the following DOCSIS 1.1 features:

- Multiple SIDs per cable modem, creating separate service flows for voice and data traffic. This allows the CMTS and cable modem to give higher priority for voice traffic, preventing the data traffic from affecting the quality of the voice calls.
- Cable modem-initiated dynamic MAC messages—Dynamic Service Addition (DSA) and Dynamic Service Deletion (DSD). These messages allow dynamic SIDs to be created and deleted on demand, so that the bandwidth required for a voice call can be allocated at the time a call is placed and then freed up for other uses when the call is over.
- Unsolicited grant service (CBR-scheduling) on the upstream—This helps provide a higher-quality channel for upstream VoIP packets from an Integrated Telephony Cable Modem (ITCM) such as the Cisco uBR924 cable access router.
- Ability to provide separate downstream rates for any given cable modem, based on the IP-precedence value in the packet. This helps separate voice signaling and data traffic that goes to the same ITCM to address rate shaping purposes.
- Concatenation allows a cable modem to send several packets in one large burst, instead of having to make a separate grant request for each.



Caution

All DOCSIS 1.0 extensions are available only when using a cable modem (such as the Cisco uBR924 cable access router) and CMTS (such as the Cisco uBR7200 series universal broadband router) that supports these extensions. The cable modem activates the use of the extensions by sending a dynamic MAC message. DOCSIS 1.0 cable modems continue to receive DOCSIS 1.0 treatment from the CMTS.

SNMPv3 Support

DOCSIS 1.1 also requires support of v3 of the Simple Network Management Protocol (SNMPv3). SNMPv3 offers a number of significant improvements over SNMPv1 and SNMPv2:

- DES 56-bit encryption that encrypts each packet to prevent interception or alteration in transit. SNMP attributes can be set and retrieved without exposing confidential information on a public network.
- Authentication based on the HMAC-MD5 or HMAC-SHA algorithms that ensures that each packet is from a valid source.
- An improved security model that provides for a larger number of security levels, with a greater granularity in determining per-user access. Each SNMPv3 user belongs to a group, which defines the security model and security level for its users. This includes the level of access to SNMP objects and the list of notifications that users can receive.

SNMPv3 Diffie-Hellman Kickstart

To ensure SNMPv3 security, the Multi-Service Operator (MSO) must perform an initialization procedure the first time the cable modem comes online. This procedure, which the DOCSIS 1.1 specification refers to as the *SNMPv3 Diffie-Hellman Kickstart*, sends a public key to the cable modem as part of the DOCSIS configuration file. The cable modem creates a secret number and encrypts it using the public key it received in the configuration file.

The cable modem then publishes the encrypted number to the CMTS, which uses its private key to decrypt it so as to produce the cable modem's secret number. This secret number becomes a shared secret value that the CMTS and CM can use to exchange SNMPv3 encryption keys.

MIB Enhancements

DOCSIS 1.1 also expands the MIB support for SNMP management, including the following changes and additions to the DOCSIS 1.0 MIB structure:

- DOCS-BPI-PLUS-MIB—Describes the Baseline Privacy Interface Plus (BPI+) attributes and replaces the DOCS-BPI-MIB, which was used in DOCSIS 1.0. This is revision 05 of the MIB.
- DOCS-QOS-MIB—Describes the quality-of-service (QoS) attributes. This is revision 04 of the MIB.
- DOCS-SUBMGT-MIB—Describes the subscriber management attributes. This is revision 02 of the MIB.
- RFC 2933—Describes the IGMP protocol attributes, as defined in RFC 2933.
- DOCS-CABLE-DEVICE-MIB—Describes the operation of the CM and the CMTS, as defined as RFC 2669.
- DOCS-CABLE-DEVICE-TRAP-MIB—Defines the traps supported by CMs and the CMTS and is the extension of RFC 2669 (DOCS-CABLE-DEVICE-MIB).
- DOCS-IF-EXT-MIB—Extends RFC 2670 (DOCS-IF-MIB) to provide information about whether the CMs and the CMTS support DOCSIS 1.0 or DOCSIS 1.1.

Additional DOCSIS 1.1 Features in Cisco IOS Release 12.2(15)CZ

The following sections describe the DOCSIS 1.1 software features that appear in Cisco IOS Release 12.2(15)CZ.

Concatenation

Concatenation allows the cable modem to make a single time-slice request for multiple packets and send all packets in a single large burst on the upstream. Concatenation was introduced in the upstream receive driver in DOCSIS1.0+ releases.

Fragmentation

Grant fragmentation allows the upstream MAC scheduler to slice large data requests to fit into the scheduling gaps between UGS (voice slots). This reduces the jitter experienced by the UGS slots when large data grants preempt the UGS slots. The grant fragmentation gets triggered in the MAC scheduler, and fragment reassembly happens in the upstream receive driver.

**Note**

DOCSIS fragmentation should not be confused with the fragmentation of IP packets, which is done to fit the packets on network segments with smaller maximum transmission unit (MTU) size. DOCSIS Fragmentation is Layer 2 fragmentation that is primarily concerned with efficiently transmitting lower-priority packets without interfering with high-priority real-time traffic, such as voice calls. IP fragmentation is done at Layer 3 and is primarily intended to accommodate routers that use different maximum packet sizes.

IP Multicast Support

By default, a DOCSIS CMTS transmits IP multicast traffic without encryption. All DOCSIS cable modems receiving that multicast traffic must forward it to its attached CPE devices, without regard to whether any of the devices have requested the traffic. This can waste network bandwidth and require network devices to waste processor power in forwarding and processing undesired multicast traffic.

A DOCSIS 1.1 CMTS can instead use the Internet Group Management Protocol (IGMP) to maintain the multicast group memberships of its DOCSIS 1.1 cable modems. BPI+ encryption is used to encrypt the multicast packets so that only the cable modems with the appropriate public keys can decrypt the packets and forward them to their attached customer premises equipment (CPE) devices.

If a cable modem has not been granted the decryption keys for a particular multicast service flow, it does not forward the traffic to its CPE devices. This ensures that only authorized subscribers can receive the multicast traffic, and prevents cable modems from loading down their local networks by forwarding unnecessary multicast traffic.

DOCSIS 1.1 uses the concept of Security Associations (SA), which are dynamically created and maintained to provide the service flows required to transmit IP multicast traffic on the downstream. A cable modem sends an SA Map Request message to request the SA for the downstream service flow that is carrying the desired multicast traffic.

If the cable modem is not authorized to receive the multicast traffic, or if the traffic is not available on BPI+ encrypted SA, the CMTS sends an SA Map Reject message. The cable modem then does not repeat any further SA Map Requests for this particular multicast traffic. However, if the traffic is available on an unencrypted service flow, it begins forwarding that traffic to its CPE devices.

If the cable modem is authorized to receive the multicast traffic, and if the traffic is available, the CMTS replies with an SA Map Reply message to provide the information that allows the cable modem to receive the multicast traffic. The SA Map Reply message contains the SA identifier (SAID) for the traffic and the cryptographic suite that is necessary to decrypt the multicast traffic.

If the cable modem supports the cryptographic suite being used, it sends a Key Request to the CMTS, requesting the public keys it needs to decrypt the multicast service flow. If the CMTS replies with a Key Reply that contains the requested public keys, the cable modem begins decrypting the multicast traffic and forwarding it to its attached CPE devices.

The multicast traffic can be mapped to the cable modem's primary SA, a static SA, or a dynamically created SA. One service flow can support multiple multicast traffic flows, each with its own SAID. Multicast traffic mapped to a primary SA can be received only by the cable modem that is assigned the associated primary service flow. Multicast traffic mapped to static and dynamic SAs can be received by all cable modems that are assigned the associated secondary service flows.

Payload Header Suppression and Restoration

The PHS feature is used to suppress repetitive or redundant portions in packet headers before transmission on the DOCSIS link. This is a new feature in the DOCSIS1.1 MAC driver. The upstream receive driver is now capable of restoring headers suppressed by cable modems, and the downstream driver is capable of suppressing specific fields in packet headers before forwarding the frames to the cable modem.

Migrating from Earlier Versions of DOCSIS

DOCSIS 1.1 cable modems have additional features and better performance than earlier DOCSIS 1.0 and 1.0+ models, but all three models can coexist in the same network. DOCSIS 1.0 and 1.0+ cable modems will not hamper the performance of a DOCSIS 1.1 cable modem, nor will they interfere with operation of DOCSIS 1.1 features. There is full forward and backward compatibility in the standards.

For this configuration...	The result is...
DOCSIS 1.1 cable modems with DOCSIS 1.0 CMTS	Cable modems receive DOCSIS 1.0 features and capabilities. BPI is supported if it is available and enabled on the CMTS.
DOCSIS 1.1 cable modems with DOCSIS 1.0+ CMTS	Cable modems receive basic DOCSIS 1.0 support. BPI is supported if it is available and enabled on the CMTS. In addition, cable modems also receive the following DOCSIS 1.1 features: <ul style="list-style-type: none"> • Multiple SIDs per cable modem • Dynamic Service MAC messaging initiated by the cable modem • Unsolicited grant service (UGS, CBR-scheduling) on the upstream • Separate downstream rates for any given cable modem, based on the IP-precedence value • Concatenation
DOCSIS 1.1 cable modems with DOCSIS 1.1 CMTS	Cable modems receive all the DOCSIS 1.1 features listed in this document. BPI+ is supported if it is available and enabled on the CMTS.

**Note**

For information about configuring the DOCSIS 1.1 feature set, see the document, *DOCSIS 1.1 for Cisco uBR905 and Cisco uBR925 Cable Access Routers and Cisco CVA122 Cable Voice Adapters*, which is at the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122cz/ftcmdc11.htm>

**Note**

In addition, you might need to upgrade the digital certificates on the Cisco cable modems. All production models of the Cisco uBR905 and Cisco uBR925 cable access routers and Cisco CVA122 cable voice adapters include digital certificate support. However, some models might require an upgrade of those certificates before being able to perform BPI+ operation. See the document, *Upgrading the DOCSIS Certificates in Cisco uBR905/uBR925 Cable Access Routers and CVA122 Cable Voice Adapters*, which is at the following URL:

<http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122cz/upgdcert.htm>

MIBs

Current MIBs

To obtain lists of supported MIBs by platform and Cisco IOS release, and to download MIB modules, go to the Cisco MIB web site on Cisco.com at

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>.

Supported MIBs

The cable voice adapter supports the following categories of MIBs:

- Cable device MIBs—These MIBs are for DOCSIS-compliant cable modems and CMTS to record statistics related to the configuration and status of the cable modem. These MIBs include support for the MIB attributes defined in RFC 2669.
- Cisco's standard MIBs—These MIBs are common across most of Cisco's router platforms. If your network management applications are already configured to support other Cisco routers, such as the Cisco 2600 series or Cisco 7200 series, no further configuration is needed unless the version of Cisco IOS software being used has updated these MIBs.
- Radio Frequency Interface MIBs—These MIBs are for DOCSIS-compliant radio frequency interfaces in cable modems and CMTS. This MIB includes support for the MIB attributes defined in RFC 2670.
- SNMP standard MIBs—These are the MIBs required by any agent supporting SNMPv1 or SNMPv2 network management.

- Cable-specific MIBs—These MIBs provide information about the cable interface and related information on the cable voice adapter. They include both DOCSIS-required MIBs and Cisco-specific enterprise MIBs. If your network management applications have not already been configured for the cable voice adapter, these MIBs must be loaded.
- Deprecated MIBs—These MIBs were supported in earlier releases of Cisco IOS software but have been replaced by more standardized, scalable MIBs. Network Management applications and scripts should convert to the replacement MIBs as soon as possible.

Cable Device MIBs

The cable voice adapter supports the Cable Device MIB, which is defined by RFC 2669 and describes DOCSIS-compliant cable modems and CMTS. The Cable Device MIB records statistics related to the configuration and status of the cable modem. Statistics include an events log and device status. The following list details the components of the Cable Device MIB:

- “docsDevBase” group extends the MIB-II “system” group with objects needed for cable device system management
- “docsDevNmAccess” group provides a minimum level of SNMP access security
- “docsDevSoftware” group provides information for network downloadable software upgrades
- “docsDevServer” group provides information about the progress of interaction with various provisioning servers
- “docsDevEven” group provides information about the progress of reporting
- “docsDevFilter” group configures filters at link layer and IP layer for bridge data traffic

The Cable Device MIB is very similar to the RFI MIB in that both allow access to statistics; they are different in that the Cable Device MIB reports statistics on the cable modem, and the RFI MIB reports statistics on the radio frequency transmissions over the cable television line.

Cisco Standard MIBs

The cable voice adapter supports the Cisco Standard MIBs, which consist of the following components:

- CISCO-PRODUCT-MIB
- CISCO-SYSLOG-MIB
- CISCO-FLASH-MIB
- BRIDGE-MIB
- IF-MIB (RFC 2233)
- CiscoWorks/CiscoView support
- SNMP standard MIBs—These are the MIBs required by any agent supporting SNMPv1 or SNMPv2 network management



Note

The *Cisco Management Information Base (MIB) User Quick Reference* publication is no longer published. For the latest list of MIBs supported by Cisco, see the *Cisco Network Management Toolkit* on Cisco.com. From the Cisco.com home page, click on this path: **Service & Support: Software Center: Network Mgmt Products: Cisco Network Management Toolkit: Cisco MIB**

Cisco Voice MIBs

The Cisco CVA 120 series cable voice adapter supports the Cisco Voice MIBs, which consist of the following components:

- CISCO-VOICE-DIAL-CONTROL-MIB
- CISCO-VOICE-ANALOG-IF-MIB
- CISCO-VOICE-IF-MIB

Uninterruptible Power Supply (UPS) and Power MIBs

These MIBs describe the Cisco CVA120 Series Cable Voice Adapter's onboard environmental monitor, which includes information about the status of the UPS and the power supply. The power and UPS attributes are described in the table, "ciscoEnvMonSupplyStatusTable." To send a trap or interrupt request whenever the cable voice adapter switches between its onboard AC power supply and the UPS, set the "ciscoEnvMonEnableRedundantSupplyNotification" attribute to "true" to enable the "ciscoEnvMonRedundantSupplyNotification" trap.

Radio Frequency Interface MIBs

The cable voice adapter supports the Radio Frequency Interface (RFI) MIB. The RFI MIB module is defined in RFC 2670 and describes DOCSIS-compliant radio frequency interfaces in cable modems and CMTS. On the cable modem, RFI MIB entries provide:

- Upstream and downstream channel characteristics
- Class of service attributes
- Physical signal quality of the downstream channels
- Attributes of cable voice adapter MAC interface
- Status of several MAC layer counters

The RFI MIB includes tables describing both the CMTS and the cable modem side of the cable interface. All cable modem tables are implemented.

Cable-Specific MIBs

[Table 3](#) shows the cable-specific MIBs that are supported on the cable voice adapter. This table also provides a brief description of each MIB's contents and the Cisco IOS software release in which the MIB was initially functional—earlier releases might have had unsupported prototype versions of the MIB; later releases might have added new attributes and functionality.



Note

The names given in [Table 3](#) are the filenames for the MIBs as they exist on Cisco's FTP site <http://www.cisco.com/public/mibs/>. Most MIBs are available in both SNMPv1 and SNMPv2 versions; the SNMPv1 versions have *VISMI* as part of their filenames. Also see the Cisco MIBs home page at <http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>.

Table 3 Supported MIBs for the Cisco CVA120 Series Cable Voice Adapter

MIB Filename	Description	Release
SNMPv2-SMI.my SNMPv2-SMI-V1SMI.my	This module specifies the Structure of Management Information (SMI) for SNMPv2, as defined in RFC 1902.	12.1(5)XU2
SNMPv2-TC.my SNMPv2-TC-V1SMI.my	This module defines the textual conventions as specified in pages 4, 10-11 of RFC 854.	12.1(5)XU2
CISCO-SMI.my CISCO-SMI-V1SMI.my	This module specifies the SMI for Cisco's enterprise MIBs.	12.1(5)XU2
CISCO-TC.my CISCO-TC-V1SMI.my	This module defines the textual conventions used in Cisco's enterprise MIBs.	12.1(5)XU2
IF-MIB.my IF-MIB-V1SMI.my	This module describes generic objects for the Layer 3 network interface sublayers. This MIB is an updated version of MIB-II's <i>if</i> table, and incorporates the extensions defined in RFC 2233.	12.1(5)XU2
CISCO-CABLE-SPECTRUM-MIB.my CISCO-CABLE-SPECTRUM-MIB-V1SMI.my	This module describes the spectrum management flap list attributes.	12.1(5)XU2
DOCS-IF-MIB.my DOCS-IF-MIB-V1SMI.my	This module describes the DOCSIS-compliant Radio Frequency (RF) interfaces in cable modems and cable modem termination systems, as described in RFC 2670.	12.1(5)XU2
DOCS-BPI-MIB.my DOCS-BPI-MIB-V1SMI.my	This module describes the attributes for the DOCSIS-specified Baseline Privacy Interface (BPI) on cable modems and the CMTS.	12.1(5)XU2
CISCO-DOCS-EXT-MIB.my CISCO-DOCS-EXT-MIB-V1SMI.my	This module extends the DOCSIS standard RFI MIB (DOCS-IF-MIB) with Cisco-specific extensions, such as Quality of Service (QoS) attributes and connection status and other information regarding the cable modems and CPE devices supported by the CMTS. Note This MIB contains information about both the CMTS and CM, but it is supported only on the CMTS. If you are using the same manager for both CM and CMTS SNMP access, you must load this MIB in the order shown.	—
DOCS-CABLE-DEVICE-MIB.my DOCS-CABLE-DEVICE-MIB-V1SMI.my	This module was previously known as the CABLE-DEVICE-MIB and contains cable-related objects for DOCSIS-compliant cable modems, as specified in RFC 2669.	12.1(5)XU2
USB-MIB.my	This module describes the cable voice adapter's Universal Serial Bus (USB) interface. It is based on an IETF draft (draft-dolnik-usb-mib-02.txt), which is available on the IETF web site at http://www.ietf.org/index.html , in the "Internet Drafts" section.	12.1(5)XU2



Note

Because of interdependencies, the MIBs must be loaded in the order given in the table.

Deprecated MIBs

A number of Cisco-provided MIBs have been replaced with more scalable, standardized MIBs; these MIBs have filenames that start with “*OLD*” and first appeared in Cisco IOS Release 10.2. The functionality of these MIBs has already been incorporated into replacement MIBs, but the old MIBs are still present to support existing Cisco IOS products or network management system (NMS) applications. However, because the deprecated MIBs will be removed from support in the future, you should update your network management applications and scripts to refer to the table names and attributes that are found in the replacement MIBs.

[Table 4](#) shows the deprecated MIBs and their replacements. In most cases, SNMPv1 and SNMPv2 replacements are available, but some MIBs are available only in one version. A few of the deprecated MIBs do not have replacement MIBs; support for these MIBs will be discontinued in a future release of Cisco IOS software.

Table 4 Replacements for Deprecated MIBs

Deprecated MIB	Replacement MIBs	
	SNMPv1 MIB	SNMPv2 MIB
OLD-CISCO-APPLETALK-MIB	RFC1243-MIB	—
OLD-CISCO-CHASSIS-MIB	ENTITY-MIB-V1SMI	ENTITY-MIB
OLD-CISCO-CPU-MIB	—	CISCO-PROCESS-MIB
OLD-CISCO-DECNET-MIB	—	—
OLD-CISCO-ENV-MIB	CISCO-ENVMON-MIB-V1SMI	CISCO-ENVMON-MIB
OLD-CISCO-FLASH-MIB	CISCO-FLASH-MIB-V1SMI	CISCO-FLASH-MIB
OLD-CISCO-INTERFACES-MIB	IF-MIB-V1SMI	IF-MIB
	CISCO-QUEUE-MIB-V1SMI	CISCO-QUEUE-MIB
OLD-CISCO-IP-MIB	—	—
OLD-CISCO-MEMORY-MI	CISCO-MEMORY-POOL-MIB-V1SMI	CISCO-MEMORY-POOL-MIB
OLD-CISCO-NOVELL-MIB	NOVELL-IPX-MIB	—
OLD-CISCO-SYS-MIB	(Compilation of other OLD* MIBs)	
OLD-CISCO-SYSTEM-MI	CISCO-CONFIG-COPY-MIB-V1SMI	CISCO-CONFIG-COPY-MIB
OLD-CISCO-TCP-MIB	CISCO-TCP-MIB-V1SMI	CISCO-TCP-MIB
OLD-CISCO-TS-MIB	—	—
OLD-CISCO-VINES-MIB	CISCO-VINES-MIB-V1SMI	CISCO-VINES-MIB
OLD-CISCO-XNS-MIB	—	—

**Note**

Some of the MIBs listed in [Table 4](#) represent feature sets that are not supported on the cable voice adapter.

Caveats

Caveats describe unexpected behavior in Cisco IOS software releases. Severity 1 caveats are the most serious caveats; severity 2 caveats are less serious. Severity 3 caveats are moderate caveats.

This section contains open and resolved caveats for Cisco IOS Release 12.2(15)CZ. All caveats in Release 12.2 T are also in Release 12.2(15)CZ.

For information on caveats in Cisco IOS Release 12.1 T, see *Caveats for Cisco IOS Release 12.1 T*, which lists severity 1 and 2 caveats and selected severity 3 caveats, and is located on Cisco.com and the Documentation CD-ROM.

Caveat numbers and brief descriptions for Release 12.2(15)CZ are listed in the following tables. For details about a particular caveat, go to Bug Toolkit at:

<http://www.cisco.com/kobayashi/bugs/bugs.html>

To access this location, you must have an account on Cisco.com. For information about how to obtain an account, go to the “[Feature Navigator](#)” [section on page 39](#).

**Note**

If you have an account with Cisco.com, you can use Bug Navigator II to find caveats of any severity for any release. To reach Bug Navigator II, go to Cisco.com and press **Login**. Then go to **Software Center: Cisco IOS Software: Cisco Bugtool Navigator II**. Another option is to go to <http://www.cisco.com/support/bugtools/>.

**Note**

This document lists the caveats that were known at the time of publication. The Bug Navigator II site has the most current information about any caveat. Also, this document may be updated as needed with any new information about caveats; the most current version is always posted on Cisco.com.

Open Caveats—Release 12.2(15)CZ3

There are no open caveats specific to Cisco IOS Release 12.2(15)CZ3 that require documentation in the release notes.

Closed or Resolved Caveats—Release 12.2(15)CZ3

Table 9 lists the significant closed or resolved caveats that exist in Cisco IOS Release 12.2(15)CZ3.

Table 5 Closed or Resolved Caveats for Release 12.2(15)CZ3

Caveat ID Number	Description
CSCei61732	<p>Cisco IOS may permit arbitrary code execution after exploitation of a heap-based buffer overflow vulnerability. Cisco has included additional integrity checks in its software, as further described below, that are intended to reduce the likelihood of arbitrary code execution.</p> <p>Cisco has made free software available that includes the additional integrity checks for affected customers.</p> <p>This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20051102-timers.shtml</p>

Open Caveats—Release 12.2(15)CZ2

There are no open caveats specific to Cisco IOS Release 12.2(15)CZ2 that require documentation in the release notes.

Closed or Resolved Caveats—Release 12.2(15)CZ2

Table 9 lists the significant closed or resolved caveats that exist in Cisco IOS Release 12.2(15)CZ2.

Table 6 *Closed or Resolved Caveats for Release 12.2(15)CZ2*

Caveat ID Number	Description
CSCsa81379	<p>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.</p> <p>If your router configuration does not currently contain the command ip flow-cache feature-accelerate, this change does not affect you.</p> <p>This removal does not require an upgrade of your existing installation.</p> <p>The removal of NetFlow Feature Acceleration does not affect any other aspects of Netflow operation, for example Access-list processing.</p> <p>The features are separate and distinct.</p> <p>Cisco Express Forwarding (CEF) supercedes the deprecated NetFlow Feature Acceleration.</p> <p>Additionally, the following MIB objects and OIDs have been deprecated and removed from the netflow mib (CISCO-NETFLOW-MIB):</p> <pre> 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 </pre>

Open Caveats—Release 12.2(15)CZ1

Table 7 lists only severity 1 and 2 caveats and select severity 3 caveats for the Cisco IOS 12.2(15)CZ1 beta release.

Table 7 *Open Caveats for Cisco IOS Release 12.2(15)CZ1*

DDTS ID Number	Description
CSCin68215	<p>Cisco ubr900 series cable modems running IOS release 12.2(15)CZ may experience memory leak when the cable interface flaps under error conditions.</p> <p>This issue is seen only in cases where cable modem was loaded with a 1.1 config file and CMTS was running an image that can support only 1.0.</p> <p>WorkAround: Using a correct version of MCNS config file, will solve this problem.</p>

Closed or Resolved Caveats—Release 12.2(15)CZ1

Table 9 lists the significant closed or resolved caveats that exist in Cisco IOS Release 12.2(15)CZ1.

Table 8 Closed or Resolved Caveats for Release 12.2(15)CZ1

Caveat ID Number	Description
CSCdx62749	<p>When ARP entry exists to the TFTP/TOD/DHCP server through E0 interface of the CM, it will forward the packets through E0. This causes spoofing/theft-of-service in MSO.</p> <p>Workaround: Please do not have ARP entry to the TFTP/TOD/DHCP servers through E0 interface. Let the device in the default state(do not add static APR to bypass TFTP/LOG servers).</p>
CSCea33942	<p>Symptoms: A Cisco uBR905 or Cisco uBR925 router may lose the configuration of the crypto map map-name local-address interface-id global configuration command from its startup configuration.</p> <p>This issue is observed when the router reloads and is related to the use of the Cable DHCP Proxy feature.</p> <p>Workaround: Set up a permanent lease for the loopback interface in the Dynamic Host Configuration Protocol (DHCP) server by using the “ethernet0” MAC address and assigning a fixed IP address on the DHCP server.</p>
CSCea47684	<p>Caller (phone number) id does not get displayed on the called party phone.</p> <p>This problem is seen in all cable modem images.</p> <p>There are no known workarounds.</p>
CSCeb68456	<p>This issue occurs when CM receives UCD while it send upstream packets. This is due to the output queue struck while processing UCD with upstream traffic on. This is very inconsistent problem only.</p> <p>Sometimes CM gets reset by itself due to DHCP renewal failure.</p> <p>Workaround: Reset the modem.</p>

Table 8 *Closed or Resolved Caveats for Release 12.2(15)CZ1*

Caveat ID Number	Description
CSCed78149	<p>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).</p> <p>These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:</p> <ol style="list-style-type: none"> 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 <p>Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.</p> <p>Multiple Cisco products are affected by the attacks described in this Internet draft.</p> <p>Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.</p> <p>This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml.</p> <p>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.</p>
CSCed87222	<p>A CPUHOG may appear on the console after a “clear crypto isa” or a “clear crypto sa” has been executed.</p> <p>This does not have any connectivity side effects and can be treated as somewhat cosmetic.</p> <p>There are no known workarounds.</p>

Table 8 Closed or Resolved Caveats for Release 12.2(15)CZ1

Caveat ID Number	Description
CSCee08584	<p>Cisco Internetwork Operating System (IOS®) Software release trains 12.1YD, 12.2T, 12.3 and 12.3T, when configured for the Cisco IOS Telephony Service (ITS), Cisco CallManager Express (CME) or Survivable Remote Site Telephony (SRST) may contain a vulnerability in processing certain malformed control protocol messages.</p> <p>A successful exploitation of this vulnerability may cause a reload of the device and could be exploited repeatedly to produce a Denial of Service (DoS).</p> <p>This advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20050119-itscme.shtml</p> <p>Cisco has made free software upgrades available to address this vulnerability for all affected customers. There are workarounds available to mitigate the effects of the vulnerability.</p> <p>This vulnerability is documented by Cisco bug ID CSCee08584.</p>
CSCee18125	<p>A Cisco 831 may crash with a SegV exception when you apply an EZVPN configuration to more than three inside interfaces and try to establish an EZVPN session.</p> <p>This issue is observed on a Cisco 831 that runs the c831-k9o3y6-mz image of Cisco IOS Release 12.3(2)XE. The issue may also occur in Release 12.3 or 12.3 T.</p> <p>Workaround: Do not apply the EZVPN configuration to more than three inside interfaces.</p>
CSCee31134	<p>Uncorrectable FEC counters associated with an UGS increase during registration process for cable modems attached to mc28u card.</p> <p>Per SID flow counters can be observed with CLI “show interface cable x/y sid z counters verbose”.</p> <p>This issue does not affect cable modem functionality.</p> <p>There are no known workarounds.</p>
CSCee92874	<p>When CM process DCC and changes to another downstream frequency, its observed that packet is not getting forwarded as the output queue is getting struck at C0 interface due to outgoing traffic.</p> <p>If the packet is not getting forwarded, after sometime, CM will get reset due to DHCP renewal failure.</p> <p>Workaround: Please reset the modem.</p>

Table 8 Closed or Resolved Caveats for Release 12.2(15)CZ1

Caveat ID Number	Description
CSCef44225	<p>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).</p> <p>These attacks, which only affect sessions terminating or originating on a device itself, can be of three types:</p> <ol style="list-style-type: none"> 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 <p>Successful attacks may cause connection resets or reduction of throughput in existing connections, depending on the attack type.</p> <p>Multiple Cisco products are affected by the attacks described in this Internet draft.</p> <p>Cisco has made free software available to address these vulnerabilities. In some cases there are workarounds available to mitigate the effects of the vulnerability.</p> <p>This advisory is posted at http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml.</p> <p>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.</p>
CSCef46191	<p>A specifically crafted Transmission Control Protocol (TCP) connection to a telnet or reverse telnet port of a Cisco device running Internetwork Operating System (IOS) may block further telnet, reverse telnet, Remote Shell (RSH), Secure Shell (SSH), and in some cases Hypertext Transport Protocol (HTTP) access to the Cisco device. Telnet, reverse telnet, RSH and SSH sessions established prior to exploitation are not affected.</p> <p>All other device services will operate normally. Services such as packet forwarding, routing protocols and all other communication to and through the device are not affected.</p> <p>Cisco will make free software available to address this vulnerability.</p> <p>Workarounds, identified below, are available that protect against this vulnerability.</p> <p>The Advisory is available at http://www.cisco.com/warp/public/707/cisco-sa-20040827-telnet.shtml</p>
CSCef60718	<p>A uBR925 running 12.3(10) reports incorrect Timing Offset.</p> <p>There are no known workarounds.</p>

Table 8 Closed or Resolved Caveats for Release 12.2(15)CZ1

Caveat ID Number	Description
CSCin75485	<p>Modem does not support DCC with BPI enabled scenario.</p> <p>There are no known workarounds.</p>
CSCin82407	<p>Cisco Internetwork Operating System (IOS) Software release trains 12.2T, 12.3 and 12.3T may contain vulnerabilities in processing certain Internet Key Exchange (IKE) Xauth messages when configured to be an Easy VPN Server.</p> <p>Successful exploitation of these vulnerabilities may permit an unauthorized user to complete authentication and potentially access network resources.</p> <p>This advisory will be posted to http://www.cisco.com/warp/public/707/cisco-sa-20050406-xauth.shtml</p>
CSCin85109	<p>Cable modem does not filter traffic based on the rules set in docsDevFilterIp Table.</p> <p>This issue is seen only when the cable modem is used in routing mode.</p> <p>Workaround: ip access-list filters could be configured using ios cli commands instead of using docsDevFilterIp Table in routing mode.</p>
CSCsa49138	<p>A ubr905 configured in routing mode and running 12.2(15)CZ can enter an init(o) loop if configured with DOCSIS TLV 11s (SNMP set operations).</p> <p>The 905 will work fine from a power up. However, once the 905 is kicked offline (i.e. clear cable modem reset on CMTS), it will fail with the following error:</p> <pre>Dec 16 22:35:04.367: 280.280 CMAC_LOG_RESET_UNABLE_TO_SET_MIB_OBJECT <130>CABLEMODEM[CISCO]: Dec 16 22:35:04.367: <73040200> TLV-11 - Illegal Set operation failed</pre> <p>This will keep the 905 in an offline-init(o) loop. The same config will work fine on 12.2T or on 12.2(15)CZ if the CM is running as a “cable-modem compliant bridge”.</p> <p>There are no known workarounds.</p>

Open Caveats—Release 12.2(15)CZ

There are no open caveats specific to Cisco IOS Release 12.2(15)CZ that require documentation in the release notes.

Closed or Resolved Caveats—Release 12.2(15)CZ

[Table 9](#) lists the significant closed or resolved caveats that exist in Cisco IOS Release 12.2(15)CZ.

Table 9 *Closed or Resolved Caveats for Release 12.2(15)CZ*

Caveat ID Number	Description
CSCee18619	<p>Cable interface may reset inubr9x5 and cva12x modems running 12.2(15)CZ release.</p> <p>This issue only occurs with debug logs for “debug cable mac message ucd” IOS CLI for any UCD message received by modem due to ny upstream parameter change.</p> <p>Workaround: Do not use this particular debug.</p>
CSCin68215	<p>Ciscoubr900 series cable modems running IOS release 12.2(15)CZ may experience memory leak when the cable interface flaps under error conditions.</p> <p>This issue is seen only in cases where cable modem was loaded with a 1.1 config file and CMTS was running an image that can support only 1.0.</p> <p>WorkAround: Using a correct version of MCNS config file, will solve this problem.</p>
CSCin71398	<p>Ciscoubr900 series cable modems running IOS release 12.2(15)CZ may experience ethernet stuck problem.</p> <p>This happens when cable interface is reset when there is a downstream traffic, with modem configured with DHCP proxy -NAT or routing mode with no ip cache entries.</p> <p>Workaround: Perform a “clear int eth 0” to clear the ethernet interface.</p>

Related Documentation

The following sections describe the documentation available for the cable voice adapter. These documents consist of hardware and software installation guides, Cisco IOS configuration guides and command references, system error messages, feature modules, and other documents.

Most documentation is available as printed manuals or electronic documents, except for feature modules and select manuals, which are available online on Cisco.com and the Documentation CD-ROM.

Use these release notes with these documents:

- [Release-Specific Documents, page 38](#)
- [Platform-Specific Documents, page 39](#)
- [Feature Modules, page 39](#)
- [Feature Navigator, page 39](#)
- [Cisco IOS Software Documentation Set Contents, page 40](#)

Release-Specific Documents

The following documents are specific to Release 12.2 and are located on Cisco.com and the Documentation CD-ROM:

- *Cross-Platform Release Notes for Cisco IOS Release 12.2*

On Cisco.com at:

Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 12.2: Release Notes: Cross-Platform Release Notes

On the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.2: Release Notes: Cross-Platform Release Notes

- Product bulletins, field notices, and other release-specific documents on Cisco.com at:

Technical Documents

- *Caveats for Cisco IOS Release 12.2 T*

As a supplement to the caveats listed in these release notes, see *Caveats for Cisco IOS Release 12.2*, which contains caveats applicable to all platforms for all maintenance releases of Release 12.2.

On Cisco.com at:

Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 12.2: Release Notes: Caveats

On the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS 12.2: Caveats



Note

If you have an account with Cisco.com, you can use Bug Navigator II to find caveats of any severity for any release. To reach Bug Navigator II, go to Cisco.com and press **Login**. Then go to **Software Center: Cisco IOS Software: Cisco Bugtool Navigator II**. Another option is to go to <http://www.cisco.com/support/bugtools/bugtool.shtml>.

Platform-Specific Documents

These documents are available for the cable voice adapter on Cisco.com and the Documentation CD-ROM:

- *Cisco CVA122 Cable Voice Adapter User Guide*
- *Cisco CVA122 Cable Voice Adapter Hardware Installation Guide*
- *Cisco CVA122 Cable Voice Adapter Features*
- *Cisco CVA122 Cable Voice Adapter Subscriber Setup Quick Start Card*
- *DOCSIS CPE Configurator Help*

On Cisco.com at:

Technical Documents: Documentation Home Page: Cisco Product Documentation: Broadband/Cable Solutions: Cisco CVA120 Series Cable Voice Adapters

On the Documentation CD-ROM at:

Cisco Product Documentation: Broadband/Cable Solutions: Cisco CVA120 Series Cable Voice Adapters

Feature Modules

Feature modules describe new features supported by Release 12.2, and are updates to the Cisco IOS documentation set. A feature module consists of a brief overview of the feature, benefits, and configuration tasks, and a command reference. As updates, the feature modules are available online only. Feature module information is incorporated in the next printing of the Cisco IOS documentation set.

On Cisco.com at:

Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 12.2: New Feature Documentation

On the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.2: New Feature Documentation

Feature Navigator

Feature Navigator is a web-based tool that enables you to quickly determine which Cisco IOS software images support a particular set of features and which features are supported in a particular Cisco IOS image.

Feature Navigator is available 24 hours a day, 7 days a week. To access Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, e-mail the Contact Database Administration group at cdbadmin@cisco.com. If you do not have an account on Cisco.com, go to <http://www.cisco.com/register> and follow the directions to establish an account.

To use Feature Navigator, you must have a JavaScript-enabled web browser such as Netscape 3.0 or later, or Internet Explorer 4.0 or later. Internet Explorer 4.0 always has JavaScript enabled. To enable JavaScript for Netscape 3.x or Netscape 4.x, follow the instructions provided with the web browser. For JavaScript support and enabling instructions for other browsers, check with the browser vendor.

Feature Navigator is updated when major Cisco IOS software releases and technology releases occur. It contains feature information about mainline-, T-, S-, and P-trains. You can access Feature Navigator at the following URL:

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

Cisco IOS Software Documentation Set Contents

The Cisco IOS software documentation set consists of the Cisco IOS configuration guides, Cisco IOS command references, and several other supporting documents. The Cisco IOS software documentation set is shipped with your order in electronic form on the Documentation CD-ROM, unless you specifically ordered the printed versions.

Documentation Modules

Each module in the Cisco IOS documentation set consists of one or more configuration guides and one or more corresponding command references. Chapters in a configuration guide describe protocols, configuration tasks, and Cisco IOS software functionality, and contain comprehensive configuration examples. Chapters in a command reference provide complete command syntax information. Use each configuration guide with its corresponding command reference.

On Cisco.com and the Documentation CD-ROM, two master hot-linked documents provide information for the Cisco IOS software documentation set.

On Cisco.com, beginning under the **Service & Support** heading:

Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 12.2: Configuration Guides and Command References

On the Documentation CD-ROM:

Cisco IOS Software Configuration: Cisco IOS Release 12.2: Configuration Guides and Command References

Cisco IOS Release 12.2 Documentation Set

[Table 10](#) lists the contents of the Cisco IOS Release 12.2 software documentation set, which is available in both electronic and printed form.



Note

You can find the most current Cisco IOS documentation on Cisco.com and the Documentation CD-ROM. These electronic documents may contain updates and modifications made after the hard-copy documents were printed.

On Cisco.com at:

Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 12.2

On the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.2

Table 10 Cisco IOS Release 12.2 Documentation Set

Books	Major Topics
<ul style="list-style-type: none"> • <i>Cisco IOS Configuration Fundamentals Configuration Guide</i> • <i>Cisco IOS Configuration Fundamentals Command Reference</i> 	Cisco IOS User Interfaces File Management System Management
<ul style="list-style-type: none"> • <i>Cisco IOS Bridging and IBM Networking Configuration Guide</i> • <i>Cisco IOS Bridging and IBM Networking Command Reference, Volume 1 of 2</i> • <i>Cisco IOS Bridging and IBM Networking Command Reference, Volume 2 of 2</i> 	Transparent Bridging SRB Token Ring Inter-Switch Link Token Ring Route Switch Module RSRB DLSw+ Serial Tunnel and Block Serial Tunnel LLC2 and SDLC IBM Network Media Translation SNA Frame Relay Access NCIA Client/Server Airline Product Set DSPU and SNA Service Point SNA Switching Services Cisco Transaction Connection Cisco Mainframe Channel Connection CLAW and TCP/IP Offload CSNA, CMPC, and CMPC+ TN3270 Server
<ul style="list-style-type: none"> • <i>Cisco IOS Dial Technologies Configuration Guide</i> • <i>Cisco IOS Dial Technologies Command Reference</i> 	Preparing for Dial Access Modem and Dial Shelf Configuration and Management ISDN Configuration Signaling Configuration Dial-on-Demand Routing Configuration Dial Backup Configuration Dial Related Addressing Service Virtual Templates, Profiles, and Networks PPP Configuration Callback and Bandwidth Allocation Configuration Dial Access Specialized Features Dial Access Scenarios
<ul style="list-style-type: none"> • <i>Cisco IOS Interface Configuration Guide</i> • <i>Cisco IOS Interface Command Reference</i> 	LAN Interfaces Serial Interfaces Logical Interfaces
<ul style="list-style-type: none"> • <i>Cisco IOS IP Configuration Guide</i> • <i>Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services</i> • <i>Cisco IOS IP Command Reference, Volume 2 of 3: Routing Protocols</i> • <i>Cisco IOS IP Command Reference, Volume 3 of 3: Multicast</i> 	IP Addressing and Services IP Routing Protocols IP Multicast
<ul style="list-style-type: none"> • <i>Cisco IOS AppleTalk and Novell IPX Configuration Guide</i> • <i>Cisco IOS AppleTalk and Novell IPX Command Reference</i> 	AppleTalk Novell IPX

Table 10 Cisco IOS Release 12.2 Documentation Set (continued)

Books	Major Topics
<ul style="list-style-type: none"> • <i>Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Configuration Guide</i> • <i>Cisco IOS Apollo Domain, Banyan VINES, DECnet, ISO CLNS, and XNS Command Reference</i> 	Apollo Domain Banyan VINES DECnet ISO CLNS XNS
<ul style="list-style-type: none"> • <i>Cisco IOS Voice, Video, and Fax Configuration Guide</i> • <i>Cisco IOS Voice, Video, and Fax Command Reference</i> 	Voice over IP Call Control Signaling Voice over Frame Relay Voice over ATM Telephony Applications Trunk Management Fax, Video, and Modem Support
<ul style="list-style-type: none"> • <i>Cisco IOS Quality of Service Solutions Configuration Guide</i> • <i>Cisco IOS Quality of Service Solutions Command Reference</i> 	Packet Classification Congestion Management Congestion Avoidance Policing and Shaping Signaling Link Efficiency Mechanisms
<ul style="list-style-type: none"> • <i>Cisco IOS Security Configuration Guide</i> • <i>Cisco IOS Security Command Reference</i> 	AAA Security Services Security Server Protocols Traffic Filtering and Firewalls IP Security and Encryption Passwords and Privileges Neighbor Router Authentication IP Security Options Supported AV Pairs
<ul style="list-style-type: none"> • <i>Cisco IOS Switching Services Configuration Guide</i> • <i>Cisco IOS Switching Services Command Reference</i> 	Cisco IOS Switching Paths NetFlow Switching Multiprotocol Label Switching Multilayer Switching Multicast Distributed Switching Virtual LANs LAN Emulation
<ul style="list-style-type: none"> • <i>Cisco IOS Wide-Area Networking Configuration Guide</i> • <i>Cisco IOS Wide-Area Networking Command Reference</i> 	ATM Broadband Access Frame Relay SMDS X.25 and LAPB
<ul style="list-style-type: none"> • <i>Cisco IOS Mobile Wireless Configuration Guide</i> • <i>Cisco IOS Mobile Wireless Command Reference</i> 	General Packet Radio Service

Table 10 *Cisco IOS Release 12.2 Documentation Set (continued)*

Books	Major Topics
<ul style="list-style-type: none"> • <i>Cisco IOS Terminal Services Configuration Guide</i> • <i>Cisco IOS Terminal Services Command Reference</i> 	ARA LAT NASI Telnet TN3270 XRemote X.28 PAD Protocol Translation
<ul style="list-style-type: none"> • <i>Cisco IOS Configuration Guide Master Index</i> • <i>Cisco IOS Command Reference Master Index</i> • <i>Cisco IOS Debug Command Reference</i> • <i>Cisco IOS Software System Error Messages</i> • <i>New Features in 12.2 T-Based Limited Lifetime Releases</i> • <i>New Features in Release 12.2 T T</i> • <i>Release Notes</i> (Release note and caveat documentation for 12.2 T-based releases and various platforms) 	

Obtaining Documentation

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

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at <http://www.cisco.com>. Translated documentation can be accessed at http://www.cisco.com/public/countries_languages.shtml.

Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or as an annual subscription.

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco product documentation from the Networking Products MarketPlace:
http://www.cisco.com/cgi-bin/order/order_root.pl
- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:
<http://www.cisco.com/go/subscription>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, in North America, by calling 800 553-NETS(6387).

Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit technical comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, for your convenience many documents contain a response card behind the front cover. Otherwise, you can mail your comments to the following address:

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

We appreciate your comments.

Obtaining Technical Assistance

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

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following web site:

<http://www.cisco.com>

Technical Assistance Center

The Cisco TAC web site is available to all customers who need technical assistance with a Cisco product or technology that is under warranty or covered by a maintenance contract.

Contacting TAC by Using the Cisco TAC Web Site

If you have a priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC web site:

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

P3 and P4 level problems are defined as follows:

- P3—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- P4—You need information or assistance on Cisco product capabilities, product installation, or basic product configuration.

In each of the above cases, use the Cisco TAC web site to quickly find answers to your questions.

To register for Cisco.com, go to the following web site:

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

If you cannot resolve your technical issue by using the TAC online resources, Cisco.com registered users can open a case online by using the TAC Case Open tool at the following web site:

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

Contacting TAC by Telephone

If you have a priority level 1 (P1) or priority level 2 (P2) problem, contact TAC by telephone and immediately open a case. To obtain a directory of toll-free numbers for your country, go to the following web site:

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

P1 and P2 level problems are defined as follows:

- P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.
- P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.

This document is to be used in conjunction with the documents listed in the “[Related Documentation](#)” section on page 38.

CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, 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 Access Registrar, 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, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, 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, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, 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. (0502R)

Copyright © 2004-2005, Cisco Systems, Inc.
All rights reserved.