



Text Part Number: 78-6982-02

Release Notes for Cisco uBR924 Cable Access Router for Cisco IOS Release 12.0(7)T

December 13, 1999

These release notes for the Cisco uBR924 cable access router support Cisco IOS Release 12.0 T, up to and including Release 12.0(4)XII1, 12.0(5)T, 12.0(7)T, or higher interim images. These release notes are updated as needed to describe new features, memory requirements, hardware support, software platform deferrals, and changes to the microcode or modem code and related documents.

For a list of software caveats that apply to Release 12.0(7)T, see the “Caveats” section on page 23 and *Caveats for Cisco IOS Release 12.0 T*. The caveats document is updated for every maintenance release and is located on Cisco Connection Online (CCO).

Use these release notes with *Cross-Platform Release Notes for Cisco IOS Release 12.0* located on CCO.

Contents

These release notes describe the following topics:

- Introduction, page 2
- System Requirements, page 3
- New and Changed Information, page 11
- Limitations and Restrictions, page 19
- Important Notes, page 20
- Caveats, page 23
- Related Documentation, page 25
- Service and Support, page 30
- Cisco Connection Online, page 31
- Documentation CD-ROM, page 32

Corporate Headquarters

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

Copyright © 1999
Cisco Systems, Inc.
All rights reserved.

Introduction

The Cisco uBR924 cable access router gives residential or small office/home office (SOHO) subscribers high-speed Internet or Intranet access and packet telephone services via a shared two-way cable system and IP backbone network. The router connects computers, telephone or fax equipment, and other customer premises devices at a subscriber site to the service provider's cable and IP backbone network.

The router is based on Data-Over-Cable Service Interface Specifications (DOCSIS) and interoperates with any bidirectional, DOCSIS-qualified Cable Modem Termination System (CMTS). The router ships from the Cisco factory with a Cisco IOS software image stored in nonvolatile memory (NVRAM) that supports DOCSIS-compliant bridging data operations. The Cisco uBR924 cable access router functions as a cable modem—a modulator/demodulator at a subscriber site to convey data communications on the cable television system.

Based on the feature licenses your company purchased, other Cisco IOS images can be downloaded from Cisco Connection Online (CCO). Each Cisco uBR924 cable access router in your network can then be configured to support Voice over IP (VoIP) and/or other special operating modes based on your service offering and the practices in place for your network. The Cisco uBR924 cable access router can function as an advanced router, providing wide area network (WAN) data connectivity in a variety of configurations.

Note Starting with Cisco IOS Release 12.0(5)T, all Cisco uBR924 cable access router images support DOCSIS Baseline Privacy (BPI) encryption/decryption. BPI is subject to export restrictions.

Early Deployment Releases

These release notes describe the Cisco uBR924 cable access router for Release 12.0(7)T. Release 12.0 T is an Early Deployment (ED) release based on Release 12.0 and announces fixes to software caveats and support for new Cisco hardware.

For information about features in Release 12.0, see *Cross-Platform Release Notes for Cisco IOS Release 12.0* on CCO.

For information about features in other ED releases, see Table 1.

For information about features in other platforms, see *Release Notes for Cisco IOS Release 12.0* on CCO.

Table 1 Early Deployment Releases for the Cisco uBR924 Cable Access Router

ED Release	Maintenance Release	Availability	Additional Software Features
Release 12.0 T	(7)	Now	<ul style="list-style-type: none"> • VPN Enhancements—Dynamic Crypto Map • NetRanger Support—IOS Intrusion Detection • Firewall (Phase II) • SGCP 1.1 • SGCP MIB
Release 12.0 T	(5)	Now	<ul style="list-style-type: none"> • Fax support over the cable network • Advanced data feature sets: <ul style="list-style-type: none"> — DOCSIS Baseline Privacy (BPI) — IPSec—56-bit encryption/decryption at network layer (Phase I) — 3DES—Triple DES (Phase I): 168-bit encryption/decryption at network layer (Phase I) — L2TP—Layer 2 tunneling protocol (Phase I) — Firewall (Phase I) • Enhanced VoIP feature integration • Enhanced bridging functionality
Release 12.0 XI1	(4)	Now	<ul style="list-style-type: none"> • Full and DOCSIS-compliant bridging • Network address translation and port address translation (NAT/PAT) • Radio frequency interface • Routing (RIP V2)

System Requirements

This section describes the system requirements for Release 12.0 T:

- Memory Requirements, page 4
- Headend Interoperability, page 7
- Hardware Supported, page 7
- Determining the Software Version, page 8
- Upgrading to a New Software Release, page 8
- Feature Set Tables, page 9

Memory Requirements

Table 2 Memory Requirements for the Cisco uBR924 Voice and Data Images

Feature Set Matrix Term	Image Name	Minimum Flash Memory	Minimum DRAM Memory	Runs From	Feature Status
IP Routing Standard Feature Sets					
12.0(7)T images					
Base IP Bridging Voice	ubr920-k1v4-mz	4 MB Flash	16 MB DRAM	RAM	Bridging-only encryption/decryption image added in Release 12.0(7)T
Home Office Voice (SGCP and H.323)	ubr920-k1v4y5-mz	4 MB Flash	16 MB DRAM	RAM	Encryption/decryption image added in Release 12.0(7)T
Small Office/Voice/FW ¹ /IDS (SGCP and H.323)	ubr920-k1o3v4y5-mz	4 MB Flash	16 MB DRAM	RAM	Firewall (Phase II) encryption/decryption image added in Release 12.0(7)T
Small Office+/Voice/FW/IDS/IPSec 56 (SGCP and H.323)	ubr920-k1o3sv4y556i-mz	4 MB Flash	16 MB DRAM	RAM	Firewall (Phase II) encryption/decryption image added in Release 12.0(7)T
Small Office+ Voice/FW/IPSec 3DES (SGCP and H.323)	ubr920-k1k2o3sv4y5-mz	4 MB Flash	16 MB DRAM	RAM	Firewall (Phase II) encryption/decryption image added in Release 12.0(7)T
Telecommuter/Voice/IPSec 56 (SGCP and H.323)	ubr920-k1sv4y556i-mz	4 MB Flash	16 MB DRAM	RAM	Encryption/decryption image added in Release 12.0(7)T
Telecommuter+/Voice/IPSec 3DES (SGCP and H.323)	ubr920-k1k2sv4y5-mz	4 MB Flash	16 MB DRAM	RAM	Encryption/decryption image added in Release 12.0(7)T
12.0(5)T images					
Home Office Voice	ubr920-k1v4y5-mz	4 MB Flash	16 MB DRAM	RAM	Encryption/decryption image added in Release 12.0(5)T
Small Office Voice/FW ¹	ubr920-k1ov4y5-mz	4 MB Flash	16 MB DRAM	RAM	Encryption/decryption image added in Release 12.0(5)T
Small Office+ Voice/FW IPSec 56	ubr920-k1osv4y556i-mz	4 MB Flash	16 MB DRAM	RAM	Encryption/decryption image added in Release 12.0(5)T
Small Office+ Voice/FW/IPSec 3DES	ubr920-k1k2osv4y5-mz	4 MB Flash	16 MB DRAM	RAM	Encryption/decryption image added in Release 12.0(5)T

Table 2 Memory Requirements for the Cisco uBR924 Voice and Data Images (continued)

Feature Set Matrix Term	Image Name	Minimum Flash Memory	Minimum DRAM Memory	Runs From	Feature Status
Telecommuter Voice/IPSec 56	ubr920-k1sv4y556i-mz	4 MB Flash	16 MB DRAM	RAM	Encryption/decryption image added in Release 12.0(5)T
Telecommuter+ Voice/IPSec 3DES	ubr920-k1k2sv4y5-mz	4 MB Flash	16 MB DRAM	RAM	Encryption/decryption image added in Release 12.0(5)T

¹FW—Firewall

Table 3 Memory Requirements for the Cisco uBR924 Data-Only Images

Feature Set Matrix Term	Image Name	Minimum Flash Memory	Minimum DRAM Memory	Runs From	Feature Status
IP Routing Standard Feature Sets					
12.0(7)T images					
Base IP Bridging	ubr920-k1-mz	4 MB Flash	16 MB DRAM	RAM	Bridging-only encryption/decryption image added in Release 12.0(7)T
Home Office	ubr920-k1y5-mz	4 MB Flash	16 MB DRAM	RAM	Encryption/decryption image added in Release 12.0(5)T Supports bridging and routing operations, Easy IP, and automated provisioning
Small Office FW ¹ /IDS	ubr920-k1o3y5-mz	4 MB Flash	16 MB DRAM	RAM	Firewall (Phase II) encryption/decryption image added in Release 12.0(7)T
Small Office+ FW/IDS/IPSec 56	ubr920-k1o3y556i-mz	4 MB Flash	16 MB DRAM	RAM	Firewall (Phase II) encryption/decryption image added in Release 12.0(7)T
Small Office+ FW/IPSec 3DES	ubr920-k1k2o3sy-mz	4 MB Flash	16 MB DRAM	RAM	Firewall (Phase II) encryption/decryption image added in Release 12.0(7)T
Small Office+/FW/IDS/IPSec 3 DES	ubr920-k1k2o3sy5-mz	4 MB Flash	16 MB DRAM	RAM	Firewall (Phase II) encryption/decryption image added in Release 12.0(7)T
Telecommuter/IPSec 56	ubr920-k1sy556i-mz	4 MB Flash	16 MB DRAM	RAM	Encryption/decryption image added in Release 12.0(5)T

Table 3 Memory Requirements for the Cisco uBR924 Data-Only Images (continued)

Feature Set Matrix Term	Image Name	Minimum Flash Memory	Minimum DRAM Memory	Runs From	Feature Status
Telecommuter+/IPSec 3DES	ubr920-k1k2sy5-mz	4 MB Flash	16 MB DRAM	RAM	Encryption/decryption image added in Release 12.0(5)T
12.0(5)T images					
Home Office	ubr920-k1y5-mz	4 MB Flash	16 MB DRAM	RAM	Encryption/decryption image added in Release 12.0(5)T Supports bridging and routing operations, Easy IP, and automated provisioning
Small Office FW ¹	ubr920-k1oy5-mz	4 MB Flash	16 MB DRAM	RAM	Encryption/decryption image added in Release 12.0(5)T
Small Office+ FW/IPSec 56	ubr920-k1osy556i-mz	4 MB Flash	16 MB DRAM	RAM	Encryption/decryption image added in Release 12.0(5)T
Small Office+ FW/IPSec 3DES	ubr920-k1k2osy-mz	4 MB Flash	16 MB DRAM	RAM	Encryption/decryption image added in Release 12.0(5)T
Telecommuter/IPSec 56	ubr920-k1sy556i-mz	4 MB Flash	16 MB DRAM	RAM	Encryption/decryption image added in Release 12.0(5)T
Telecommuter+/IPSec 3DES	ubr920-k1k2sy5-mz	4 MB Flash	16 MB DRAM	RAM	Encryption/decryption image added in Release 12.0(5)T

¹FW—Firewall

The image subset legend for Table 2 and Table 3 is as follows:

- y5=Reduced IP image with easy IP functionality (PAT/NAT/DHCP server)
- v4=Voice set—Additional SGCP protocol is supported for voice in Cisco IOS Release 12.0(7)T and Cisco IOS Release 12.0(7)XR
- s=Plus set includes L2TP—Available in Cisco IOS Release 12.0(7)T; not available in Cisco IOS Release 12.0(7)XR
- o=Firewall (Phase I) feature set—Available in Cisco IOS Release 12.0(5)T
- o3=Firewall (Phase II) feature set—Available in Cisco IOS Release 12.0(7)T
- k1=DOCSIS baseline privacy
- 56i=56-bit IPSec—Available in Cisco IOS Release 12.0(7)T; not available in Cisco IOS Release 12.0(7)XR
- k2=Triple DES (Phase I)—Available in Cisco IOS Release 12.0(5)T; enhancements available in 12.0(7)T

Headend Interoperability

Voice

In Cisco IOS Release 12.0(7)T, Simple Gateway Control Protocol (SGCP) is introduced. SGCP is an alternative to the H.323 protocol that provides signaling and feature negotiation via a remote Call Agent (CA). SGCP eliminates the need for a dial plan mapper. It also eliminates the need for static configuration on the router to map IP addresses to telephone numbers because this function is provided by the remote CA.

To configure the Cisco uBR924 cable access router 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. The first CoS is used for data (and voice if no other CoS is defined), and a second CoS can be defined to give higher priority for voice traffic. Lower-priority traffic can then be fragmented to avoid interfering with the timeslots allocated for voice traffic.

When configured to support voice in Cisco IOS Releases 12.0(4)XI1 and 12.0(5)T, the Cisco uBR924 cable access router packetizes and transports voice in compliance with the H.323 protocol. H.323v2 is integrated in Cisco gatekeeper/gateway products, such as the Cisco 2600 series and Cisco 3600 series, using Cisco IOS Release 12.0(5)T or higher interim images. The gatekeeper must be running Cisco IOS Release 12.0(5)T or higher in order to support registration of the full E.164 address for each Cisco uBR924 cable access router port.

Note In Cisco IOS Release 12.0(5)T, the CMTS images, if you are using Cisco uBR7200 series equipment, support static multi-SID. Static multi-SID provides better-than-best-effort transmission of either data and voice or a combination of data and voice packets.

Advanced Data Feature Sets

Note Starting with Cisco IOS Release 12.0(5)T, all Cisco uBR924 cable access router images support DOCSIS Baseline Privacy (BPI) encryption/decryption. BPI is subject to export restrictions.

To support encryption/decryption, Cisco IOS images must contain encryption/decryption software at both the CMTS router and the Cisco uBR924 cable access router. Both the CMTS router and the Cisco uBR924 cable access router must be enabled and configured per the software feature set.

If you are using Cisco 7200 series equipment, also refer to applicable release notes for the corresponding images at the headend that support the encryption/decryption software and the VPN solution set.

Hardware Supported

The Cisco uBR924 cable access router contains:

- A single F-connector interface to the cable system.
- Four RJ-45 (10BaseT Ethernet) hub ports to connect:

- Up to three computers directly to the four Ethernet hub ports at the rear of the Cisco uBR924 cable access router when operating in bridging mode using Cisco IOS Release 12.0(4)XI or higher interim images. When operating in routing mode, all four Ethernet hub ports can be connected directly to four computers.

Note When using Cisco IOS Release 12.0(5)T or higher, four computers can be connected directly to the four Ethernet hub ports in bridging mode.

- One of the four Ethernet hub ports at the rear of the Cisco uBR924 cable access router can be connected to an Ethernet hub, which then connects additional computers or devices at the site when operating in routing or bridging mode using Cisco IOS Release 12.0(5)T or higher.
- Two RJ-11 Foreign Exchange Station (FXS) ports to connect telephones and fax devices to the cable system and IP backbone; the router ships from the Cisco factory with the voice ports disabled. FXS ports on the Cisco uBR924 cable access router are to be connected to analog telephones or fax machines and not used for PBX extensions.
- One RJ-11 port to connect to a standard, analog telephone line (optional) to provide a backup Plain Old Telephone Service (POTS) connection to the Public Switched Telephone Network (PSTN) should the Cisco uBR924 cable access router lose power.
- One RJ-45 console port (optional) to connect to a laptop computer or console terminal when locally configuring the Cisco uBR924 cable access router; the router ships from the Cisco factory with the console port enabled.

Determining the Software Version

To determine the version of Cisco IOS software running on your Cisco uBR924 cable access router, log in to the Cisco uBR924 cable access router and enter the **show version** EXEC command:

```
router#show ver
Cisco Internetwork Operating System Software
IOS (tm) 920 Software (UBR920-Y5-M), Version 12.0(7)T, EARLY DEPLOYMENT RELEASE
SOFTWARE (fc2)
TAC:Home:SW:IOS:Specials for info
Copyright (c) 1986-1999 by cisco Systems, Inc.
```

Upgrading to a New Software Release

For information about upgrading to a new software release, see the product bulletin *Cisco IOS Software Release 12.0 T Upgrade Paths and Packaging Simplification (#819: 1/99)* on CCO at:

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

Under **Cisco IOS 12.0**, click **Cisco IOS Software Release 12.0 T Upgrade (#819: 1/99)**

Note The *Cisco IOS Software Release 12.0 T Upgrade Paths and Packaging Simplification* can also be found at this URL: <http://www.cisco.com/kobayashi/library/12.0/120MigrPaths.pdf>. You must have an account on CCO to access this URL.

Feature Set Tables

The Cisco IOS software is packaged in feature sets consisting of software images—depending on the platform. Each feature set contains a specific set of Cisco IOS features. (See Table 4.)

Release 12.0 T supports the same feature sets as Release 12.0, but Release 12.0 T can include new features supported by the Cisco uBR924 cable access router.

The Cisco uBR924 cable access router IP routing capabilities conserve IP addresses by using port-level multiplexed Network Address Translation (NAT) and Port Address Translation (PAT). Dynamic Host Configuration Protocol (DHCP) is used to distribute these or real IP addresses to the devices the Cisco uBR924 cable access router supports. NAT/PAT is bundled with DHCP server into a feature referred to as “Easy IP.”



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

Table 4 lists the features and feature sets supported by the Cisco uBR924 cable access router in Cisco IOS Release 12.0 T and uses the following conventions:

- Yes—The feature is supported in the feature set.
- No—The feature is not supported in the feature set.
- In—The number in the “In” column indicates the Cisco IOS release in which the feature was first introduced.

Note This feature set table only contains a selected list of features. This table is not cumulative—nor does it list all the features in each image.

Both Table 4 and Table 5 list the Cisco IOS software images by feature sets. Table 4 lists the voice and data software images; Table 5 lists the data-only software images.

Table 4 Feature List by Feature Set for the Cisco uBR924 Cable Access Router Voice and Data

Features	In	Software Images by Feature Set Matrix Term						
		Base IP Bridging/ Voice	Home Office Voice	Small Office Voice/FW/ IDS	Small Office+ Voice/FW/ IDS/ IPSec 56	Small Office+ Voice/FW/ IPSec 3DES	Telecom- muter/ Voice/ IPSec 56	Telecom- muter+ Voice/ IPSec 3DES
Full and DOCSIS-Compliant Bridging	(4)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
DOCSIS Baseline Privacy (BPI)	(5)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Easy IP	(4)	No	Yes	Yes	Yes	Yes	Yes	Yes
Triple DES (Phase I) (3DES)	(5)	No	No	No	No	Yes	No	Yes
IPSec Network Security (IPSec)	(5)	No	No	No	Yes	Yes	Yes	Yes

System Requirements

Table 4 Feature List by Feature Set for the Cisco uBR924 Cable Access Router Voice and Data (continued)

Features	In	Software Images by Feature Set Matrix Term							
		Base IP Bridging/ Voice	Home Office Voice	Small Office Voice/FW/ IDS	Small Office+ Voice/FW/ IDS/ IPSec 56	Small Office+ Voice/FW/ IPSec 3DES	Telecom- muter/ Voice/ IPSec 56	Telecom- muter+ Voice/ IPSec 3DES	
Layer 2 Tunneling Protocol (L2TP)	(5)	No	No	No	Yes	Yes	Yes	Yes	
Routing (RIP V2)	(4)	No	Yes	Yes	Yes	Yes	Yes	Yes	
H.323 Protocol	(5)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
Simple Gateway Control Protocol (SGCP)	(7)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
Network Management									
DOCSIS 1.0 Baseline Privacy MIB	(5)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
Cable Device MIB	(4)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
Cisco Standard MIBs	(4)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
Cisco Voice MIBs	(4)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
Radio Frequency Interface MIB	(4)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
SGCP MIB	(7)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	

Table 5 Feature List by Feature Set for the Cisco uBR924 Cable Access Router Data Only

Features	In	Software Images by Feature Set Matrix Term							
		Base IP Bridg- ing	Home Office	Small Office FW/ IDS	Small Office+ FW/IDS/ IPSec 56	Small Office+ FW/IPSec 3DES	Small Office+/ FW/IDS/ IPSec 3DES	Telecom- muter/ IPSec 56	Telecom- muter+/ IPSec 3DES
Full and DOCSIS-Compliant Bridging	(4)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
DOCSIS Baseline Privacy (BPI)	(5)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
Easy IP	(4)	No	Yes	Yes	Yes	Yes	Yes	Yes	
Triple DES (Phase I) (3DES)	(5)	No	No	No	No	Yes	Yes	No	
IPSec Network Security (IPSec)	(5)	No	No	No	Yes	Yes	Yes	Yes	
Layer 2 Tunneling Protocol (L2TP)	(5)	No	No	No	Yes	Yes	Yes	Yes	
Routing (RIP V2)	(4)	No	Yes	Yes	Yes	Yes	Yes	Yes	
Network Management									
DOCSIS 1.0 Baseline Privacy MIB	(5)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
Cable Device MIB	(4)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
Cisco Standard MIBs	(4)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
Cisco Voice MIBs	(4)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
Radio Frequency Interface MIB	(4)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	
SGCP MIB	(7)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	

New and Changed Information

The following sections list the new hardware and software features supported by the Cisco uBR924 cable access router for Release 12.0 T.

No New Hardware Features in Release 12.0(7)T

There are no new hardware features supported by the Cisco uBR924 cable access router for Release 12.0(7)T.

New Software Features in Release 12.0(7)T

The following new software features are supported by the Cisco uBR924 cable access router for Release 12.0(7)T.

VPN Enhancement—Dynamic Crypto Map

Dynamic crypto map is one of the PIX IPSec network security commands. IPSec provides security for transmission of sensitive information over unprotected networks such as the Internet.

The **dynamic crypto map** command is used to create policy templates that are used when processing negotiation requests for new security associations from a remote IPSec peer, even if you do not know all of the crypto map parameters required to communicate with the remote peer (such as the peer's IP address). The dynamic crypto map allows you to accept requests for new security associations from previously unknown peers. These requests, however, are not processed until the ISAKMP (IKE) authentication has completed successfully.

When the firewall receives a negotiation request via IKE from another IPSec peer, the request is examined to see if it matches a crypto map entry. If the negotiation does not match any explicit crypto map entry, it will be rejected unless the crypto map set includes a reference to a dynamic crypto map.

If the firewall accepts the peer's request, at the point that it installs the new IPSec security associations, it also installs a temporary crypto map entry. This entry is filled in with the results of the negotiation. At this point, the firewall performs normal processing, using this temporary crypto map entry as a normal entry, even requesting new security associations if the current ones are expiring (based on the policy specified in the temporary crypto map entry). After all of the corresponding security associations expire, the temporary crypto map entry is removed.

Dynamic crypto map sets are not used for initiating IPSec security associations. However, they are used for determining whether or not traffic should be protected.

Note The only parameter required in a **dynamic crypto map** is the **set transform-set**. All other parameters are optional.

NetRanger Support—IOS Intrusion Detection

Cisco IOS Release 12.0(7)T supports NetRanger programming. NetRanger is an Intrusion Detection System (IDS) composed of three parts:

- A management console (director) that is used to view the alarms as well as to manage the sensors.
- A sensor that monitors traffic. This traffic is matched against a list of known signatures to detect misuse of the network. This is usually in the form of scanning for vulnerabilities or of attacking systems. When a signature is matched, the sensor can track certain actions. In the case of the appliance sensor, it can reset (via TCP/rst) sessions, or enable “shuns” of further traffic. In the case of the IOS-IDS, it can drop traffic. In all cases, the sensor can send alarms to the director.
- Communications through automated report generation of standardized and customizable reports and QoS/CoS monitoring capabilities.

Firewall (Phase II)

Cisco IOS Release 12.0(7)T enhances the Cisco IOS Firewall feature set with the Cisco IOS Firewall (Phase II) set of features:

- Context-Based Access Control (CBAC) that intelligently filters TCP and UDP packets based on the application-layer protocol. This includes Java applets, which can be blocked completely or allowed only from known and trusted sources.
- Detection and prevention of the most common denial of service (DoS) attacks, such as ICMP and UDP echo packet flooding, SYN packet flooding, half-open or other unusual TCP connections, and deliberate mis-fragmentation of IP packets.
- Support for a broad range of commonly used protocols, including H.323 and NetMeeting, FTP, HTTP, MS Netshow, RPC, SMTP, SQL*Net, and TFTP.
- Authentication Proxy for authentication and authorization of web clients on a per-user basis.
- Dynamic port mapping that maps the default port numbers for well-known applications to other port numbers. This can be done on a host-by-host basis or for an entire subnet, providing a large degree of control over which users can access different applications.
- Configurable alerts and audit trail.
- Intrusion Detection System (IDS) that recognizes the signatures of 59 common attack profiles. When an intrusion is detected, IDS can either send an alarm to a syslog server or to NetRanger Director, drop the packet, or reset the TCP connection.
- User-configurable audit rules.
- Configurable real-time alerts and audit trail logs.

For general information, see the description of the *Cisco IOS Firewall Feature Set* in the *Cisco Product Catalog*. For detailed information, see the *Cisco IOS Firewall Feature Set* documentation set, as well as the sections on Traffic Filtering and Firewalls in the *Security Configuration Guide* and *Security Command Reference* (available on the Documentation CD-ROM and CCO).

Simple Gateway Control Protocol 1.1

The Cisco uBR924 cable access router supports Simple Gateway Control Protocol (SGCP). SGCP is an out-of-band signaling protocol that interacts with the external Call Agent (CA) to establish telephone calls. SGCP eliminates the need for a dial plan mapper and static configuration on the router to map IP addresses to telephone numbers because this function is provided by the external CA.

The Cisco uBR924 cable access router supports SGCP residential gateway (RGW), as opposed to trunking gateway (TGW), which controls the telephone call.

SGCP MIB

The Simple Gateway Control Protocol (SGCP) Management Information Base (MIB) supports configuration, performance, and fault management of the SGCP interface. The SGCP MIB components are as follows:

- **xgcpInBadVersions**—Number of incoming messages delivered to the protocol entity and that are for an unsupported protocol version
- **xgcpRequestTimeout**—Timeout value used for retransmitting an unacknowledged message
- **xgcpRequestRetries**—Number of retries for a request that exceeds timeout
- **xgcpAdminStatus**—Desired state of the protocol entity
- **xgcpOperStatus**—Current operational status of the protocol entity
- **xgcpUnRecognizedPackets**—Number of unrecognized packets since reset
- **xgcpMsgStatTable**—Table that contains SGCP statistics information since reset
- **xgcpMsgStatEntry**—Row in the xgcpMsgStatTable that contains information about SGCP message statistics per IP address of the Media Gateway Controller (MGC)
- **xgcpIPAddress**—IP address of the MGC
- **xgcpSuccessMessages**—Number of successful messages that communicate with the MGC on that IP address
- **xgcpFailMessages**—Number of failed messages that communicate with the MGC on that IP address
- **xgcpUpDownNotification**—Notification sent when the protocol status changes between up and down

No New Hardware Features in Release 12.0(5)T

There are no new hardware features supported by the Cisco uBR924 cable access router for Release 12.0(5)T.

New Software Features in Release 12.0(5)T

Note All Cisco IOS Release 12.0(5)T images were deferred because of DDTS entries CSCdm64438 and CSCdm66365. See *Resolved Caveats—Release 12.0(5)T1*.

The following new software features are supported by the Cisco uBR924 cable access router for Release 12.0(5)T.

Fax

Fax support is introduced in Cisco IOS Release 12.0(5)T images that support voice. The two Cisco uBR924 cable access router VoIP ports can now be connected to telephone or fax devices. Also refer to *New Hardware Features In Release 12.0(4)X11*.

Note Only one voice call (telephone or fax) per VoIP line is active at a time.

Enhanced Bridging

The Cisco uBR924 cable access router contains four RJ-45 (10BaseT Ethernet) hub ports. Using Cisco IOS Release 12.0(5)T or higher interim images, these hub ports can be connected to four computers directly or one of the four ports to an Ethernet hub. The Ethernet hub connects additional computers or devices at the site. A maximum of three devices can be bridged using Cisco IOS 12.0(4)XI or higher interim images. A maximum of 254 devices can be bridged using Cisco IOS 12.0(5)T or higher interim images. (No limit exists in routing mode.)

DOCSIS Baseline Privacy

The DOCSIS Baseline Privacy feature is based on the DOCSIS Baseline Privacy Interface Specification. It provides data privacy across the HFC network by encrypting traffic flows between the Cisco uBR924 cable access router and the cable operator's Cable Modem Termination System (CMTS).

Baseline Privacy security services are defined as a set of extended services within the DOCSIS MAC sublayer. Two new MAC management message types, BPKM-REQ and BPKM-RSP, are employed to support the Baseline Privacy Key Management (BPKM) protocol.

The BPKM protocol does not use authentication mechanisms such as passwords or digital signatures; it provides basic protection of service by ensuring that a cable modem, uniquely identified by its 48-bit IEEE MAC address, can only obtain keying material for services it is authorized to access. The Cisco uBR924 cable access router is able to obtain two types of keys from the CMTS: the Traffic Exchange Key (TEK), which is used to encrypt and decrypt data packets, and the Key Exchange Key (KEK), which is used to decrypt the TEK.

For more information on this feature, refer to the DOCSIS Baseline Privacy Interface Specification (SP-BPI-IO1-970922).

IPSec Network Security

IPSec Network Security (IPSec) is an IP security feature that provides robust authentications and encryption of IP packets. IPSec is a framework of open standards developed by the Internet Engineering Task Force (IETF). IPSec provides security for transmission of sensitive information over unprotected networks such as the Internet. IPSec acts at the network layer, protecting and authenticating IP packets between participating IPSec devices ("peers") such as the Cisco uBR924 cable access router.

IPSec provides the following network security services:

- Privacy—IPSec can encrypt packets before transmitting them across a network.
- Integrity—IPSec authenticates packets at the destination peer to ensure that the data has not been altered during transmission.
- Authentication—Peers authenticate the source of all IPSec-protected packets.
- Anti-replay protection—Prevents capture and replay of packets; helps protect against denial-of-service attacks.

Triple DES (Phase I)

Data Encryption Standard (DES) is a standard cryptographic algorithm developed by the United States National Bureau of Standards. The Triple DES (3DES) images increase the encryption/decryption from the 56-bit IPsec feature set to 168 bit.

Layer 2 Tunneling Protocol

Layer 2 Tunneling Protocol (L2TP) is an emerging Internet Engineering Task Force (IETF) standard that combines Cisco's Layer 2 Forwarding (L2F) and Microsoft's Point-to-Point Tunneling Protocol (PPTP). L2TP is an extension of the Point-to-Point Protocol (PPP), which is an important component for Access Virtual Private Networks (VPNs).

Traditional dial-up networking services only supported registered IP addresses, which limited the types of applications that could be implemented over VPNs. L2TP supports multiple protocols and unregistered and privately administered IP addresses over the Internet. This allows the existing access infrastructure, such as the Internet, modems, access servers, and ISDN terminal adapters (TAs), to be used.

L2TP can be initiated wherever PPTP or L2F is currently deployed and can be operated as a client initiated tunnel, such as PPTP, or a network access server (NAS) initiated tunnel, such as L2F.

Refer to the *Limitations and Restrictions* section for information regarding the functionality of the Cisco uBR924 cable access router in L2TP applications.

Firewall (Phase I)

The Firewall (Phase I) feature set extends the security technology currently available in Cisco IOS software to the Cisco uBR924 cable access router, providing firewall-specific capabilities. Firewall (Phase I) features include stateful, application-based filtering, dynamic per-user authentication and authorization, defense against network attacks, Java blocking, and real-time alerts. Firewall (Phase I) is interoperable with Cisco IOS software features including NAT, VPN tunneling protocols, Cisco Express Forwarding (CEF), AAA extensions, Cisco encryption technology, and Cisco IOS IPsec.

Baseline Privacy Management Information Base

The Baseline Privacy Management Information Base (MIB), as currently defined, is now available in Cisco IOS Release 12.0(5)T code. BPI allows an SNMP manager to monitor and manage the Cisco uBR924 cable access router's BPI configuration, including whether BPI is enabled, status of current authorization keys, current timeout values, real-time status counters, and additional information about authorization errors.

Note The SNMP manager must load the DOCSIS-BPI-MIB.my MIB to access the BPI attributes.

New Hardware Features In Release 12.0(4)XI1

The following new hardware feature is supported by the Cisco uBR924 cable access router for Release 12.0(4)XI1.

The Cisco uBR924 cable access router contains two FXS VoIP ports that are labeled V1+V2 and V2 at the rear of the unit. These ports can be connected directly to telephones or to adapters that allow multiple telephones to be connected to each of the two VoIP telephone lines. The Ringer Equivalence Number (REN) determines how many telephones can be connected to a telephone line.

Note In most areas, the sum of the RENs of all devices on any one line should not exceed 5. If too many devices are attached, they may not ring properly.

Between 5 and 10 voice devices can be connected to each of the two VoIP telephone lines, provided each telephone line does not exceed the 5 REN limit. Typical length of the 26-gauge telephone wire is 3,000 feet or more.

The Cisco uBR924 cable access router can support the number of telephones typically found in small businesses.

New Software Features In Release 12.0(4)XI1

Note All Cisco IOS Release 12.0(4)XI images were deferred because of the DDTS entries CSCdm34966, CSCdm40915, and CSCdm47138. See *Resolved Caveats—Release 12.0(5)T*.

The following new software features are supported by the Cisco uBR924 cable access router for Cisco IOS Release 12.0(4)XI1.

Full and DOCSIS-Compliant Bridging

Full and DOCSIS-Compliant Bridging allows the Cisco uBR924 cable access router to operate with any DOCSIS-qualified CMTS.

The ability of the Cisco uBR924 cable access router to grant access to Customer Premises Equipment (CPE) devices is controlled by the “MAX CPE” field in the DOCSIS configuration file. The Cisco uBR924 cable access router defaults to one MAX CPE address unless this option is set to a higher number. The valid MAX CPE address range is 1 to 3 for bridging operation using Cisco IOS Release 12.0(4)XI1. In Cisco IOS Release 12.0(5)T or higher interim images, the valid MAX CPE address range is 1 to 254 for bridging operation.

Easy IP

Dynamic Host Configuration Protocol (DHCP) Server:

With the introduction of Easy IP, Cisco IOS Release 12.0(4)XI1 supports Intelligent DHCP Relay and DHCP Client functionality. A DHCP Relay Agent is any host that forwards DHCP packets between clients and servers. A DHCP Relay Agent enables the client and server to reside on separate subnets. If the Cisco IOS DHCP server cannot satisfy a DHCP request from its own database, it can forward the DHCP request to one or more secondary DHCP servers defined by the network administrator using standard Cisco IOS IP helper-address functionality.

Network Address Translation and Port Address Translation (NAT/PAT):

- Allows customers to maintain their own private networks while giving them full Internet access through the use of one or more global IP addresses
- Allows several private IP addresses to use the same global IP address by using address overloading
- Facilitates configuration and permits a large network of users to reach the network by using one Cisco uBR924 cable access router and the same DOCSIS cable interface IP address

- Eliminates the need to readdress all hosts with existing private network addresses (one-to-one translation) or by enabling all internal hosts to share a single registered IP address (many-to-one translation, also known as Port Address Translation [PAT])
- Enables packets to be routed correctly to and from the outside world by using the Cisco uBR924 cable access router
- Allows personal computers on the Ethernet interface to have IP addresses to be mapped to the cable interface's IP address

Routing protocols will run on the Ethernet interface instead of the cable interface, and all packets received will be routed out the Ethernet interface or use the default gateway to reach the CMTS. This eliminates the need to run RIP on the cable interface.

To implement NAT on the Cisco uBR924 cable access router, the Ethernet interface is configured with an "inside" address and the cable interface is configured with an "outside" address. The Cisco uBR924 cable access router also supports configuration of static connections, dynamic connections, and address pools.

Routing (RIP V2)

A routing configuration for the Cisco uBR924 cable access router is most likely used when the cable access router is being added to an existing personal computer network. When configured in routing mode, the Cisco uBR924 cable access router will automatically configure the headend's IP address as its IP default gateway. When the IP host-routing is being configured, this automatic configuration of the headend's IP address as its IP default gateway will allow the Cisco uBR924 cable access router to send packets not intended for the Ethernet interface to the headend.

RIP V2 routing is useful for small internetworks in that it enables optimization of Network Interface Center (NIC)-assigned IP addresses by defining VLSMs for network addresses, and it allows Classless Interdomain Routing (CIDR) addressing schema.

Voice Support

Acceptable voice quality and reduction in network bandwidth usage are achieved by using several voice processing techniques. Digital Signal Processors (DSPs), in combination with DSP firmware in the Cisco uBR924 cable access router, provide the stream-to-packet and packet-to-stream conversion, as well as voice processing capabilities. Typical voice processing services include echo cancellation, voice compression, Voice Activity Detection (VAD) or silence compression and Dual Tone Multi-Frequency (DTMF) tone detection and generation. Supported vocoders include:

- G.711 A Law 64000 bps
- G.711 u Law 64000 bps
- G.723.1 5300 bps
- G.723.1 6300 bps
- G.726 16000 bps
- G.726 24000 bps
- G.726 32000 bps
- G.728 16000 bps
- G.729 Annex-A 8000 bps
- G.729 8000 bps—Default CODEC for telephone calls

Use of the H.323 protocol typically involves a dial plan and mapper at the headend to map IP addresses to telephone numbers. You can also set static routes. Use dial peer commands to define local and remote peers. For the backup POTS port, define port and E.164 addresses. For remote peers, define remote peers' IP addresses and E.164 addresses.

Note If you have Cisco Network Registrar (CNR) version 3.0 with the extension scripts **relay.tci** and **setrouter.tci**, you can assign E.164 addresses to local ports and use a gatekeeper to resolve the remote peers' IP addresses. CNR uses the DHCP option (merit dump file) containing an ASCII string that defines the E.164 address-to-port assignments. The Cisco uBR924 cable access router software creates dial peers, starts H.323 RAS gateway support, and registers the E.164 addresses with the gatekeeper. Functionality is augmented in Cisco IOS Release 12.0(5)T and higher.

Cable Device MIB

The Cable Device MIB is for 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.
- **docsDevEvent** 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 Cisco Standard MIBs consist of the following components:

- CISCO-PRODUCT-MIB
- CISCO-SYSLOG-MIB
- CISCO-FLASH-MIB
- BRIDGE-MIB
- IF-MIB
- CiscoWorks/CiscoView

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 Connection Online (CCO). From the CCO home page, click on this path: **Service & Support: Software Center: Network Mgmt Products: Cisco Network Management Toolkit: Cisco MIB**

Cisco Voice MIBs

The Cisco Voice MIBs consist of the following components:

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

Radio Frequency Interface MIB

The Radio Frequency Interface (RFI) MIB module is for 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 access router 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.

With IPSec, data can be transmitted across a public network without fear of observation, modification, or spoofing. This enables applications such as VPNs, extranets, and remote user access.

IPSec services are similar to those provided by Cisco Encryption Technology, a proprietary security solution introduced in Cisco IOS Software Release 11.2. However, IPSec provides a more robust security solution, and is standards based.

Limitations and Restrictions

This section describes warnings and cautions about using Cisco IOS Release 12.0 T software.

Using Multiple PCs with a Cisco uBR924 Cable Access Router

The MAX CPE parameter in a Cisco uBR924 cable access router's DOCSIS configuration file determines how many PCs (or other CPE devices) are supported by that Cisco uBR924 cable access router. The default value for the MAX CPE parameter is 1, which means only one PC can be connected to the Cisco uBR924 cable access router.

The DOCSIS 1.0 specification states that a CMTS cannot age-out MAC addresses for CPE devices, so the first PC that is connected to a Cisco uBR924 cable access router is normally the only one that the CMTS recognizes as valid. If a subscriber replaces an existing PC or changes its network interface card (NIC) to one that has a different MAC address, the CMTS will refuse to let the PC come online because this would exceed the maximum number of CPE devices specified by the MAX CPE parameter.

To allow a subscriber to replace an existing PC or NIC, the following workarounds are possible:

- If using a Cisco uBR7200 series router as the CMTS, enter the **clear cable host MAC address** command on the Cisco uBR7200 series router to remove the PC's MAC address from the router's internal address tables. The PC's MAC address will be rediscovered and associated with the correct Cisco uBR924 cable access router during the next DHCP lease cycle.
- Increase the value of the MAX CPE parameter in the Cisco uBR924 cable access router's DOCSIS configuration file so that it can accommodate the desired number of PCs. Reset the Cisco uBR924 cable access router to force it to load the new configuration file.

Layer 2 Tunneling Protocol

Implementation of L2TP in Cisco IOS Release 12.0(5)T is dependent on a PPP connection supported on one of the directly attached interfaces. A dial-up PPP connection is required in order to initiate an L2TP Tunnel connection. This is a requirement of the L2TP Access Concentrator (LAC). In Cisco IOS Release 12.0(5)T, the Cisco uBR924 cable access router cannot function as the LAC; it can only function as the L2TP Network Server (LNS), which terminates a tunnel created elsewhere in the network.

Important Notes

This section contains important information about using Cisco IOS Release 12.0 T software.

Last Maintenance Release of Cisco IOS Release 12.0 T

Cisco IOS Release 12.0(6)T has been renamed 12.0(7)T to align this release with the 12.0(7) mainline release. The closed caveats for Release 12.0(7)T are identical to the caveats closed in the 12.0(7) mainline release. There was no change in the feature content of the renamed release—the features in 12.0(6)T are the same as 12.0(7)T. Release 12.0(7)T is the last maintenance release of the 12.0 T release train.

Customers needing closure of caveats for the 12.0 T features should migrate to the 12.1 mainline release, which has the complete feature content of Release 12.0 T and will eventually reach General Deployment (GD). Release 12.0 T is a superset of the 12.0 mainline release, so all caveats closed in the 12.0 mainline are also closed in 12.0 T.

Voice

For Cisco IOS Release 12.0(4)XI1 software images, the Cisco uBR924 cable access router would only work with a routing headend. This is no longer true in Cisco IOS Release 12.0(5)T or later software images.

Supplemental and Corrected Text for the Online Feature Module

Troubleshooting Tips for the uBR924 Cable Access Router, page 15, indicates: “Some CATV systems use alternative frequency plans such as the IRC (Incrementally Related Carrier) and HRC (Harmonically Related Carrier) plans. Most of the IRC channel slots overlap the EIA plan. The HRC plan is not supported by Cisco's cable access routers since so few cable plants are using this plan.”

The correction should read: “For the Cisco uBR924 cable access router, both the IRC (Incrementally Related Carrier) and HRC (Harmonically Related Carrier) plans are supported. Most of the IRC channel slots overlap the EIA plan. For the Cisco uBR924 cable access router, both the IRC and HRC plans are supported.

The list of downstream search bands added for HRC have appropriate center frequencies and step values for an HRC channel plan. The expanded search band list may increase the amount of time required by the Cisco uBR924 cable access router to acquire the downstream signal on the HRC channel plan, which can add to the total time for complete registration of the modem the very first time it is added to the cable system.”

Supported MIBs

The Cisco uBR924 cable access router supports the following categories of MIBs:

- **SNMP standard MIBs**—These are the MIBs required by any agent supporting SNMPv1 or SNMPv2 network management.
- **Cisco’s platform and network-layer enterprise 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.
- **Cable-specific MIBs**—These MIBs provide information about the cable interface and related information on the Cisco uBR924 cable access router. They include both DOCSIS-required MIBs and Cisco-specific enterprise MIBs. If your network management applications have not already been configured for the Cisco uBR924 cable access router, 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.

The *Cable-Specific MIBs* and *Deprecated MIBs* are described in the following sections. For information on the SNMP standard MIBs and Cisco’s platform and network-layer enterprise MIBs, see Cisco’s MIB website at <http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>.

Cable-Specific MIBs

Table 6 shows the cable-specific MIBs that are supported on the Cisco uBR924 cable access router. 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. Because of interdependencies, the MIBs must be loaded in the order given in the table.

Note The names given in Table 6 are the filenames for the MIBs as they exist on Cisco’s FTP site (<ftp://ftp.cisco.com/pub/mibs/> or <http://www.cisco.com/public/mibs>). Most MIBs are available in both SNMPv1 and SNMPv2 versions; the SNMPv1 versions have *V1SMI* as part of their filenames.

Important Notes

Table 6 Supported MIBs for the Cisco uBR924 Cable Access Router

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.	12.0(4)XI
SNMPv2-TC.my SNMPv2-TC-V1SMI.my	This module defines the textual conventions as specified in pages 4, 10-11 of RFC 854.	12.0(4)XI
CISCO-SMI.my CISCO-SMI-V1SMI.my	This module specifies the Structure of Management Information (SMI) for Cisco's enterprise MIBs.	12.0(4)XI
CISCO-TC.my CISCO-TC-V1SMI.my	This module defines the textual conventions used in Cisco's enterprise MIBs.	12.0(4)XI
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 1229.	12.0(4)XI
CISCO-CABLE-SPECTRUM-MIB.my CISCO-CABLE-SPECTRUM-MIB-V1SMI.my	This module describes the spectrum management flap list attributes.	12.0(5)T1
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. (This MIB is being updated on a release basis to add RFC2670 support as needed.)	12.0(4)XI
DOCS-BPI-MIB.my	This module—available in an snmpv2 version only—describes the attributes for the DOCSIS-specified Baseline Privacy Interface (BPI) on cable modems and the CMTS.	12.0(5)T
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 QoS attributes and connection status and other information regarding the cable modems and CPE devices supported by the CMTS. Note Cisco IOS releases prior to 12.0(5)T1 provide only partial support for the attributes in this MIB.	partial support: 12.0(4)XI full support: 12.0(5)T1
CABLE-DEVICE-MIB.my CABLE-DEVICE-MIB-V1SMI.my	This module contains generic cable-related objects for DOCSIS-compliant cable modems.	12.0(4)XI
CISCO-CABLE-MODEM-MIB.my	This module—available in an snmpv2 version only—contains the Cisco enterprise objects for DOCSIS-compliant cable modems.	12.0(4)XI
DOCS-CABLE-DEVICE-MIB	This module—available in an snmpv2 version only—is the DOCSIS-specified MIB for DOCSIS-compliant cable modems.	12.0(4)XI

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 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 7 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 7 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 CISCO-QUEUE-MIB-V1SMI	IF-MIB CISCO-QUEUE-MIB
OLD-CISCO-IP-MIB		
OLD-CISCO-MEMORY-MIB	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-MIB	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 7 represent feature sets that are not supported on the Cisco uBR924 cable access router.

Caveats

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

For information on caveats in Cisco IOS Release 12.0 T, see *Caveats for Cisco IOS Release 12.0 T*.

All caveats in Release 12.0 are also in Release 12.0 T.

For information on caveats in Cisco IOS Release 12.0, see *Caveats for Cisco IOS Release 12.0* which lists severity 1 and 2 caveats, and is located on CCO and the Documentation CD-ROM.

Note If you have an account with CCO, you can use Bug Navigator II to find caveats of any severity for any release. You can reach Bug Navigator II on CCO at **Software Center: Cisco IOS Software: Cisco IOS Bug Toolkit: Cisco Bug Navigator II**, or at <http://www.cisco.com/support/bugtools>.

Open Caveats—Release 12.0(7)T

This section describes possibly unexpected behavior by Release 12.0(7)T. This section only describes severity 1 and 2 caveats.

- CSCdm38753

The Cisco uBR924 cable access router, when running the NAT and firewall features, crashes if establishing roughly 150 Solaris_telnet sessions.

Open Caveats—Release 12.0(5)T1

This section describes possibly unexpected behavior by Release 12.0(5)T1. This section only describes severity 1 and 2 caveats.

- CSCdm38753

The Cisco uBR924 cable access router, when running the NAT and firewall features, crashes if establishing roughly 150 Solaris_telnet sessions.

Resolved Caveats—Release 12.0(5)T1

All the caveats listed in this section are resolved in Release 12.0(5)T1. This section only describes severity 1 and 2 caveats.

- CSCdm64438

When more than one Cisco uBR924 cable access router is networked, bandwidth requests are sent to the CMTS simultaneously if the bandwidth request backoff is not set correctly on the cable modem interface of the Cisco uBR924 cable access router. This results in a bandwidth request collision, possibly indicating an upstream transmit driver/MAC problem. Whenever a long string of ping timeouts is detected, the Cisco uBR924 cable access router does not send bandwidth requests to the CMTS. The Cisco uBR924 cable access router ping timeout occurs then with all CMTS images.

This caveat caused the deferral from Cisco IOS Release 12.0(5)T images.

- CSCdm66365

The Cisco uBR924 cable access router crashes in certain instances due to cable modem registration problems: segV with deb cab mac mess reg-rsp on. This is due to no vendor ID in the message. The crash occurs when using the ubr920-k1y5-mz image.

This caveat caused the deferral from Cisco IOS Release 12.0(5)T images.

Resolved Caveats—Release 12.0(5)T

All the caveats listed in this section are resolved in Release 12.0(5)T. This section only describes severity 1 and 2 caveats.

- CSCdm28470

Values selected for Initial Ranging backoffs in Cisco IOS Release 12.0(4)XI images were not random enough. This could cause several Cisco uBR924 cable access routers powered on at the same time to take a long time to get through initial ranging and bring the cable interface up.

- CSCdm34966

After receiving a UCC request using Cisco IOS Release 12.0(4)XI images, the Cisco uBR924 cable access router could complete initial ranging too soon. This could cause the router to fail in secondary ranging because the unit took too long to get through secondary ranging.

This caused the deferral from Cisco IOS Release 12.0(4)XI to Cisco IOS Release 12.0(4)XI1.

- CSCdm40915

Voice accounting to RADIUS server did not work. Cisco IOS Release 12.0(5)T images permit RADIUS to be used to authenticate subscribers (typically incoming calls) on the Cisco uBR924 cable access router acting as a gateway.

This caused the deferral from Cisco IOS Release 12.0(4)XI to Cisco IOS Release 12.0(4)XI1.

- CSCdm47138

A CMTS would send a UCD for every upstream channel available in a given downstream channel. The Cisco uBR924 cable access router downstream MAC message processing did not have enough buffers to handle several MAC messages at the same time and as a result would only process the first four UCDs received. The Cisco uBR924 cable access router would never know about and never be able to use any upstream other than the upstreams for which the first four UCDs were sent.

This caused the deferral from Cisco IOS Release 12.0(4)XI to Cisco IOS Release 12.0(4)XI1.

Related Documentation

The following sections describe the documentation available for the Cisco uBR924 cable access router. These documents consist of hardware and software installation guides, Cisco IOS configuration and command references, system error messages, feature modules, and other documents.

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

Use these release notes with these documents:

- Release-Specific Documents, page 25
- Platform-Specific Documents, page 26
- Feature Modules, page 26
- Cisco IOS Software Documentation Set, page 27

Release-Specific Documents

The following documents are specific to Release 12.0 and are located on CCO and the Documentation CD-ROM:

- *Cross-Platform Release Notes for Cisco IOS Release 12.0*

On CCO at:

Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 12.0

On the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.0: Release Notes: Cross-Platform Release Notes

- Product bulletins, field notices, and other release-specific documents on CCO at:

Technical Documents

- *Caveats for Cisco IOS Release 12.0 T*

As a supplement to the caveats listed in these release notes, see *Caveats for Cisco IOS Release 12.0* and *Caveats for Cisco IOS Release 12.0 T*, which contains caveats applicable to all platforms for all maintenance releases of Release 12.0 T.

On CCO at:

Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 12.0: Caveats

On the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS 12.0: Caveats

Note If you have an account with CCO, you can use Bug Navigator II to find caveats of any severity for any release. You can reach Bug Navigator II on CCO at: **Software Center: Cisco IOS Software: Cisco IOS BugToolkit: Cisco Bug Navigator II**, or at <http://www.cisco.com/support/bugtools>.

Platform-Specific Documents

These documents are available for the Cisco uBR924 cable access router on CCO and the Documentation DC-ROM:

- *Cisco uBR924 Cable Access Router Quick Start Guide*
- *Cisco uBR924 Cable Access Router Installation and Configuration Guide*
- *Bridging and Routing Features for the Cisco uBR924 Cable Access Router*
- *Troubleshooting Tips for the Cisco uBR924 Cable Access Router*

On CCO at:

Technical Documents: Documentation Home Page: Cisco Product Documentation: Broadband/Cable Solutions: Cisco uBR900 Series Cable Access Routers

On the Documentation CD-ROM at:

Cisco Product Documentation: Broadband/Cable Solutions: Cisco uBR900 Series Cable Access Routers

Feature Modules

Feature modules describe new features supported by Release 12.0 T, and are updates to the Cisco IOS documentation set. A feature module consists of a brief overview of the feature, benefits, 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 CCO at:

Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 12.0: New Feature Documentation

On the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.0: New Feature Documentation

Cisco IOS Software Documentation Set

The Cisco IOS software documentation set consists of the Cisco IOS configuration guides, Cisco IOS command references, and several other supporting documents.

Documentation Modules

Each module in the Cisco IOS documentation set consists of two books: a configuration guide and a corresponding command reference. Chapters in a configuration guide describe protocols, configuration tasks, 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 CCO and the Documentation CD-ROM, two master hot-linked documents provide information for the Cisco IOS software documentation set.

On CCO at:

Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 12.0: Configuration Guides and Command References

On the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.0: Configuration Guides and Command References

Release 12.0 Documentation Set

Table 8 describes the contents of the Cisco IOS Release 12.0 software documentation set, which is available in electronic form and in printed form upon request.

You can find the most current Cisco IOS documentation on CCO and the Documentation CD-ROM.

On CCO at:

Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 12.0

On the Documentation CD-ROM at:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS Release 12.0

Table 8 Cisco IOS Software Release 12.0 Documentation Set

Books	Chapter Topics
<ul style="list-style-type: none"> • <i>Configuration Fundamentals Configuration Guide</i> • <i>Configuration Fundamentals Command Reference</i> 	<ul style="list-style-type: none"> Configuration Fundamentals Overview Cisco IOS User Interfaces File Management System Management
<ul style="list-style-type: none"> • <i>Bridging and IBM Networking Configuration Guide</i> • <i>Bridging and IBM Networking Command Reference</i> 	<ul style="list-style-type: none"> Transparent Bridging Source-Route Bridging Token Ring Inter-Switch Link Remote Source-Route Bridging DLSw+ STUN and BSTUN LLC2 and SDLC IBM Network Media Translation DSPU and SNA Service Point SNA Frame Relay Access Support APPN Cisco Database Connection NCIA Client/Server Topologies Cisco Mainframe Channel Connection Airline Product Set
<ul style="list-style-type: none"> • <i>Dial Solutions Configuration Guide</i> • <i>Dial Solutions Command Reference</i> 	<ul style="list-style-type: none"> X.25 over ISDN Appletalk Remote Access Asynchronous Callback, DDR, PPP, SLIP Bandwidth Allocation Control Protocol ISDN Basic Rate Service ISDN Caller ID Callback PPP Callback for DDR Channelized E1 & T1 Dial Backup for Dialer Profiles Dial Backup Using Dialer Watch Dial Backup for Serial Lines Peer-to-Peer DDR with Dialer Profiles DialOut Dial-In Terminal Services Dial-on-Demand Routing (DDR) Dial Backup Dial-Out Modem Pooling Large-Scale Dial Solutions Cost-Control Solutions Virtual Private Dialup Networks Dial Business Solutions and Examples
<ul style="list-style-type: none"> • <i>Cisco IOS Interface Configuration Guide</i> • <i>Cisco IOS Interface Command Reference</i> 	<ul style="list-style-type: none"> Interface Configuration Overview LAN Interfaces Logical Interfaces Serial Interfaces
<ul style="list-style-type: none"> • <i>Network Protocols Configuration Guide, Part 1</i> • <i>Network Protocols Command Reference, Part 1</i> 	<ul style="list-style-type: none"> IP Overview IP Addressing and Services IP Routing Protocols
<ul style="list-style-type: none"> • <i>Network Protocols Configuration Guide, Part 2</i> • <i>Network Protocols Command Reference, Part 2</i> 	<ul style="list-style-type: none"> AppleTalk Novell IPX

Table 8 Cisco IOS Software Release 12.0 Documentation Set (continued)

Books	Chapter Topics
<ul style="list-style-type: none"> • <i>Network Protocols Configuration Guide, Part 3</i> • <i>Network Protocols Command Reference, Part 3</i> 	Network Protocols Overview Apollo Domain Banyan VINES DECnet ISO CLNS XNS
<ul style="list-style-type: none"> • <i>Security Configuration Guide</i> • <i>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
<ul style="list-style-type: none"> • <i>Cisco IOS Switching Services Configuration Guide</i> • <i>Cisco IOS Switching Services Command Reference</i> 	Switching Services Switching Paths for IP Networks Virtual LAN (VLAN) Switching and Routing
<ul style="list-style-type: none"> • <i>Wide-Area Networking Configuration Guide</i> • <i>Wide-Area Networking Command Reference</i> 	Wide-Area Network Overview ATM Frame Relay SMDS X.25 and LAPB
<ul style="list-style-type: none"> • <i>Voice, Video, and Home Applications Configuration Guide</i> • <i>Voice, Video, and Home Applications Command Reference</i> 	Voice over IP Voice over Frame Relay Voice over ATM Voice over HDLC Frame Relay-ATM Internetworking Synchronized Clocks Video Support Universal Broadband Features
<ul style="list-style-type: none"> • <i>Quality of Service Solutions Configuration Guide</i> • <i>Quality of Service Solutions Command Reference</i> 	Policy-Based Routing QoS Policy Propagation via BGP Committed Access Rate Weighted Fair Queueing Custom Queueing Priority Queueing Weighted Random Early Detection Scheduling Signaling RSVP Packet Drop Frame Relay Traffic Shaping Link Fragmentation RTP Header Compression
<ul style="list-style-type: none"> • <i>Cisco IOS Software Command Summary</i> • <i>Dial Solutions Quick Configuration Guide</i> • <i>System Error Messages</i> • <i>Debug Command Reference</i> 	

Note *Cisco Management Information Base (MIB) User Quick Reference* is no longer published. For the latest list of MIBs supported by Cisco, see *Cisco Network Management Toolkit* on Cisco Connection Online. From CCO, click on the following path: **Service & Support: Software Center: Network Mgmt Products: Cisco Network Management Toolkit: Cisco MIB.**

Service and Support

For service and support for a product purchased from a reseller, contact the reseller, who offers a wide variety of Cisco service and support programs described in “Service and Support” of *Cisco Information Packet* that shipped with your product.

Note If you purchased your product from a reseller, you can access CCO as a guest. CCO is Cisco Systems’ primary real-time support channel. Your reseller offers programs that include direct access to CCO services.

For service and support for a product purchased directly from Cisco, use CCO.

Software Configuration Tips on the Cisco Technical Assistance Center Home Page

If you have a CCO login account, you can access the following URL, which contains links and tips on configuring your Cisco products:

http://www.cisco.com/kobayashi/serv_tips.shtml

This URL is subject to change without notice. If it changes, point your Web browser to CCO and click on this path: **Products & Technologies: Products: Technical Tips.**

The following sections are provided from the Technical Tips page:

- Access Dial Cookbook—Contains common configurations or recipes for configuring various access routes and dial technologies.
- Field Notices—Notifies you of any critical issues regarding Cisco products and includes problem descriptions, safety or security issues, and hardware defects.
- Frequently Asked Questions—Describes the most frequently asked technical questions about Cisco hardware and software.
- Hardware—Provides technical tips related to specific hardware platforms.
- Hot Tips—Describes popular tips and hints gathered from the Cisco Technical Assistance Center (TAC). Most of these documents are available from the TAC Fax-on-demand service. To reach Fax-on-demand and receive documents at your fax machine from the United States, call 888-50-CISCO (888-502-4726). From other areas, call 650-596-4408.
- Internetworking Features—Lists tips on using Cisco IOS software features and services.
- Sample Configurations—Provides actual configuration examples that are complete with topology and annotations.
- Software Products—Contains Cisco IOS Software Bulletins, Cisco TCP/IP Suite 100, General Cisco IOS, Internet/Intranet Applications and Software, Network Management, Network Protection Software Tips, and WAN Switching Products and Software.

- Special Collections—Lists other helpful documents, including Case Studies, References & Request for Comments (RFCs), and Security Advisories.

Cisco Connection Online

Cisco Connection Online (CCO) is Cisco Systems' primary, real-time support channel. Maintenance customers and partners can self-register on CCO to obtain additional information and services.

Available 24 hours a day, 7 days a week, CCO provides a wealth of standard and value-added services to Cisco's customers and business partners. CCO services include product information, product documentation, software updates, release notes, technical tips, the Bug Navigator, configuration notes, brochures, descriptions of service offerings, and download access to public and authorized files.

CCO serves a wide variety of users through two interfaces that are updated and enhanced simultaneously: a character-based version and a multimedia version that resides on the World Wide Web (WWW). The character-based CCO supports Zmodem, Kermit, Xmodem, FTP, and Internet e-mail, and it is excellent for quick access to information over lower bandwidths. The WWW version of CCO provides richly formatted documents with photographs, figures, graphics, and video, as well as hyperlinks to related information.

You can reach CCO in the following ways:

- WWW: <http://www.cisco.com>
- WWW: <http://www-europe.cisco.com>
- WWW: <http://www-china.cisco.com>
- Telnet: [cco.cisco.com](telnet://cco.cisco.com)
- Modem: From North America, 408 526-8070; from Europe, 33 1 64 46 40 82. Use the following terminal settings: VT100 emulation; databits: 8; parity: none; stop bits: 1; and connection rates up to 28.8 kbps.

For a copy of CCO's Frequently Asked Questions (FAQ), contact cco-help@cisco.com. For additional information, contact cco-team@cisco.com.

Note If you are a network administrator and need personal technical assistance with a Cisco product that is under warranty or covered by a maintenance contract, contact Cisco's Technical Assistance Center (TAC) at 800 553-2447, 408 526-7209, or tac@cisco.com. To obtain general information about Cisco Systems, Cisco products, or upgrades, contact 800 553-6387, 408 526-7208, or cs-rep@cisco.com.

Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package. The Documentation CD-ROM, a member of the Cisco Connection Family, is updated monthly. Therefore, it might be more current than printed documentation. To order copies of the Documentation CD-ROM, contact your local sales representative or call customer service. The CD-ROM package is available as a single package or as an annual subscription. You can also access Cisco documentation on the World Wide Web at <http://www.cisco.com>, <http://www-china.cisco.com>, or <http://www-europe.cisco.com>.

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

This document is to be used in conjunction with the documents listed in the "Related Documentation" section on page 25.

Access Registrar, AccessPath, Any to Any, AtmDirector, Browse with Me, CCDA, CCDE, CCDP, CCIE, CCNA, CCNP, CCSI, CD-PAC, the Cisco logo, Cisco Certified Internetwork Expert logo, *CiscoLink*, the Cisco Management Connection logo, the Cisco NetWorks logo, the Cisco Powered Network logo, Cisco Systems Capital, the Cisco Systems Capital logo, Cisco Systems Networking Academy, the Cisco Systems Networking Academy logo, the Cisco Technologies logo, ConnectWay, Fast Step, FireRunner, Follow Me Browsing, FormShare, GigaStack, IGX, Intelligence in the Optical Core, Internet Quotient, IP/VC, Kernel Proxy, MGX, MultiPath Data, MultiPath Voice, Natural Network Viewer, NetSonar, Network Registrar, the Networkers logo, *Packet*, PIX, Point and Click Internetworking, Policy Builder, Precept, ScriptShare, Secure Script, ServiceWay, Shop with Me, SlideCast, SMARTnet, *The Cell*, TrafficDirector, TransPath, ViewRunner, Virtual Loop Carrier System, Virtual Service Node, Virtual Voice Line, VisionWay, VlanDirector, Voice LAN, Wavelength Router, Wavelength Router Protocol, WaRP, WebViewer, Workgroup Director, and Workgroup Stack are trademarks; Changing the Way We Work, Live, Play, and Learn, Empowering the Internet Generation, The Internet Economy, and The New Internet Economy are service marks; and ASIST, BPX, Catalyst, Cisco, Cisco IOS, the Cisco IOS logo, Cisco Systems, the Cisco Systems logo, the Cisco Systems Cisco Press logo, Enterprise/Solver, EtherChannel, EtherSwitch, FastHub, FastLink, FastPAD, FastSwitch, GeoTel, IOS, IP/TV, IPX, LightStream, LightSwitch, MICA, NetRanger, Post-Routing, Pre-Routing, Registrar, StrataView Plus, Stratm, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. or its affiliates in the U.S. and certain other countries. All other trademarks mentioned in this document are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any of its resellers. (9911R)

Copyright © 1999, Cisco Systems, Inc.
All rights reserved.