



Text Part Number: 78-6005-07 Rev. A0

Release Notes for Cisco MC3810 for Cisco IOS Release 12.0 T

July 2, 2002

These release notes for the Cisco MC3810 multiservice access concentrator support Cisco IOS Release 12.0 T, up to and including Release 12.0(7)T. These release notes are updated as needed to describe new features, memory requirements, hardware support, software platform deferrals, and changes to related documents.

For a list of software caveats that apply to Release 12.0(7)T, refer to the document *Caveats for Cisco IOS Release 12.0 T* that accompanies these release notes. The caveats document is updated for every maintenance release and is located on Cisco Connection Online (CCO) and the Documentation CD-ROM.

Use these release notes with the cross-platform *Release Notes for Cisco IOS Release 12.0* located on Cisco Connection Online (CCO) and the Documentation CD-ROM.

Contents

These release notes describe the following topics:

- Introduction, page 2
- System Requirements, page 2
- New and Changed Information, page 15
- Important Notes, page 35
- Important Notes, page 35
- Caveats, page 42
- Related Documentation, page 42
- Service and Support, page 47
- Cisco Connection Online, page 48
- Documentation CD-ROM, page 49

Corporate Headquarters

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

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

Introduction

As part of an enterprise backbone or as customer premises equipment (CPE) to serve provider-managed network services, the Cisco MC3810 multiservice access concentrator reduces operating costs and complexity, and increases network throughput and performance. The Cisco MC3810 is fully supported by Cisco IOS software for multiprotocol routing, bridging, and Systems Network Architecture (SNA).

To make file management easier, the Cisco MC3810 provides a complete file system for software images, message files, and reports. The standard Flash memory size is 8 MB, and a 16-MB upgrade option is available. The 16-MB version can hold two code images simultaneously for fail-safe upgrades.

Management and configuration of the Cisco MC3810 should be familiar to the Cisco IOS user and compatible with existing management systems. As such, it provides a superset of the Cisco command-line interface (CLI). The Cisco MC3810 can be managed by standard Cisco management platforms and facilities such as CiscoView and the native remote log-in facilities provided by Telnet and rlogin. Three types of configuration interfaces are provided:

- Cisco CLI
- HTTP-based configuration server
- SNMP-based Management Information Base (MIB)

The HTTP-based interface allows configuration from any Web browser such as Netscape Navigator or Microsoft Explorer. The SNMP MIB allows management of the Cisco MC3810 from SNMP managers (for example, HP OpenView).

System Requirements

This section describes the system requirements for Cisco IOS Release 12.0(7)T:

- Memory Requirements, page 3
- Hardware Supported, page 3
- Determining the Software Version, page 5
- Upgrading to a New Software Release, page 5
- Feature Set Table, page 6
- New and Changed Information, page 15

Memory Requirements

Table 1 Memory Requirements for the Cisco MC3810

Feature Set	Image Name	Required Flash Memory	Required DRAM Memory	Runs from
IP	mc3810-i-mz	4 MB ¹	16 MB ²	RAM
IP Plus	mc3810-is-mz	8 MB	32 MB	RAM
IP/ATM Plus	mc3810-a2is-mz	8 MB	32 MB	RAM
IP Plus ATM MCM H323	mc3810-a2isx-mz	8 MB	32 MB	RAM
Enterprise Plus	mc3810-js-mz	8 MB	32 MB	RAM
Enterprise/ATM Plus	mc3810-a2js-mz	8 MB	32 MB	RAM
Enterprise Plus ATM MCM H323	mc3810-a2jsx-mz	8 MB	32 MB	RAM

1 Required flash for IP feature set; default configuration includes 8 MB.

2 Required DRAM for IP feature set; default configuration includes 32 MB.

Hardware Supported

Cisco IOS Release 12.0(7)T supports the Cisco MC3810 multiservice access concentrator. The Cisco MC3810 base chassis is a semi-fixed configuration router that can be customized for a specific application at the factory or in the field by a qualified technician. The base chassis includes the following components:

- One fixed Ethernet LAN port
- A console port and an auxiliary port
- Two synchronous serial ports
- Five mounting areas for functional modules that support additional capabilities
- AC, DC, or redundant power supply option

Cisco MC3810 series concentrators are supplied in various standard hardware configurations. These are equipped with different sets of functional modules to provide specific functional capability. Many configurations are possible, but they are all variations of the basic categories described in Table 2. Supported hardware is shown in Table 3. The chassis opening for any mounting area not equipped with a functional module is closed off with a removable cover plate.

Table 2 Cisco MC3810 Series Standard Hardware Categories

Category	Service Types Supported	Required Modules	Optional Modules
Base chassis	Base chassis services ¹	None	Optional modules can be added to create other chassis variations.
Analog voice chassis	Base chassis services ¹ plus compressed analog voice connections to telephone, fax, central office, analog PBX	AVM (analog voice module) with 1 to 6 APMs (analog personality modules) VCM3 or VCM6 (voice compression modules)	MFT ² to support a channelized T1 or E1 trunk MFT ² and VDM ³ to support video codec dialing
Digital voice chassis	Base chassis services ¹ plus compressed digital voice through digital PBX	DVM VCM3 and/or VCM6 (1 or 2 VCMs)	MFT ² to support a channelized T1 or E1 trunk MFT ² and VDM to support video codec dialing
BRI voice chassis	Base chassis services ¹ plus compressed digital voice through PINX	BVM and MFT ¹ VCM3 and/or VCM6 (1 VCM required)	MFT to support a channelized T1 or E1 trunk MFT ² and VDM ³ to support video codec dialing
T1/E1 trunk chassis	Base chassis services ¹ plus channelized T1 or E1	MFT ¹	DVM to support digital cross-connect voice (channel bank functionality/ drop-and-insert) through digital PBX or channel bank VDM ³ to support video codec dialing VCM3 and/or VCM6 (1 or 2 VCMs) to support voice compression

- 1 Base chassis services include administrative access, Ethernet, data transport, and video transport.
- 2 The MFT is available with or without BRI backup.
- 3 If a VDM is installed, an MFT is required to support ATM for the video dialing network connection.

Table 3 Hardware Supported on the Cisco MC3810 for Cisco IOS Release 12.0(7)T

Module or Other Hardware Option	Product Number	
Voice Interface Modules	6-port AVM ¹	MC3810-AVM6
	1-port E1 DVM, connects to PBX/channel bank/key system ²	MC3810-DVM-E1
	1-port T1 DVM, connects to PBX/channel bank/key system ²	MC3810-DVM-T1
	1-port unbalanced E1 DVM, connects to PBX/channel bank/key system ²	MC3810-DVM-BNC
	4-port BRI voice module ³	MC3810-BVM4
Video Dialing Module	Supports an RS-366 Automatic Calling Equipment (ACE) interface to the DTE port of the videoconferencing equipment ⁴	MC3810-VDM

Table 3 Hardware Supported on the Cisco MC3810 for Cisco IOS Release 12.0(7)T

Module or Other Hardware Option	Product Number	
Analog Personality Modules⁵	1-port E & M analog module	MC3810-APM-EM
	1-port FXS analog module	MC3810-APM-FXS
	1-port FXO analog module	MC3810-APM-FXO
	1-port FXO analog module, approved for the U.K.	MC3810-FXO-UK
	1-port FXO analog module, approved for Germany	MC3810-FXO-GER
	1-port FXO analog module, approved for PR2 ⁶ countries	MC3810-FXO-PR2
	1-port FXO analog module, approved for PR3 ⁷ countries	MC3810-FXO-PR3
Voice Compression Modules⁸	3-DSP VCM, supports up to 6 channels ⁹ of compressed voice	MC3810-VCM3
	6-DSP VCM, supports up to 12 channels ⁹ of compressed voice	MC3810-VCM6
Multiflex Trunk Modules with Optional BRI	1-port MFT with RJ-48 channelized T1 interface	MC3810-MFT-T1
	1-port MFT with RJ-48 channelized E1 interface	MC3810-MFT-E1
	1-port MFT with unbalanced E1-BNC interface	MC3810-MFT-BNC
	1-port MFT with RJ-48 channelized T1 and BRI S/T interfaces	MC3810-MFT-TBS
	1-port MFT with unbalanced E1-BNC and BRI S/T interfaces	MC3810-MFT-EUS

- 1 Requires one to six APMs and one voice compression module (VCM3 or VCM6).
- 2 Requires one or two voice compression modules (VCM6) for processed voice.
- 3 Requires one voice compression module (VCM3 or VCM6) and Cisco IOS Release 12.0(4)T or a later release.
- 4 Requires MFT for ATM connectivity and Cisco serial V.35 DCE cable (product order number 72-1721-01) that includes a Ringing Indicator (RI) conductor, and a Cisco RS-366 ACE cable (product order number 72-1722-01) to connect the VDM to the videoconferencing equipment RS-366 dial-up DTE port.
- 5 For use with analog voice modules; one AVM requires at least one APM and supports up to six APMs.
- 6 PR2 countries currently include Australia and New Zealand.
- 7 PR3 countries currently include Japan and Singapore.
- 8 VCMs and Cisco IOS Plus feature sets are required for voice processing (for example, switching, compression, echo cancellation, and silence suppression) but not for drop-and-insert applications.
- 9 Cisco MC3810 maximum voice channel support by compression algorithm: G.711 at 64 kbps = 6 channels; G.726 at 32 kbps = 12 channels; G.729 at 8 kbps = 12 channels; G.729a at 8 kbps = 24 channels.

Determining the Software Version

To determine the version of Cisco IOS software running on a Cisco MC3810, log in and enter the **show version EXEC** command:

```
MC3810>show version
Cisco Internetwork Operating System Software
IOS (tm) MC3810 Software (mc3810-js-mz), Version 12.0(7)T, RELEASE SOFTWARE
```

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

Feature Set Table

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.

Table 4 Feature Sets Supported by the Cisco MC3810

Feature Sets	Feature Set Matrix Term	Software Image
IP Standard Feature Sets	IP Plus	mc3810-is-mz
	IP/ATM Plus	mc3810-a2is-mz
	IP Plus ATM MCM H323	mc3810-a2isx-mz
Enterprise Standard Feature Sets	Enterprise Plus	mc3810-js-mz
	Enterprise ATM Plus	mc3810-a2js-mz
	Enterprise Plus ATM MCM H323	mc3810-a2jsx-mz

Table 5 lists the features and feature sets supported by the Cisco MC3810 in Cisco IOS Release 12.0(7)T and uses the following conventions:

- Yes—The feature is supported in the software image.
- No—The feature is not supported in the software image.
- In—The number in the “In” column indicates the Cisco IOS release in which the feature was first introduced. For example, (3) means a feature was introduced in Release 12.0(3)T. If a cell in this column is empty, the feature was included in the initial base release.

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.

Table 5 Feature List by Feature Set for the Cisco MC3810

Features	In	Feature Set						
		IP	IP Plus	IP/ATM Plus	IP Plus ATM MCM H.323	Enterprise Plus	Enterprise ATM Plus	Enterprise Plus ATM MCM H.323
ATM Access								
ATM LANE FSSR Protocol	(5)	No	Yes	Yes	Yes	Yes	Yes	Yes
Frame Relay–ATM Interworking (FRF.5)		No	No	Yes	Yes	No	Yes	Yes
Frame Relay–ATM Interworking (FRF.5) Enhancements	(7)	No	No	Yes	Yes	No	Yes	Yes
Frame Relay–ATM Interworking (FRF.8)	(7)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
PPP Over ATM		No	No	Yes	Yes	No	Yes	Yes
RFC 1483		No	No	Yes	Yes	No	Yes	Yes
rtVBR, nrtVBR, CBR, UBR		No	No	Yes	Yes	No	Yes	Yes
Structured CES ¹		No	No	Yes	Yes	No	Yes	Yes
Traffic Shaping		No	No	Yes	Yes	No	Yes	Yes

Table 5 Feature List by Feature Set for the Cisco MC3810 (continued)

Features	In	Feature Set						
		IP	IP Plus	IP/ATM Plus	IP Plus ATM MCM H.323	Enterprise Plus	Enterprise ATM Plus	Enterprise Plus ATM MCM H.323
UNI 3.1 ²		No	No	Yes	Yes	No	Yes	Yes
UNI 4.0 (with ILMI)		No	No	Yes	Yes	No	Yes	Yes
IBM Support								
APPN		No	No	No	No	No	No	No
APPN High-Performance Routing		No	No	No	No	No	No	No
APPN MIB Enhancements		No	No	No	No	No	No	No
APPN over Ethernet LAN Emulation		No	No	No	No	No	No	No
APPN Scalability Enhancements		No	No	No	No	No	No	No
BAN for SNA Frame Relay Support		No	Yes	Yes	Yes	Yes	Yes	Yes
Bisync		No	Yes	Yes	Yes	Yes	Yes	Yes
Bridging Code Rework		No	No	No	No	No	No	No
Caching and Filtering		Yes	Yes	Yes	Yes	Yes	Yes	Yes
DLSw+		No	Yes	Yes	Yes	Yes	Yes	Yes
DLSw+ Enhanced Load Balancing	(3)	No	Yes	Yes	Yes	Yes	Yes	Yes
DLSw+ Ethernet Redundancy	(5)	No	Yes	Yes	Yes	Yes	Yes	Yes
DLSw+ Peer Clusters	(3)	No	Yes	Yes	Yes	Yes	Yes	Yes
DLSw (RFC 1795)		No	Yes	Yes	Yes	Yes	Yes	Yes
DLSw+ RSVP	(5)	No	Yes	Yes	Yes	Yes	Yes	Yes
DLSw+ RSVP Bandwidth Reservation	(3)	No	Yes	Yes	Yes	Yes	Yes	No
DLSw Version 2 (RFC 1266)		No	Yes	Yes	Yes	Yes	Yes	Yes
Downstream PU Concentration (DSPU)		No	Yes	Yes	Yes	Yes	Yes	Yes
Frame Relay SNA Support (RFC 1490)		No	Yes	Yes	Yes	Yes	Yes	Yes
NCIA		No	Yes	Yes	Yes	Yes	Yes	Yes
NetView Native Service Point		No	Yes	Yes	Yes	Yes	Yes	Yes
Polled Async		No	Yes	Yes	Yes	Yes	Yes	Yes
QLLC		No	Yes	Yes	Yes	Yes	Yes	Yes
Response Time Reporter		No	Yes	Yes	Yes	Yes	Yes	Yes
RIF Passthru in DLSw+		No	Yes	Yes	Yes	Yes	Yes	Yes
SDLC Integration		No	Yes	Yes	Yes	Yes	Yes	Yes
SDLC Transport (STUN)		No	Yes	Yes	Yes	Yes	Yes	Yes
SDLC-to-LAN Conversion (SDLLC)		No	Yes	Yes	Yes	Yes	Yes	Yes
SNA and NetBIOS WAN Optimization		No	Yes	Yes	Yes	Yes	Yes	Yes
SRB/RSRB		No	Yes	Yes	Yes	Yes	Yes	Yes
SRT		No	No	No	No	No	No	No

Table 5 Feature List by Feature Set for the Cisco MC3810 (continued)

Features	In	Feature Set						
		IP	IP Plus	IP/ATM Plus	IP Plus ATM MCM H.323	Enterprise Plus	Enterprise ATM Plus	Enterprise Plus ATM MCM H.323
SRTLB		No	Yes	Yes	Yes	Yes	Yes	Yes
TG/COS		No	No	No	No	No	No	No
TN3270		No	No	No	No	Yes	Yes	Yes
TN3270 LU Nailing		No	Yes	Yes	Yes	Yes	Yes	Yes
TN3270 Server Enhancements		No	Yes	Yes	Yes	Yes	Yes	Yes
IP Routing								
BGP		Yes	Yes	Yes	Yes	Yes	Yes	Yes
BGP4		Yes	Yes	Yes	Yes	Yes	Yes	Yes
EGP		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Enhanced IGRP		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Enhanced IGRP Optimizations		Yes	Yes	Yes	Yes	Yes	Yes	Yes
ES-IS		No	No	No	No	Yes	Yes	Yes
GRE VPN		No	No	No	No	Yes	Yes	Yes
IGRP		Yes	Yes	Yes	Yes	Yes	Yes	Yes
IS-IS		No	No	No	No	Yes	Yes	Yes
Named IP Access Control List		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Network Address Translation (NAT)		Yes	Yes	Yes	Yes	Yes	Yes	Yes
NHRP		Yes	Yes	Yes	Yes	Yes	Yes	Yes
On Demand Routing		Yes	Yes	Yes	Yes	Yes	Yes	Yes
OSPF		Yes	Yes	Yes	Yes	Yes	Yes	Yes
OSPF Not-So-Stubby-Areas (NSSA)		Yes	Yes	Yes	Yes	Yes	Yes	Yes
OSPF On Demand Circuit (RFC 1793)		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Protocol-Independent Multicast (PIM)		Yes	Yes	Yes	Yes	Yes	Yes	Yes
PIM Version 2		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Policy-Based Routing		Yes	Yes	Yes	Yes	Yes	Yes	Yes
RIP		Yes	Yes	Yes	Yes	Yes	Yes	Yes
RIP Version 2		Yes	Yes	Yes	Yes	Yes	Yes	Yes
LAN Support								
Apollo Domain		No	No	No	No	Yes	Yes	Yes
AppleTalk Phase 2		No	No	No	No	Yes	Yes	Yes
Banyan VINES		No	No	No	No	Yes	Yes	Yes
Concurrent Routing and Bridging		Yes	Yes	Yes	Yes	Yes	Yes	Yes
DECnet IV		No	No	No	No	Yes	Yes	Yes
DECnet V		No	No	No	No	Yes	Yes	Yes
GRE		No	No	No	No	Yes	Yes	Yes

Table 5 Feature List by Feature Set for the Cisco MC3810 (continued)

Features	In	Feature Set						
		IP	IP Plus	IP/ATM Plus	IP Plus ATM MCM H.323	Enterprise Plus	Enterprise ATM Plus	Enterprise Plus ATM MCM H.323
Integrated Routing and Bridging (IRB)		Yes	Yes	Yes	Yes	Yes	Yes	Yes
IP		Yes	Yes	Yes	Yes	Yes	Yes	Yes
LAN Extension Host		No	No	No	No	No	No	No
Multiring		No	No	No	No	No	No	No
Novell IPX		No	No	No	No	Yes	Yes	Yes
OSI		No	No	No	No	Yes	Yes	Yes
Source-Route Bridging		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Transparent and Translational Bridging		Yes	Yes	Yes	Yes	Yes	Yes	Yes
VLANs (ISL & IEEE 802.10)		No	No	No	No	No	No	No
XNS		No	No	No	No	Yes	Yes	Yes
Management								
AutoInstall		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Automatic Modem Configuration		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Cisco IOS File System		Yes	Yes	Yes	Yes	Yes	Yes	Yes
CLI String Search	(5)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
HTTP Server		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Response Time Reporter (RTR) Enhancements	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
RMON Events and Alarms		No	No	No	No	No	No	No
RMON Full		No	No	No	No	No	No	No
Service Assurance Agent (formerly RTR) Enhancements	(5)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SNMP		Yes	Yes	Yes	Yes	Yes	Yes	Yes
SNMP Inform Request		Yes	Yes	Yes	Yes	Yes	Yes	Yes
SNMP version 3	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Telnet		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Multimedia and Quality of Service								
Application Specific Routing	(3)	No	No	No	No	No	No	No
Gateway Support for Alternate Gatekeeper	(7)	No	No	No	Yes	No	No	Yes
Generic Traffic Shaping		Yes	Yes	Yes	Yes	Yes	Yes	Yes
H.323 Gatekeeper and Proxy	(3)	No	No	No	Yes	No	No	Yes
H.235 Accounting and Security Enhancements for Cisco Gateways	(7)	No	No	No	Yes	No	No	Yes
H.323 Version 2	(5)	No	No	No	Yes	No	No	Yes
H.323 Multizone Enhancements	(7)	No	No	No	Yes	No	No	Yes

Table 5 Feature List by Feature Set for the Cisco MC3810 (continued)

Features	In	Feature Set						
		IP	IP Plus	IP/ATM Plus	IP Plus ATM MCM H.323	Enterprise Plus	Enterprise ATM Plus	Enterprise Plus ATM MCM H.323
H.323 Hot Standby Routing Protocol (HSRP)	(3)	No	No	No	Yes	No	No	Yes
Multicast Routing Monitor	(5)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Multimedia Conference Manager	(3)	No	No	No	Yes	No	No	Yes
PGM Router Assist	(5)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Process MIB	(3)	Yes	Yes	Yes	No	Yes	Yes	No
Random Early Detection (RED)		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Response Time Reporter Enhancements	(3)	Yes	Yes	Yes	No	Yes	Yes	No
RSVP		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Other Routing								
AURP		No	No	No	No	Yes	Yes	Yes
IPX RIP		No	No	No	No	Yes	Yes	Yes
NLSP		No	No	No	No	Yes	Yes	Yes
RTMP		No	No	No	No	Yes	Yes	Yes
SMRP		No	No	No	No	Yes	Yes	Yes
SRTP		No	No	No	No	Yes	Yes	Yes
Protocol Translation								
LAT		No	No	No	No	Yes	Yes	Yes
PPP		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Rlogin		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Telnet		Yes	Yes	Yes	Yes	Yes	Yes	Yes
TN3270		No	No	No	No	Yes	Yes	Yes
X.25		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Remote Node								
ARAP 1.0/2.0		No	No	No	No	Yes	Yes	Yes
Asynchronous Master Interfaces		Yes	Yes	Yes	Yes	Yes	Yes	Yes
ATCP		No	No	No	No	Yes	Yes	Yes
CPPP		Yes	Yes	Yes	Yes	Yes	Yes	Yes
CSLIP		Yes	Yes	Yes	Yes	Yes	Yes	Yes
DHCP		Yes	Yes	Yes	Yes	Yes	Yes	Yes
IP Pooling		Yes	Yes	Yes	Yes	Yes	Yes	Yes
IPX and ARAP on Virtual Async Interfaces		No	No	No	No	Yes	Yes	Yes
IPXCP		No	No	No	No	Yes	Yes	Yes
MacIP		No	No	No	No	Yes	Yes	Yes

Table 5 Feature List by Feature Set for the Cisco MC3810 (continued)

Features	In	Feature Set						
		IP	IP Plus	IP/ATM Plus	IP Plus ATM MCM H.323	Enterprise Plus	Enterprise ATM Plus	Enterprise Plus ATM MCM H.323
NASI		No	No	No	No	Yes	Yes	Yes
NetBEUI over PPP		No	No	No	No	Yes	Yes	Yes
PPP		Yes	Yes	No	No	Yes	Yes	Yes
SLIP		Yes	Yes	No	No	Yes	Yes	Yes
Scalability								
Airline Product Set (ALPS)		No	No	No	No	No	No	No
Cisco IOS File System		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Cisco MC3810 – IGX 8400 Interworking	(2)	No	Yes	Yes	Yes	Yes	Yes	Yes
Entity MIB		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Expression MIB		Yes	Yes	Yes	Yes	Yes	Yes	Yes
OSPF Point to Multipoint		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Per Port Debugging (Conditionally Triggered Debugging)		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Priority Queuing Support Enhancement for Cisco MC3810-IGX Interworking	(3)	No	Yes	Yes	Yes	Yes	Yes	Yes
SNMP Manager		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Security								
Access Lists		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Access Security		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Additional Vendor-Proprietary RADIUS Attributes		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Authenticating ACLs		No	No	No	No	No	No	No
Automated Double Authentication		No	No	No	No	Yes	Yes	Yes
Certificate Authority Interoperability		No	No	No	No	No	No	No
Context-Based Access Control (CBAC)		No	No	No	No	No	No	No
Extended Access Lists		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Internet Key Exchange Security Protocol		No	No	No	No	No	No	No
IPSec Network Security		No	No	No	No	No	No	No
Kerberized Login		No	No	No	No	Yes	Yes	Yes
Kerberos V Client Support		No	No	No	No	Yes	Yes	Yes
Lock and Key		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Mac Security for Hubs		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Md5 Routing Authentication		Yes	Yes	Yes	Yes	Yes	Yes	Yes

Table 5 Feature List by Feature Set for the Cisco MC3810 (continued)

Features	In	Feature Set						
		IP	IP Plus	IP/ATM Plus	IP Plus ATM MCM H.323	Enterprise Plus	Enterprise ATM Plus	Enterprise Plus ATM MCM H.323
MS-CHAP Support		No	No	No	No	Yes	Yes	Yes
Named Method Lists for AAA Authentication & Accounting		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Network Layer Encryption (40-bit or Export Controlled 56-bit DES)		No	No	No	No	No	No	No
RADIUS		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Router Authentication		No	No	No	No	No	No	No
Sublock Phase 1		Yes	Yes	Yes	Yes	Yes	Yes	Yes
TACACS+		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Time-Based Access Lists	(5)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Tunneling Endpoint Discovery	(5)	No	No	No	No	Yes	Yes	Yes
Switching								
Enhanced ATM VC Configuration and Management		No	No	Yes	Yes	No	Yes	Yes
Multiple ISDN Switch Types		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Terminal Services								
LAT		No	No	No	No	Yes	Yes	Yes
Rlogin		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Telnet		Yes	Yes	Yes	Yes	Yes	Yes	Yes
TN3270		No	No	No	No	Yes	Yes	Yes
X.25 Pad		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Xremote		No	No	No	No	Yes	Yes	Yes
Voice and Multimedia								
Analog Signaling		No	Yes	Yes	Yes	Yes	Yes	Yes
ATM Video SVCs	(7)	No	No	Yes	Yes	No	Yes	Yes
ATM Voice SVCs	(7)	No	No	Yes	Yes	No	Yes	Yes
Call Detail Records (CDR)	(2)	No	Yes	Yes	Yes	Yes	Yes	Yes
E1 CAS Signaling ³		No	Yes	Yes	Yes	Yes	Yes	Yes
Fancy Queuing on Frame Relay or Cisco HDLC	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
G.726 (ADPCM)	(2)	No	Yes	Yes	Yes	Yes	Yes	Yes
Gain Control		No	Yes	Yes	Yes	Yes	Yes	Yes
ISDN BRI Voice Module ⁴	(4)	No	Yes	Yes	Yes	Yes	Yes	Yes
ISDN PRI QSIG Digit Forwarding ⁴	(4)	No	Yes	Yes	Yes	Yes	Yes	Yes
ISDN PRI QSIG Voice Signaling ⁴	(2)	No	Yes	Yes	Yes	Yes	Yes	Yes
Local Dialing		No	Yes	Yes	Yes	Yes	Yes	Yes
Local Voice Busy Out	(3)	No	Yes	Yes	Yes	Yes	Yes	Yes

Table 5 Feature List by Feature Set for the Cisco MC3810 (continued)

Features	In	Feature Set						
		IP	IP Plus	IP/ATM Plus	IP Plus ATM MCM H.323	Enterprise Plus	Enterprise ATM Plus	Enterprise Plus ATM MCM H.323
Multiple Ring Tones		No	Yes	Yes	Yes	Yes	Yes	Yes
Multiflex Trunk		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Multi-length Dial Patterns	(2)	No	Yes	Yes	Yes	Yes	Yes	Yes
Off-Net Dialing		No	Yes	Yes	Yes	Yes	Yes	Yes
On-Net/Off-Net Call Rerouting		No	Yes	Yes	Yes	Yes	Yes	Yes
OPX Ring-Through	(2)	No	Yes	Yes	Yes	Yes	Yes	Yes
Pass-Through Voice		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Permanent Connection	(2)	No	Yes	Yes	Yes	Yes	Yes	Yes
PLAR		No	Yes	Yes	Yes	Yes	Yes	Yes
Preference-based Hunt Groups	(2)	No	Yes	Yes	Yes	Yes	Yes	Yes
Remote Dialing		No	Yes	Yes	Yes	Yes	Yes	Yes
T1 CAS Signaling		No	Yes	Yes	Yes	Yes	Yes	Yes
Transparent CCS	(2)	No	Yes	Yes	Yes	Yes	Yes	Yes
Voice Activity Detection		No	Yes	Yes	Yes	Yes	Yes	Yes
Voice over ATM		No	No	Yes	Yes	No	Yes	Yes
Voice over Frame Relay		No	Yes	Yes	Yes	Yes	Yes	Yes
Voice over Frame Relay Using FRF.11 and FRF.12	(4)	No	Yes	Yes	Yes	Yes	Yes	Yes
Voice over HDLC		No	Yes	Yes	Yes	Yes	Yes	Yes
Voice over IP		No	No	No	No	No	No	No
WAN Optimization								
Bandwidth-on-Demand		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Custom and Priority Queuing ⁵		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Dial Backup		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Dial-on-Demand		Yes	Yes	Yes	Yes	Yes	Yes	Yes
DRP Server Agent		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Header, Link and Payload Compression		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Snapshot Routing		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Weighted Fair Queuing ⁵		Yes	Yes	Yes	Yes	Yes	Yes	Yes
WAN Services								
Always On/Direct ISDN		No	No	No	No	No	No	No
ATM LAN Emulation: Decnet Routing and Banyan Vines Support		No	No	Yes	Yes	No	Yes	Yes
ATM LAN Emulation: (HSRP and SSRP)		No	No	Yes	Yes	No	Yes	Yes

Table 5 Feature List by Feature Set for the Cisco MC3810 (continued)

Features	In	Feature Set						
		IP	IP Plus	IP/ATM Plus	IP Plus ATM MCM H.323	Enterprise Plus	Enterprise ATM Plus	Enterprise Plus ATM MCM H.323
ATM: Rate Queues for SVC per Subinterface		No	No	Yes	Yes	No	Yes	Yes
ATM UNI 3.1 Signaling		No	No	Yes	Yes	No	Yes	Yes
ATM UNI 4.0 (with ILMI)		No	No	Yes	Yes	No	Yes	Yes
Combinet Packet Protocol (CPP)		No	No	No	No	No	No	No
Dialer Profiles		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Dialer Watch		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Facility Data Link Capabilities on Multiflex Trunk	(2)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Frame Relay Compression (FRF.9)		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Frame Relay End-to-End Keepalive	(5)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Frame Relay SVCs Support (DTE)		No	No	No	No	No	No	No
Frame Relay Traffic Shaping		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Frame Relay Switching		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Frame Relay UNI		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Frame Relay-ATM Interworking (FRF.5)		No	No	Yes	Yes	No	Yes	Yes
Frame Relay-ATM Interworking (FRF.8)	(7)	No	No	Yes	Yes	No	Yes	Yes
Half Bridge/Half Router For CPP And PPP		Yes	Yes	Yes	Yes	Yes	Yes	Yes
HDLC		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Integrated BRI Backup ⁴	(2)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
IPXwan 2.0		No	No	No	No	Yes	Yes	Yes
ISDN		Yes	Yes	Yes	Yes	Yes	Yes	Yes
ISDN Advise of Charge		Yes	Yes	Yes	Yes	Yes	Yes	Yes
ISDN Caller ID Callback		Yes	Yes	Yes	Yes	Yes	Yes	Yes
ISDN NFAS		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Leased Line ISDN at 128 kbps		No	No	No	No	No	No	No
MPPC-MS PPP Compression		Yes	Yes	Yes	Yes	Yes	Yes	Yes
MS Callback		No	No	No	No	No	No	No
Multicast Source Discovery Protocol (MSDP)	(7)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Multichassis Multilink PPP (MMP)		No	No	No	No	Yes	Yes	Yes
National ISDN Switch Type		Yes	Yes	Yes	Yes	Yes	Yes	Yes
PPP		Yes	Yes	Yes	Yes	Yes	Yes	Yes
SMDS		Yes	Yes	Yes	Yes	Yes	Yes	Yes

Table 5 Feature List by Feature Set for the Cisco MC3810 (continued)

Features	In	Feature Set						
		IP	IP Plus	IP/ATM Plus	IP Plus ATM MCM H.323	Enterprise Plus	Enterprise ATM Plus	Enterprise Plus ATM MCM H.323
Stackable Home Gateway		No	No	No	No	No	No	No
Switched 56		Yes	Yes	Yes	Yes	Yes	Yes	Yes
Virtual Private Dialup Network (VPDN)		No	No	No	No	Yes	Yes	Yes
X.25		Yes	Yes	Yes	Yes	Yes	Yes	Yes
X.25 Enhancements		Yes	Yes	Yes	Yes	Yes	Yes	Yes
X.25 Closed User Groups	(7)	No	Yes	Yes	Yes	Yes	Yes	Yes
X.25 Switch Local Acknowledgment	(7)	No	Yes	Yes	Yes	Yes	Yes	Yes
X.25 on ISDN		Yes	Yes	Yes	Yes	Yes	Yes	Yes
X.25 over Frame Relay (Annex G)	(3)	Yes	Yes	Yes	Yes	Yes	Yes	Yes
X.25 Switching between PVCs and SVCs		Yes	Yes	Yes	Yes	Yes	Yes	Yes

1 Voice signaling on CES is not available.

2 ATM PVCs only. SVCs are not supported.

3 Includes T1 CAS protocols, plus UK Standard CAS (Mercury protocol) and CEPT standard E&M.

4 When the older motherboard (SCB 6.06) is used with this feature, serial port 1 cannot be used. When the new motherboard (SCB 6.07 and later versions) is used, serial port 1 can be used in DCE mode only.

5 Applicable to data-only interfaces.

New and Changed Information

The following sections list the new hardware and software features supported by the Cisco MC3810 for Release 12.0 T.

New Hardware Feature in Cisco IOS Release 12.0(7)T

Release 12.0(7)T supports a new hardware feature for the Cisco MC3810.

Video over ATM Switched Virtual Circuits on the Cisco MC3810

Video over ATM switched virtual circuits (SVCs) on the Cisco MC3810 expands the capabilities of the Cisco MC3810 multiservice access concentrator to provide cost-effective, dynamic, and flexible videoconferencing system support. By using a plug-in video dialing module (VDM) to provide an RS-366 dialing interface to an H.320 video codec, the Cisco MC3810 automatically accepts dial-out requests from the video system. The codec connects to either one of the Cisco MC3810 serial ports and also to the Cisco MC3810 RS-366 dial-up port.

In addition, permanent virtual circuit (PVC) support is enhanced to permit PVC connections with automatic connection through a serial port. Each codec must place a call to the other videoconferencing system before the expiration of the video codec time-out period. By using a video dial map, each system reconciles the dialed number with a PVC that has already been configured, allowing fast connectivity.

For details, see the online feature module.

New Software Features in Cisco IOS Release 12.0(7)T

Release 12.0(7)T supports new software features for the Cisco MC3810.

Cisco H.235 Accounting and Security Enhancements for Cisco Gateways

The Cisco H.323 gateway now supports the use of CryptoH323Tokens for authentication.

The CryptoH323Token Is defined in H.225 Version 2 and supports the following features:

- Used in a “password-with-hashing” security scheme described in section 10.3.3 of the H.235 specification.
- Can be included in any RAS message
- Is used to authenticate the sender of the message.
- A separate database for user ID and password verification.

With this release, Cisco H.323 gateways support three levels of authentication:

- Endpoint—The RAS channel used for gateway-to-gatekeeper signaling is not a secure channel. To ensure secure communications, H.235 allows gateways to include an authentication key in their RAS messages. The gatekeeper uses this key to authenticate the source of the messages. At the endpoint level, all messages from the gateway are validated. The cryptoTokens are validated by using the password configured for the gateway.
- Per-Call—When the gateway receives a call over the telephony leg, the gateway prompts the user for an account number and personal identification number (PIN). These two numbers are included in certain RAS messages sent from the endpoint and authenticate the originator of the call.
- All—This option is a combination of the other two levels of authentication. With this option, the validation of cryptoTokens in ARQ messages is based on an the account number and PIN of the user making a call; the validation of cryptoTokens sent in all the other RAS messages is based on the password configured for the gateway.

You can configure the level of authentication for the gateway by using the Cisco IOS software command line interface.

CryptoTokens for registration requests (RRQ), unregistration request (URQ), disengage request (DRQ) and the terminating side of admission request (ARQ) messages contain information about the gateway that generated the token, including the gateway ID (which is the H.323 ID configured on the gateway) and the gateway password.

CryptoTokens for the originating side ARQ messages contain information about the user who is placing the call, including the user ID, and personal identification number (PIN).

Cisco H.323 Multizone Enhancements

Cisco H.323 Multizone enhancements allow a Cisco gateway to provide information to the gatekeeper with additional fields in the RAS (registration, admission, and status) messages.

Previously, the source gateway attempted to set up a call to a destination IP address as provided by the gatekeeper in an Admission Confirm (ACF) message. If the gatekeeper was unable to resolve the destination E.164 phone number to an IP address, the incoming call was terminated.

This version of the H.323 software adds support to allow a gatekeeper to provide additional destination information and modify the destinationInfo field in the ACF. The gateway includes the canMapAlias associated destination information in setting up the call to the destination gateway.

With the canMapAlias functionality, this version includes support for the gatekeeper to indicate to the gateway that the call should be sent to a new E.164 number. The gatekeeper indicates this by sending an Admission Confirm message with an IP address of 0.0.0.0 in the destCallSignalAddress field and the new destination E.164 phone number in the destinationInfo field.

The gateway receiving such an ACF falls back to routing the call based on this new E.164 address and performing a new lookup of the gateway's configured dial plan. This can result in the call being routed back to the PSTN or to an H.323 endpoint.

Frame Relay—ATM Service Interworking—FRF.8 on the Cisco MC3810

Frame Relay-to-ATM Service Interworking for data transfer is outlined in Frame Relay Forum implementation agreement FRF.8 and designed for the Cisco MC3810 multiservice access concentrator.

FRF.8 Frame Relay-ATM Service Interworking:

- Allows Frame Relay traffic to connect across high-speed ATM trunks.
- Connects a Frame Relay network to an ATM network while the networks:
 - function independently
 - allow bidirectional PVC protocol conversion functions
 - provide a standards-based solution for service providers, enterprises, and end users.
- Supports two modes of operation of the interworking function (IWF) for upper-layer user protocol encapsulation:
 - In Service Interworking translation mode, Frame Relay PVCs are mapped to ATM PVCs without the need for symmetric topologies—the paths can terminate on the ATM side. The ATM-connected Cisco MC3810 does not have to be directly linked to a Frame Relay network, and some network devices in a Frame Relay network can evolve to ATM without all the network devices doing so.
 - In Service Interworking, transparent mode does not map encapsulations but sends them unaltered. This mode is used when translation is not practical because encapsulation methods do not conform to the supported standards for Service Interworking.

For details, see the online feature module.

Frame Relay—ATM Network Interworking—FRF.5 Enhancement on the Cisco MC3810

The Frame Relay-ATM Network Interworking (FRF.5) feature that was first introduced in 11.3(1)MA has been enhanced to allow setting the mode of the Discard Eligibility and Cell Loss Priority fields as defined in the FRF.5 implementation agreement.

Network Interworking allows the transparent tunneling of Frame Relay user traffic and PVCs over ATM. This function is often used to link Frame Relay networks over an ATM backbone. The most distant nodes must be configured to interoperate with one another—in contrast to Service Interworking—because intact Frame Relay frames are sent over the ATM network. The ATM backbone is used as an alternative to a leased line and provides cost savings over leased lines. There can be a one-to-one relationship between Frame Relay and ATM PVCs, or multiple Frame Relay PVCs can be multiplexed into a single ATM PVC.

For details, see the online feature module.

Gateway Support for Alternate Gatekeeper

The Alternate Gatekeeper feature provides redundancy for a gatekeeper in a system where gatekeepers are used. This enhancement allows a gateway to use up to two alternate gatekeepers as a backup in case a primary gatekeeper failure.

A gatekeeper manages H.323 endpoints in a consistent manner, allowing the endpoints to register with the gateway and to locate another gatekeeper.

The gatekeeper provides logic variables for proxies or gateways in a call path to:

- Provide connectivity with the public switched telephone network (PSTN)
- Improve Quality of Service (QoS)
- Enforce security policies

You can configure multiple gatekeepers to communicate with one another either by integrating their addresses into the Domain Naming System (DNS) or by using Cisco IOS configuration options.

Low Latency Queueing (CSCdm84810)

The Low-Latency Queueing (LLQ) feature brings strict priority queueing to Class-Based Weighted Fair Queueing (CBWFQ). Strict priority queueing allows delay-sensitive data, such as voice, to be dequeued and sent first (before packets in other queues are dequeued), giving delay-sensitive data preferential treatment over other traffic.

Without LLQ, CBWFQ provides weighted fair queueing based on defined classes with no strict priority queue available for real-time traffic. CBWFQ allows you to define traffic classes and then assign characteristics to that class. For example, you can designate the minimum bandwidth delivered to the class during congestion. This scheme poses problems for voice traffic, which is largely intolerant of delay—especially variation in delay. The delay introduces irregularities of transmission manifesting as jitter in the heard conversation.

The LLQ feature provides strict priority queueing for CBWFQ, reducing jitter in voice conversations. Configured by using the **priority** command, LLQ enables use of a single, strict priority queue within CBWFQ at the class level, allowing you to direct traffic belonging to a class to the CBWFQ strict priority queue.

Although it is possible to enqueue various types of real-time traffic to the strict priority queue, we strongly recommend that you direct only voice traffic to it. Voice traffic is well-behaved, whereas other types of real-time traffic are not. Furthermore, voice traffic requires that delay be nonvariable in order to avoid jitter. Real-time traffic, such as video, can introduce variation in delay, thereby thwarting the steadiness of delay required for successful voice traffic transmission.

When the bandwidth has been exceeded during congestion, policing is used to drop packets. Voice traffic enqueued to the priority queue is UDP-based; therefore it is not adaptive to the early packet drop characteristic of Weighted Random Early Detection (WRED).

When congestion occurs, traffic destined for the priority queue is metered to ensure that the bandwidth allocation configured for the class to which the traffic belongs is not exceeded.

Multicast Source Discovery Protocol

Multicast Source Discovery Protocol (MSDP):

- Connects multiple Protocol Independent Multicast (PIM) sparse-mode (SM) domains.
- Allows multicast sources for a group to be known to all rendezvous points (RPs) in different domains.

Each PIM-SM domain uses its own RPs and does not depend on RPs in other domains. An RP runs MSDP over TCP to discover multicast sources in other domains.

An RP in a PIM-SM domain has an MSDP peering relationship with MSDP-enabled routers in another domain. The peering relationship occurs over a TCP connection where primarily a list of sources sending to multicast groups is exchanged. The TCP connections between RPs are achieved by the underlying routing system. The receiving RP uses the source lists to establish a source path.

The purpose of this topology is to have domains discover multicast sources in other domains. If the multicast sources are of interest to a domain that has receivers, multicast data is delivered over the normal source-tree building mechanism in PIM-SM.

- Allows you to announce sources that are sending to a group. These announcements must originate at the domain's RP. You should run MSDP in your domain's RPs that act as sources, and that send to global groups for announcement to the Internet.
- Depends heavily on (M)BGP for interdomain operation.

Voice over ATM Switched Virtual Circuits on the Cisco MC3810

Voice over Asynchronous Transfer Mode (VoATM) switched virtual circuits (SVCs) on the Cisco MC3810:

- Allows the Cisco MC3810 to transfer voice data dynamically and as needed—without tying up the resources required for static, manually provisioned permanent virtual circuits (PVCs). An SVC connection is initiated for each call, and each request includes the bandwidth and quality-of-service (QoS) information required for the connection. SVCs are ideal for networks that are highly interconnected, where scalability is essential, and in situations where traffic is sporadic. In addition, service providers often offer more advantageous, usage-based pricing options for SVCs than they do for PVCs.
- Includes all the voice features that the Cisco MC3810 supports for PVCs and for Frame Relay transport.
- Is based on dial peers.
- Uses ATM Adaptation Layer 5 (AAL5).

For details, see the online feature module.

X.25 Closed User Groups

The X.25 specification for Closed User Groups (CUG):

- Provides an application access security service that restricts users who do not have subscribed access to the host location.
- Provides a privacy technique that you can use to create private subnets or virtual networks out of a public data network.

Note Previously, Cisco supported only the ability to specify the CUG value but did not enforce restriction. Cisco currently enforces this security restriction.

X.25 Switch Local Acknowledgment

Cisco offers an X.25 switch function that creates virtual connections (VC) by connecting channels between X.25 class services.

The following X.25 class services are supported:

- X.25, Connection-Mode Network Service (CMNS)
- X.25 over TCP (XOT)
- Switched Virtual Circuits (SVCs) and Permanent Virtual Circuits (PVCs) are both supported and can be switched to each other (converted).

The current Cisco implementation provides end-to-end acknowledgment, which means that flow control or window and packet size acknowledgment is between the originating and terminating data terminal equipment (DTE).

Acknowledgment is not local to the DTE and data communications equipment (DTE), and the overall effect is low throughput.

New Software Features in Cisco IOS Release 12.0(5)T

Release 12.0(5)T supports new software features for the Cisco MC3810.

AAA Server Group

The AAA server-group feature introduces a way to group the existing server hosts. The server-group feature allows the user to select a subset of the configured server hosts and use them for a particular service.

A server-group is a list of server hosts of a particular type. Currently supported server host types are Remote Authentication Dial In User Service (RADIUS) server hosts and Terminal Access Controller Access Control System+ (TACACS+) server hosts. Server-group is used in conjunction with a global server host list. The server-group lists the IP addresses of the selected server hosts.

ATM LANE Fast Simple Server Replication Protocol

To improve the ATM LAN Emulation (LANE) Simple Server Redundancy Protocol (SSRP), Cisco has introduced the ATM LANE Fast Simple Server Redundancy Protocol (FSSRP). FSSRP differs from LANE SSRP in that all configured LANE servers of an emulated LAN (ELAN) are always active. FSSRP-enabled LANE clients have VCs linked to up to four LANE server broadcast-and-unknown servers (BUSs). If a LANE server goes down, the LANE client quickly switches over to a new LANE server and BUS resulting in no data or LE-ARP table entry losses and no extraneous signaling.

CNS Client for Cisco IOS Software

Cisco Networking Services (CNS) Client feature for Cisco IOS software enables authenticated directory access. CNS Client for Cisco IOS software includes the following components:

- Lightweight Directing Access Protocol (LDAP) V.3 client
- Support to use Kerberos V.5 as security protocol for LDAP V.3 client
- CNS Event Services Client
- CNS Locator Services Client
- CNS IP Security (IPSec) virtual private network (VPN) Provisioning Agent
- CNS Configuration Change Notification Agent
- CNS Provisioning Agent

LDAP V.3 client functionality enables Cisco IOS software-based applications to securely authenticate to a CNS for Active Directory (CNS/AD) server using Kerberos V.5 as security protocol to retrieve or store information such as policy and configuration data. Cisco IOS software-based applications publish or subscribe to events using CNS event services client, enabling external applications using the application programming interface (API) features of CNS to receive events or publish events to the Cisco IOS device. This Cisco IOS software-based device will use CNS locator services client to locate the nearest directory server using Domain Name System. The administrator need not configure the device to locate the nearest directory server.

All the above-mentioned functionality is intended for use by internal Cisco IOS application developers. CNS IPSec VPN provisioning agent enables the router to retrieve IPSec policies stored in the CNS/AD server and configure itself, automating the provisioning of customer premises equipment devices for IPSec VPN. CNS provisioning agent enables Cisco IOS device to be provisioned using CNS event services.

DLSw+ Ethernet Redundancy

The DLSw+ Ethernet Redundancy feature provides redundancy in an Ethernet environment. It enables DLSw+ to support parallel paths between two points in an Ethernet environment, ensuring resiliency in the case of a router failure and providing load balancing for traffic load.

DLSw+ could provide redundancy prior to this feature in a Token Ring environment or via backup peers. When an end station on an Ethernet LAN had multiple active paths into a DLSw+ network, problems occurred.

Redundancy is not possible in an Ethernet environment because, unlike Token Ring, it does not have a RIF field in its packet. The RIF notifies a router of the path a packet has traveled by tracking each ring number and bridge it travels along a path. If a bridge notices that the next ring matches a ring already in the RIF, then the frame is not copied on to that ring. The RIF prevents unreliable local reachability information, circuit contention, and undetected looping explorers.

DLSw+ Fast HPR

The DLSw+ Fast HPR feature provides mechanisms by which DLSw+ can more efficiently switch and prioritize APPN ANR traffic. APPN nodes use LLC1 UI frames to encapsulate HPR over LAN media such as Token Ring or Ethernet. In Cisco IOS Release 11.3, DLSw+ was enhanced to allow circuits to start when the peer received a non-broadcast UI frame. Currently, DLSw+ creates lite circuits to carry APPN HPR traffic. Although this method is sufficient to transport HPR data flows, it has some performance weaknesses.

HPR has its own retransmission mechanism and does not need the reliable transport provided by DLSw+ TCP peer connections. When DLSw+ with TCP/IP encapsulation transports the HPR data, the TCP/IP layer of the DLSw+ packet handles the retransmission and sequencing necessary for traffic traveling across a WAN. HPR, however, has no knowledge about the underlying secured transport layer. Performance issues arise because APPN HPR has its own retransmission and sequencing capabilities that compete against the capabilities of DLSw+. The result is unreliable transport of HPR frames over DLSw+.

DLSw+ with FST encapsulation is another method to transport HPR traffic. Because FST does not terminate the local media DLC, data packet delivery is not guaranteed. DLSw+ with FST encapsulation does, however, drop "out-of-order" packets to prevent packet retransmissions. While this reliability mechanism is necessary, HPR has its own resequencing capabilities. The DLSw+ FST encapsulation of "out-of-order" packets competes against the HPR resequencing capabilities. The result is that DLSw+ drops the frames that are received out of sequence for an FST peer, causing unnecessary retransmission of HPR traffic.

DNS-Based X.25 Routing

Managing a large TCP/IP network requires accurate and up-to-date maintenance of IP addresses and X.121 address mapping information on each router database in the network. Currently, this data is managed manually. Because these addresses are constantly being added and removed in the network, the routing table of every router frequently needs to be updated, which is a time-consuming and error-prone task.

X.25 has long operated over an IP network, specifically using Transmission Control Protocol (TCP) as a reliable transport mechanism. This method is known as X.25 over TCP (XOT). However, large networks and financial legacy environments experienced problems with the amount of route configuration that needed to be performed manually because each router switching calls over TCP needed every destination configured. Every destination from the host router needed a static IP route statement, and for larger environments, these destinations could be as much as several thousand per router. Until now, the only way to map X.121 addresses and IP addresses was on a one-to-one basis using the **x25 route x121address xot ipaddress** command.

The solution to this problem was to centralize route configuration that routers could then access for their connectivity needs. This centralization is the function of the DNS-Based X.25 Routing feature, because the DNS server is a database of all domains and addresses on a network.

Frame Relay End-to-End Keepalive

The Frame Relay End-to-End Keepalive feature enables the router to keep track of permanent virtual circuit (PVC) status, independent of the switches in the Frame Relay network. The routers at both ends of a PVC in a Frame Relay network engage in a keepalive session where one router issues keepalive messages and the router at the other end of the PVC connection responds. The time interval for the keepalive is configurable and is enabled on a per-PVC basis. As long as the keepalive-issuing router receives response messages, the PVC status is up. When response messages are not received (because of line failure, a faulty switch in the Frame Relay network, or a router failure), the PVC is down. This mechanism enables bidirectional communication of PVC status to both routers at the ends of a PVC connection.

H.323 Version 2 Support (Gatekeeper and Proxy Features)

The H.323 Version 2 Support feature upgrades Cisco IOS software to comply with the mandatory requirements in the version 2 specification. This upgrade enhances the existing Voice over IP (VoIP) Gateway, the Multimedia Conference Manager (gatekeeper and proxy), and the DTMF digital relay using H.245.

DTMF is the tone generated on a touch-tone telephone when you press keypad digits. The tones are compressed into a single stream at one end of a call and decompressed at the other end by using H.245 messages. However, this compression and decompression can lead to distortion, depending upon the codec used. Thus, the DTMF-relay is used to configure one of three methods to transport DTMF tones generated after the call is established out-of-band. The three methods are:

- The standard H.323 out-of-band method uses H.245 to send digits as audible DTMF tones along with voice (the “h245-signal” option).
- The H.245 “alphanumeric” method (the “h245-alphanumeric” option) uses User Input Indication as part of a control channel, and is another standard H.245 transmission method.
- The “cisco-rtp” method sends the voice stream but with an identifier indicating that the DTMF tones are added.

H.323 Version 2 defines a lightweight registration procedure that requires full registration for initial registration, but uses an abbreviated renewal procedure to update the gatekeeper and minimize overhead. Lightweight registration requires each endpoint to specify a Time To Live (TTL) value in its Registration Request (RRQ) message.

The H.323 Version 2 gateway supports the registration of fully qualified E.164 numbers with the gatekeeper for telephones connected directly to the gateway. Tunneling through H.225 User-to-User Information Element (UUIE) facilitates transparent handling of supplementary services between two endpoints through a VoIP network. This tunneling eliminates the need to interpret various supplementary signaling messages in the VoIP gateways.

H.323 Version 2 gatekeeper selects a destination gateway by choosing from among all gateways registered in a zone by allowing you to assign selection priorities to these gateways based on the dialed prefix. Gateway resource reporting allows the gateway to notify the gatekeeper when H.323 resources are getting low. The gatekeeper uses this information to determine which gateway it will use to complete a call. The gatekeeper maintains a separate gateway list, ordered by priority, for each of its zone-prefixes.

IP RTP Priority

The new IP RTP Priority feature provides a strict priority queueing scheme for delay-sensitive data such as voice. Voice traffic can be identified by its Real-Time Transport Protocol (RTP) port numbers and classified into a priority queue configured by the **ip rtp priority** command. The result is that voice is serviced as strict priority in preference to other nonvoice traffic.

This feature extends and improves on the functionality offered by the IP RTP Reserve feature by allowing you to specify a range of UDP/RTP ports whose voice traffic is guaranteed strict priority service over any other queues or classes using the same output interface. Strict priority means that if packets exist in the priority queue, they are dequeued and sent first—that is, before packets in other queues are dequeued. Cisco recommends that you use the **ip rtp priority** command instead of the **ip rtp reserve** command for voice configurations.

IPX Display and Debug Enhancements

Several IPX display and debug enhancements have been added to the Cisco IOS 12.0(5)T software to improve its flexibility and ease of maintenance:

- Watchdog spoofing prevents watchdog keepalive packets from causing unnecessary calls on dial-on-demand routing (DDR) interfaces. Spoofing makes a server view a client as always connected, even when it isn't, thus reducing the number of available licenses. Users can set the duration of IPX watchdog spoofing and periodically disable it so that NetWare servers can clean up inactive connections.
- A Get General Service (GGS) response filter allows users to filter services advertised in general SAP response packets.
- To aid network debugging, you can now clear IPX and NLSP traffic counters and display a snapshot of them.

ISDN Cause Code Override

the ISDN Cause Code Override function overrides cause codes that are sent to ISDN applications. Currently, the Cisco IOS software contains ISDN cause codes that handle specific functions such as modem availability and resource pooling. The ISDN Cause Code Override feature is more general in its functionality and will override the specific ISDN cause codes.

When the command associated with this feature is implemented, the configured cause codes are sent to the switch; otherwise, default cause codes of the application are sent.

To override an ISDN cause code, enter the following command:

```
isdn disconnect-cause {cause-code-number | busy | not-available}
```

where *cause-code-number* is a cause code number from 1 to 127.

Multimedia Conference Manager Enhancements

Multimedia Conference Manager provides gatekeeper and proxy capabilities required for service provisioning and management of H.323-compliant networks. It conforms to the H.323 standard (version 1) for transmitting audio, video, and data conferencing data on an IP-based internetwork. The Multimedia Conference Manager Enhancements feature provides additional functionality for the gatekeeper endpoint. It provides:

- A way to force a disconnect on a specific call or all calls active on a particular gatekeeper.
- Enhanced output for the **show gatekeepers calls** command.

PAD French Enhancement

Extended dialog mode for packet assembler/disassembler (PAD) service signals is now available in the French language as well as English with the PAD French Enhancement. The French language service signals will be maintained in a table. When configured for French language via PAD parameter 6, the PAD service signals will map to this table, giving the appropriate French equivalent output. The internal table maintenance will be based upon the contents of the Annex-C/X.28 standard. Section 3.5/X.28 outlines Parameter 6 and how it relates to extended mode dialog in multiple languages.

PGM Router Assist

The PGM Router Assist feature allows Cisco routers to support the optimal operation of Pragmatic General Multicast (PGM). The PGM Reliable Transport Protocol itself is implemented on the hosts of the customer.

PGM is a reliable multicast transport protocol for applications that require ordered, duplicate-free, multicast data delivery from multiple sources to multiple receivers. PGM guarantees that a receiver in a multicast group either receives all data packets from transmissions and retransmissions, or can detect unrecoverable data packet loss. PGM is intended as a solution for multicast applications with basic reliability requirements. It is network-layer independent; the Cisco implementation of the PGM Router Assist feature supports PGM over IP.

Service Assurance Agent

The Service Assurance (SA) Agent is both an enhancement to and a new name for the Response Time Reporter (RTR) feature that was introduced in Cisco IOS Release 11.2. The feature allows you to monitor network performance by measuring key Service Level Agreement metrics such as response time, network resources, availability, jitter, connect time, packet loss, and application performance.

With Cisco IOS Release 12.0(5)T, the SA Agent provides new capabilities that enable you to:

- Monitor the Domain Name Server, DHCP Server, and DLSw peer stack and tunnel performance. Thresholds can be used to trigger additional collection of time delay statistics.
- Monitor network one-way delay variance (jitter) and packet loss.
- Monitor web server response time.

Subnetwork Bandwidth Manager

Resource Reservation Protocol (RSVP) is a signaling mechanism that supports request of specific levels of service such as reserved bandwidth from the network. RSVP and its service class definitions are largely independent of the underlying network technologies. This independence requires that a user define the mapping of RSVP onto subnetwork technologies.

The Subnetwork Bandwidth Manager (SBM) feature answers this requirement for RSVP in relation to IEEE 802-based networks. SBM specifies a signaling method and protocol for LAN-based admission control for RSVP flows. SBM allows RSVP-enabled routers and Layer 2 and Layer 3 devices to support reservation of LAN resources for RSVP-enabled data flows. The SBM signaling method is similar to that of RSVP itself.

SBM protocol entities have the following features:

- Reside in Layer 2 or Layer 3 devices.
- Can manage resources on a segment. A segment is a Layer 2 physical segment shared by one or more senders, such as a shared Ethernet or Token Ring wire.
- Can become candidates in a dynamic election process that designates one SBM as the segment manager. The elected candidate is called the Designated Subnetwork Bandwidth Manager (DSBM). The elected DSBM is responsible for exercising admission control over requests for resource reservations on a managed segment.

Tunnel Endpoint Discovery

IP Security Protocol (IPSec) requires a peer router to be statically configured before initiating an Internet Key Exchange (IKE). An IKE is necessary to encrypt and decrypt packets. The Cisco router crypto maps require the capability to dynamically determine the IPSec peer. The Tunnel Endpoint Discovery protocol automatically discovers remote tunnel endpoints and enables secure IPSec communications.

Dynamic Tunneling Endpoint Discovery allows IPSec to scale to larger networks by reducing the multiple encryptions, reducing the setup time, and allowing for simple configurations on participating peer routers. Each node has a simple configuration that defines the local network that the router is protecting and the IPSec transforms required, if any.

Voice over Frame Relay Queuing Enhancement

When there are multiple sets of flows being handled by weighted fair queueing (WFQ), the algorithm provides the low weight/reserved queued voice packets with higher priority but only until some of the other data packets have waited enough time and therefore it is now their turn to be dequeued. Even if interleaving is active, the WFQ algorithm will not dequeue a voice packet until these data packets are transmitted. This causes voice quality problems.

The solution consists of adding a special queue at the PVC level where all VoFR packets will be queued. This special queue runs in parallel to the WFQ and is serviced before any of the WFQs.

As of this release, reserved queues are no longer required to support VoFR.

X.25 Remote Failure Detection

Static routes are used over a packet-switched data network in order to reduce volume-based costs of the network. Until now, if two routers were connected by multiple X.25 links (a primary and a secondary), a router could not detect failure of the primary link. If a failure occurred, the data was not transferred to the second link because X.25 was unable to determine whether remote links were up or down. Therefore X.25 could not use an alternate connection to a destination.

The X.25 Remote Failure Detection feature is important for X.25 users because now, after a primary link failure, the router can establish a secondary link and continue sending data. This feature is a way for the router to detect a call failure and to use a secondary route to send subsequent packets to the remote destination, at the same time as making periodic attempts to reconnect to its primary link.

New Hardware Feature in Cisco IOS Release 12.0(4)T

Release 12.0(4)T supports a new hardware feature for the Cisco MC3810.

ISDN BRI Voice on the Cisco MC3810

With the optional BRI voice module (BVM) installed, the Cisco MC3810 multiservice access concentrator provides four ISDN Basic Rate Interface (BRI) ports for connection to ISDN PBXs (PINXs). The BVM has four ISDN BRI ports for voice traffic. Each BRI port supports two voice channels (ISDN B channels) and one signaling channel (ISDN D channel). The BRI voice ports have the following features:

- ITU I.430 BRI
- Full-duplex S/T interfaces supporting 2 bearer channels and 1 signaling channel (2B + D)
- Total of 8 simultaneous voice channels
- LT-S mode: Line termination of subscriber lines from PINX, with port configured as network termination (NT)
- LT-T mode: Line termination of an ISDN trunk from an ISDN exchange switch, with port configured as terminal equipment (TE)
- Each port individually configurable as NT or TE
- Configurable clock recovery and distribution

New Software Features in Cisco IOS Release 12.0(4)T

Release 12.0(4)T supports new software features for the Cisco MC3810.

QSIG Digit Forwarding on the Cisco MC3810

The QSIG Digit Forwarding feature extends support for dial-peer digit forwarding to ISDN PRI QSIG signaling calls on the Cisco MC3810. When ISDN PRI QSIG signaling was first introduced on the Cisco MC3810 in Cisco IOS Release 12.0(2)T, digit forwarding on POTS dial peers was not supported with ISDN PRI QSIG. In this release, digit forwarding is now supported with ISDN PRI QSIG.

Voice over Frame Relay Using FRF.11 and FRF.12

The Voice over Frame Relay (VoFR) capabilities that were introduced on the Cisco MC3810 multiservice access concentrator beginning with IOS Release 11.3 are now extended to the Cisco 2600, 3600, and 7200 series router platforms.

The following additional functionality is supported in Release 12.0(4)T:

- FRF.11-compliant Voice over Frame Relay trunking
- FRF.12-compliant end-to-end fragmentation

- Dynamic call switching and termination
- Permanent trunks over dynamic switched calls

When VoFR is implemented on a Cisco router, the router is able to carry voice traffic, such as telephone calls and faxes over a Frame Relay network.

This feature also adds support for full FRF.11 and FRF.12 compliance to the Cisco MC3810 and is backward-compatible with earlier versions of the Cisco MC3810, which used a fragmentation format based on an early draft version of FRF.12.

New Software Features in Cisco IOS Release 12.0(3)T

New software features are available for the Cisco MC3810 in Cisco IOS Release 12.0(3)T.

Annex G (X.25 over Frame Relay)

Annex G (X.25 over Frame Relay) facilitates the migration from an X.25 backbone to a Frame Relay backbone by permitting encapsulation of CCITT X.25/X.75 traffic within a Frame Relay connection. Annex G has been developed to accommodate the many Cisco customers in Europe, where X.25 still is a popular protocol. With Annex G, the process of transporting X.25 over Frame Relay has been simplified, by allowing direct X.25 encapsulation over a Frame Relay network.

This simple process is largely achieved using X.25 profiles (similar to dialer profiles), which were created to streamline the configuration of X.25 on a per-DLCI basis. X.25 profiles can contain any existing X.25 command and, once created and named, can be simultaneously associated with more than one Annex G DLCI connection, just using the profile name.

CDP Additions for Cisco IOS

The Cisco Discovery Protocol (CDP) is a media-independent device discovery protocol that runs on all Cisco-manufactured equipment, including routers, bridges, access servers, and switches. Each device sends periodic messages to a multicast address. Each device listens to the periodic messages sent by others in order to learn about neighboring devices and determine when their interfaces to the media go up or down. With CDP, network management applications can learn the device type and the SNMP agent address of neighboring devices. This process enables applications to send SNMP queries to neighboring devices.

CDP runs on all media that support Subnetwork Access Protocol (SNAP), including local-area network (LAN), Frame Relay, and Asynchronous Transfer Mode (ATM) media. CDP runs over the data link layer only. Therefore, two systems that support different network-layer protocols can learn about each other.

Each device configured for CDP sends periodic messages to a multicast address. Each device advertises at least one address at which it can receive SNMP messages. The advertisements also contain time-to-live, or holdtime, information, which indicates the time a receiving device should hold CDP information before discarding it.

Additions for Cisco Discovery Protocol (CDP) include a new **cdp advertise-v2** command and new output from **show cdp** commands

The benefits include, transparent support of X.25 encapsulation over the Frame Relay network; direct X.25 configurations on a per DLCI basis; multiple Annex G DLCIs can use the same X.25 profile; multiple logical X.25 SVCs per Annex G link, and the fact that Cisco routers already contain the functionality necessary to perform the framing and frame removal required by Annex G.

DLSw+ Enhanced Load Balancing

In a network with multiple capable paths, the DLSw+ Load Balancing Enhancements feature improves traffic load balancing between peers by distributing new circuits based on existing loads and the desired ratio.

For each capable peer (peers that have the lowest or equal cost specified), the DLSw+ Load Balancing feature calculates the difference between the desired and the actual ratio of circuits being used on a peer. It detects the path that is underloaded in comparison to the other capable peers and assigns new circuits to that path until the desired ratio is achieved.

DLSw+ Peer Clusters

The DLSw+ Peer Clusters feature reduces the explorer packet replication that typically occurs in a large DLSw+ Peer Group design, where there are multiple routers connected to the same LAN.

The DLSw+ Peer Clusters feature associates DLSw+ peers (that are connected to the same LAN) into logical groups. When the multiple peers are defined in the same peer group cluster, the DLSw+ Border Peer recognizes that it does not have to forward explorers to more than one member within the same peer group cluster.

DLSw+ RSVP Bandwidth Reservation

The DLSw+ RSVP Bandwidth Reservation feature allows DLSw+ to reserve network bandwidth for the DLSw+ TCP connection between DLSw+ peers.

Although it has been possible in the past to reserve bandwidth for a particular existing DLSw+ peer connection through the RSVP CLI support in Cisco IOS software, the CLI required prior knowledge of the TCP ports for which the reservation was being made. Because DLSw+ uses one well-known port and one randomly assigned port, the reservation could not be made until after the peer connection was active.

The DLSw+ RSVP feature permits new DLSw+ peer connections to automatically request bandwidth reservations upon connection, thereby removing the need for user intervention after the peer is connected. This feature assures the reservation will survive a network or device failure and that the DLSw+ traffic carried over a TCP connection is not affected by congestion.

Fancy Queuing on Frame Relay for Cisco HDLC

In previous releases, when the **voice-encap** option was configured on Frame Relay or Cisco HDLC, all fancy queuing (such as weighted fair queuing, custom queuing, and priority queuing) on the interface was disabled, and queuing was handled on a first-come first-served (FCFS) basis. In this release, new enhancements have been made to support fancy queuing on Frame Relay and Cisco HDLC.

For Frame Relay, a new interface command, **frag-pre-queuing**, has been added that allows you to set the queuing to be performed after the data segmentation. The command is available for Frame Relay interfaces only. The syntax for this new command is:

frag-pre-queuing

no frag-pre-queuing

By default, this command is enabled, which allows only FCFS queuing at the interface level. If you enter **no frag-pre-queuing**, you can configure weighted fair queuing, custom queuing, or priority queuing at the interface level. Note that if you enter **no frag-pre-queuing**, you still must explicitly configure the fancy queuing type on the interface.

For HDLC encapsulation, the queuing now takes place after segmentation when the **voice-encap** option is entered. Weighted fair queuing, custom queuing, and priority queuing are now supported on an interface configured for Cisco HDLC.

Local Voice Busy Out

The local voice busyout feature for the Cisco MC3810 is designed to busy out the trunks assigned to a PVC whose pipe is broken so that the PBX will not attempt to seize the circuit. This allows the PBX to route or reroute a given call based on the actual availability of trunks.

This feature is different from the concept of busy-back. Busy-back refers to the signal sent from within the network to the calling party that indicates a busy (or congested) state anywhere along the route, up to and including the condition of the called part. When the number of available DSPs is less than the number of incoming trunks from a PBX, a call from the PBX will connect to dead air. The capability to provide a busy-back signal because no DSPs are available is not supported on the Cisco MC3810 as part of this feature.

Multimedia Conference Manager

Use the Multimedia Conference Manager to enable your current internetwork to route bit-intensive data such as audio telephony, video and audio telephony, and data conferencing using existing telephone and ISDN links, without degrading the network's current level of service. The Multimedia Conference Manager feature provides H.323 application options previously unavailable. Using Multimedia Conference Manager, you can implement H.323-compliant applications on existing networks in an incremental fashion without upgrades.

This feature also provides networking capabilities, including:

- A means to implement Quality of Service (QoS), which is required for the successful deployment of H.323 applications.
- Interzone routing in the E.164 address space. When using H.323-ID format addresses, interzone routing is done through domain names.

The Multimedia Conference Manager feature provides network administration mechanisms to support H.323 applications without impacting the mission critical applications running on today's networks. Multimedia Conference Manager is implemented on Cisco IOS software. Multimedia Conference Manager provides the network administrator with these abilities:

- Identify H.323 traffic and apply appropriate policies
- Limit H.323 traffic on the local-area network (LAN) and wide-area network (WAN)
- Provide user accounting for records based on service utilization
- Insert QoS for the H.323 traffic generated by applications such as Voice over IP (VoIP), data conferencing, and video conferencing
- Implement security for H.323 communications

Multimedia Conference Manager has two principal functions: *gatekeeper* and *proxy*. This document describes the value of the Multimedia Conference Manager gatekeeper and proxy functions for end-to-end implementation of H.323-compliant multimedia applications. These functions are unique to Multimedia Conference Manager. Similar robust features are currently not available in other vendor solutions.

Gatekeeper subsystems provide:

- User authorization where authorization, authentication, and accounting (AAA) account holders are permitted to register and use the services of Multimedia Conference Manager
- Accounting using AAA call detail records
- Zone bandwidth management to limit the number of active sessions
- H.323 call routing
- Address resolution

Starting with Cisco IOS Releases 11.3(6)Q and 11.3(7)NA and later, you can configure Cisco gatekeepers to use the Cisco Hot Standby Routing Protocol (HSRP), so that when one gatekeeper fails, the standby gatekeeper assumes its role.

Proxy subsystems provide:

- H.323 traffic consolidation
- Tight bandwidth controls
- QoS mechanisms such as IP Precedence and RSVP
- Secure communication over extranets

Priority Queuing Support Enhancement for Cisco MC3810-IGX Interworking

When the Cisco MC3810-IGX Interworking feature for the Cisco MC3810 was introduced in Cisco IOS Release 12.0(2)T, the FTC trunk could only support first-come-first-served queuing. In Cisco IOS Release 12.0(3)T, the Cisco MC3810-IGX Interworking feature has been enhanced to support priority queuing, custom queuing, and generic traffic shaping. Standard IOS commands for priority queuing, custom queuing, and generic traffic shaping are supported.

Note The Cisco MC3810-IGX Interworking feature does not support weighted fair queuing.

Process MIB

The addition of the CISCO-PROCESS-MIB and changes to the CISCO-MEMORY-POOL-MIB allow the retrieval of additional CPU and memory statistics and their reporting by SNMP. The CISCO-PROCESS-MIB provides CPU 5-second, 1-minute, and 5-minute statistics. In addition, this MIB provides CPU utilization and memory allocation/deallocation statistics for each process on each CPU listed in the CISCO-PROCESS-MIB.

The CISCO-PROCESS-MIB is enabled when the first SNMP command is configured. The background statistics collection for VIP cards and the master CPU occurs even if the SNMP subsystem is not initialized.

Response Time Reporter Enhancements

The Response Time Reporter (RTR) feature allows you to monitor network performance, network resources, and applications by measuring response times and availability. RTR statistics can be used to perform troubleshooting, problem notifications and pre-problem analysis. The RTR enhancements extend IP support, such as Type of Service, and allow you to measure various types of IP traffic, such as UDP, TCP, and HTTP.

SNMP v3

Simple Network Management Protocol version 3 (SNMPv3) addresses issues related to the large scale deployment of SNMP for configuration, accounting, and fault management. Currently, SNMP is predominantly used for monitoring and performance management. The primary goal of SNMPv3 is to define a secure version of the SNMP protocol. SNMPv3 also facilitates remote configuration of the SNMP entities which make remote administration of SNMP entities a much simpler task. SNMPv3 builds on top of SNMPv1 and SNMPv2 to provide a secure environment for the management of systems and networks.

SNMPv3 provides an identification strategy for SNMP devices to facilitate communication only between known SNMP entities. Each SNMP device has an identifier called the SNMP EngineID which is a copy of SNMP. Each SNMP message contains an SNMP EngineID. SNMP communication is possible only if an SNMP entity knows the identity of its peer SNMP device.

SNMPv3 also contains a security model or security strategy that exists between an SNMP user and the SNMP group to which the user belongs. A security model may define the security policy within an administrative domain or an intranet. The SNMPv3 protocol consists of the specification for the User-Based Security Model (USM).

Definition of security goals where the goals of message authentication service include the following protection strategies:

- **Modification of Information** or protection against some unauthorized SNMP entity altering in-transit SNMP messages generated on behalf of an authorized principal
- **Masquerade** or protection against attempting management operations not authorized for some principal by assuming the identity of another principal that has the appropriate authorizations
- **Message Stream Modification** or protection against messages getting maliciously re-ordered, delayed, or replayed in order to effect unauthorized management operations
- **Disclosure** or protection against eavesdropping on the exchanges between SNMP engines. Three different types of communication mechanisms are available for this protection strategy. They are:
 - Communication without authentication and privacy (NoAuthNoPriv)
 - Communication with authentication and without privacy (AuthNoPriv)
 - Communication with authentication and privacy (AuthPriv)

New Hardware Feature in Cisco IOS Release 12.0(2)T

The following section describes a new hardware feature that the Cisco MC3810 supports in Cisco IOS Release 12.0(2)T.

Multiflex Trunk Module with Integrated BRI Interface

This module provides all the same functionality as the existing MFT module but supplies an additional interface for BRI data backup. The BRI module provides an S/T interface only, which can be used for European deployment. An inexpensive NT1 can be used to provide connectivity to ISDN services in the United States.

New Software Features in Cisco IOS Release 12.0(2)T

The following sections describe new software features that the Cisco MC3810 supports in Cisco IOS Release 12.0(2)T.

Call Detail Records

The Call Detail Records (CDR) feature provides the ability to track records for calls being processed by the Cisco MC3810. CDR data is collected for all POTS call attempts, and the data is collected for each call leg and also by each Cisco MC3810 involved in the call session.

The call legs for which CDR data is collected are:

- POTS lines if the call both originates and terminates on the same Cisco MC3810
- POTS line and the trunk for calls that either originate or terminate on another Cisco MC3810
- Two trunks in the case of a tandem call

CDR data is stored in an internal buffer on the Cisco MC3810 at call termination time, and becomes available to be polled periodically by the Cisco network management system (NMS) applications. The CDR/call history entries cannot be retrieved after a power loss or a software reload on the Cisco MC3810, so the Cisco NMS is considered the final destination for storing and tailoring the CDR call history table into report form.

Cisco MC3810 – IGX 8400 Interworking

For locations terminating a large number of voice channels, the Cisco IGX provides scalability for a network design in which connections can be made between remote Cisco MC3810 concentrators.

Cisco MC3810 – IGX 8400 Interworking allows the Cisco IGX 8400 to be used as a larger, central site access device that can do the following:

- Support greater numbers of voice channels
- Connect PBXs and larger routers
- Provide Quality of Service
- Provide an integrated network topology view via StrataView+
- Extend the segmented connection type to the Cisco MC3810. There are two connection segment types:
 - A connection within the IGX cloud.
 - A connection segment on the Cisco MC3810 from the concentrator's network port to the concentrator's user port. This segmented connection applies to both data and voice.

Common Channel Signaling Features

Cisco IOS Release 12.0(2)T introduces support for three new Common Channel Signaling (CCS) features that are described in the following sections.

QSIG PRI Voice Switching

This release adds support for QSIG, which is a Private Integrated Services Network Exchange (PINX) signaling protocol that provides connectivity between PINXs in a corporate environment. Using the ISDN PRI QSIG Voice Signaling feature, the Cisco MC3810 can be used as an access device to allow corporate PINX networks at remote sites to be interconnected via a data network (WAN). The Cisco MC3810 QSIG software allows incoming voice calls from a PINX to be routed across the WAN to a destination PINX. The Cisco MC3810 is responsible for establishing the necessary connection to the peer Cisco MC3810 across the WAN where both signaling and voice packets can be transported on behalf of the PINXs.

The Cisco MC3810 also performs intelligent functions such as call routing to other Cisco MC3810 concentrators in the WAN (for example, tandem switching) and interworking with other types of signaling already supported on the Cisco MC3810. Transport of Supplementary Services transparent through the network is also supported.

CCS Frame Forwarding

This release adds support for CCS frame forwarding, which enables the Cisco MC3810 Digital Voice Module (DVM) to connect two CCS Private Integrated Services Network Exchanges (PINXs) without having to interpret CCS signaling information for call processing. This feature provides transparent CCS frame forwarding for PBXs that use proprietary forms of CCS. CCS frame forwarding forwards CCS messages by encapsulating them in either Frame Relay or ATM.

With CCS frame forwarding, the voice connections between PBXs over the network are configured as point-to-point links. Voice Activity Detection (VAD) detects when a call is in progress.

CCS Transparent Signaling

This release adds support for transparent Common Channel Signaling, which provides point-to-point PINX connection capability to Cisco MC3810 digital voice module (DVM) interfaces when the PINX does not support QSIG, or when the PINX has a proprietary solution.

Default Routes

The default routes feature can be used to reduce the number of dial peers to be configured. It is designed for situations where, for example, the ports on a Cisco MC3810 have extension numbers, but all calls not terminating on those extensions should be sent to a central Cisco MC3810, usually for forwarding to a PBX. Instead of defining all the number blocks that can be called, the default route is a dial peer that automatically matches any call not terminated by other dial peers on the Cisco MC3810.

Facility Data Link (FDL) Capability on the Multiflex Trunk Module

This release adds support for Facility Data Link (FDL) on the MFT module. You can specify the FDL format to use as either the ANSI T1.403 standard, or the AT&T TR54016 standard, or both.

G.726 (ADPCM)

This newly supported vocoder provides higher reliability for digit transport in networks with greater hop counts and can be used to support lower-speed modems (up to 9.6 kbps).

Multi-Length Dial Patterns

Dial strings of multiple lengths can now be supported in the same network and on the same Cisco MC3810.

OPX Ring-Through

This feature allows a port on the Cisco MC3810 to act like an “Off-Premise Extension” to the PBX. When the PBX attempts to make a connection to the remote voice port on a Cisco MC3810, OPX Ring-through allows the PBX to reroute the call if there is no answer.

Preference-Based Hunt Group

The Multichassis hunt group has been enhanced to allow the preference command to be used to select remote dial peers before local dial peers using the priority values. This greatly extends the capability to support on-net to off-net rerouting of calls and alternate call center applications.

Existing IOS Features Supported on the Cisco MC3810 in Cisco IOS Release 12.0(2)T

The Cisco MC3810 supports the following existing IOS features in Cisco IOS Release 12.0(2)T:

- Bisync
- Polled Async
- PPP over ATM

For more information on Bisync and Polled Async, refer to the Cisco IOS Release 12.0 *Bridging and IBM Networking Configuration Guide*. For more information on PPP Over ATM, refer to the Cisco IOS Release 12.0 *Wide-Area Networking Configuration Guide*.

Important Notes

This section contains important information about the use of your Cisco IOS Release 12.0 T software.

The last maintenance release of the 12.0T release train is 12.0(7)T. The migration path for customers needing bug fixes for the 12.0 T features is 12.1 Mainline. 12.1 Mainline has the complete feature content of 12.0T and this release will eventually reach General Deployment (GD).

The last maintenance release was renamed from 12.0(6)T to 12.0(7)T to reflect that 12.0(7)T has all the bug fixes of 12.0(7) mainline. 12.0 T is a superset of 12.0 mainline, hence any defect fixed in 12.0 mainline is also fixed in 12.0 T. The set of features for 12.0(6)T is the same as that of 12.0(7)T. There was no change in the feature content of the release. The release was renamed so that the releases would be consistent with Cisco’s release process.

Cisco IOS Syslog Failure

Certain versions of Cisco IOS software can fail or hang when they receive invalid User Datagram Protocol (UDP) packets sent to their *syslog* ports (port 514). At least one commonly-used Internet scanning tool generates packets that can cause such problems. This fact has been published on public Internet mailing lists, which are widely read both by security professionals and by security crackers. This information should be considered in the public domain.

Attackers can cause Cisco IOS devices to repeatedly fail and reload, resulting in a completely disabled Cisco IOS device that will need to be reconfigured by its administrator. Some Cisco IOS devices have been observed to hang instead of failing when attacked. These devices do not recover until they are manually restarted by reset or power cycling. An administrator must personally visit an attacked, hung device to restart it, even if the attacker is no longer actively sending any traffic. Some devices have failed without providing stack traces; some devices might indicate that they were “restarted by power-on,” even when that is not the case.

Assume that any potential attacker is likely to know about this problem and the ways to exploit it. An attacker can use tools available to the public on the Internet. An attacker does not need to write any software to exploit the problem. Minimal skills and no special equipment are required.

Despite Cisco specifically inviting such reports, Cisco has received no actual reports of malicious exploitation of this problem.

This vulnerability notice was posted on Cisco’s World Wide Web site:

<http://www.cisco.com/warp/public/770/iossyslog-pub.shtml>

This information was also sent to the following e-mail and Usenet news recipients:

- cust-security-announce@cisco.com
- bugtraq@netspace.org
- first-teams@first.org (includes CERT/CC)
- first-info@first.org
- cisco@spot.colorado.edu
- comp.dcom.sys.cisco
- nanog@merit.edu

Affected Devices and Software Versions

Vulnerable devices and software versions are specified in Table 6 on page 39. Affected versions include 11.3AA, 11.3DB, and all 12.0 versions (including 12.0 mainline, 12.0 S, 12.0 T, and any other regular releases whose number starts with 12.0), up to the repaired releases listed in Table 6. Cisco is correcting the problem in certain special releases and will correct it in future maintenance and interim releases. See the “Software Versions and Fixes” section on page 39 for details. Cisco intends to provide fixes for all affected Cisco IOS variants.

No particular configuration is needed to make a Cisco IOS device vulnerable. It is possible to filter out attack traffic by using access lists. See the “Workarounds” section on page 38 for techniques. However, except at Internet firewalls, the appropriate filters are not common in customer configurations. Carefully evaluate your configuration before assuming that any filtering protects you against this attack.

The most commonly used or asked-about products are listed below. If you are unsure whether your device is running classic Cisco IOS software, log in to the device and issue the **show version** command. Cisco IOS software will identify itself simply as “IOS” or “Internetwork Operating

System Software”. Other Cisco devices will not have the **show version** command, or they will identify themselves differently in their output. The most common Cisco devices that run Cisco IOS software include the following:

- Cisco routers in the AGS/MGS/CGS/AGS+, IGS, RSM, 800,ubr900, 1000, 2500, 2600, 3000, 3600, 3800, 4000, 4500, 4700, AS5200, AS5300, AS5800, 6400, 7000, 7200 (including the ubr7200), 7500, and 12000 series
- Most recent versions of the LS1010 ATM switch
- Some versions of the Catalyst 2900XL LAN switch
- Cisco DistributedDirector

Affected software versions, which are relatively new, are not necessarily available on every device listed above. If you are not running Cisco IOS software, you are not affected by this problem.

The following Cisco devices are *not* affected:

- 700 dialup routers (750, 760, and 770 series)
- Catalyst 1900, 2800, 2900, 3000, and 5000 LAN switches are not affected, except for some versions of the Catalyst 2900XL. However, optional router modules running Cisco IOS software in switch backplanes, such as the RSM module for the Catalyst 5000 and 5500, are affected.
- WAN switching products in the IGX and BPX lines
- MGX (formerly known as the AXIS shelf)
- Host-based software
- Cisco PIX Firewall
- Cisco LocalDirector
- Cisco Cache Engine

This problem has been assigned Cisco caveat ID CSCdk77426.

Solution

Cisco offers free software updates to correct this problem for all affected customers—regardless of their contract status. However, because this vulnerability information has been disseminated by third parties, Cisco has released this notice before updates are available for all software versions. Table 6 gives Cisco’s projected fix dates.

Make sure your hardware had adequate RAM to support the new software before installing it. The amount of RAM is seldom a problem when you upgrade within a major release (say, from 11.2(11)P to 11.2(17)P), but it is often a factor when you upgrade between major releases (say, from 11.2 P to 11.3 T).

Because fixes will be available for all affected releases, this problem will rarely, if ever, require an upgrade to a new major release. Cisco recommends very careful planning for any upgrade between major releases. Make certain no known bugs will prevent the new software from working properly in your environment.

Further upgrade planning assistance is available on Cisco’s World Wide Web site at:

<http://www.cisco.com>

If you have a service contract, you should obtain new software through your regular update channels (generally via Cisco’s World Wide Web site). You can upgrade to any software release, but you must remain within the boundaries of the feature sets you have purchased.

If you do not have a service contract, you may upgrade to obtain only the bug fixes; Cisco is not offering upgrades to versions newer than the versions required to resolve the defects. In general, you will be restricted to upgrading to a version represented within a single row of Table 6 on page 39. However, Cisco will make an exception to this policy when no upgrade within the same row is available in a timely manner. Obtain updates by contacting one of the following Cisco Technical Assistance Centers (TACs):

- +1 800 553 2447 (toll-free from within North America)
- +1 408 526 7209 (toll call from anywhere in the world)
- tac@cisco.com

Give the URL of this notice (<http://www.cisco.com/warp/public/770/iossyslog-pub.shtml>) as evidence for a free update. Non-contract customers must request free updates through the TAC. Please do not contact either "psirt@cisco.com" or "security-alert@cisco.com" for software updates.

Workarounds

You can work around this problem by preventing any affected Cisco IOS device from receiving or processing UDP datagrams addressed to its port 514. This can be done either using packet filtering on surrounding devices, or by using input access list filtering on the affected Cisco IOS device itself.

If you use an input access list, apply that list to all interfaces to which attackers might be able to send datagrams. Interfaces include—not only physical LAN and WAN interfaces—but virtual subinterfaces of those physical interfaces, as well as virtual interfaces and interface templates corresponding to GRE, L2TP, L2F, and other tunneling protocols.

The input access list must block traffic destined for UDP port 514 at any of the Cisco IOS device's own IP addresses, as well as at any broadcast or multicast addresses on which the Cisco IOS device might be listening. Be sure to block both old-style "all-zeros" broadcasts and new-style "all-ones" broadcasts. It is not necessary to block traffic being forwarded to other hosts; only traffic actually addressed to the Cisco IOS device is of interest.

No single input access list works in all configurations. Know the effect of your access list in your specific configuration before activating it.

The following example shows a possible access list for a three-interface router, along with the configuration commands needed to apply the list. The example assumes input filtering is not needed, other than as a workaround for this problem:

```
! Deny all multicasts, and all unspecified-net broadcasts, to port 514
access-list 101 deny udp any 224.0.0.0 31.255.255.255 eq 514
! Deny old-style unspecified-net broadcasts
access-list 101 deny udp any host 0.0.0.0 eq 514
! Deny network-specific broadcasts. This example assumes that all of
! the local interfaces are on the class B network 172.16.0.0, subnetted
! everywhere with mask 255.255.255.0. This will differ from network
! to network. Note that we block both new-style and old-style broadcasts.
access-list 101 deny udp any 172.16.0.255 0.0.255.0 eq 514
access-list 101 deny udp any 172.16.0.0 0.0.255.0 eq 514
! Deny packets sent to the addresses of our own network interfaces.
access-list 101 deny udp any host 172.16.1.1 eq 514
access-list 101 deny udp any host 172.16.2.1 eq 514
access-list 101 deny udp any host 172.16.3.3 eq 514
! Permit all other traffic (default would be to deny)
access-list 101 permit ip any any

! Apply the access list to the input side of each interface
interface ethernet 0
ip address 172.16.1.1 255.255.255.0
ip access-group 101 in
```

```

interface ethernet 2
ip address 172.16.2.1 255.255.255.0
ip access-group 101 in

interface ethernet 3
ip address 172.16.3.3 255.255.255.0
ip access-group 101 in

```

Listing all possible addresses—especially all possible broadcast addresses—to which attack packets can be sent is complicated. If you do not need to forward any legitimate syslog traffic received on an interface, you can block all syslog traffic arriving on that interface. Remember that blocking will affect traffic routed through the Cisco IOS device as well as traffic destined to the device; if the IOS device is expected to forward syslog packets, you will have to do the detailed filtering. Because input access lists impact system performance, install them with caution—especially on systems running very near their capacity.

Software Versions and Fixes

Many Cisco software images have been or will be specially reissued to correct this problem. For example, Release 12.0(2) is vulnerable, as are interim Releases 12.0(2.1) through 12.0(2.3). The first fixed interim version of Release 12.0 mainline software is Release 12.0(2.4). However, a special Release 12.0(2a), contains only the fix for this problem and does not include any other bug fixes from later 12.0 interim releases.

If you are running Release 12.0(2) and want to fix this problem without risking possible instability presented by installing the Release 12.0(2.4) interim release, you can upgrade to Release 12.0(2a). Release 12.0(2a) is a “code branch” from the Release 12.0(2) base, which will merge back into the 12.0 mainline at Release 12.0(2.4).

Special releases, like Release 12.0(2a), are one-time, spot fixes, and they will not be maintained. Thus, the upgrade path from Release 12.0(2a) is to 12.0(3).

Table 6 specifies information about affected and repaired software versions.

Note All dates within this table are subject to change.

Table 6 Affected and Repaired Software Versions

Cisco IOS Major Release	Description	Special Fix ¹	First Fixed Interim Release ²	Fixed Maintenance Release ³
Unaffected Releases				
11.2 and earlier—all variants	Unaffected early releases (no syslog server)	Unaffected	Unaffected	Unaffected
11.3, 11.3T, 11.3DA, 11.3MA, 11.3NA, 11.3WA, 11.3(2)XA	11.3 releases without syslog servers	Unaffected	Unaffected	Unaffected
Releases based on 11.3				
11.3AA	11.3 early deployment for Cisco AS58xx	11.3(7)AA2, 8-JAN-1999 ⁴	11.3(7.2)AA	11.3(8)AA, 15-FEB-1999
11.3DB	11.3 for Cisco NRP routing blade in Cisco 6400 xDSL DSLAM			11.3(7)DB2, 18-JAN-1999

Important Notes

Table 6 Affected and Repaired Software Versions (continued)

Cisco IOS Major Release	Description	Special Fix ¹	First Fixed Interim Release ²	Fixed Maintenance Release ³
Releases based on 12.0				
12.0	12.0 Mainline	12.0(2a), 8-JAN-1999	12.0(2.4)	12.0(3), 1-FEB-1999
12.0 T	12.0 new technology early deployment	12.0(2a)T1, 11-JAN-1999	12.0(2.4)T	12.0(3)T, 15-FEB-1999
12.0S	ISP support; Cisco 7200, RSP, GSR		12.0(2.3)S, 27-DEC-1998	12.0(2)S ⁵ , 18-JAN-1999
12.0DB	12.0 for Cisco 6400 universal access concentrator node switch processor (lab use)			12.0(2)DB, 18-JAN-1999
12.0(1)W	12.0 for Catalyst 8500 and LS1010	12.0(1)W5(5a) and 12.0(1a)W5(5b) (LS1010 platform only)	12.0(1)W5(5.15)	12.0(1)W5(6) (platform support for Catalyst 8540M will be in 12.0(1)W5(7))
12.0(0.6)W5	One-time early deployment for CH-OC12 module in Catalyst 8500 series switches	Unaffected; one-time release	Unaffected	Unaffected; general upgrade path is via 12.0(1)W5 releases
12.0(1)XA3	Short-life release; merged to 12/0 T at 12.0(2)T	Obsolete	Merged	Upgrade to 12.0(2a)T1 and/or to 12.0(3)T
12.0(1)XB	Short-life release for Cisco 800 series; merged to 12.0 T and 12.0(3)T	12.0(1)XB1	Merged	Upgrade to 12.0(3)T
12.0(2)XC	Short-life release for new features in Cisco 2600, Cisco 3600, ubr7200, ubr900 series; merged to 12.0 T at 12.0(3)T	12.0(2)XC1, 7-JAN-1999	Merged	Upgrade to 12.0(3)T
12.0(2)XD	Short-life release for ISDN voice features; merged to 12.0 T at 12.0(3)T	12.0(2)XD1, 18-JAN-1999	Merged	Upgrade to 12.0(3)T
12.0(1)XE	Short-life release	12.0(2)XE, 18-JAN-1999	Merged	Upgrade to 12.0(3)T

1 A special fix is a one-time release that provides the most stable immediate upgrade path.

2 Interim releases are tested less rigorously than regular, maintenance releases; interim releases might contain serious bugs.

3 Fixed maintenance releases are on a long-term upgrade path. Other long-term upgrade paths also exist.

4 All dates in this table are estimates, subject to change.

5 This entry is not a misprint. Release 12.0(2.3)S is available before Release 12.0(2)S in which the problem is fixed.

Serial Interface Command Change in Cisco IOS Release 12.0(2)T

In Cisco IOS Release 11.3(1) MA, serial 2 was a valid port number. Beginning with Cisco IOS Release 12.0(1), the **interface serial 2** designation on the Cisco MC3810 is no longer valid. Depending on the application, you enter different designations for this interface as follows:

- If configuring Voice over Frame Relay or Voice over HDLC, enter **interface serial 0:x**, where *x* represents the channel group number configured with the **channel-group** controller configuration command.

- If configuring Voice over ATM, first enter the **mode atm** command in controller configuration mode, which creates logical interface ATM0. Then, enter **interface atm0** to configure the interface.

Deprecated MIBs

Old Cisco Management Information Bases (MIBs) will be replaced in a future release. OLD-CISCO-* MIBs are currently being migrated into more scalable MIBs—without affecting existing Cisco IOS products or NMS applications. You can update from deprecated MIBs to the replacement MIBs as shown in the following table.

Table 7 **Deprecated MIBs**

Deprecated MIB	Replacement
OLD-CISCO-APPLETALK-MIB	RFC1243-MIB
OLD-CISCO-CHASSIS-MIB	ENTITY-MIB
OLD-CISCO-CPUK-MIB	In Development
OLD-CISCO-DECNET-MIB	NA
OLD-CISCO-ENV-MIB	CISCO-ENVMON-MIB
OLD-CISCO-FLASH-MIB	CISCO-FLASH-MIB
OLD-CISCO-INTERFACES-MIB	IF-MIB CISCO-QUEUE-MIB
OLD-CISCO-IP-MIB	NA
OLD-CISCO-MEMORY-MIB	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
OLD-CISCO-TCP-MIB	CISCO-TCP-MIB
OLD-CISCO-TS-MIB	NA
OLD-CISCO-VINES-MIB	CISCO-VINES-MIB
OLD-CISCO-XNS-MIB	NA

Using the Cisco MC3810 with QSIG or BRI

Serial port 1 is restricted to DCE operation when the following occurs:

- QSIG is enabled.
- BRI voice module (BVM) is installed and BRI is enabled.
- BRI S/T backup port is installed and enabled on the MFT.

Using the Cisco MC3810 with the PSTN

This section includes important notes regarding use of the Cisco MC3810 with the Public Switched Telephone Network (PSTN).

Connections to the PSTN

Exercise care when connecting switched voice ports on the Cisco MC3810 directly to the PSTN because improper configurations can expose the corporate network to telephone fraud.

Switched Access from the PSTN

The Cisco MC3810 can connect a user from the PSTN directly to the corporate wide-area telephone network. You can configure the Cisco MC3810 as a phone switch that can switch a user to any location in that network, even to remote locations that are connected again to another PSTN. However, the Cisco MC3810 does not provide any mechanism to restrict users from calling after they are connected. Without proper network design, this condition could result in the unauthorized use of the corporate network for making calls at the corporation's expense. To prevent this from occurring, Cisco does not recommend connecting a switched voice interface on the Cisco MC3810 directly to the PSTN. Instead, it should be connected to a PBX that implements a security scheme that prevents unauthorized use.

Non-Switched Calls

The same opportunity for illicit use does not exist for non-switched call types such as pass-through connections, although the possibility for fraud does exist at the direct contact point. Pass-through calls create a path to only a single location specified by the network administrator. For example, a pass-through connection might be used to pass a trunk from a PBX to the PSTN. In this case, the trunk on the PBX always passes straight through the Cisco MC3810 to the PSTN. As a result, the necessary security is provided by the PBX.

Caveats

Caveats describe unexpected behavior or defects in Cisco IOS software releases. For information on caveats in Cisco IOS Release 12.0 T, refer to the *Caveats for Cisco IOS Release 12.0 T* document.

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

For information on caveats in Cisco IOS Release 12.0, please refer to the *Caveats for Cisco IOS Release 12.0* document, which lists severity 1 and 2 caveats, and is located on CCO and the Documentation CD-ROM. Severity 1 caveats are the most serious caveats; severity 2 caveats are less serious.

Note If you have an account with CCO, you can use Bug Navigator II to find caveats of any severity for any release. From the CCO home page, log in and click on this path: **Software Center: Cisco IOS Software: Cisco IOS Bug Toolkit: Cisco Bug Navigator II**. You can also find Bug Navigator II at <http://www.cisco.com/support/bugtools>

Related Documentation

The following sections describe the documentation available for the Cisco MC3810. Typically, 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 the documents listed in the following sections:

- Release-Specific Documents, page 43
- Platform-Specific Documents, page 43
- Feature Modules, page 44
- Cisco IOS Software Documentation Set, page 44

Release-Specific Documents

The following documents are specific to or support Cisco IOS Release 12.0(7)T. They are located on CCO and the Documentation CD-ROM:

- *Release Notes for Cisco IOS Release 12.0*

To reach the cross-platform *Release Notes for Cisco IOS Release 12.0* on CCO, follow this path, beginning under the **Service & Support** heading:

Technical Documents: Documentation Home Page: Cisco IOS Software Configuration: Cisco IOS Release 12.0: Release Notes: Cross-Platform Release Notes

To reach the cross-platform *Release Notes for Cisco IOS Release 12.0* on the Documentation CD-ROM, follow this path:

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

To reach these documents, refer to the Service & Support section at this path on CCO:

Technical Documents

- Caveats document

The *Caveats for Cisco IOS Release 12.0 T* document contains caveats applicable to all platforms for all maintenance releases of Cisco IOS Release 12.0 T.

To reach the caveat document on CCO, follow this path, beginning under the **Service & Support** heading:

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

To reach the caveat document on the Documentation CD-ROM, follow this path:

Cisco Product Documentation: Cisco IOS Software Configuration: Cisco IOS 12.0: Caveats: Caveats for Cisco IOS Release 12.0 T

Note If you have an account with CCO, you can use Bug Navigator II to find caveats of any severity for any release. From the CCO home page, log in and click on this path: **Software Center: Cisco IOS Software: Cisco IOS Bug Toolkit: Cisco Bug Navigator II**. You can also find Bug Navigator II at <http://www.cisco.com/support/bugtools>

Platform-Specific Documents

The documents listed below are available for the Cisco MC3810. These documents are also available online at Cisco Connection Online (CCO) and on the Documentation CD-ROM.

- *Cisco MC3810 Multiservice Access Concentrator Hardware Installation Guide*
- *Quick Start Guide: Cisco MC3810 Multiservice Access Concentrator Installation and Startup*
- *Cisco MC3810 Multiservice Access Concentrator Regulatory Compliance and Safety Information*
- *Installing and Removing Field-Replaceable Units in the Cisco MC3810 Multiservice Access Concentrator*
- *Cisco Redundant Power System Hardware Installation Guide*
- *Cisco MC3810 Multiservice Access Concentrator Software Configuration Guide*

To reach Cisco MC3810 documentation on CCO, follow this path, beginning under the **Service & Support** heading:

Technical Documents: Documentation Home Page: Access Servers and Access Routers: Multiservice Access Concentrators

To reach Cisco MC3810 documentation on the Documentation CD-ROM, follow this path:

Cisco Product Documentation: Access Servers and Access Routers: Multiservice Access Concentrators

Feature Modules

Feature modules describe new features supported by Cisco IOS 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 features modules are available online only. The feature module information is incorporated into the next printing of the Cisco IOS documentation set.

To reach the feature modules on CCO, follow this path, beginning under the **Service & Support** heading:

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

To reach the feature modules on the Documentation CD-ROM, follow this path:

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. These documents are 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 two books: a configuration guide and a corresponding command reference. Chapters in a configuration guide describe protocols, configuration tasks, Cisco IOS software functionality, and comprehensive configuration examples. Chapters in a command reference provide complete command syntax information. Each configuration guide can be used 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 and the Documentation CD-ROM, two master hot-linked documents provide information for the Cisco IOS software documentation set: configuration guides and command references.

To reach these documents on CCO, follow this path, beginning under the **Service & Support** heading:

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

To reach these documents on the Documentation CD-ROM, follow this path:

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

Cisco IOS 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.

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

To reach the Cisco IOS documentation set from CCO, click on this path, beginning under the **Service & Support** heading:

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

To reach the Cisco IOS documentation set on the Documentation CD-ROM, click on this path:

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> 	Configuration Fundamentals Overview Cisco IOS User Interfaces File Management System Management

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

Books	Chapter Topics
<ul style="list-style-type: none"> • <i>Bridging and IBM Networking Configuration Guide</i> • <i>Bridging and IBM Networking Command Reference</i> 	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> 	Dial-In Port Setup Dial-In Terminal Services Dial-on-Demand Routing (DDR) Dial Backup Dial-Out Modem Pooling Large-Scale Dial Solutions Cost-Control Solutions ISDN X.25 over ISDN VPDN 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> 	Interface Configuration Overview
<ul style="list-style-type: none"> • <i>Network Protocols Configuration Guide, Part 1</i> • <i>Network Protocols Command Reference, Part 1</i> 	IP Addressing IP 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> 	AppleTalk Novell IPX
<ul style="list-style-type: none"> • <i>Network Protocols Configuration Guide, Part 3</i> • <i>Network Protocols Command Reference, Part 3</i> 	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 Paths for IP Networks Virtual LAN (VLAN) Switching and Routing

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

Books	Chapter Topics
<ul style="list-style-type: none"> • <i>Wide-Area Networking Configuration Guide</i> • <i>Wide-Area Networking Command Reference</i> 	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 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> 	Classification Scheduling Packet Drop Traffic Shaping ATM QoS SNA QoS Line Protocols
<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> 	

Service and Support

For service and support for a product purchased from a reseller, contact the reseller. Resellers offer a wide variety of Cisco service and support programs, which are described in the section “Service and Support” in the information packet shipped with your product.

Note If you purchased your product from a reseller, you can reach 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 reach the following URL, which contains links and helpful tips on configuring your Cisco products:

http://www.cisco.com/kobayashi/technotes/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—Designed to notify you of any critical issues regarding Cisco products. These notices include problem descriptions, safety or security issues, and hardware defects.
- Hardware—Technical Tips related to specific hardware platforms.
- Hot Tips—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—Tips on using and deploying Cisco IOS software features and services.
- Sample Configurations—Actual configuration examples that are complete with topology and annotations.
- Software Products—MultiNet & Cisco Suite 100, Network Management, Cisco IOS Software Bulletins, and CiscoPro Configurations.
- Special Collections—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, which ships with your product. 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 additional 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 reach 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 with the documents listed in the "Related Documentation" section on page 42.

CCIP, the Cisco *Powered* Network mark, the Cisco Systems Verified logo, Cisco Unity, Follow Me Browsing, FormShare, Internet Quotient, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ Logo, iQ Net Readiness Scorecard, Networking Academy, ScriptShare, SMARTnet, TransPath, and Voice LAN are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, Discover All That's Possible, The Fastest Way to Increase Your Internet Quotient, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, IOS, IP/TV, LightStream, MGX, MICA, the Networkers logo, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, SlideCast, StrataView Plus, Stratum, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site 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. (0203R)

Copyright © 1998–2002, Cisco Systems, Inc.
All rights reserved.

