



## **Cisco Broadband Local Integrated Services Solution Release 1.5 Troubleshooting Guide**

September 15, 2004

### **Corporate Headquarters**

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
<http://www.cisco.com>  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 526-4100

Customer Order Number:



THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCSP, the Cisco Square Bridge logo, Cisco Unity, Follow Me Browsing, FormShare, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, Registrar, ScriptShare, SlideCast, SMARTnet, StrataView Plus, SwitchProbe, TeleRouter, The Fastest Way to Increase Your Internet Quotient, TransPath, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0406R)

*Cisco Broadband Local Integrated Services Solution Release 1.5 Troubleshooting Guide*  
Copyright © 2004, Cisco Systems, Inc. All rights reserved.



<b>About this Guide</b>	<b>xi</b>
Audience	xi
Assumptions	xi
Document Organization	xii
Cisco Documentation Suite	xiii
Document Conventions	xiv
References	xv
Obtaining Documentation	xvi
Cisco.com	xvi
Ordering Documentation	xvi
Documentation Feedback	xvi
Obtaining Technical Assistance	xvii
Cisco Technical Support Website	xvii
Submitting a Service Request	xvii
Definitions of Service Request Severity	xvii
Obtaining Additional Publications and Information	xviii

---

**CHAPTER 1**

<b>Solution Overview</b>	<b>1-1</b>
Architectural Overview	1-2
Architectural Features	1-3
Operational Features	1-3
Solution Assumptions	1-5
Specifications Supported	1-5
Functional Architecture	1-6
Physical Architecture	1-7
Solution Components	1-8
Cable Access Components	1-9
Cable Aggregation Components	1-13
Core Switching Components	1-15
Trunking Components	1-16
Call Control Components	1-19

- Solution Features **1-25**
  - Network Features **1-26**
  - Route Selection **1-31**
  - Subscriber Features **1-35**
  - Operation, Administration, Maintenance, and Provisioning Features **1-46**
- Cisco NMS/OSS for Broadband Services **1-48**
  - Service Fulfillment Applications **1-50**
  - Service Assurance Applications **1-52**

**CHAPTER 2**

**Troubleshooting Overview 2-1**

- Troubleshooting Basics **2-1**
- Troubleshooting Strategy **2-2**
  - Detailed Troubleshooting Methodology **2-5**
  - Preparing Yourself to Troubleshoot **2-8**
  - Taking Preventive Action **2-9**
  - Scope of Troubleshooting **2-9**
- Troubleshooting Tools **2-11**
  - Software Tools **2-11**
  - Diagnostic Commands **2-12**
  - Hardware Tools **2-15**
  - High-End Cable Testers **2-16**

**CHAPTER 3**

**Trouble Isolation Procedures 3-1**

- Finding System Information **3-1**
- Troubleshooting Hardware Components **3-8**
- Call Traces **3-10**
- Component States **3-10**
  - Signaling Gateway Process **3-11**
  - Signaling Destinations **3-11**
  - Destination Point Code Status **3-12**
  - Aggregation Status **3-12**
  - Media Gateway **3-13**
  - Subscriber Termination **3-14**
  - Trunk Group **3-20**
  - Trunk Termination **3-23**

**CHAPTER 4****Troubleshooting with Call Flows 4-1**

- Understanding MGCP 4-2
  - MGCP Transactions 4-2
- Understanding SS7 4-10
  - Processing a Telephone Call 4-10
  - ISUP Signaling Messages 4-11
- Call Flow Analysis 4-13
  - MGCP Key Fields 4-13
  - MGCP Message Correlation 4-13
  - Call Flow Problems 4-15
- Voice Quality Problems 4-22
  - Lost or Distorted Audio 4-23
  - Voice Network Troubleshooting Procedures 4-24

**CHAPTER 5****Troubleshooting DOCSIS Networks 5-1**

- DOCSIS 1.0+ 5-1
- Understanding Initialization States 5-3
  - Physical and MAC Configuration 5-3
  - Network Layer Configuration And Above 5-6
- Radio Frequency (RF) Issues 5-9
- Troubleshooting RF Problems 5-10
  - Troubleshooting Tools 5-10
- Measuring RF Signals 5-11
  - Measuring Downstream IF and RF 5-11
  - Comparing Measurements to Recommended Settings 5-15
  - Measuring Upstream RF Signals 5-17
- Troubleshooting Slow Performance 5-17
  - Hardware and Software Versions 5-17
  - Determining Levels of Performance 5-17
  - Potential Reasons for Poor Performance 5-21
  - High CPU Utilization on the CMTS 5-30
  - Conclusion 5-32

**CHAPTER 6**

**Troubleshooting MTAs 6-1**

- Troubleshooting EMTA Provisioning **6-1**
  - Know The Basics **6-1**
  - Troubleshooting Tools **6-4**
  - Troubleshooting Scenarios **6-5**
- Motorola Surfboard **6-8**
  - Major Features **6-8**
  - Physical Interfaces **6-9**
  - Voice Features **6-9**
  - Signaling, Data, Routing Features **6-9**
  - Security Features **6-10**
  - Management Features **6-10**
- Arris MTAs **6-10**

**CHAPTER 7**

**Troubleshooting the CMTS 7-1**

- Console Connections **7-2**
- Physical Interfaces **7-3**
- Features **7-3**
- Troubleshooting the Cisco uBR7246VXR **7-5**
  - Troubleshooting the Cable Modem State **7-6**
  - Monitoring the Cisco uBR7246VXR Flap List **7-25**
  - Additional Diagnostic Commands **7-36**
  - Displaying Type of Service (ToS) Specifications **7-41**
  - Displaying Cable Interface Data **7-41**
  - Using Debug Commands **7-45**

**CHAPTER 8**

**Troubleshooting the Cisco Catalyst 6509 8-1**

- Troubleshooting the Switch **8-3**
- Troubleshooting Port Connectivity **8-3**
- Before Calling the Cisco Systems TAC Team **8-8**
- Cisco GSR-12000 Series Gigabit Switch Router **8-9**
  - Cisco 12000 Series IP Services Engine (ISE) **8-9**
  - Gigabit/Fast Ethernet (GE/FE) **8-10**
  - Packet Over SONET/Synchronous Digital Hierarchy (POS/SDH) **8-10**
  - Dynamic Packet Transport (DPT) **8-10**

Troubleshooting Serial Lines	<b>8-10</b>
Optical Signal Input/Output Problems	<b>8-10</b>
Using Bit Error Rate Tests	<b>8-13</b>
Using Loopback Tests	<b>8-16</b>

**CHAPTER 9****Troubleshooting Cisco Media Gateways 9-1**

Media Gateway Management	<b>9-1</b>
MGCP on Cisco IOS Software	<b>9-2</b>
DHCP on Cisco IOS Software	<b>9-2</b>
Cisco MGX8850	<b>9-2</b>
MGX 8850 Diagnostics	<b>9-3</b>
Command Line Interface	<b>9-4</b>
Diagnostic Troubleshooting	<b>9-7</b>
Troubleshooting Alarms	<b>9-8</b>
Viewing and Responding to Alarms	<b>9-8</b>
AXSM Card Controls	<b>9-11</b>
RPM-PR Card Controls	<b>9-12</b>
Displaying Alarm Reports in the CLI	<b>9-13</b>
PXM45x Alarm Issues	<b>9-17</b>
Displaying Log File Information	<b>9-20</b>
Troubleshooting the Gateways	<b>9-20</b>
D-Channel	<b>9-20</b>
Data Path Troubleshooting	<b>9-23</b>
There Is No Voice	<b>9-23</b>
Fax/Modem Fails	<b>9-26</b>
COT/Testline Fails	<b>9-26</b>
Tone Detection/Play Fails	<b>9-26</b>
Line Interface and Switching Path Troubleshooting	<b>9-27</b>
Call Control	<b>9-28</b>
Debugging Commands	<b>9-28</b>
Turning on Trace Debugging	<b>9-29</b>
Media Gateway Errors	<b>9-30</b>
System Redundancy	<b>9-30</b>
Troubleshooting VISM Cards	<b>9-31</b>
VISM Card LEDs	<b>9-32</b>
VISM and PXM Display, Log, and Diagnostic Loopback Path CLI Commands	<b>9-34</b>

- VISM Alarms **9-36**
- UNIX Snoop Trace Tool **9-36**
- Symptoms and Solutions **9-37**
  - VISM Card Did Not Become Active **9-37**
  - T1/E1 Configuration Mismatch **9-37**
  - DSP Download Failure **9-39**
  - VISM Front Card/Back Card Mismatch **9-39**
  - Cannot Use the **cc** Command to Access a VISM Card **9-40**
  - VISM Card Resets Intermittently **9-40**
  - VISM Card Does Not Accept a Firmware Download **9-40**
  - Echo Is Heard on a Voice Call **9-41**
  - VISM Card LEDs Are Not Lighted **9-41**
  - Firmware Does Not See the Card Insert Bit Status As Set **9-41**
- Physical Indicators **9-41**
  - Line LEDs **9-41**
  - Port LED indications **9-42**
  - VISM Logs **9-45**
  - VISM to RPM Connection Problems **9-45**

**CHAPTER 10**

**Troubleshooting the Cisco BTS 10200 Softswitch 10-1**

- Architecture **10-1**
  - Call Agent **10-2**
  - Terminations **10-2**
  - Interfaces **10-3**
- Components **10-5**
  - Rack Configuration **10-6**
  - Feature Server Architecture **10-8**
  - EMS Architecture **10-8**
  - Cisco BTS 10200 Softswitch Controller Hosts **10-9**
  - Reference Documentation **10-9**
- Troubleshooting **10-10**
  - Verify Running Processes **10-10**
  - Verify Current Status **10-10**
- Cisco BTS 10200 Failure **10-17**
- Operating System Failure **10-17**



---

**CHAPTER 11****Element Management and MIBs 11-1**Cisco uBR7246vvr MIBs **11-1**CISCO-CABLE-SPECTRUM-MIB.my **11-1**CISCO-DOCS-EXT-MIB.my **11-6**DOCS-CABLE-DEVICE-MIB.my **11-24**DOCS-IF-MIB.my **11-35**





## About this Guide

---

This guide describes methods and procedures for troubleshooting the Residential Cable VoIP (RCVoIP) implementation of the Cisco Broadband Local Integrated Service Solution (BLISS) Release 1.5 on broadband networks with the focus on the Cisco equipment used in the solution. It also provides additional information on some of the technology issues related to VoIP over a cable network.

This document covers troubleshooting guidelines specific to the cable access portion of the network, the PSTN interconnect portion of the network, and the Cisco BTS 10200 Softswitch node.

## Audience

This document is intended to be used by Cisco Customer Support Engineers, service provider personnel involved with operating and troubleshooting the solution, and anyone else who might be responsible for troubleshooting an RCVoIP network.

The audience for this document is assumed to have a thorough knowledge of the following areas:

- UNIX commands and operation of the Cisco BTS10200 Softswitch
- Provisioning the Cisco BTS10200 Softswitch for trunk-side and line-side services
- Configuring the Cisco MGX8850 voice gateway for connectivity to the PSTN
- Configuring the Cisco uBR7246vxr/uBR10012 for connectivity to the cable headend
- SS7, MGCP, NCS, and DQoS signaling protocols
- DOCSIS™ 1.1, PacketCable™ 1.0 specifications

References to related documentation are supplied in this preface and in each chapter of the guide.

## Assumptions

The BLISS for Cable Release 1.5 solution is deployable as either a primary line or secondary line residential voice solution, dependent on the whether the service provider chooses to install line-powered MTAs. BLISS for Cable Release 1.5 supports the G.711 CODEC, with other CODECs and CODEC negotiation planned for a later release. Not all MTAs support 3-way calling, so that feature also depends on which MTAs the service provider chooses to install. BLV/OI is not supported in this release.

The BLISS for Cable Release 1.5 solution adheres to the following [PacketCable™ specifications](#):

- PacketCable™ Dynamic Quality of Service (DqoS) Specification, PKT-SP-DQOS-I03-020116
- PacketCable™ Security Specification, PKT-SP-SEC-I05-020116

- DOCSIS Baseline Privacy Plus Interface Specification, SP-BPI+-I08-020301
- PacketCable™ MTA Device Provisioning Specification, PKT-SP-PROV-I03-011221
- PacketCable™ Network-Based Call Signaling Protocol Specification, PKT-SP-EC-MGCP-I04-011221
- PacketCable™ PSTN Gateway Call Signaling Protocol Specification, PKT-SP-TGCP-I02-011221
- PacketCable™ Electronic Surveillance Specification, PKT-SP-ESP-I01-991229.
- PacketCable™ Event Messages Specification, PKT-EM-I03-011221.
- PacketCable™ CMS to CMS Signaling Specification, PKT-SP-CMSS-I01-001128.
- PacketCable™ Audio/Video Codecs Specification, PKT-SP-CODEC-I03-011221

## Document Organization

The BLISS for Cable Release 1.5 architecture is based on Open Packet Telephony and consists of multiple functional planes:

- **Customer Premise Equipment Layer**—Includes the CPE equipment
- **Access Gateway Layer**—Includes the uplink technology
- **Aggregation Layer**—Aggregates traffic from the CPE uplinks
- **Core Switching Layer**—Provides the packet network backbone
- **Trunking Layer**—Provides the PSTN and SP interfaces
- **Call Control and Management Layer**—Provides call control/signaling support, Feature Server interfaces, and support for network resource interfaces such as Announcement Servers, CALEA servers, Record Keeping Servers, and so on.
- **Network Management Layer**—Provides the EMS and network management components
- **Operational Support System**—Provides the operational interfaces and applications required to manage the network and the solution.

This Guide is organized to correspond with the architectural layers described above as follows:

<a href="#">Chapter 1</a>	<a href="#">Solution Overview</a>	Provides an overview of the solution architectures, hardware devices, protocols, network operations and the information needed to operate, maintain, and troubleshoot the BLISS for Cable solution.
<a href="#">Chapter 2</a>	<a href="#">Troubleshooting Overview</a>	Provides basic troubleshooting methodology for packet cable networks, IP networks, and signaling networks. Guidelines for preventing problems before they occur are presented, as well as brief descriptions of the troubleshooting tools available and guidelines for their use.
<a href="#">Chapter 3</a>	<a href="#">Trouble Isolation Procedures</a>	This chapter presents a comprehensive set of trouble isolation procedures.
<a href="#">Chapter 4</a>	<a href="#">Troubleshooting with Call Flows</a>	Provides information on how to use call flows to help diagnose network and signaling problems and pinpoint causes.

Chapter 5	<a href="#">Troubleshooting DOCSIS Networks</a>	Provides information on DOCSIS and troubleshooting DOCSIS -related problems, including RF and poor performance problems.
Chapter 6	<a href="#">Troubleshooting MTAs</a>	Provides some accumulated experience with troubleshooting MTAs.
Chapter 7	<a href="#">Troubleshooting the CMTS</a>	Provides specific information for troubleshooting the Cisco uBR7246 or the Cisco uBR10012.
Chapter 8	<a href="#">Troubleshooting the Cisco Catalyst 6509</a>	Describes procedures for troubleshooting the Cisco Catalyst 6509 switch.
Chapter 9	<a href="#">Troubleshooting Cisco Media Gateways</a>	Describes procedures for troubleshooting the Cisco MGX8850
Chapter 10	<a href="#">Troubleshooting the Cisco BTS 10200 Softswitch</a>	Provides specific information for troubleshooting the Cisco BTS 10200 Softswitch.
Chapter 11	<a href="#">Element Management and MIBs</a>	Provides information on the Cisco Element Manager (CEM) and SNMP MIBs.

## Cisco Documentation Suite

Refer to the following documents for more information on deploying and maintaining this solution.

[Cisco BTS10200 Softswitch](#) documentation for Release 3.5, including:

- *Release Notes for Release 3.5*
- *System Description*
- *Cabling Procedures*
- *Site Surveys*
- *Application Installation*
- *Jumpstart Procedures*
- *Operations Manual*
- *Disaster Recovery Procedures*
- *Error Messages and Alarms Reference Guide*
- *Billing Interface Guide*
- *Command Reference Guide*
- *CORBA Programmer's Guide*
- *Packet Cable Feature Module*
- *CALEA Feature Module*
- *ISDN Enhancements*
- *Digit Manipulation Feature Module*
- *SNMP Interface*
- *Congestion Detection and Protection*
- *Local Number Portability*
- *Continuous Computing Documentation*

**Cisco MGX8850 Media Gateway** documentation, including:

- [Cisco MGX 8850 \(PXM1E/PXM45\) Software Configuration Guide](#)
- [Cisco MGX 8850 \(PXM1E/PXM45\) Command Reference](#)
- [Cisco Voice Interworking Services \(VISM\) Configuration Guide and Command Reference](#)

**Cisco uBR7246VXR Cable Modem Termination System** documentation, including:

- [Cisco CMTS Feature Guide](#)
- [Cisco Broadband Cable Command Reference Guide](#)

## Document Conventions

Command descriptions use the following conventions:

<b>boldface font</b>	Commands and keywords are in boldface.
<i>italic font</i>	Arguments for which you supply values are in italics.
[ ]	Elements in square brackets are optional.
{ x   y   z }	Alternative keywords are grouped in braces and separated by vertical bars.
[ x   y   z ]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A set of characters not in quotes. Do not use quotation marks around the string or the string will include the quotation marks

Screen examples use the following conventions:

screen font	Terminal sessions and information system displays are in screen font.
<b>boldface screen font</b>	Information you must enter is in boldface screen font.
<i>italic screen font</i>	Arguments for which you supply values are in italic screen font.
Æ	This pointer highlights an important line of text in an example.
^	The symbol ^ represents the key labeled Control. For example, the key combination ^D in a screen display means hold down the Control key while you press the D key.
< >	Description of text you are expected to enter vs. the actual characters, such as <password>, is in angle brackets.
[ ]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Notes use the following conventions:



### Note

**Note** Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

Cautions use the following conventions:

**Caution**

**Caution** means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Warnings use the following conventions:

**Warning**

**Warning** means danger. **You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents.**

## References

The following documents contain essential background information for the Cisco BLISS for Cable 1.0 solution:

- Cisco Voice Routing Center, version 1.1:  
[http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/vrc/vrc1\\_1/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/vrc/vrc1_1/index.htm)
- Cisco MGC Node Manager User's Guide:  
<http://www.cisco.com/univercd/cc/td/doc/product/access/sc/rel9/cmm21/index.htm>
- Cisco CNS Intelligence Engine IE2100 Series, version 1.2  
[http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/ie2100/cnfg\\_reg/rel\\_1\\_2/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/ie2100/cnfg_reg/rel_1_2/index.htm)
- John T. Chapman, "Multimedia Traffic Engineering for HFC Networks", February 21, 2000.  
This document is available online at [http://www.cisco.com/warp/public/cc/so/cuso/sp/hfcn\\_wp.pdf](http://www.cisco.com/warp/public/cc/so/cuso/sp/hfcn_wp.pdf)

# Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain technical assistance and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

## Cisco.com

You can access the most current Cisco documentation at this URL:

<http://www.cisco.com/univercd/home/home.htm>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

[http://www.cisco.com/public/countries\\_languages.shtml](http://www.cisco.com/public/countries_languages.shtml)

## Ordering Documentation

You can find instructions for ordering documentation at this URL:

[http://www.cisco.com/univercd/cc/td/doc/es\\_inpk/pdi.htm](http://www.cisco.com/univercd/cc/td/doc/es_inpk/pdi.htm)

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Ordering tool:  
<http://www.cisco.com/en/US/partner/ordering/index.shtml>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

## Documentation Feedback

You can send comments about technical documentation to [bug-doc@cisco.com](mailto:bug-doc@cisco.com).

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems  
Attn: Customer Document Ordering  
170 West Tasman Drive  
San Jose, CA 95134-9883

We appreciate your comments.



# Obtaining Technical Assistance

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, Cisco Technical Support provides 24-hour-a-day, award-winning technical assistance. The Cisco Technical Support Website on Cisco.com features extensive online support resources. In addition, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not hold a valid Cisco service contract, contact your reseller.

## Cisco Technical Support Website

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

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

Access to all tools on the Cisco Technical Support Website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

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

## Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool automatically provides recommended solutions. If your issue is not resolved using the recommended resources, your service request will be assigned to a Cisco TAC engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco TAC engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553 2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

## Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

## Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:

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

- The *Cisco Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the Cisco Product Catalog at this URL:

<http://cisco.com/univercd/cc/td/doc/pcat/>

- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:

<http://www.ciscopress.com>

- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:

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

- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:

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

- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

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

- World-class networking training is available from Cisco. You can view current offerings at this URL:

<http://www.cisco.com/en/US/learning/index.html>



## Solution Overview

---

**The best possible troubleshooting tool is an extensive, in-depth understanding of the solution and all components; their installation, configuration, provisioning, operation, and maintenance in your environment.**

---

PacketCable™ is a CableLabs® -led initiative aimed at developing interoperable interface specifications for delivering advanced, real-time multimedia services over two-way cable plant. Built on top of the industry's highly successful cable modem infrastructure, PacketCable networks use Internet Protocol (IP) technology to enable a wide range of multimedia services, such as IP telephony, multimedia conferencing, interactive gaming, and general multimedia applications.

The Cisco Broadband Local Integrated Services Solution (BLISS) for Cable is Cisco's Voice over IP (VoIP) based Class 5 local services solution for cable systems. The Cisco BLISS for Cable solution builds on the earlier BLISS for T1 solution and expands the framework to include new elements, new features, and cable access technology using packetized data transmission over the cable television Hybrid Fiber Coaxial (HFC) network.

Cisco's BLISS for Cable product is based on Cisco's Open Packet Telephony (OPT), CableLabs PacketCable specifications, and a centralized call control architecture, using the Cisco BTS 10200 Softswitch for call control, Cisco media gateways to carry bearer traffic, and the associated management systems. The BLISS for Cable solution uses MGCP 1.0/ NCS 1.0 signaling between the Call Agent and MTA end points for call control, providing interoperability between compatible media gateways.

The VoIP over Cable access network and the PacketCable specifications allow cable Multiple System Operators (MSOs) to leverage existing cable plant infrastructure to offer integrated voice and data services for residential customers. The solution uses the Data Over Cable Service Interface Specification (DOCSIS) to provide these residential services by utilizing the basic interactive cable infrastructure that MSOs have installed to deliver High Speed Data (HSD) services, including cable modems, head-end equipment, and the distribution plant, to deliver high quality local telephone service.

The Cisco BLISS for Cable Release 1.0 solution introduced the following high level capabilities:

- Implementation of CableLabs® PacketCable™ components for telephony service including:
  - Support for the DOCSIS 1.1-based HFC cable plant, including PacketCable compliant MTAs and Cable Modem Termination Systems (CMTS).
  - Cable Modem Termination System (CMTS) - Cisco uBR7246VXR and Cisco uBR10012
  - High Density Media Gateway (MG) - Cisco MGX8850 Trunking Gateway
  - Call Management Server (CMS) - Cisco BTS10200 Softswitch
  - Media Gateway Controller (MGC) - Cisco BTS10200 Softswitch
  - Signaling Gateway (SG) - Cisco BTS10200 Softswitch

- Support for additional resources, such as:
  - Enhanced compliance with CableLabs PacketCable specifications
  - Call Agent support for Event Messaging and DQoS
  - Announcement/IVR Server
  - Voice Mail Server
  - CALEA Server
  - Record Keeping Server (RKS)
  - Full Element Management layer
  - Flow through MTA provisioning
  - Fault Management

This chapter provides an overview of the Cisco Broadband Local Integrated Services Solution (BLISS) Release 1.5, including brief descriptions of the solution's components.

This chapter contains the following sections:

- [Architectural Overview, page 1-2](#)
- [Solution Components, page 1-8](#)
- [Solution Features, page 1-25](#)
- [Cisco NMS/OSS for Broadband Services, page 1-48](#)

## Architectural Overview

The Cisco BLISS for Cable solution architecture allows Multiple System Operators (MSOs) to leverage their existing cable plant infrastructure to offer integrated voice and data services for residential customers. The BLISS for Cable solution provides residential telephony services utilizing the basic two-way, interactive infrastructure cable MSOs have installed to deliver High Speed Data (HSD) services. This service utilizes the common HSD infrastructure including cable modems, head-end equipment, and the distribution plant, to deliver high quality, local telephone service.

The Cisco BLISS for Cable solution architecture provides a number of benefits for cable system operators, including:

- One network, one transport protocol capable of delivering multiple services (voice, video and data)
- Increase revenue, profits, and customer loyalty by delivering additional services over existing cable infrastructure
- Rapid deployment of advanced services such as voice messaging, video services, and so on
- Proven, industry-leading network components for reliable, scalable, carrier-class packet networks
- Structured architectures for flexible, high-performance network services

This section includes the following topics:

- [Architectural Features, page 1-3](#)
- [Operational Features, page 1-3](#)
- [Functional Architecture, page 1-6](#)
- [Physical Architecture, page 1-7](#)

## Architectural Features

The BLISS solution provides the following architectural features:

- Link redundancy for traffic
- Call agent redundancy
- Catalyst switch redundancy
- Trunk redundancy on TGW failure
- SS7 load sharing
- CMTS uplink load sharing
- TGW WAN link load sharing
- Overload call control (call gapping)
- Multi-city support
- Multiple dial plans
- 911/0+ dialing

## Operational Features

The BLISS solution provides the following operational features:

### **Toll Bypass (Class 4 Exchange) Features**

- Per subscriber long Distance LPIC (FGD) - Intra LATA
- Per subscriber long Distance CIC
- Carrier access codes/Dial around
- International dialing
- Automatic Number Identification (ANI)

### **Local Exchange (Class 5 Exchange) Features**

- FXS
- Feature Group D (MF trunks)
- Call progress tones (ringing, busy, and so on)
- Support split NPA

### **General Connectivity Features**

- Bellcore GR-63-CORE (NEBS) level 3 compliant
- Telcordia Certification for SS7

### **Supported Protocols**

- ANSI MTP 1-3 (SS7)
- SCCP
- TCAP
- AIN 0.1
- IN
- G.165 and G.168 Echo cancellation
- E.164 Numbering Plan
- SNMP version 1 & 2

- Diffserv Codepoint (DSCP) for Signalling
- Diffserv Codepoint (DSCP) or TOS for Bearer
- LLQ
- MGCP 1.0
- DOCSIS 1.1
- NCS 1.0
- Q.850 cause codes
- Real-time Transport Protocol (RTP)
- Packet header suppression
- Telnet Client / Server
- FTP Client / Server
- TFTP (Trivial File Transfer Protocol) Client / Server
- RADIUS (Remote Access Dial-In Subscriber Service)
- Internet Protocol (IP v4)
- Transaction Capabilities Protocol (TCP)
- User Datagram Protocol (UDP)
- NTP (Network time Protocol)
- Synchronization (time-of-day)
- Clocking Interface
- Open Shortest Path First (OSPF)
- Router Discovery Protocol (IRDP)
- Session Description Protocol (SDP)

#### **Supported CODECs**

- G.711 Voice ( $\mu$ -law)
- VAD
- Packet loss concealment
- Comfort noise insertion/generation
- Adaptive jitter buffer
- Modem pass through (G.711)

#### **Billing Features**

- Post-paid billing system support
- Real time billing (CDR access after call ends)
- Bellcore AMA support
- CDR or Event Message generation
- CDR additional contents
- Recording Keeping System (RKS)

#### **Security Features**

- SSH Support (Client)
- SSH Support (Server)
- Multiple security levels and passwords

**Management Features**

- Remote software upgrades/management/control
- Non-service affecting upgrades (Call Agent)
- CORBA
- Support the registering of devices and pushing of device configurations via a provisioning API
- Support assignment of proper IP addresses to CPE equipment based on type (via DHCP)
- Support web-based GUI provisioning for the Cisco BTS10200 Call Agent

**Backbone Connectivity Features**

- Packet over SONET (POS)

**Trunking Gateway Features**

- TGW allows gain control (padding) to be provisioned
- Detection of Loss of Connection
- Loopback COT
- Transponder COT

## Solution Assumptions

The following assumptions apply to the Cisco BLISS for Cable Release 1.5 software:

- It is a secondary line solution
- 3-way Calling is not supported
- BLV/OI is not a requirement
- Only the G.711 CODEC is supported
- Complete compliance with the PacketCable Security requirements is not required
- Network management for BLISS is provided by the Cisco NMS/OSS for Broadband Services solution

## Specifications Supported

The following PacketCable specifications are supported in Cisco BLISS for Cable Release 1.5:

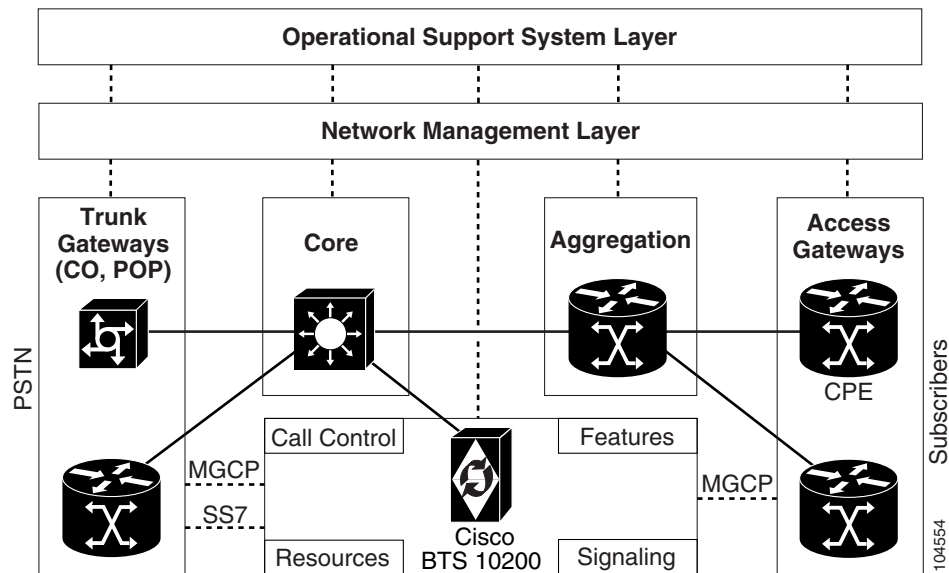
- DOCSIS Baseline Privacy Plus Interface Specification, SP-BPI+-I08-020301
- PacketCable™ Network-based Call Signaling (NCS) Protocol Specification (PKT-SP-EC-MGCP-I04-011221)
- PacketCable™ PSTN Gateway Call Signaling Protocol Specification, PKT-SP-TGCP-I02-011221
- PacketCable™ Security Specification, PKT-SP-SEC-I05-020116
- PacketCable™ Electronic Surveillance Specification (CALEA Support PKT-SP-ESP-I01-991229)
- PacketCable™ Dynamic Quality of Service (DQoS) Specification (PKT-SP-DQOS-I03-020116)
- PacketCable™ Event Message Specification (PKT-EM-I03-011221)
- PacketCable™ MTA Device Provisioning Specification (PKT-SP-PROV-I03-011221)
- PacketCable™ CMS to CMS Signaling Specification, PKT-SP-CMSS-I01-001128.
- PacketCable™ Audio/Video Codecs Specification, PKT-SP-CODEC-I03-011221

## Functional Architecture

The generic Cisco BLISS for Cable solution architecture consists of multiple functional planes, as illustrated in Figure 1-1:

- **Customer Premise Equipment (CPE) layer**—Includes MTA equipment and access gateways
- **Aggregation layer**—Includes the CMTS, which aggregates traffic from all of the CPE uplinks
- **Core Switching layer**—Provides the IP core network (packet backbone)
- **Trunking layer**—Provides the off-net PSTN and Internet access interfaces
- **Call Control layer**—Provides the call control/signaling support, Feature Server interfaces, and support for network resource interfaces
- **Network Management layer**—Provides the EMS and network management components
- **Operational Support System Layer**—Provides the operational interfaces and applications required to manage the network and the Cisco BLISS for Cable solution

Figure 1-1 Cisco BLISS for Cable Functional Architecture



In the access plane, the Cisco BLISS for Cable solution supports multiple access technologies and customer premise equipments. The architectural framework allows any given plane to be indifferent to other planes. For instance, the non-access parts of the network are, for the most part, transparent to the technology being used on the access side of the network.

On the switching/SuperPop side of the network, new trunking gateways along with the announcement, media, and CALEA servers are connected to the IP core through a Cisco Catalyst 6509 LAN switch.

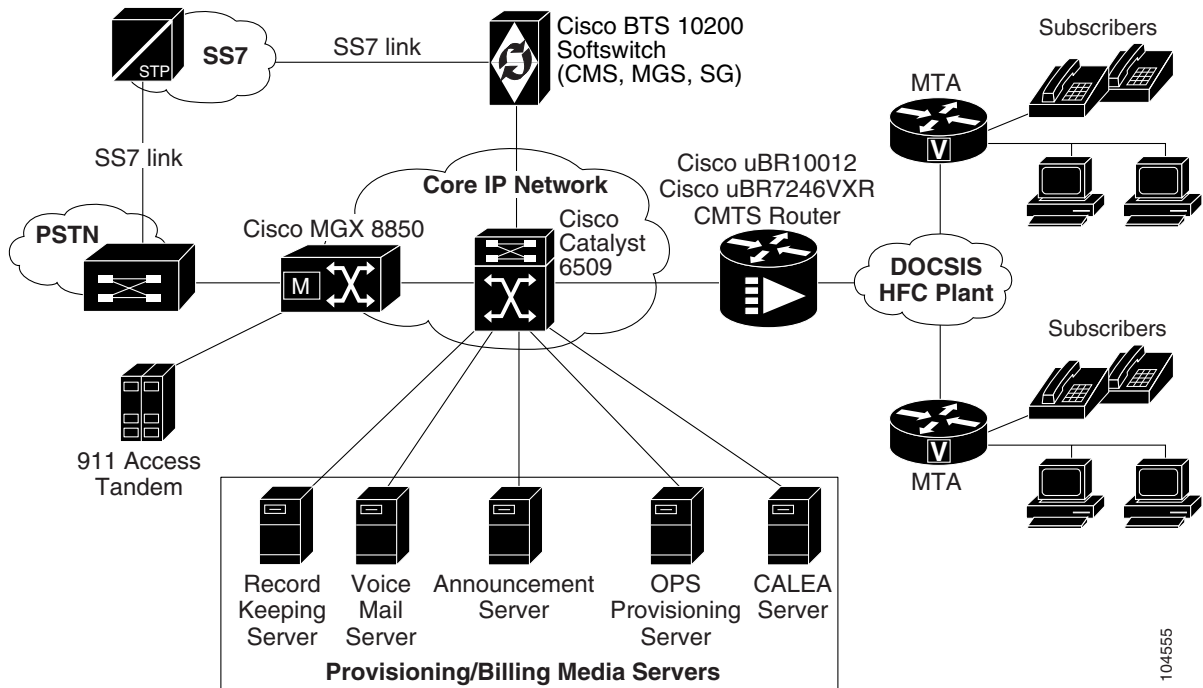


## Physical Architecture

The BLISS for Cable solution architecture, as illustrated in [Figure 1-2](#), is based on the CableLabs® PacketCable™ 1.0 architecture. The BLISS for Cable solution utilizes the CableLabs® DOCSIS™ 1.1 HFC access network architecture along with the Multi-Service over Cable (MSOC) [1] backbone architecture. In the BLISS for cable solution, the Cisco BTS10200 performs the functions of the Call Management Server (CMS), the Media Gateway Controller (MGC) and the Signaling Gateway (SG) as defined in the PacketCable™ 1.0 specifications.

The basic physical elements of the BLISS architecture are as shown here.

**Figure 1-2 Cisco BLISS for Cable Physical Architecture**



Connectivity to the service provider for Internet access can be through a GSR router in the IP core network, or it can be from the Cisco Catalyst 6509 switch, depending on customer deployment plans. The call control signaling is NCS 1.0 for the MTA call control and Media Gateway Control Protocol (MGCP) 1.0 for Trunking Gateway (TGW) interactions. The interface to a 911 Access Tandem, Operator Positions, and FGD trunks is provided via the MGX 8850/VISM trunking gateway. The IMTs from the PSTN also terminate on the trunking gateway. SS7 ISUP links terminate on the Cisco BTS 10200 Softswitch, which runs the Call Agent process.

104555

# Solution Components

The service provider's SuperPoP/Regional Office hosts all servers needed to provide solution services. Trunking gateways are also typically located here. It includes the following components, as shown in Figure 1-2 and listed in Table 1-1 and Table 1-2:

- [Cable Access Components, page 1-9](#)
- [Cable Aggregation Components, page 1-13](#)
- [Core Switching Components, page 1-15](#)
- [Trunking Components, page 1-16](#)
- [Call Control Components, page 1-19](#)
- [Cisco NMS/OSS for Broadband Services, page 1-48](#)

**Table 1-1 Cisco Broadband Local Integrated Services Solution Components and Software**

Platform	Cards	Code Release	Description
Motorola CG4501 Motorola SBV4200 Arris TM02DA102	none	5.4.03 7.3.2 TS030204-092903	DOCSIS 1.0 and DOCSIS 1.1 compliant cable modem(s)
Cisco uBR7246vxx with NPE-G1	uBR-MC16C & S PA-SRP-OC12 PA-POS-OC3	12.2(15)BC1b	Cable Modem Termination System (CMTS)
Cisco uBR10012		12.2(15)BC1b	Cable Modem Termination System (CMTS)
Cisco 7500	RSP 4+ SRPIP-OC12 VIP 4-80 PA-2FE; PA-POS-GigE	12.0(22)S	Aggregation router
Cisco Catalyst 6509	SUP1A (including 2x GigE (MSFC2) 48x 10/100 (X6348-RJ45) 16x GigE (X6416-GBIC) 8x GigE (x6408A-GBIC)	12.1(13)E06	LAN switch
Cisco Catalyst 2429	n/a	12.0.5WC5	LAN switch
MGX8850	PXM1 RPM-XF VISM-PR	1.2.21 12.2(15)T2 3.2	Trunking gateway
MGX8850	PXM45 RPM-XF VISM-PR	3.0.23 12.2(15)T2 3.2	Trunking gateway
Cisco BTS10200 Softswitch	CA, FS, EMS	3.5.3 V00	redundant Call Agents CableLabs certified MGC/CMS

**Table 1-2 Cisco NMS/OSS for Broadband Services Components**

Component	Version
Cisco Broadband Access Center for Cable (BAC-C)	2.5
Cisco Network Registrar (CNR)	6
Cisco Resource Manager Essentials (RME)	3.5
Cisco Broadband Troubleshooter (CBT)	3.0
Cisco Information Center (CIC)	3.5
Cisco Extensible Provisioning and Operations Manager (EPOM)	1.3 and 1.5

The following sections describe the individual Cisco BLISS for Cable components in greater detail.

## Cable Access Components

The cable access components of the network architecture for the BLISS for Cable 1.5 solution consist of the following:

- **Customer Premises Equipment (CPE)**

CPE includes all devices at residences/home offices, including:

- Motorola SBV4200 Cable Modem
- Arris TTN-102A Cable Modem

- **Hybrid Fiber-Coax (HFC) Network**

The HFC network includes the HFC distribution system, which is composed of elements such as coaxial cables, fiber-optic cables, and fiber-optic nodes to interconnect CPE devices to HFC hubs; this equipment depends on the service providers network and is discussed only in terms of general requirements in this document.

## Customer Premises Equipment

Customer Premises Equipment (CPE) includes those portions of the architecture located at the subscribers' premises, including the following:

- **Multimedia Terminal Adapters (MTAs)**—Cable modems or multimedia terminal adapters (MTAs) are provided by the subscriber and are a part of this solution. The Motorola SBV4200 cable modem is representative of this type of equipment; however, it is not sold or supported by Cisco.

The Motorola SBV4200 is based on the Motorola SURFboard® SB4200 Cable Modem and Motorola's proven cable modem experience. As part of the Motorola Broadband family of telephony products, the SBV4200 is capable of converging voice and data on one network in one product.

For more information on the Motorola SBV4200, see

<http://www.gi.com/catalog/productdetail.asp?image=large&productID=208>.

- **Premises Wiring**—Premises wiring is also provided by the subscriber. It may be necessary to place filters between a customer's inside wiring and the rest of the network to ensure that a subscriber's activities do not adversely affect the rest of the cable plant.

## Multimedia Terminal Adapters

Multimedia Terminal Adapters (MTA) are managed by service providers, but are physically located on the customers premises. MTAs are combined with cable modems to form the primary CPE component of the system that interfaces with the cable and provides the user with both Ethernet and telephone access.

The MTA consists of a cable modem section and a telephone interface section.

- The cable modem section provides cable to Ethernet connectivity, using the DOCSIS specification as a basis.
- The telephone interface section of the MTA provides a conversion from standard analog Plain Old Telephone Service (POTS) telephone sets to digital (packetized) voice traffic.

A cable modem typically connects a cable wall hookup to a PC's 10 base-T Ethernet card. Utilizing an always-on connection, cable modems transfer data across local cable TV lines, toggling between analog and digital signals. With data transfer rates comparable to DSL, cable modems (1.5 - 2.5 Mbps) are considerably faster than both dial-up modems (28.8 - 56 Kbps) and ISDN (128 Kbps).

### Physical Interfaces

The following physical interfaces will usually be encountered on a typical MTA:

- **Cable Interface**—The cable interface conforms to the MCNS DOCSIS 1.0 and DOCSIS 1.0+ specifications.
- **Ethernet Interface**—The cable modem has a 10 BaseT interface on an RJ45 connector for data access and features from two to four RJ11 interfaces supporting telephone, modem, and fax communications.
- **Telephone Interface**—One or two channels of FXS (Foreign Exchange Station) POTS are provided on RJ11 and RJ12 connectors.

### Call Control, Signaling and Media Streams

In Cisco's BLISS for Cable solution, MGCP is used as the signaling protocol between the MTA and the Cisco BTS 10200 Call Agent. MGCP is used to set up the various parameters of connections, including IP addresses, UDP ports, and so on. Audio streams are then passed directly between endpoints (typically between an MTA and a CMTS).

In addition to setting up audio stream connections, MGCP allows the Call Agent to set up digit maps, request events, and to apply signaling to the MTA. MGCP provides control while voice over IP transport between MTAs and CMTSs is done by Real-Time Transport Protocol (RTP) for real-time applications.

### DOCSIS QoS and Security Features

The MTA supports DOCSIS 1.0 and DOCSIS 1.0+ features, including baseline privacy (BPI) with some additional QoS capabilities as defined for DOCSIS 1.1. Each MTA will have multiple Service IDs (SID) to enable independent security and QoS for voice and data services.

### Systems Management Interfaces

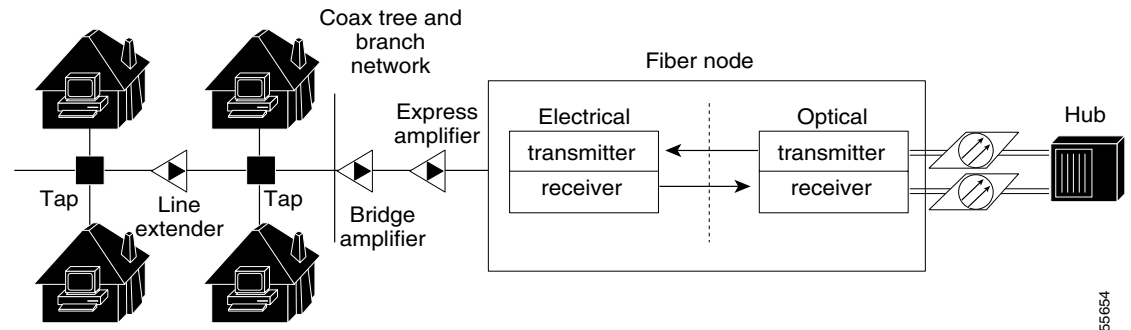
The MTA has been designed to be simple to install and configure. The MTA contains a DHCP client so that, within the solution, IP addresses can be assigned dynamically via DHCP. Also returned from DHCP as part of the DHCP-OFFER is the name of the MTA configuration file in the "boot file" name field.

The MTA also contains an SNMP agent that supports Cisco proprietary voice MIBs, as well as a pre-released version of DOCSIS MIBs [MCNS10], allowing the MTA to be managed via SNMP.

## Hybrid Fiber-Coax (HFC) Network

The HFC infrastructure, which is provisioned and maintained by the Multiple Service Operator (MSO), is responsible for providing a high speed link to the headend for multiple households. Voice data packets traversing the BLISS for Cable solution initially pass over a neighborhood cable network referred to as an HFC network. The fiber node receives electrical signals from all households passed and transforms them into an optical signal for a high-speed transfer to the hub/headend. Figure 1-3 displays the components in a typical HFC network.

**Figure 1-3 HFC Cable Network**



The HFC network is composed of a combination of fiber optic lines and nodes, standard commercial grade coaxial cable, amplifiers, and so on needed to interconnect household communication devices (including telephones, personal computers, television sets, and fax machines) to HFC hubs. The HFC distribution network topology is strictly MSO-specific.

The following physical devices/interfaces will usually be encountered on a typical HFC cable network:

- **Coaxial Cable**—The physical, broadband network cable used within a subscriber’s premises and the headend.
- **Taps**—Taps are the origination point of the HFC network’s “last mile” connection to the customer’s residence. Taps are the local tie-in point located along the street outside of the customer’s residence where the cable MSOs can initiate and/or terminate the residential coaxial cable connection that connects the cable backbone running through a neighborhood to an individual premises.
- **Fiber/Optic Nodes**—The coaxial cable that connects to the subscribers’ premises is terminated at a fiber node. Fiber nodes are responsible for providing high-speed links to the Hub/Headend for multiple households.
  - In the upstream direction, the fiber node converts the electrical signal it receives from the coax network to an optical signal.
  - In the downstream direction, the fiber node converts the optical signal it receives from the CMTS to an electrical signal that it sends out on the coax network.
- **RF amplifiers**—In order to support a reliable two-way traffic flow over the HFC network, you must ensure that the network is equipped with bidirectional amplifiers to pass voice packets back and forth between the MTA at the voice customer’s residence and the local cable headend CMTS. Two-way RF amplifiers boost the downstream and upstream signal strength on the HFC network.



**Note**

Some older cable network installations feature only single-direction data amplifiers that can only pass data in the downstream direction. These types of HFC networks do not meet Cisco’s BLISS for Cable solution requirements.

**Diplex Filters**—For coax cabling, diplex filters must be installed in the RF path between the cable modem cards in the CMTS and cablemodems and/or STBs. A diplexer has three ports: low, high, and common. The downstream cable attaches to the high port because high frequency signals flow in the downstream direction from the CMTS to cable modems and STBs. The upstream cable attaches to the low port because low frequency signals flow in the upstream direction from the cable modems to the CMTS. The common port attaches to a splitter attached to one or more MTAs and/or STBs.

In two-way data cable networks, the diplexer takes the upstream and downstream and combines them on one cable for the MTA. Downstream output signals from the CMTS run through the upconverter, then enter the high filter port of the diplex filter. The signal exits the common port of the filter and is distributed to the MTAs. The upstream signal from the MTAs enters the low port of the diplex filter and flows to the upstream receive ports of the CMTS's cable modem cards.

- **Fiber-Optic Cable**—Transports signals between the fiber node and the headend location. In most systems, at least two fiber links connect each fiber node to the headend; one for upstream traffic and one for downstream traffic
- **Multimedia Terminal Adapter**—The MTA converts analog voice signals into digitized voice samples, which are then packetized into IP packets.
  - For data connections, the MTA interacts with the core IP network to provide data connectivity at the customer premises.
  - For voice connections, the MTA interfaces with the Cisco BTS 10200 Call Agent and other elements of the network to establish on-net or off-net voice calls.
- **Fiber Links**—In most systems, a minimum of two fiber links connect each fiber node to the hub, one for the upstream traffic and one for the downstream traffic.

**Upstream Traffic**—In the upstream direction, the MTA encapsulates these IP packets into DOCSIS frames for transmission uplink to the hub/headend (Cable Modem Termination System, CMTS) over the Hybrid Fiber Coax (HFC) distribution network. The fiber node converts the electrical signal it receives from the coax tree and branch network to an optical signal.

The upstream frequency between 5 and 42 MHz can be divided into channels of varying width (between 0.20 to 3.20 MHz). Frequency ranges and channel widths are chosen based on known typical ingress patterns. Assuming a typical cable plant, it might select upstream data channels of 1.6 MHz in the unused frequency ranges of the upstream frequency range. Depending on specific HFC plant characteristics, it might select either QPSK (Quadrature Phase Shift Keying) or QAM16 as the upstream modulation technique. When a 1.6 MHz channel is selected, 1280 kilo-symbols/sec are supported. Hence, QPSK can theoretically support up to 2.56 Mbps and 16 QAM can theoretically support up to 5.12 Mbps.

**Downstream Traffic**—In the downstream direction, the CMTS converts the IP packets received from the remote end into DOCSIS frames for delivery on the downlink between the CMTS and the MTA. The MTA then removes the IP packets from DOCSIS frames, retrieves the digitized samples from IP packets and converts them into voice to be sent to the analog end points. The fiber node converts the optical signal to an electrical signal that it sends out on the coax tree and branch network to MTAs.

The downstream frequency above 50 MHz is divided into 6 MHz channels, most of which are used to support the CATV company's video service. One or more of these channels is designated to support downstream data transmission. Digital data is modulated onto the 6 MHz channel using either 64QAM (Quadrature Amplitude Modulation) or 256 QAM. With 64 QAM, each 6 MHz channel can support up to 27 Mbps of data. With 256 QAM, each 6 MHz channel can support up to 38 Mbps of data.

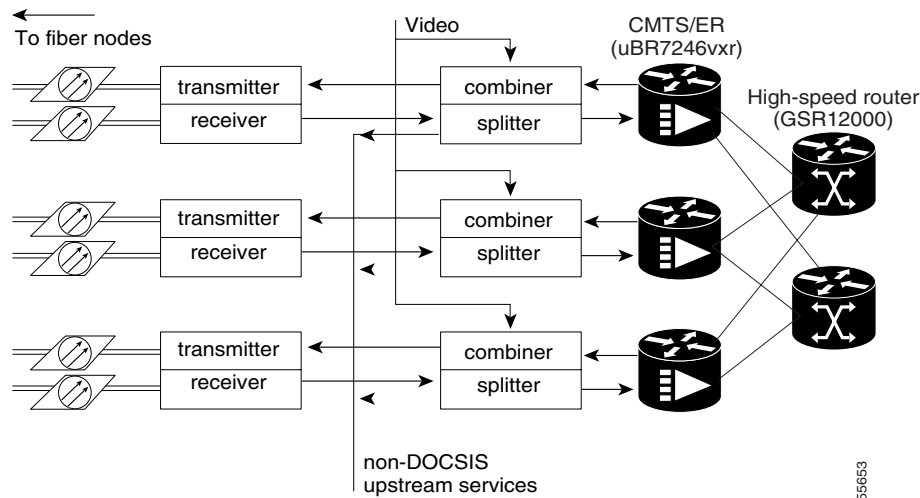
## Cable Aggregation Components

The cable aggregation components of the network architecture for the BLISS for Cable 1.5 solution are usually located at the HFC headend at the service provider's POP or IP Central Office (IPCO).

### HFC Headend

The headend is where all downstream signals originate and where all upstream signals terminate. Figure 1-4 shows the headend components included in the BLISS for Cable solution, which are described in the following sections.

**Figure 1-4 Headend Architecture**



The viability and the quality of VoIP on the HFC network is dependent on how the network is designed and configured to handle the traffic to and from an ever-increasing number of residential MTAs. The Cisco white paper *Multimedia Traffic Engineering for HFC Networks* by John J. Chapman, which is available at [http://www.cisco.com/warp/public/cc/so/cuso/sp/hfcn\\_wp.pdf](http://www.cisco.com/warp/public/cc/so/cuso/sp/hfcn_wp.pdf), describes many sizing and scaling issues. In his white paper, Mr. Chapman provides a series of formulas for calculating minimum and maximum loads, combined with practical advice on managing sizing and scaling issues.

### Headend Components

The following physical devices/interfaces are usually located at the headend on an HFC cable network:

- **Cable Modem Termination System (CMTS)**—Connectivity to the service provider (SP) for PSTN access is through a Cable Modem Termination System (CMTS) as defined in the DOCSIS 1.1 specification. CMTSs are managed by the service providers and are physically located at the cable headend. All of the traffic from the cable portion of the network is aggregated on the CMTS. The CMTS forwards IP data to/from the HFC infrastructure using the DOCSIS standard..

Cable Modem Termination Systems (CMTS) in the Cisco BLISS for Cable solution include:

- Cisco uBR7246VXR CMTS
- Cisco uBR10012 CMTS

### Cisco uBR7246VXR CMTS

In the BLISS for Cable solution the CMTS is a Cisco Universal Broadband Router, uBR7246VXR, which integrates a CMTS with a Cisco7200 series router allowing it to terminate IP packets on its network interface. This enables the Cisco uBR7246VXR to connect cable modems on the Hybrid Fiber Coaxial (HFC) Cable network using Cisco MCxx cable modem cards. The modem cards provide the interface between the Cisco uBR7246VXR protocol control information (PCI) bus and the radio frequency (RF) signal on the DOCSIS HFC network.

The Cisco7200 router portion of the Cisco uBR7246VXR is based on the NPE-400 Network Processing Engine (NPE) which provides over 100 Kpps (kilo packets per second) of fast switching capability, or the newly available NPE-1G NPE. The chassis is fully radio frequency (RF) hardened to ensure noise-free transmission, and all major components are hot swappable to guarantee maximum reliability. The Cisco uBR7246VXR supports a broad set of residential and commercial multiservice offerings, including IP telephony, multicast, streaming media, and Virtual Private Network (VPN) applications.

The Cisco uBR7246VXR supports 1+1 and N+1 redundancy of the complete line of DOCSIS™ 1.0-qualified and DOCSIS™ 1.1-based modem cards, including both cable and wireless cards. A range of network interfaces is available, including Fast Ethernet, SONET, and the Cisco Dynamic Packet Transport (DPT) port adapters, which provide direct, high-speed optical connectivity combined with add-drop multiplexer capability.

### Cisco uBR10012 CMTS

The Cisco uBR10012 Universal Broadband Router delivers the industry's highest-capacity CMTS and integrated router. The Cisco uBR10012 resides on the edge of the network in a balanced system that employs a mix of distributed, centralized, and parallel processing. Parallel eXpress Forwarding (PXF) provides consistently high performance and sophisticated IP decision-making capabilities, while protecting investment and providing a software re-programmable architecture.

The Cisco uBR10012 enables cable service providers to deliver feature-rich, high-speed data, voice, and video services to very high subscriber penetrations, typically 10,000 to 25,000 subscribers per chassis. Using Cisco IOS® Software, the product delivers a comprehensive suite of DOCSIS™ and high-speed IP services that includes DOCSIS™ 1.1 quality of service (QoS), access control lists, and Multiprotocol Label Switching (MPLS). The Cisco uBR10012 enables service providers to deploy a wide variety of value-added services.

For more information on the Cisco uBR7246VXR or the Cisco uBR10012, see [Chapter 7, “Troubleshooting the CMTS.”](#)

- **Fiber-Optic Laser Transmitters and Receivers**—If the downstream channels of your cable plant originate at the headend over fiber-optic lines, ensure you have a fiber-optic laser transmitter allocated for each downstream channel in your network. If the upstream channels of your cable plant terminate at the headend over fiber-optic lines, ensure that you have a fiber-optic laser receiver allocated for each upstream channel in your network.



#### Note

Laser transmitters and receivers need to be properly tuned so that the frequency of their output signal matches the transmit or receive frequency of the downstream or upstream channel on the Cisco uBR7246VXR router with which they have been paired.



- **IF-to-RF Upconverters**—To be compatible with cable television system frequency division multiplexing (FDM), install an external IF-to-RF upconverter that translates the IF signal to RF carrier frequency. The upconverter also allows you to maintain your existing channel lineup.

Upconverters are available from many manufacturers and can be found in configurations ranging from a fixed number of ports to flexible multislot, multiport models. Install and configure enough upconverter ports to support the number of downstream cable modem card ports installed in each CMTS you are installing. The number of units needed depends on the upconverter manufacturer.

The *Cisco uBR7200 Series Universal Broadband Router Hardware Installation Guide* lists upconverter manufacturers, web sites for more information on upconverter products, and models of upconverters that are compatible with the Cisco uBR7246VXR.

The upconverter is installed between the Cisco uBR7246VXR and the combiner. (See [Figure 1-4](#).) The combiner refers to all cables, amplifiers, and taps at the headend or cable distribution center that connect the Cisco uBR7246VXR to the HFC network.

Depending on the channel plan you are employing, your upconverter(s) must support different functionality. In the North American channel environment, your upconverter needs to receive a 44-MHz downstream IF transmission from cable modem cards in the Cisco uBR7246VXR CMTS and transmit 6-MHz RF channel bands in the 54 to 860 MHz range. In an 8-MHz European channel environment your upconverter needs to receive a 36.125 MHz downstream IF transmission from cable modem cards in the Cisco uBR7246VXR CMTS and transmit 8-MHz RF channel bands in the 85 to 860 MHz range.

Refer to the documentation that ships with your upconverter for specific details on upconverter operation and configuration.

**Note**

An analog channel modulator with external IF loops is not suitable for use as a digital Quadrature Amplitude Modulation (QAM) upconverter. These units typically do not have the phase noise performance levels required for 64- and 256-QAM digital signals, and they might cause degraded performance and possible system failure.

## Core Switching Components

The core switching layer provides the IP core network (packet backbone). Included in this layer is the Cisco Catalyst 6509 Ethernet LAN switch that provides connectivity between the Cisco BTS 10200 Softswitch and all of the solution components that it must communicate with.

### Cisco Catalyst 6509 Ethernet Switch

Cisco Catalyst 6509 Ethernet switches, deployed in a redundant configuration to provide high reliability, are used in the BLISS for Cable solution to provide Layer 2 connectivity among the IP core, Cisco BTS 10200 Softswitch, and ancillary servers and element management components necessary to provision and maintain the BLISS for Cable solution, such as web cache, e-mail, and so on.

The Cisco Catalyst 6509 also provides Layer 3 functionality for routing signaling packets to edge and trunking gateways, and to interconnect all servers within the SuperPOP. Each switch is configured with redundant processors, switch fabric, internal clock, power supply and fans to provide high level redundancy with redundant router modules.

The Cisco Catalyst 6509 can also be used to aggregate the traffic from multiple CMTSs into a single interface on a uBR. (The uBR component is optional depending on the network architecture.)

## Edge Routers

**Cisco GSR 12000** (optional)—the Cisco GSR 12000 Gigabit Switch Router can be used to connect CMTSSs to the rest of the IP network. It can be located in a headend, in the regional backbone, or in a service providers Internet Protocol Central Office (IPCO).

## Trunking Components

The Media Gateway Control Protocol (MGCP) 1.0 is used to control Voice over IP (VoIP) calls by external call-control elements known as call agents (CAs). It is described in detail in IETF RFC 2705. MGCP 1.0 is the call control protocol that runs between call agents and trunking gateways (TGWs) in a packet cable / IP telephony network.

PacketCable Labs developed the NCS and TGCP protocols, which contain extensions and modifications to MGCP while preserving the basic MGCP architecture and constructs. NCS is designed for use with analog, single-line user equipment on residential gateways (MTAs), while TGCP is intended for use in VoIP-to-PSTN trunking gateways in a packet cable environment.

As in the earlier implementations of the protocol, the trunking gateway handles the translation between audio signals from the PSTN and the packet cable network. The trunking gateways interact with the Call Agent, which performs signal and call processing on the gateways' calls. Call support has been expanded to include MTAs, which provide an interface between analog (RJ11) calls and the VoIP over cable network.

MGCP 1.0, including the NCS 1.0 and TGCP 1.0 profiles feature, provides protocols for MTAs and trunking gateways (TGWs), which sit at the edge of the packet network to provide interfaces between traditional, circuit-based voice services and the packet network. MTAs offer a small number of analog line interfaces, while trunking gateways generally manage a large number of digital trunk circuits.

In the Cisco BLISS for Cable solution, the Cisco BTS 10200 Softswitch communicates with SS7-based PSTN switches and service control points (SCPs) using a SIGTRAN-based signaling gateway (SG). The SIGTRAN interface carries all SS7 messages encapsulated in IP packets. The Cisco IP Transfer Point (ITP) is one of the SGs used with the Cisco BTS 10200 Softswitch for this purpose.

Bearer traffic connections to the PSTN are through ISDN User Part (ISUP) trunks with a TGW providing the bearer connections (for example, T1 carrier connections to the Cisco MGX8850). Either ISUP or multifrequency (MF), Feature Group-D (FGD), OS signaling trunks are used to interconnect to a service bureau (or ILEC) providing operator services, directory services and positions for 311, 611 and 711 services. E911 calls are routed to an E911 tandem, which has the appropriate databases and interfaces with the Presentation-Service Access Points (PSAP).

Connectivity to other networks includes PSTN connectivity, IP Backbone connectivity, and Internet connectivity. IP backbone and Internet connectivity is accomplished via the GSR 12000 in the IPCO.

## Cisco MGX8850 Trunking Gateway

This section describes the Cisco MGX 8850 trunking gateway (TGW) in the Call Agent node. The Cisco MGX 8850 is the primary ISUP trunk, 911 trunk, and Operator Services/411 TGW.

All TGWs must support redundant IP network interfaces with each interface able to handle the full capacity for media streams based on fully loaded PSTN interconnect.

TGWs can be configured with a virtual IP address associated with a loop-back port—independent of the two IP addresses associated with the Ethernet interfaces. This loop-back IP address is the one that the Call Agent should know about when talking to the TGW. It provides the optimum way of communicating with the TGW in cases where one of the Ethernet interfaces (or the switch) fails.

The Cisco MGX 8850 provides the interface to a 911 tandem, or Public Safety Answering Point (PSAP), and Operator Services by means of Feature Group D (FGD) trunks. All SS7-controlled bearer channels (Inter-Machine Trunks or IMTs) from the Public Switched Telephone Network (PSTN) terminate here.

The Cisco MGX8850 Trunking Gateway is a scalable carrier class platform that delivers a complete portfolio of voice services (trunking with PSTN) in combination with other BLISS for Cable components and interconnects the BLISS for Cable IP infrastructure with the PSTN permitting the routing of voice, modem, and fax traffic between the IP network and the PSTN.

All components of the Cisco MGX8850 are optionally redundant to 100-percent system redundancy, including the control processor, IP modules, switching fabric, network interfaces, service interfaces, critical backplane signals, power supplies, power modules, and cooling fans. All Trunking Gateways must support redundant IP network interfaces with each interface able to handle the full capacity for media streams based on fully loaded PSTN interconnect.

The Cisco MGX8850 platform can be configured with different combinations of line and processor cards. The Cisco BLISS for Cable solution supports the following platform configurations:

- MGX8850/PXM1/RPM-XF/VISM-PR/SRM
- MGX8850/PXM45/RPM-XF/VISM-PR/SRM-E

The Cisco MGX8850 chassis supports up to 32 single-height front cards (or a number between 12 and 24 for a mix of single-height and double-height front cards). The Cisco MGX8850 supports up to 32 back cards. Each double-height service module is capable of supporting two single-height back cards, and each single-height front card is capable of supporting a single-height back card. Four back card slots are dedicated to the Service Resource Modules and can be used to provide bulk distribution to the service module slots. The final four back cards are dedicated to the redundant PXM modules. Each PXM has a User Interface (UI) back card, and a back card with broadband ports.

Combinations of single-height and double-height service modules can coexist in a single Cisco MGX8850 chassis subject to configuration rules. The single-height slots are easily converted into double-height slots by removing a slot partition. There are seven field-removable slot partition inserts, one for each adjacent pair of service bays (slots 1-2, 3-4, 5-6, 9-10, 11-12, and 13-14). There is also a separate removable slot partition for the two SRM service bays (slots 15-16) when full height SRM cards are available. The back cards for all slots are single height, and the partition separators on the back of the chassis are not removable.

## VISM Modules

The Cisco MGX8850/VG VISM card provides standard T1 or E1 interfaces. Each Cisco MGX 8850 chassis supports up to 24 VISM modules, or 22 VISM with 1:N redundancy. Each VISM card supports 8 T1/E1 connections providing for 4608 T1 DS0's or 5952 E1 DS0's. In the upper shelf there are six Cell Buses that can be shared by 12 VISM cards (two cards each). Each Cell Bus runs at an OC-3 rate. The two Cell Buses in the lower shelf also run at an OC-3 rate, but are shared among 6 slots each.

At one Erlang of traffic (fully loaded, all active) on all VISM on the lower shelf, at G.711 10 msec with no VAD, and for E1 cards (248 channels on each VISM), the lower Cell Bus capacity would not be adequate to carry all traffic. These traffic assumptions are not realistic, so this limitation is not a concern.

Each VISM unit installed in a Cisco MGX 8850 consists of a front card and a back card (if not in bulk mode). This two-card set provides interfaces to TDM T1/E1 lines through ports located on the back card.

Available T1 back cards are:

- RJ48-8T1-LM—supports eight T1 lines using RJ48 connectors.
- R-RJ48-8T1-LM—used with a T1 front card in redundant configurations.

The Cisco MGX8000/VG SRMSRM/C card is a high-density bulk distribution card that provides up to 3 T3s per card. The T1s are extracted and routed to the VISM cards via C-bit parity or M-frame format.

The SRM/E card is another high-density bulk distribution card that removes some restrictions of the SRM card. These cards support both ANSI and ITU-T interfaces of these optical and electrical options:

- opticalOptical: OC-1/OC-3, STM-0/STM-1 with APS
- electricalElectrical: STS-0/STS-1, STM-0, STM-1

The VISM modules create VoIP packets which are transported out the Cisco MGX88500 via the ATM uplink on the PXM backcard.

## PXM Modules

The Cisco MGX 8850 chassis supports the PXM45 processor card (along with PXM1 card). There are two double-height slots (7/23 and 8/24) in positions seven and eight that are reserved for the redundant Processor Switch Modules (PXMs). The PXM45 will provide up to 45 Gbps of switching capacity.

Additionally, four single-height slots in positions 15, 16, and 31, 32, are reserved for the other Service Resource Modules (SRM or SRM/C). The SRMSRM/C module enables 1:N redundancy for the service modules, BERT testing, and built-in M13 grooming. The remaining slots in positions 1-6, 9-14, 17-22, and 25-30 are used for the service modules.

Trunking gateways can be configured with a "virtual" IP address associated with what is referred to as the loop-back port-independent of the two IP addresses associated with the Ethernet interfaces. This loop-back IP address is the one that the Call Agent should know about when talking to the Trunking Gateway. It provides the optimum way of communicating with the Trunking Gateway in cases where one of the Ethernet interfaces (or the Ethernet switch it is connected to) fails.

The Trunking Gateways can also be located in remote offices (remote from a Regional Center). For this solution, we can use both remote and local Trunking Gateways. The gateway configuration (in terms of line cards support) is the same for both remote and local Trunking Gateways. For instance in the case of the MGX 8850, VISM and VISM-PR can be located in remote as well as in the regional center locations.

## MF/CAS Trunks

For MF/CAS trunks, CAS signaling (ABCD signaling bits and MF tones) will be converted to/from MGCP signaling requests and events by the Trunking Gateway. This includes:

- MF tones converted to/from digit strings inside either an MGCP Notify or Notification Request (or combined with a Connection or Modify Connection Request).
- Off-hook and on-hook indications converted to/from events inside either an MGCP Notify or Notification Request (or combined with a Connection or Modify Connection Request).

However, lower level signaling and timing will be done within the trunking gateway itself (e.g. wink-start) rather than controlling via MGCP. MF wink-start incoming trunks for Busy Line Verify and Operator Interrupt is compatible with the Feature Group D [TR-NPL-00258] termination protocol.

MF trunks for 911 and operator services are compatible with Feature Group D [TR-NPL-00258], Operator Service (OS) Signaling protocol. In this case the customer network appears to be a Regional Bell Operating Company (RBOC) network.

## ISUP Trunks

Given that there is no signaling on ISUP trunks, interaction with the Call Agent is limited to making connections and doing continuity tests. MGCP 1.0 is used to send requests to the TGW to make or modify connections in order to set up RTP media streams and to request connections for continuity tests.

## Call Control Components

The Cisco BLISS for Cable solution relies on interoperability with partner systems for various functions that are not directly supported. The partner systems include multimedia terminal adapters (MTAs), announcement systems, interactive voice response systems, voice mail systems, billing mediation systems and electronic surveillance systems.

### Cisco BTS 10200 Softswitch

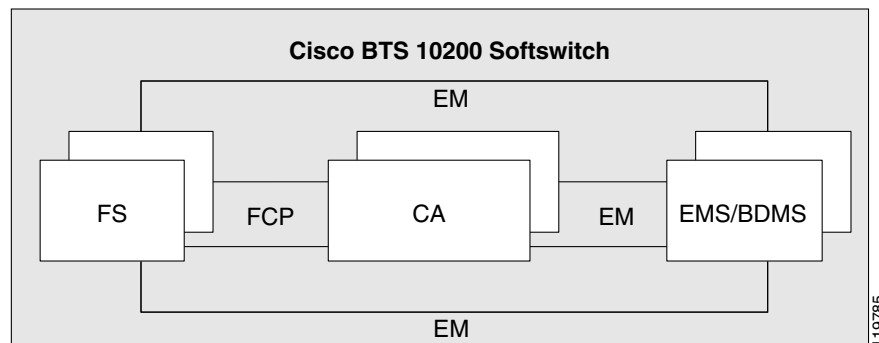
The Cisco BTS10200 provides the call processing intelligence of the network, handling call control for the establishment and tear-down of telephony calls, the service logic required to deliver services, the linkages to signaling networks, familiarity with dialing plans, and appropriate hooks to operational support systems. Release 3.5 of the BTS10200 softswitch is to be used in the solution (three cable packages in 3.5 release).

The Cisco BTS 10200 consists of four logical components (Figure 1-5) in a distributed architecture:

- **Call Agent**—The call agent (CA) component serves as a call management system and media gateway controller. It handles the establishment, processing, and tear-down of telephony calls.
- **Feature Servers**—The feature servers (FS) provide POTS, Centrex, Tandem, and Advanced Intelligent Network (AIN) services to the calls controlled by the CAs and also provides processing for service features such as call forwarding, call waiting, local number portability, and so forth. The FS processes are independent from the CA process.
- **Element Management System**—The element management system (EMS) controls the entire Cisco BTS 10200, and acts as a mediation device between an NMS and one or more CAs. It is also the interface for the provisioning, administration, and reporting features of the Cisco BTS 10200.
- **Bulk Data Management System**—The bulk data management system (BDMS) coordinates the collection of billing data from the CA, and the forwarding of billing records to the billing server.

The EMS and BDMS are colocated on one host machine and the CA and FS are colocated on another host machine. Interworking of CA and FS with media gateways (MGW) provides PSTN-parity voice service and a reliable migration platform for next-generation services.

**Figure 1-5 Cisco BTS 10200 High Level Block Diagram**



EM – Element management link  
 FCP – Feature control protocol  
 CA – Call agent  
 EMS/BDMS – Element management system/bulk data management system

## Cisco BTS 10200 Capabilities

At a high level, the Cisco BTS10200 Softswitch provides the following capabilities:

- Support for MGCP call control with the TGWs and NCS signaling on the MTA side.
- Call signaling capabilities including SS7/ISUP interactions with the PSTN SS7 network, which includes support for SCP database dip applications like 800 number and LNP services.
- Universal Signaling interworking functions between protocols associated with each leg of the call.
- Address resolution and call routing.
- CDR or event message generation.
- Resource management and connection control.
- Service access function for services executing on external server platforms (such as Feature Servers, SCPs, and so on).
- Management interfaces (using SNMP and/or CORBA and/or CLIs).
- Gate management function and DQoS support.

The Cisco BTS 10200 Softswitch, [Figure 1-6](#), is deployed in a fully redundant active/standby configuration where the secondary call agent takes over if the primary call agent fails. It has been designed for high availability (99.999%) with no single point of failure. A single Call Agent consists of an active unit, a standby unit, and a separate set of links to terminate SS7 traffic.

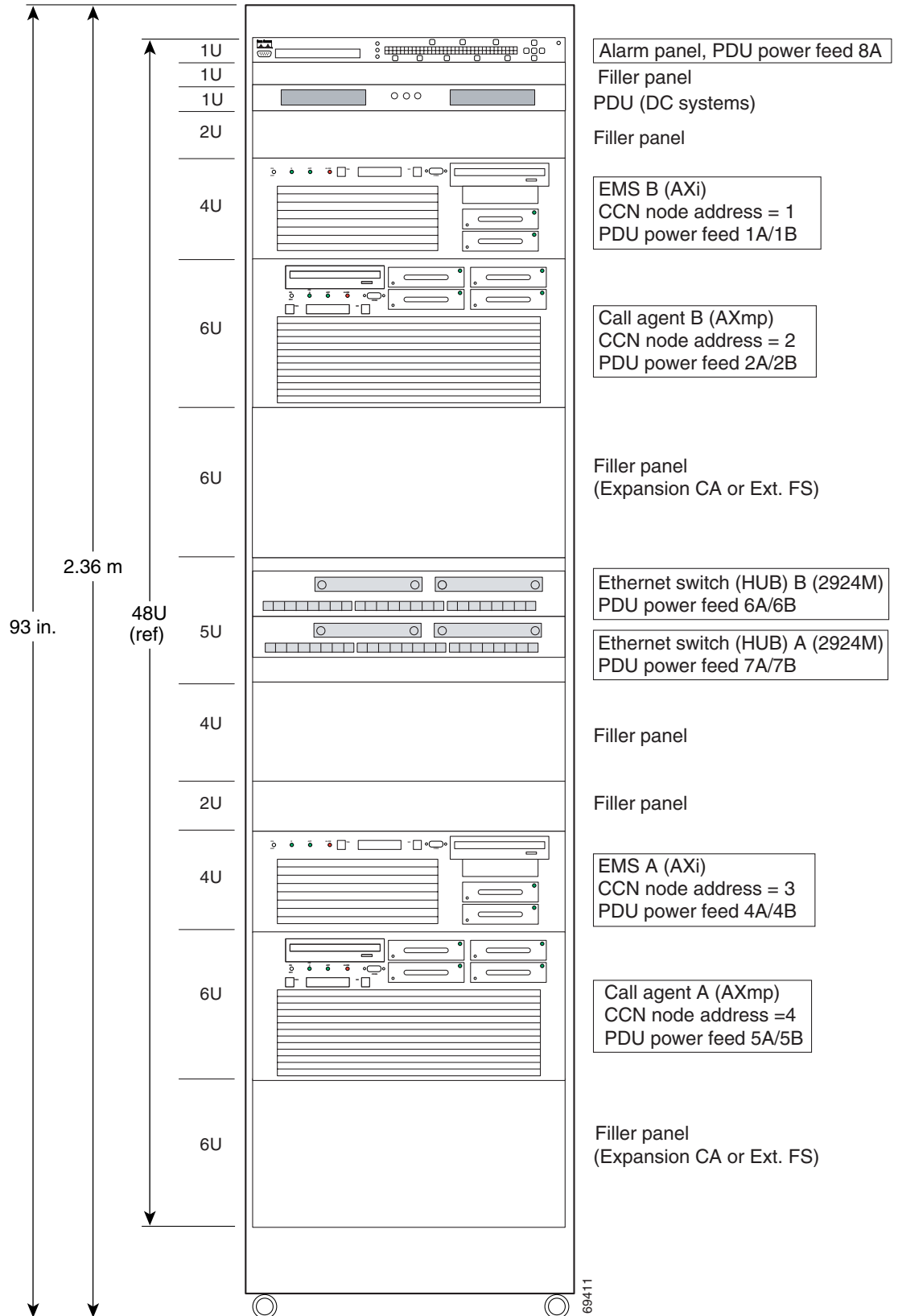
Other Cisco BTS 10200 elements, including Feature Servers and EMSs, are also deployed in active/standby configurations with real time synchronization of data between the active and standby elements. If no response is received from the primary call agent, the alternate call agent becomes the primary CA. Call state information is copied from the active to the standby call agent. This ensures that no established calls are lost in a switch over from active to standby.

The call control signaling between the gateways and the call agent uses the standard MGCP 1.0 specifications where when no response is received from the primary call agent, the alternate call agent becomes the primary call agent. Feature Control Protocol (FCP) is used to interact with third party application platforms for enhanced services and SIP-T is used for inter-call agent communications. The control interaction between the messaging platform and the Cisco BTS10200 is via SIP or SIP-T. The Cisco BTS 10200 EMS collects the call information including billing CDRs (or event messages) and call logs and sends it to the Record Keeping Server (RKS).

The Call Agent runs on a Continuous Computing platform or on Sun Solaris hardware and SS7/ISUP trunks terminate on this platform. It provides the call processing intelligence for the network, handling call control for the establishment and tear-down of calls, the service logic required to deliver services, the linkages to signaling networks and the appropriate hooks to operational support systems (OSS). Call processing is performed with MGCP 1.0/NCS 1.0 call control signaling.

Feature servers, which provide the logic for enhanced services, are part of this complex. An EMS system which manages the Call Agent and the Feature Servers and provides subscriber/network provisioning functions is also part of the Call Agent infrastructure residing in the SuperPOP. The Cisco BTS 10200 Softswitch also supports deployment of Feature Servers on separate platforms. The call routing intelligence resides on the Call Agent and feature logic on the Feature Server.

Figure 1-6 Cisco BTS 10200 Softswitch



## Signaling System 7 (SS7) Links

The SS7 links provides an interface between the Call Agent and the SS7 network. The signaling links carrying SS7 messages terminate on signaling interfaces in the Call Agent.

Telcordia's [GR-246-CORE] document provides the necessary requirements that the SS7 interfaces need to perform for:

- SS7 message handling (message discrimination, message distribution, and message routing)
- Signaling Network Management, which is grouped under following three categories:
  - Signaling Link Management (link activation, deactivation)
  - Signaling Route Management (managing PC route status based on route received management messages)
  - Signaling Traffic Management (diversion of traffic based on unavailability, availability, restriction of signaling link, route, and PC)

## Ancillary Servers

The following servers are also components of the Cisco BLISS for Cable solution that might be located in a headend, in the regional backbone, or in a service providers Internet Protocol Central Office (IPCO).

Refer to the manufacturer's documentation for detailed information on these servers.

- [Record Keeping Server, page 1-22](#)
- [Announcement Servers, page 1-23](#)
- [CALEA Server, page 1-24](#)
- [DHCP, DNS, TFTP and TOD Servers, page 1-24](#)

## Record Keeping Server

When a call is initiated, the Record Keeping Server (RKS) receives messages from the Call Agent representing one of two events. The first event occurs when a call is established. The second event occurs at the termination of the call. In the case of unsuccessful calls, only a failure message is logged. The service providers accounting gateway converts this information into Bellcore Automatic Messaging Accounting Format (BAF) records and sends these BAF records to a mediation system using FTP.

To create appropriate BAF records, the event information produced by the Call Agent must have appropriate information for the telephone service required. This includes, but is not limited to, the following elements:

- phone number of the calling party (customer)
- phone number of the called party (customer)
- time call is placed
- duration of the phone call
- use of any discretionary features

**Bellcore Automatic Message Accounting Format (BAF)**—is the standard AMA format used by circuit-switching systems, packet-switching systems, and other network elements to provide billing usage measurement data. This data is needed either to permit charging the customer for use of network services or to permit charging other carriers (including Interexchange Carriers [IECs] and other Local Exchange Carriers [LECs]) for assistance in placing call connections.



In terms of billing for on-net versus off-net calls, different BAF structures are generated between on-net calls, which are defined as calls completed within the service providers network, and off-net calls, which are defined as calls completed outside the service providers network, such as PSTN calls.

**RADIUS**—is the protocol defined in Internet Engineering Task Force (IETF) Request for Comments (RFC) 2138, Remote Authentication Dial In User Service (RADIUS). The use of the RADIUS protocol for accounting purposes is defined in IETF RFC 2139, RADIUS Accounting, which defines the use of two RADIUS packet types for accounting: Accounting-Request and Accounting-Response.

- Accounting-Request packets are mainly used to convey raw usage data. These packets are also used to indicate when accounting has been turned on or off at the RADIUS Accounting Client, which is the component that generates usage data and creates Accounting-Request packets.
- Accounting-Response packets are used by the RADIUS Accounting Server, which is the recipient of Accounting-Request packets, to acknowledge the receipt of Accounting-Request packets.

In the defined BLISS for Cable architecture, the role of the RADIUS Accounting Client is played by the Cisco BTS 10200, and the role of the RADIUS Accounting Server is played by the accounting gateway.

## Announcement Servers

The Announcement Server (AS) receives MGCP signaling control messages from the Cisco BTS 10200 Call Agent and sends announcements to specified destinations, such as subscriber MTAs, using RTP.

The Announcement Server supports the following capabilities:

- Announcement servers store local copies of all audio announcements
- The Call Agent communicates with an announcement server to provide announcement services using MGCP.

These communications include:

- A request from the Call Agent to create a connection context
- A request from the Call Agent to start sending a specified announcement file to a specific address/port on the IP network.

The announcement server sends announcements as a series of RTP packets over the IP network. The request also dictates whether an announcement is to be sent once, a specified number of times, or in a continuous loop.

- A request from the Call Agent to terminate the connection context and end the play operation
- A message from the Announcement Server to the Call Agent indicating that the play operation has been terminated.

The announcement server does not support the following:

- data dependent announcements
- Only G.711 encoding is supported in the first solution release
- Only single announcements are supported.

In addition, there are no indicators present in the Call Agent to allow user specified multilingual announcements.

- Signaling tones, such as a busy signal, can be played by the MTA, but Special Information Tones (SIT) can be included as part of an announcement file.

## CALEA Server

The Cisco BTS 10200 supports the Communications Assistance for Law Enforcement Act (CALEA).

- The Cisco BTS 10200 provides the PacketCable EMS/RADIUS interface for the transmission of call identifying information (call data) to the CALEA delivery function (DF) server. The BTS 10200 implementation is independent of the access network application, such as packet cable or T1.
- The call content function captures voice in the form of a replicated realtime transport protocol (RTP) stream. The replicated RTP stream is sent to the CALEA DF server upon request from the CA. The CA request is addressed to the appropriate intercept access point, such as:
  - An aggregation router—Sent via control commands based on the Common Open Policy Service (COPS) protocol
  - A trunking gateway—Sent via MGCP commands



### Note

The CALEA call data and call content features are currently based on industry-developed standards, including the PacketCable Electronic Surveillance Specification (PKT-SP-ESP-I01-991229). Cisco will post information regarding the impact of any future technical requirements necessary to permit telecommunications carriers to comply with CALEA's assistance capability requirements.

### CALEA Call Data Function

There are two call data functions supported by the Cisco BTS 10200.

- The Cisco BTS 10200 supports a secure provisioning interface to process intercept and wiretap requests from law enforcement agencies. (The service provider organization can limit viewing and provisioning of these parameters to selected authorized personnel.) The applicable parameters (entered via CLI) include the subscriber ID and DN, trap type, and call data channel for data transmission. The trap type specifies whether the tap order is a pen register (outgoing call information), a trap and trace (incoming call information), a pen and trace (incoming and outgoing call information), or an intercept (bidirectional plus the call content).
- The Cisco BTS 10200 supports the requirements of the enhanced PacketCable Event Messages Specification (EMS) PKT-SP-EM-I02-001128 tailored for CALEA as specified by the PacketCable Electronic Surveillance Specifications PKT-SP-ESP-I01-991229 and PKT-SP-ESP-D02-991207. Full call-identifying information (call data) is shipped to a CALEA DF server from the Cisco BTS 10200 for the subject under surveillance for various call types (basic call, call forwarding, and so on). A CALEA DF server compliant with the PacketCable Electronic Surveillance Specifications, and per Cisco wiretap interface specification, must be deployed in the network.

## DHCP, DNS, TFTP and TOD Servers

A DHCP server must be installed at the headend. The DHCP server must also offer a time-of-day (TOD) server option that is compliant with RFC 868.

In conjunction with the DHCP server, a Domain Name System (DNS) server must be installed to translate names of network nodes into IP addresses. A Trivial File Transfer Protocol (TFTP) server must be installed to facilitate the transfer of DOCSIS configuration files over the broadband network.

Cisco provides a configuration tool with every Cisco uBR7246VXR universal broadband router—Cisco Network Registrar (CNR)—to automate dynamic IP address allocation to cable modems, PCs, and other devices on the broadband network. CNR provides integrated DHCP and DNS services for your network configuration.

### MTA Provisioning

The Cisco Subscriber Registration Center (CSRC) v1.5 [with Cisco Network Registrar (CNR) 5.0] provides a specialized provisioning environment using CSRC component products that help you automate subscriber service provisioning, such as VoIP, e-mail, Web access, and configuration of subscriber MTAs, including DOCSIS-compliant MTAs. CSRC 1.5 works in conjunction with CNR to provide DHCP and TFTP services.

Provisioning system servers include the following:

- **DHCP and DNS Server**—CSRC provides IP addresses to CPEs and customer IP devices (PCs) using DHCP. CSRC also provides configuration information to the CPEs that allow them to connect to the network and access the features that they are authorized for. The provisioning system provides a DNS server functionality that maps fully qualified domain names (FQDN) to IP addresses.
- **TFTP Server**—The RFC1350-compliant trivial file transfer protocol (TFTP) server provides the cable modem with the DOCSIS standard configuration file containing QoS parameters and other information required for the MTAs to become operational. The TFTP file server can also be used to provide software upgrade files for the MTAs using the Software Upgrade Filename parameter in the DOCSIS configuration file.
- **Time of Day (TOD) Server**—The time of day server provides the MTA with the correct time of day from Universal Coordinated Time (UTC). The correct time is used to calculate the local time for time-stamping error logs. The TOD server resides on the same physical machine as the TFTP server.

### Cisco BTS 10200 OSS Interfaces

The Cisco BTS 10200 Softswitch OSS interface consists of the following parts:

- Command Line Interface (CLI) over Telnet
- Common Object Request Broker Architecture (CORBA)
- SNMP traps, status, control and measurement
- Billing interface (FTP)
- Bulk provisioning (FTP)

## Solution Features

The features provided by the Cisco BLISS for Cable 1.5 solution fall into the following categories:

- [Network Features, page 1-26](#)
- [Route Selection, page 1-31](#)
- [Subscriber Features, page 1-35](#)

The features included in each category are detailed in the following sections. Additional details of the features can be found in the “Cisco BTS 10200 Softswitch System Description for Release 3.1” located at [http://www.cisco.com/univercd/cc/td/doc/product/voice/bts10200/bts3\\_0/sysdesc/index.htm](http://www.cisco.com/univercd/cc/td/doc/product/voice/bts10200/bts3_0/sysdesc/index.htm).



#### Note

Access to the user documentation for the Cisco BTS 10200 Softswitch is restricted. Contact your Cisco representative for the necessary User ID and Password information.

The Cisco BLISS for Cable solution can be deployed using various network technologies in the MSOC core network.

## Network Features

The network features supported by the Cisco BTS 10200 Softswitch include numbering plan and dialing procedures, tandem service, regulatory features and other network features. Some of these features are defined in Telcordia LSSGR documents. In general, Cisco BTS 10200 Softswitch features delivered via gateway clients behave identically to their PSTN counterparts.

This section includes the following topics:

- [Numbering Plan and Dialing Procedures, page 1-26](#)
- [Tandem Service, page 1-28](#)
- [Regulatory Features, page 1-29](#)
- [Other Network Features, page 1-30](#)
- [Default Office Service ID, page 1-31](#)

## Numbering Plan and Dialing Procedures

Numbering plan and dialing procedures consist of Casual Dialing (Dial Around), Directory Services (411, 555-1212, 0+ Listing Services), Easily Recognizable Codes, Emergency Services (911), Information Service Calls (900 and 976), n11 support (311, 411, 611, 711, 811), Operator Services, Toll Free Services and Vertical Service Codes.

### Casual Dialing (Dial Around, 101XXXX+Digits)

Casual dialing, also known as dial around, specifies whether the carrier supports 101XXXX calls. The digit map CLI command tokens provide the digit pattern. The digit pattern specifies all possible acceptable patterns. An example of a casual digit pattern is 1010321 or 1010220. The digit map table tells the MGW how to collect and report dialed digits to the CA. Subscribers can prefix their interLATA or international calls with 101XXXX.

### Directory Services (411,555-1212, 0+Listing Services)

Directory services allows a subscriber to obtain the listed telephone number for a given name and address. The caller dials a specific service number to reach directory services, also referred to as directory assistance (DA). The supported directory services numbers are:

- 411 or 555-1212 (DA)
- 1+411 or 1+555-1212 (toll DA)
- 1-NPA-555-1212 (mostly for out-of-town/state numbers)
- 1-800/888-555-1212 (toll free numbers)
- 0+ listing services

### Easily Recognizable Codes (500, 700)

The Easily Recognizable Codes (ECRs) supported by the Cisco BTS 10200 Softswitch are:

- 500 personal communications services (PCS)
- 700 service access calls (SAC)
- Toll free service call features (800, 888, 877, 866, 855, 844)
- 900/976 information service calls

### Information Service Calls (900 and 976)

Information service calls (ISC) provide a variety of announcement-related services on a national or local basis. The two general categories of this service are Public announcement services (PAS)-Weather, sports, horoscope, and so forth, and Media stimulated calling (MSC)-Telephone voting, radio station call-ins, and so forth. National calls are dialed as 1-900-xxx-xxxx and local calls are dialed as NPA-976-xxxx.

### N11 support (311, 411, 611, 711, 811)

The N11 services supported by the Cisco BTS 10200 Softswitch are:

- Nonemergency Services (311)
- Directory Assistance (411)
- Repair Service (611)
- Telecommunications Relay Services (711)
- Local Billing Services (811)

### Operator Services Subscriber Access (0,00,0+,01+,CAC+0+,CAC+01+)

Operator services is a call-processing function whereby callers can access either a live operator or an automated function to complete calls or gain access to information. The service provider can provide this feature or outsource it to a third-party vendor. Some additional functions accomplished by operator services include automatic call distribution, billing detail recording, and information retrieval. The numbers commonly used to access operator services are:

- 0—Local operator support
- 00—Operator support outside the “local” calling area, using a presubscribed interexchange carrier (PIC)
- 0+ area code and number—Operator support when the destination number is known (that is, for collect calls, calling card calls, person-to-person calls, and so forth), using PIC
- CAC+0+—Operator services, using a dialed carrier access code (CAC)
- 01+CC+NN—international operator services, using PIC
- CAC+01+CC+NN—International operator services, using a dialed CAC

### Operator Services Busy Line Verification and Operator Interrupt

Busy line verification (BLV) service permits the user to obtain operator assistance to determine if a called line is in use. The user dials 0, waits for the operator to pick up the line, and requests BLV service. If not prohibited in advance by the party on the called line, the operator interrupts the conversation in progress and relays a message. At the user’s request, the operator has the option to directly connect the user to the called line.

### Toll Free Services

The purpose of toll free services is to have the called party, rather than the calling party, charged for the call. These calls are prefixed with the 1+800 or 1-8nn service access codes. The seven digits following the 800/8nn codes are used for routing the call. The Cisco BTS 10200 Softswitch communicates with a database called the toll-free database service, which contains information for routing the call. The database service provides information about the network service provider selected to complete the call, and information for translating the toll-free number to a specific 10-digit directory number (DN).

The routing of the call can vary depending on the arrangements made between the toll-free subscriber and the network service provider. These arrangements can include selective routing based on the time of day, day of week, and location from which the call originates.

## Vertical Service Codes (\*XX)

Vertical service codes (VSC) allow subscribers to activate and deactivate services from their own station. The pre-provisioned VSCs are:

- \*57 Access the Customer-Originated Trace (CT) Function
- \*60 Selective Call Rejection (SCR) Activation
- \*61 Distinctive Ringing on Call Waiting (DRCW) Activation
- \*63 Selective Call Forwarding (SCF) Activation
- \*64 Selective Call Acceptance (SCA) Activation
- \*66 Automatic Callback (AC) Activation
- \*67 Calling Number Delivery Blocking (CNDB)
- \*69 Automatic Recall (AR) Activation
- \*70 Cancel Call Waiting (CCW)
- \*72 Call Forwarding Unconditional Activation (CFUA)
- \*73 Call Forwarding Unconditional Deactivation (CFUD)
- \*74 Access the speed call feature (for 8-number speed call)
- \*75 Access the speed call feature (for 30-number speed call)
- \*77 Anonymous Call Rejection (ACR) Activation
- \*78 Do not disturb activation
- \*79 Do not disturb deactivation
- \*80 Selective Call Rejection (SCR) Deactivation
- \*81 Distinctive Ringing on Call Waiting (DRCW) Activation
- \*82 Calling Identity Delivery and Suppression Per Call (CIDS)
- \*83 Selective Call Forwarding (SCF) Deactivation
- \*84 Selective Call Acceptance (SCA) Deactivation
- \*86 Automatic Callback (AC) Deactivation
- \*87 Anonymous Call Rejection (ACR) Deactivation
- \*89 Automatic Recall (AR) Deactivation
- \*90 Call Forwarding Busy Variable Activation (CFBVA)
- \*91 Call Forwarding Busy Variable Deactivation (CFBVD)
- \*92 Call Forwarding No Answer Variable Activation (CFNAVA)
- \*93 Call Forwarding No Answer Variable Deactivation (CFNAVD)
- \*95 Calling Name Delivery Blocking (CNAB)

## Tandem Service

Tandem service on the Cisco BTS 10200 Softswitch consists of ANI screening and Class of Service (COS) restrictions.

## ANI Screening

Automatic number identification (ANI) is used for long distance access service. The ANI screening feature validates the ANI on incoming feature group D calls from the PSTN before routing. All ANIs supported by the Cisco BTS 10200 Softswitch are stored in the feature server database. If an ANI is not available, or does not appear in the feature server ANI table, the TG default data is checked to see if casual calls are allowed. If casual calls are not allowed, the call is denied and routed to an announcement. If the ANI exists in the table, the ANI status is checked next. The ANI status can either be allowed or blocked. If the status is blocked, the call is blocked and routed to an announcement. The ANI table also includes information on class of service (COS), and authorization/account codes.

## Class Of Service (COS) Restrictions

This service allows blocking calls based on their originating line type, for example, regular subscriber, hotel/motel, coin- phone, prison lines, and so forth. When the CA receives the called and calling party numbers, the following screening checks are performed (in this order):

- II white list and black list
- Called number white list and black list (domestic or international)
- Directory assistance calling restriction
- Operator-assisted calling restriction
- Type of call restrictions (local calling or international calling toll restriction, for example)
- Calling party is allowed to call the called party (check if restricted by COS)

When multiple COS restrictions are assigned to a call, then the most restrictive COS for that call is used.

## Regulatory Features

Regulatory features on the Cisco BTS 10200 Softswitch consists of Emergency Services (911), Local Number Portability, NPA Split Support and Legal Intercept.

### Emergency Services (911)

Emergency services is a public safety feature providing emergency call routing to a designated emergency service bureau (ESB), normally called the public safety answering point (PSAP) in the United States. The 3-digit 911 number is assigned for public use in many areas of the United States and Canada for reporting an emergency and requesting emergency assistance. Depending on municipal requirements and procedures, an ESB attendant can transfer the call to the proper agency, collect and relay emergency information to the agency, or dispatch emergency aid directly for one or more participating agencies.

### Local Number Portability

Local Number Portability (LNP) permits subscribers who change their local phone company to keep their existing telephone number. An FCC order requires this feature in the 100 top metropolitan service areas in the United States. LNP permits calls to be routed to the subscriber's new local switch without any particular per-call action required of either the calling or called party.

## NPA Split Support

When DNs are exhausted within an NPA, an additional NPA is assigned to the region. The new NPA may be allocated as an overlay over the existing NPA, in which case there is no major impact to the Cisco BTS 10200 Softswitch. However, when the new NPA is assigned based on a geographical split of the region, there are significant impacts. The assignment of the new NPA based on a geographical split is referred to as split-NPA.

## Legal Interception (CALEA)

The Cisco BTS10200, as well as the Cisco uBR7246VXR and the Cisco MGX 8850 support the PacketCable Electronic Surveillance Specification. These products, in conjunction with a third party mediation device, provide a MSO with the ability to comply with the requirements of the Communications Assistance for Law Enforcement Act (CALEA) for providing call detail information or call detail/call content information to law enforcement for a specific DN in response to a court order.

## Other Network Features

Other network features on the Cisco BTS 10200 Softswitch consists of Dialing Parity, Toll-Free Database Service and Trunk Testing.

### Dialing Parity (IntraLATA Toll Presubscription)

Dialing parity—also known as intraLATA toll presubscription—allows subscribers to select a telecommunications company for intraLATA calls (local toll calls) in the same way they select a long distance provider. With dialing parity, subscribers are able to dial the number they want and have a preselected carrier—a CLEC, ILEC, or a long distance carrier—automatically handle the call if it is a local (intraLATA) toll call. Preselecting a local toll carrier eliminates the need for dial-around service for local toll calls (101XXXX numbers).

### Toll-Free Database Service

The Cisco BTS 10200 Softswitch provides the ability to translate inbound/outbound 800 numbers at the FS using a local 800 database. The 800 service supports the following features:

- Origin dependent routing
- Time of day routing
- Percentage based routing
- Information digit-based screening
- Black/white list screening

The Cisco BTS 10200 Softswitch also supports optional DNIS service. In an 800 DNIS service, when a call is terminated to a PBX (call center), 4 digits are outpulsed to the PBX to identify the originally dialed 800 number. In case of custom DNIS, up to 22 digits can be outpulsed with additional information such as:

- Original 800 number dialed
- Automatic number identification (ANI)
- Originating line information of the calling party



## Trunk Testing

Trunk testing is used to determine the transmission quality of the shared trunks that interconnect switching systems. Trunk testing is extremely important in monitoring system health, because it is the only practical way to objectively determine the performance of individual trunks.

### Near End Test Origination Test Calls

The Cisco BTS 10200 Softswitch supports calls used to test individual trunks that connect a local gateway with a gateway or PSTN switch at a remote office. The Cisco BTS 10200 Softswitch supports OTL and TTL capability. User-provided test equipment and, optionally, test controllers may be connected to the test lines. Proper selection of test equipment and test functions helps to ensure interoperability between different carriers.

### 1XX Test Line

When the Cisco BTS 10200 Softswitch is the near end switch, the remote switch recognizes the trunk test prefix (9581 or 9591) on the incoming signal, and the test type is used to route the test to the appropriate test line. The appropriate tests are performed on the test set and additional test processes may occur, depending on the specific test configuration.

When the Cisco BTS 10200 Softswitch is supporting the TTL capability (test call originated at another switch), it receives the 958 or 959 call, recognizes the 958 or 959 type, and routes the test to the appropriate test line.

## Default Office Service ID

One service ID (the default office service ID, typically ID=999) is reserved for provisioning of switch-based features. These switch-based features can include certain network features and certain usage-sensitive features. The service provider must provision this service ID in the service table, and define these features in the feature table.

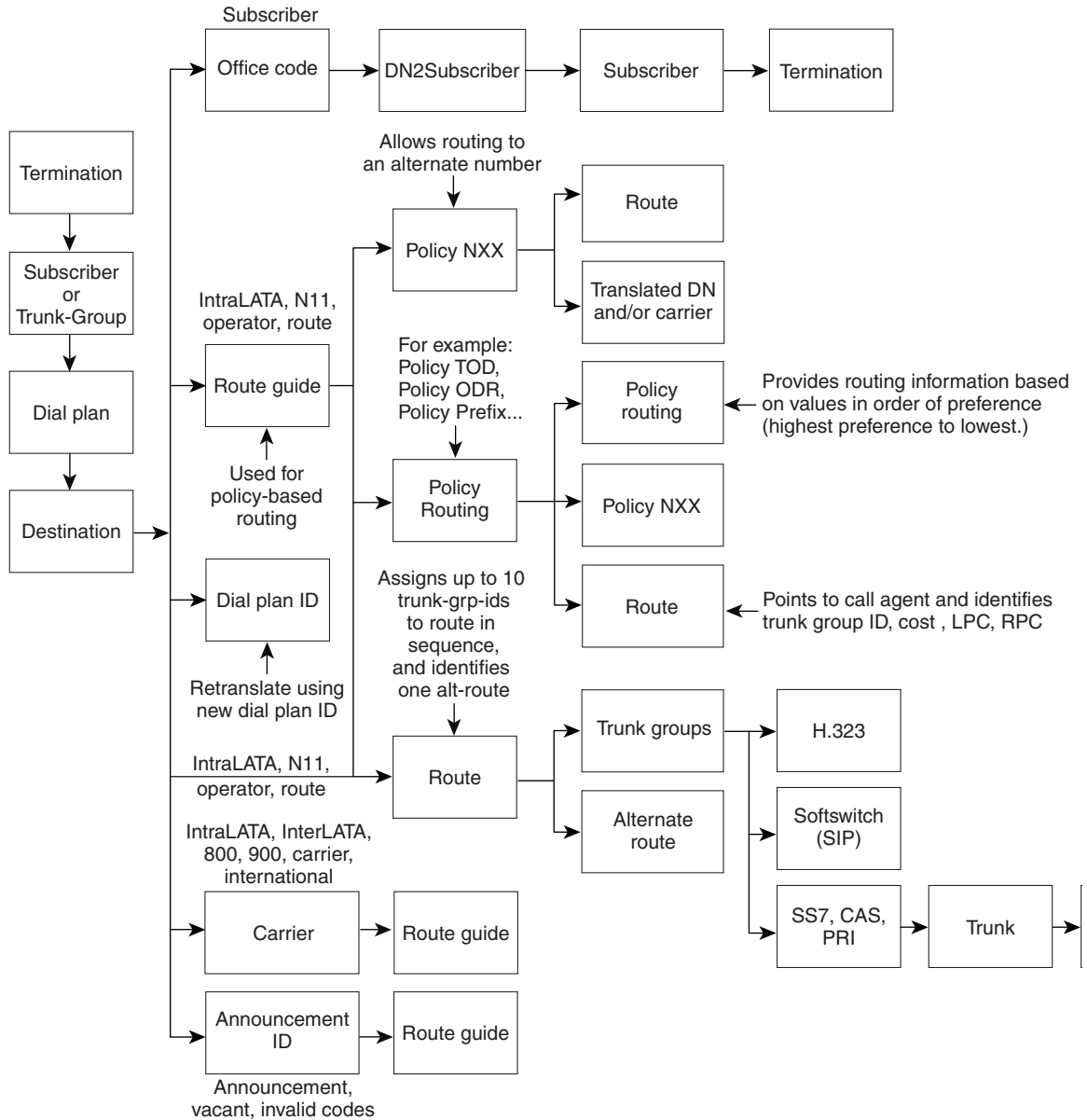
## Route Selection

As shown in [Figure 1-7](#), when a request for routing is received by the routing subsystem, the subsystem first searches through the termination table to determine whether the called number is a subscriber.

If the called number is a subscriber, the dial plan table processes the call through the dn2subscriber and subscriber tables. If the called number is not a subscriber, the call is either routed to the appropriate trunk using one of the following:

- [Policy-Based Routing, page 1-32](#)
- [Carrier-Based Routing, page 1-34](#)
- [Trunk Group Selection Policies, page 1-34](#)

Figure 1-7 Route Selection Flowchart



## Policy-Based Routing

If policy-based routing is required, the dial plan entry for the corresponding called number (NPA/NXX) is associated with the route group ID. The Cisco BTS 10200 supports all of the following:

- [Least-Cost Routing, page 1-33](#)
- [Prefix-Based Routing, page 1-33](#)
- [Line-Based Routing, page 1-33](#)
- [ANI-Based Routing, page 1-33](#)
- [Region-Based Routing, page 1-33](#)
- [Time of Day \(TOD\) Routing, page 1-33](#)

- [Percentage-Based Routing, page 1-34](#)
- [Route ID, page 1-34](#)

### Least-Cost Routing

With least-cost routing (LCR), the least expensive Trunk Group (TG) in a route is chosen. The TGs in a list may be provisioned in any order. The call processing function will find the relative cost of each TG in the route from the TG table and order them from least to most expensive. The least expensive idle trunk will be selected from this newly ordered TG list.

### Prefix-Based Routing

Prefix-based routing is used to route calls to an inter-exchange carrier. A service provider can choose to route calls over different TGs based on the prefix dialed.

The supported call types and their associated prefixes are:

- National (1+)
- International (011+)
- Operator (0-, 00)
- National operator (0+)
- International operator (01+)
- Toll free (8xx)
- Cut-through calls (101xxxx+#)
- Directory assistance (555-1212, NPA-555-1212)

### Line-Based Routing

Routing of calls can be based on the originating subscriber line class (such as coin, coinless, hotel/motel or multiparty). If an incoming call is received over a feature group D SS7 TG, the originating line information parameter is used to determine the route.

### ANI-Based Routing

Automatic Number Identification (ANI) routing is based on the subscriber ID of the calling party. The service provider can enable ANI-based routing by setting the ANI-BASED-ROUTING flag in the TRUNK-GRP table. When a call is received by the Cisco BTS 10200, the Cisco BTS 10200 performs a subscriber lookup based on the ANI (DN), and uses the subscriber properties to route the call.

### Region-Based Routing

If region-based routing is required, the Cisco BTS 10200 uses a look-up table to convert the calling party's dialing number (DN) to a region. The Cisco BTS 10200 then routes the call according to the information provisioned for this region. If ANI is not available, the Cisco BTS 10200 routes the call according to the region assigned to the originating TG.

### Time of Day (TOD) Routing

TOD routing is based on day of year (DOY) and day of week (DOW)/time of day (TOD). If a matching DOY entry is found, the call is routed on the basis of the DOY. Otherwise the call is routed based on the DOW/TOD table. If an entry corresponding to the DOW/TOD is not found, a default entry should be provided in the database for routing.

## Percentage-Based Routing

Percentage-based routing allows call distribution of a specified percentage of calls to different route groups. The percentage ranges can be specified to a granularity of 1 percent, and the ranges should cover a total of 100 percent. A random number generator is used to sort calls into the specified percentage ranges, and the percentage range is used to route each call.

## Route ID

The route table is used when the routing policy is specified as route ID. A TG is selected based on the trunk group selection policy specified in the route table.

## Carrier-Based Routing

In a wholesale network environment, the wholesale network operator (NO) owns and operates the facility. The NO provides transport facilities to carry voice calls on behalf of smaller SPs and for SPs that are not facility based. Some SPs may own facilities terminating directly on NO equipment. The Cisco BTS 10200 can route calls over the SP facilities, if a route exists on the SP facilities, or route calls over NO facilities if SP based facilities do not exist.

This section includes the following topics:

- [Carrier Selection for Outgoing Calls, page 1-34](#)
- [Carrier Selection for TG-Originated Calls, page 1-34](#)

### Carrier Selection for Outgoing Calls

For outgoing interLATA calls, the Cisco BTS 10200 selects the carrier based on the subscriber's presubscribed inter-exchange carrier (PIC), or the dialed carrier ID if the call was a casual call.

For outgoing toll-free calls, the Cisco BTS 10200 receives the carrier ID based on a toll-free query to a service control point (SCP).

For outgoing 500 (PCS rate) and 900 (premium rate) calls, the DESTINATION table can be provisioned with unique carrier IDs for each of these call types. The Cisco BTS 10200 routes the calls via these assigned carriers.

### Carrier Selection for TG-Originated Calls

In a Class 4 environment, the Cisco BTS 10200 is connected to several PSTN switches. For trunk groups (TGs) between the Cisco BTS 10200 and a Tandem switch, the TG table can be provisioned to route the call based on either the carrier ID or the SP ID.

## Trunk Group Selection Policies

The TG selection policies are applied once a route has been selected. If all the TGs in a route are busy, the route can point to an alternate route.

TG selection policies are also applied based on the user requirements. The TG selection policies are not applied if the user has not requested any capabilities. The selection policy supported is selection of TG by cost.

## Trunk Selection Policies in the TG

Trunk selection policies are applied to each TG, and allow the service provider to control the assignment of trunks. The CA can be provisioned to select trunks in ascending order (default), select trunks in descending order, select only even numbered trunks, select only odd numbered trunks or select the least recently used trunk.

## Glare Resolution Parameter in the TG

The glare parameter in the TG table is provisioned for bothway trunks. The glare parameter defines whether a trunk group is master of odd numbered trunks, a trunk group is master of even numbered trunks, a trunk group is master of all trunks or a trunk group yields any trunk in glare condition.

# Subscriber Features

The Cisco BTS 10200 Softswitch supports subscriber features, including selected custom local area signaling service (CLASS) features. Most of these features are defined in Bellcore LSSGR documents. In general, Cisco BTS 10200 Softswitch features delivered via gateway clients behave identically to their PSTN counterparts. Some features can be accessed and controlled by the subscriber using a handset and vertical service codes (VSCs). VSCs are provisionable by the service provider.

This section includes the following topics:

- [Call Forwarding Features, page 1-35](#)
- [Calling Identity Features, page 1-36](#)
- [Class of Service \(COS\) Restrictions, page 1-37](#)
- [Direct Inward/Outward Dialing for PBX, page 1-40](#)
- [General Subscriber Features, page 1-40](#)
- [Default Office Service ID, page 1-45](#)

## Call Forwarding Features

Call forwarding is a group of features allowing incoming calls to a subscriber line to be forwarded to another telephone number, including a cellular phone number, under various circumstances. Call forwarding features allow a subscriber line to be forwarded to a number that itself can be forwarded. This chaining of call forwards is allowed to a maximum of five different stations as long as none of the station numbers appears twice in the forwarding list (in order to prevent loops). Before forwarding a call outside of a zone or off net, the system must determine if the forwarding station already has an active call that has been forwarded to the same destination. If so, forwarding is denied to the second call and a station busy signal is returned to the caller.

### Call Forwarding Unconditional (CFU)

CFU allows the user to forward all calls regardless of the status of the user's line. A typical forwarding address is voicemail, a remote telephone, or an attendant. A user whose station is idle, and that has CFU activated, receives a reminder ring when incoming calls are forwarded, but is not able to answer the call. A reminder ring is a half second burst of ringing. The reminder ring is not applied when the forwarding station is off hook. CFU can be activated permanently at subscription time by the service provider or activated and deactivated by the user using VSCs.

## Remote Activation of Call Forwarding (RACF)

Remote activation of call forwarding (RACF) permits the user to control their CFU functions when they are away from their phone. The service provider sets up this function for the user, and designates a DN the user should call to access IVR functions that control the RACF feature. Once set up for RACF, the user can activate CFU, deactivate CFU, and change the target DN of CFU from a remote station.

## Remote Call Forwarding (RCF)

RCF allows incoming 7-digit or 10-digit calls to be routed automatically to a remote DN, which can be in another NANP area. RCF is activated by the service provider at customer request. With the RCF feature, all calls to the specified DN are always forwarded to a remote address.

## Call Forwarding on Busy (CFB)

CFB allows a user (the called party) to instruct the network to forward calls when their line is busy. A typical forwarding number is voicemail. Since the forwarding station is off hook when the CFB feature is executed, no reminder ring is generated. CFB can be activated permanently at subscription time by the service provider or activated and deactivated by the user using VSCs.

If a user with CFB and Call waiting (CW) is already involved in a call, the next incoming call is not forwarded. However, any additional simultaneous incoming calls will be forwarded. If a user with CFB and CW has gone off hook but has not yet completed a call or the call is in a ringing state, and there is an incoming call, the call will be forwarded.

## Call Forwarding on No Answer (CFNA)

CFNA allows a user (the called party) to instruct the network to forward calls when their own station does not answer the incoming call within the first 5 rings (default setting, but number of rings is configurable). A typical forwarding number is voicemail. Because the forwarding station is ringing when the CFNA feature is executed, no reminder ring is generated. CFNA can be activated permanently at subscription time by the service provider or activated and deactivated by the user using VSCs.

## Calling Identity Features

Calling identity features include Calling Identity Delivery Blocking, Calling Number Delivery Blocking, Calling Name Delivery Blocking, Calling Identity Delivery and Suppression, Calling Number Delivery, Calling Name Delivery and Calling Identity Delivery on Call Waiting.

## Calling Identity Delivery Blocking (CIDB)

CIDB allows caller to control whether or not their calling identity information is delivered with outgoing calls. Identity includes directory number (DN) and/or name of the caller. CIDB does not affect the presentation of caller's information when making 911 calls. The CIDB feature affects the presentation status (PS) of the calling identity information. The PS is a flag that lets the network know if it is permissible to deliver the information to the called party. Both the calling number and calling name have PS information associated with them. The subscriber can request the service provider to provision a permanent PS (PPS) at subscription time. A caller with the CIDB feature enabled can override the default values for the PS flags using Per-call PS (PCPS).

### Calling Number Delivery Blocking (CNDB)

CNDB allows the caller to control the status of their caller number privacy on a per-call basis. For all new calls, the privacy status reverts back to the PPS.

### Calling Name Delivery Blocking (CNAB)

CNAB allows the caller to control the status of their caller name privacy on a per-call basis. For all new calls, the privacy status reverts back to the PPS.

### Calling Identity Delivery and Suppression (CIDS)

CIDS allows a caller to explicitly indicate on a per-call basis whether both the calling name and calling number will be treated as private or public. For all new calls, the privacy status reverts back to the PPS.

### Calling Number Delivery (CND)

The CND feature provides CPE with the date, time, and DN of an incoming call. When the called subscriber line is on hook, the calling party information is delivered during the long silent interval of the first ringing cycle.

### Calling Name Delivery (CNAM)

CNAM is a terminating user feature allowing CPE connected to a switching system to receive a calling party's name, number, and the date and time of the call during the first silent interval. If a private status is assigned with the name, the name will not be delivered and a private indicator code P is sent to the CPE. If the name is not available for delivery, the switch sends an out-of-area/unavailable code O to the CPE.

### Calling Identity Delivery on Call Waiting (CIDCW)

CIDCW is a service that enables a called party to receive information about a calling party on a waiting call while off hook on an existing call. CIDCW provides the capability of calling identity delivery (CID) information to the called party on waiting calls. CIDCW is considered an enhancement of the CW feature, and requires the basic CW feature, along with the CND or CNAM feature.

If the calling party's caller ID is not available (for example, if the caller has blocked caller ID) then the called party's caller ID display will indicate an anonymous call or other unidentified caller message as in the caller ID feature.

## Class of Service (COS) Restrictions

The class of service (COS) restrictions are defined for a for a subscriber or a location. Restrictions can be call category restrictions or black list/white list restrictions.

### Authorization Codes and Precedence

Authorization codes can be assigned to call category restrictions. If a user is restricted from making a certain category of call, and has a subscription to an authorization code, the call can be allowed if the user enters the correct authorization call. Authorizations codes cannot be provided for black/white list restrictions.

## Casual Call Restrictions (101XXXX)

The casual call restrictions are used to allow/restrict calls dialed with a casual code prefix (101XXX). The following restrictions can be provisioned:

- No casual calls allowed—User cannot make 101XXXX calls
- All casual calls allowed—User can make 101XXXX calls
- 101XXXX white list—Only a predefined set of XXXX codes can be dialed
- 101XXXX black list—All XXXX codes can be dialed except for a predefined set

For NANP operator calls (0+NPA-NXX-XXXX) and international operator calls (01+CC+NN), casual-call screening is not performed, even if the casual-call restriction is provisioned in the cos-restrict table for the calling party.

## NANP Call Restrictions (Toll Restrictions)

The NANP call restrictions are used to allow/restrict calls to destinations based on a predefined grouping of LATA, state, country, or group of countries. Customers can subscribe to one of the following:

- All NANP calls—There are no restrictions on calls to NANP areas
- National Only—Calls are restricted to within the country
- IntraState Only—Calls are restricted to within the state
- IntraLATA Only—Calls are restricted to within the area defined as the local service area
- Local Only—Calls are restricted to local only

For NANP operator calls (0+NPA-NXX-XXXX), NANP call restriction screening is not performed, even if the NANP call restriction is provisioned in the cos-restrict table for the calling party.

## International Call Restrictions

The international call restrictions are used to restrict/block calls made outside the country, and to certain countries within the NANP. The following restrictions can be applied:

- No international calls allowed—Does not allow any international calls outside NANP
- International white list—Allows only those calls that have a prefix noted in the white list
- International black list—Does not allow any calls that have a prefix noted in the black list
- All international calls allowed—No restrictions are applied on any international calls

For international operator calls (01+CC+NN), international call restriction screening is not performed, even if the international call restriction is provisioned in the cos-restrict table for the calling party.

## NANP Black and White Lists (Number Blocking)

This restriction allows/blocks NANP category calls to a predefined list. Customers can subscribe to one of the following:

- No restrictions (default)
- NANP white list—Only calls within a predefined prefix list can be called. The list could consist of NPA or NPANXX codes. Three to ten digits can be specified for this restriction.
- NANP black list—All calls within a predefined prefix list are blocked. The list could consist of NPA or NPANXX codes. Three to ten digits can be specified for this restriction.



## Other Restrictions

The service provider can provision blocking or unblocking of any or all of the following services based on customer requests:

- Block 900 Calls—allows all calls of the form 1-900-XXX-XXXX to be blocked.
- Block 976 Calls—allows all calls of the form 976-XXXX or NPA-976-XXXX to be blocked.
- Block DA Calls—allows all calls of the form 411, 1+411 or NPA-976-XXXX to be blocked.
- Block Info Calls—allows all calls to information services to be blocked.
- Block Time/Weather Calls—allows all calls to time and weather services to be blocked.
- Block NANP Operator Assistance Calls—allows all 0+ calls (0+NPA-NXX-XXXX) to be blocked.
- Block International Operator Assistance Calls—allows all 01+ calls (01+CC+NN) to be blocked.

## Combination of Call Categories and Associated Restrictions

For any call, it is possible that a combination of call categories are applicable—for example, a casual operator-assisted national call. Under these conditions the restrictions are applied based on the following priority.

- Highest priority—InterLATA, IntraLATA, International, 900, 976, DA call restrictions
- Lower priority—0-, 0+ and 01+ calls
- Lowest priority—Casual call restrictions

If a customer is subscribed to an authorization code, the system checks for all restrictions before prompting the subscriber to enter the code. When the proper code is entered, the call will be placed.

## Account Codes and Authorization Codes

The Cisco BTS 10200 Softswitch supports account codes and authorization codes as specified in LSSGR module FSD-02-02-1010 (TR-NWT-000605), Authorization Codes for Automatic Flexible Routing (AFR) and Account Codes for Basic Business Group and AFR.

### Account Code Description

Account codes provide collection of 1 to 12 digits to allow call charging to user projects, departments or special accounts. The user activates account codes by dialing a number (usually a long distance call) that requires an account code for call completion. Account codes are not collected for any of the following call types, even if an account code requirement is provisioned in the cos-restrict table for the calling party:

- 0+, NANP Operator calls
- 01+, INTL Operator calls
- Local calls

### Authorization Code Description

Authorization codes, also referred to as validated account codes, can be used by an intended user or group to override selected COS calling restrictions. An example of the authorization code would be one in which a user may be restricted from making long distance calls. The user can override the restriction by dialing an authorization code that has enough privileges to make long distance calls.

## Number Blocking

Number blocking prevents certain types of calls from being completed from a particular line or station. When the caller encounters a call that is blocked, the caller can receive any of several blocking treatments such as reorder tone, announcement or routing to an attendant. Number blocking is activated/deactivated and administered by the service provider on a per line or per group of lines basis. The service provider can prohibit calls based on different dialing plans and formats (for example, NPA, NPA-NXX-XXXX, 011+ for international calls, and so forth) combined with other restriction criteria such as type of service (for example, flat rate versus usage rate).

## Direct Inward/Outward Dialing for PBX

The Cisco BTS 10200 Softswitch supports the direct inward dialing (DID) and direct outward dialing (DOD) features for PBX.

### Analog DID for PBX

The Cisco BTS 10200 Softswitch supports analog DID for PBX as specified in TIA/EIA-464B, Requirements for Private Branch Exchange (PBX) Switching Equipment, April 1, 1996. The analog DID one-way feature allows incoming calls to a local PBX network to complete to a specific station without attendant assistance. The station address is provided by the CA that controls an access gateway (AGW) connecting to the PBX. The number of digits to be outpulsed by the AGW to the PBX is configurable in the CA.

### DOD For PBX

The DOD feature allows outgoing calls from a specific station to be completed through the local PBX network without attendant assistance. The CA serving the PBX recognizes the station address and routes the call to the PBX.

## General Subscriber Features

The general subscriber features available are Anonymous Call Rejection, Automatic Callback, Automatic Recall, Call Block, Call Waiting, Cancel Call Waiting, Call Transfer, Customer-Originated Trace, Do Not Disturb, Hotline Service, Interactive Voice Response Functions, Multiline Hunt Group, Multiple Directory Numbers, Speed Call, Subscriber-Controlled Services and Screening List Editing, Three-Way Calling, Usage-Sensitive Three-Way Calling, Visual Message Waiting Indicator and Warmline Service.

### Anonymous Call Rejection (ACR)

The ACR feature allows users to reject calls from parties that have set their privacy feature to prevent calling number delivery. When ACR is active the called party receives no alerting of incoming calls that are rejected. The incoming call is rerouted to a denial announcement indicating that private numbers are not accepted by the called party. To complete a call to the party with ACR, the calling party must activate CID and then place a call to the party with ACR. Incoming calls to the called party with ACR are checked even if the called party is offhook.

### Automatic Callback (AC) – Repeat Dialing

AC, also called repeat dialing, allows the user to request the system to automatically call the most recently dialed number. The system will keep attempting to call the number for up to 30 minutes, and the remote station will be rung automatically when the called party becomes idle. The system alerts the user with distinctive ringing. Up to 20 AC requests can be active at any time. The service provider can set up this service for the user, or the user can access it on a usage-sensitive basis.

### Automatic Recall (AR) - Call Return

AR, also called Call Return, allows the user to request the system to automatically redial of last incoming call (that is, the station that called the user) when that station becomes idle. The system will keep attempting to call the number for up to 30 minutes, and the remote station will be rung automatically when the called party becomes idle. The system alerts the user with distinctive ringing. Up to 20 AR requests can be active at any time. The service provider can set up this service for the user, or the user can access it on a usage-sensitive basis.

### Call Block (Reject Caller)

The call block (reject caller) feature allows the user to block incoming calls from the DN of the last received call. For the call block feature to work, the user must already be subscribed to the selective call rejection (SCR) feature. Once call block is activated against a specified DN, that DN remains in the SCR list of the subscriber. A subscriber who wishes to block callers (like sales calls, etc.) but does not know the caller's DN, can use this feature. Call block can be provided to POTS, CENTREX and MLHG subscribers.

The user can deactivate call block for this DN by removing the DN from their SCR list. This is done by using the screen list editing (SLE) function of the SCR feature.

### Call Waiting (CW)

CW informs a busy station that another call is waiting through the application of a 300 ms, 440 Hz tone. Ten seconds after the initial tone, a second tone is applied if the waiting call has not been answered. To answer the waiting call and place the original call on hold, the user presses the Flash button or hookswitch. A subsequent flash returns the user to the original call. Additional flashes can be used to toggle between the two calls as long as they are both still connected. The waiting call hears ringing until it is answered.

When a waiting call is accepted, there are two active sessions. To end the currently active session, the user goes on hook. The user's phone will then ring to indicate that the other caller is still holding. The user can pick up the phone to resume that session.

Only one instance of CW can be active for a given subscriber line at any given time. Thus, if a subscriber line were involved in both an active call and a waiting call, then an additional incoming call attempt results in the caller receiving a busy tone or being forwarded (CFB). The user involved in the CW call is not aware of the additional incoming call attempt.

### Cancel Call Waiting (CCW)

CCW allows a user to disable CW, which also disables the calling identity delivery/call waiting (CIDCW) feature for the duration of a call. CCW is normally included as an integral part of a service package containing the CW and CIDCW features. CCW is useful when the user does not want to be interrupted during an important call or during an outgoing data/fax call. After the current call is completely released, the CW service will be back in effect automatically.

## Call Transfer (CT)

CT allows a user to add a third party or second call to an existing two-party call. CT also allows the user to hang up while involved in the two calls and connect the remaining two parties in a two-way connection.

## Customer-Originated Trace (COT)

Customer-originated trace (COT) allows users who have been receiving harassing or prank calls to activate an immediate trace of the last incoming call, without requiring prior approval or manual intervention by telephone company personnel. After an harassing or prank call is terminated, a user who wishes to trace the call goes off hook, receives a dial tone, and dials the COT activation code (\*57). When the trace has been completed, the user receives a COT success tone or announcement, such as, “You have successfully traced your last incoming call. Please contact your telephone company for further assistance.” (Information about a traced call is made available to the telephone company or to a telco designated agency, usually law enforcement, but not to the user who initiated the trace). Because COT is activated on a per-call basis, the service is deactivated when the user goes on hook.

## Do Not Disturb (DND)

The do not disturb feature is activated and deactivated by the user. It routes calls destined to the user’s DN either to a special do not disturb announcement or to a special tone. A user can dial the activation code (\*78) to enable this service, and dial the deactivation code (\*79) to disable the service.

## Hotline Service

Hotline service is a dedicated private line between a subscriber phone and a predetermined DN. The service is activated by the service provider at the request of the subscriber. When the hotline user picks up the phone, the Cisco BTS 10200 Softswitch rings the predetermined DN instantly. Only the service provider can deactivate hotline service.

## Interactive Voice Response (IVR) Functions

The Cisco BTS 10200 Softswitch supports interactive voice response (IVR) functions for activation of remote call forwarding (RACF) and screening list editing (SLE) features.

## Multiline Hunt Group (MLHG)

A multiline hunt group (MLHG) is a telecommunications channel between two points, such as a telephone company CO/switching center and a call center, PBX or key system. Typically, a business has more stations (telephones) than lines, and hunting features allow sharing of a group of lines by many individual stations for both incoming and outgoing calls. Hunting refers to the process of a call reaching a group of lines. The call tries the first line of the group. If that line is busy it tries the second line, then it hunts to the third, etc. A hunt group is simply a series of lines organized in such a way that if the first line is busy the next line is hunted and so on until a free line is found. Often this arrangement is used on a group of incoming lines. Each line in a MLHG has a terminal number that identifies its position in the group.

## Multiple Directory Numbers (MDN)

Multiple directory numbers (MDN) service is also known as teen service. It enables one primary DN and one or two secondary DNs to be assigned to a single line termination. A specific unique ringing pattern is assigned to each DN, so that each incoming call can be individually identified. A distinctive CW tone is also assigned to each DN so that each incoming call can be individually identified when the line is busy.

## Speed Call

The speed call feature is available for individual subscribers or groups of subscribers.

### Speed Call for Individual Subscribers

The speed call feature allows a user to program the phone line so that they can dial selected or frequently called numbers using just one or two digits. After programming the line from their handset, the user can enter the one- or two-digit number, followed by the # symbol or a four-second delay, and the system automatically dials the applicable DN. The programming data is stored in the SC1D (one-digit) or SC2D (two-digit) table of the Cisco BTS 10200 Softswitch. These tables can also be programmed by the service provider via CLI commands.

### Group Speed Call

The group speed call feature allows members of a Centrex group or multiline hunt group (MLHG) to program a list so that they can select and dial frequently called numbers using one or two digits. A customer is allowed both one- and two-digit speed calling. In the case of shared lists for group speed calling, only one of the customers sharing the list may have the customer-changeable option. The switch is able to provide a given line with both a shared list and an individual list with the requirement that one must be a one-digit list and the other a two-digit list. If speed calling is assigned to a multiline hunt group, all members of that group have access to the shared group speed call list. If, however, a line in the group also has individual speed calling, then the individual speed calling will take precedence over the group speed calling.

## Subscriber-Controlled Services and Screening List Editing

Subscriber-controlled services allow individual users to screen and manage their incoming calls. The user can specify lists of DNs for which incoming calls are to be screened and given any of the following treatments:

- Selective Call Forwarding
- Selective Call Acceptance
- Selective Call Rejection
- Distinctive Ringing/Call Waiting

The user can create screening lists, add DNs to the lists, and edit the lists, via the screening list editing (SLE) function. The user performs the SLE functions, and activates/deactivates the services, via VSCs. Each VSC connects the user to the appropriate IVR media server functions. The VSCs are preprovisioned in the Cisco BTS 10200 Softswitch.

**Selective Call Forwarding (SCF)**

The selective call forwarding (SCF) feature screens each incoming call to determine whether the DN is on a list of DNs, provisioned by the user (called party), to receive automatic forwarding treatment. The user also sets the forward-to number. Any incoming calls from DNs that are on the SCF screening list are forwarded to the designated number. Any incoming calls from DNs not on the SCF screening list receive regular treatment (they are not forwarded).

The user accesses and controls the SCF properties from their handset via a VSC and IVR interaction. The user can add or delete DNs on the screening list, change the forward-to number, review the screening list, and activate or deactivate SCF. As a convenience, the system allows the user to add or delete the last caller's number to the screening list by entering 01 at the prompt. The system recognizes the "01" command and translates it into the last-received DN.

**Selective Call Acceptance (SCA)**

The selective call acceptance (SCA) feature screens each incoming call to determine whether the DN is on a list of DNs, provisioned by the user (called party), to be accepted. Any incoming calls from DNs on the SCA screening list are accepted, but any incoming calls from DNs not on the SCA screening list are blocked (receive terminating treatment).

The user accesses and controls the SCA properties from their handset via a VSC and IVR interaction. The user can add or delete DNs on the screening list, review the screening list, and activate or deactivate SCA. As a convenience, the system allows the user to add or delete the last caller's number to the screening list by entering 01 at the prompt. The system recognizes the 01 command and translates it into the last-received DN.

**Selective Call Rejection (SCR)**

The selective call rejection (SCR) feature screens each incoming call to determine whether the DN is on a list of DNs, provisioned by the user (called party), to be blocked. The blocked caller is connected to an announcement stating that their call is not presently being accepted by the called party. Any incoming calls from DNs not on the SCR screening list receive regular treatment (they are not blocked).

The user accesses and controls the SCR properties from their handset via a VSC and IVR interaction. The user can add or delete DNs on the screening list, review the screening list, and activate or deactivate SCR. As a convenience, the system allows the user to add or delete the last caller's number to the screening list by entering 01 at the prompt. The system recognizes the 01 command and translates it into the last-received DN.

**Distinctive Ringing/Call Waiting (DRCW)**

The distinctive ringing/call waiting (DRCW) feature screens each incoming call to determine whether the DN is on a list of DNs, provisioned by the user (called party), to receive special ringing or CW alerting treatment. If the incoming DN is on the DRCW screening list, the system alerts the user with a special ring or a special CW tone. Any incoming calls from DNs not on the SCR screening list receive regular treatment (regular ringing and CW alerting tones).

The user accesses and controls the DRCW properties from their handset via a VSC and IVR interaction. The user can add or delete DNs on the screening list, review the screening list, and activate or deactivate DRCW. As a convenience, the system allows the user to add or delete the last caller's number to the screening list by entering 01 at the prompt. The system recognizes the 01 command and translates it into the last-received DN.

**Three-Way Calling (TWC)**

TWC is a feature provisioned by the service provider in response to a request from the subscriber. TWC allows a subscriber to add a third party to an existing two party conversation.

## Usage-Sensitive Three-Way Calling (USTWC)

USTWC allows a user to add a third party to an existing two party conversation. It provides all the functionality of TWC without requiring the user to subscribe to the service. The service provider may charge differently for the use of this service. The usage-sensitive features can be enabled/inhibited per user by turning on/off the usage-sensitive option for the user.

## Visual Message Waiting Indicator (VMWI)

The visual message waiting indicator (VMWI) is associated with the voice mail service. When a call is forwarded to a voice mail system, and the caller leaves a message, the voice mail system sends the Cisco BTS 10200 Softswitch an MWI signal via SIP. The Cisco BTS 10200 Softswitch forwards a VMWI signal to the called party, and the called party's telephone indicator light turns on. When the called party retrieves the message, the voice mail system signals the Cisco BTS 10200 Softswitch to clear the VMWI indicator, and the light on the telephone turns off.

## Warmline Service

Warmline service is a combination of hotline service and regular phone service on the same line. The service is activated by the service provider at the request of the subscriber. The service provider provisions a timeout parameter in the FEATURE table (default is four seconds), and if the user takes the handset off hook, receives dial tone, but does not dial any digits before the timeout expires, the system automatically calls the predetermined DN.

## Default Office Service ID

One service ID (the default office service ID, typically ID=999) is reserved for provisioning of switch-based features. These switch-based features can include certain network features and certain usage-sensitive features, as described below. The service provider must provision this service ID in the service table, and define these features in the feature table.

- Network features—When provisioned, the system makes these features available for all subscriber lines:
  - Local network portability (LNP)
  - Toll-free services (8XX)
  - Emergency services (911)
  - Busy line verification (BLV)
- Usage-sensitive features—When provisioned, the system makes these features available to all subscribers without the need to actually subscribe these features to individual lines:
  - Usage-sensitive three-way calling (USTWC)
  - Customer originated trace (COT)
  - Automatic callback activation and deactivation—AC\_ACT and AC\_DEACT (or AC, if the AC umbrella feature was created)
  - Automatic recall activation and deactivation—AR\_ACT and AR\_DEACT (or AR, if the AR umbrella feature was created)

## Operation, Administration, Maintenance, and Provisioning Features

Cable Management and Services are at the application layer. The two most widely used are the Simple Network Management Protocol (SNMP) along with Cisco Network Registrar (CNR) described earlier.

SNMP is a part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite and it facilitates the exchange of management information between network devices. It enables network operators to manage network performance, find and solve network problems, and plan network growth.

- **Management Interface**—The Cisco BTS 10200 Softswitch provides several management interfaces to monitor, control, and configure the system.
- **CLI**—The Cisco BTS 10200 Softswitch supports CLI commands. It also supports query of operational and administrative states using CLI commands over Telnet, and it supports provisioning using CLI commands and/or scripts (see below).
- **SNMP**—The Cisco BTS 10200 Softswitch supports SNMP interfaces for fault and performance management data such that external management systems can be utilized to manage the switch.
- **FTP**—FTP interface on the Cisco BTS 10200 Softswitch is supported for retrieval of Billing records and retrieval of Measurements data
- **Provision configuration data using CLI commands over Telnet**—The Cisco BTS 10200 Softswitch enables the user to provision and configure the system using the Telnet interface for the entry of CLI commands or the FTP interface for batch files of CLI commands.
- **Provision dial plan using CLI commands over Telnet**—The Cisco BTS 10200 Softswitch enables the user to provision dial plans using the Telnet interface for entry of CLI commands or the FTP interface for download of batch files containing CLI commands.
- **Dynamic reconfiguration of provisioned objects**—Administration and configuration changes are performed concurrently with call processing.




---

**Note**

Some dynamic reconfiguration operations do impact call processing performance (see below in Issues section).

---

- **IP Routing (provisioning enhancement)**—During provisioning of gateways, IP address of gateway interfaces can be added to the static “host based routing” tables of Solaris OS.




---

**Note**

Subnet-based IP routing is generally preferred to static routing; however, Solaris v6 does not fully support subnet-addressing; static IP addresses of gateways are inserted into the hosts table on the Solaris machine. The static approach has the advantage of not waiting for IP network convergence to find an alternate route.

---

- **Security** —The Cisco BTS 10200 Softswitch runs in a standard Sun Solaris operating system which supports standard UNIX security capabilities.
- **Event Notification Log**—All applications events are captured in a log file, each can be configured to report logging level of: DEBUG, TRACE, CRITICAL, WARNING, ERROR, INFO, in order of decreasing detail and severity. See Diagnostic Tools below on viewing the log.
- **Fault Handling**—Fault handling deals with the following capabilities: Trouble Detection, Trouble Isolation, Recovery, Trouble Notification, Trouble Verification, Repair, Repair Verification.



- **Alarm Generation**—The Cisco BTS 10200 host generates autonomous messages to notify the operator of network problems and conditions. Alarms are stored on the Cisco BTS 10200 host and may be viewed using CLI commands and/or specialized tools. At user discretion, the autonomous alarm message stream can be addressed to single or multiple destinations, such as CMNM, HP Open View, or other third party SNMP managers.
- **Trouble Notification**—The Cisco BTS 10200 Softswitch supports two mechanisms to notify the operator of a trouble: Alarm/Event messages and SNMP traps.
- **Threshold Crossing Alerts (TCA)**—When a counter exceeds a threshold value, an alarm is raised. Each measurement may or may not have a threshold assigned to it. Thresholds have an *upper mark value* and a *lower mark value*. When the upper mark value is reached within a specified *time interval*, an alarm is raised. When the counter value decreases to the *lower mark* value, the associated alarm clear event is generated.
- **Trouble Detect/ Recovery for Communication Faults**—The Cisco BTS 10200 Softswitch detects and recovers from the loss of communication with the CAT6509.
- **Software BackUp and Restore**—Backup versions of software and data can be created using facilities provided by the Solaris operating system
- **Billing**—The Cisco BTS 10200 Softswitch generates the Billing information which is stored to disk
- **Billing Message Format**—The billing data format is a binary format.
- **Call Detail Blocks (CDB)**—CDR files consist of blocks of data called CDBs. CDBs are generated at various points in the call and mark the beginning or end of the file.

The defined CDBs are:

- Answer Call Event—Call went through and was answered.
  - Deselected Outgoing Circuit Event—Circuit can not be used, passed to another
  - Aborted Attempt Call Event—Call did not get to setup status
  - Release Call Event—Released call
  - Interrupted Call Event—Call terminating without release message
  - On-going Call Event—Long call
  - Maintenance CDB Record—Circuit maintenance
  - External Access CDB—Call sent a query to SCP (or other external device or database)
  - File Header CDB—beginning of each CDR file
  - File Footer CDB—end of each CDR file
  - End of Call CDB—This CDB is generated when the Cisco BTS 10200 Softswitch is configured to have only one CDB per call.
- **Call data elements (CDEs) values**—The Cisco BTS 10200 Softswitch supports three data element formats: ANSI, ITU, and generic format
  - **CDR calculated time duration**—Insert call duration into CDR (regular CDR has epoch timestamps for points in call not total duration)
  - **Measurements**—The Cisco BTS 10200 Softswitch produces various performance measurements, which are generally maintained in 15 minute, 30 minute, 60 minute and 24 hour intervals. These intervals can be configured differently for different measurements.
  - **Diagnostic Tools**—The Cisco BTS 10200 Softswitch provides diagnostic tools for quick and effective access to troubleshooting and diagnostic data.

# Cisco NMS/OSS for Broadband Services

The Cisco NMS/OSS for Broadband Services solution is an optional offering that provides a complete end-to-end OSS solution for architectures based on PacketCable and DOCSIS standards. The NMS/OSS solution provides a foundation for advanced IP services by:

- Leveraging existing business processes and implementations
- Providing end-to-end plug-and-play management of the cable operator's network
- Managing devices and applications supporting CableLabs DOCSIS and PacketCable standards

Cisco NMS/OSS for Broadband Services solution is a framework designed for next-generation, IP-based services and packet network infrastructure. Cisco NMS/OSS for Broadband Services is a foundation of integrated product offerings, products, partners, and standards to provide end-to-end management enablement of intelligent network services.

With this framework and foundation, cable operators can incrementally extend network management system (NMS) and operations support system (OSS) functions in step with new service offerings, creating flow-through processes to achieve a higher level of efficiency and automation. The Cisco NMS/OSS for Broadband Services solution adds to operational efficiency, accelerates delivery of tailored next-generation services, and scales to support the global Internet.

Cisco NMS/OSS for Broadband Services offers a broad suite of services designed to allow:

- “Plug-and-Play” capability of devices, applications, and services
- Programmability (customization) of a network's behavior based on user policies
- Self-adaptive optimization of networks based on the networks' knowledge base
- Secure and scalable IP services creation across multiple platform products

Cisco NMS/OSS for Broadband Services increases the value of operations by freeing cable operators to divert valuable personnel from many routine management tasks toward more revenue-generating activities. Cisco accomplishes this by placing intelligent and robust automated management capabilities into the network itself. Automating much of the provisioning processes through the Cisco CNS Programmable Network (policy management and publish-and-subscribe capability).

Cisco NMS/OSS for Broadband Services is based on industry standards for protocols, links, and application programming interfaces (APIs), and Cisco ecosystem partners can build products or write applications that easily integrate with an existing broadband services framework. Cable operators can select components to create a custom NMS/OSS that meets their specific business model and integrates easily with their existing business-management, customer-service, and billing systems.

Cisco Systems realizes that customers prefer to select the network management components that they feel best meet their needs. Cisco ensures that all products have open interfaces and are configurable so that the products can be easily integrated into the service provider's existing NMS environment.

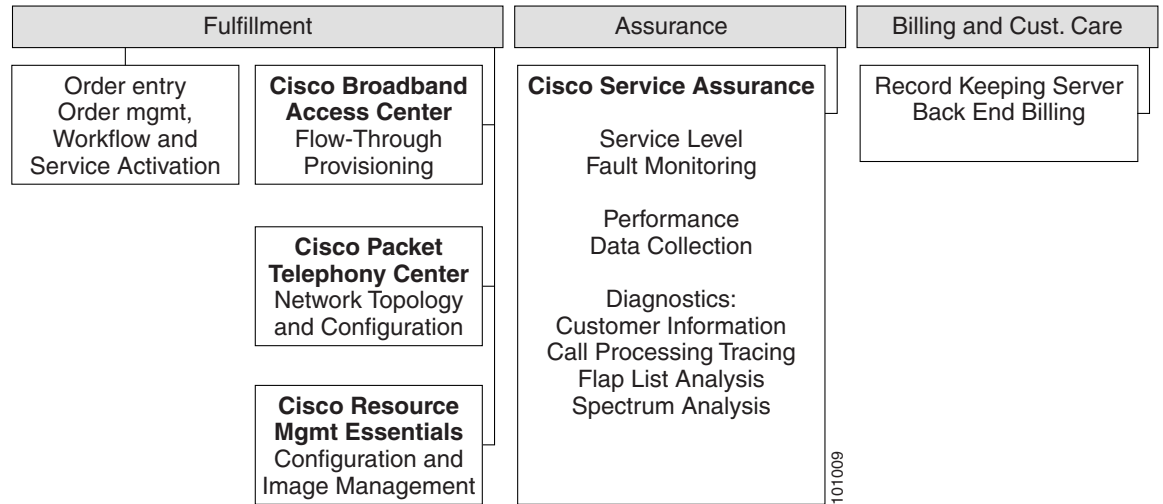
While products can be individually selected, Cisco also realizes the value of testing the tools in an end-to-end environment, so a level of preintegration is performed in the Cisco solution test lab. The tools are tested in an environment that is reflective of a typical cable operator environment. Preintegrations exist for Order Management/Workflow to Cisco Broadband Access Center and the Cisco BTS10200 Softswitch for subscriber and eMTA provisioning. Packet Telephony Center Virtual Switch provisions trunks for the Cisco MGX8000 series trunk gateways and the Cisco BTS 10200 from a central topology.

Cisco Information Center contains all of the rule sets for managing the underlying Cisco components. All of the trap parsing and recognition for Cisco devices already exists on Cisco Information Center. Cisco Broadband Troubleshooter and Cisco Packet Telephony Center can be launched directly from Cisco Information Center. This provides NOC engineers with the capability of detecting and diagnosing faults from one single location. Cisco expects that the cable operator already has a performance report application that interfaces to data collectors such as the Cisco CNS Performance Engine.

As shown in Figure 1-8, the Cisco NMS/OSS for Broadband Services encompasses three specific areas of network management applications for the cable operator:

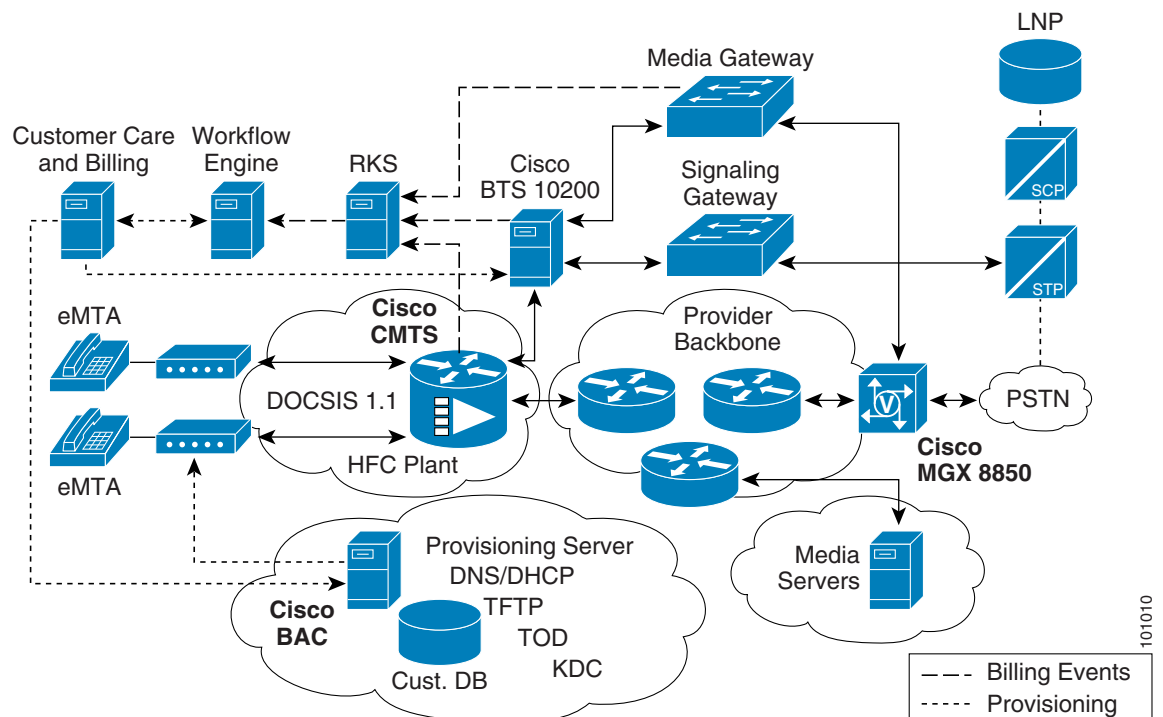
- Service Fulfillment Applications, page 1-50
- Service Assurance Applications, page 1-52

Figure 1-8 Cisco NMS/OSS for Broadband Services



The Cisco NMS/OSS for Broadband Services, as shown in Figure 1-9, starts with taking a cable customer order for voice service. The order for voice service is passed to an application that manages the order, activates the service, and manages order workflow.

Figure 1-9 Cisco NMS/OSS for Broadband Services Functionality



## Service Fulfillment Applications

The following sections provide a high-level overview of the functions performed by the components of the Cisco NMS/OSS for Broadband Services that help cable operators enable service to customers:

- [Cisco Broadband Access Center for Cable, page 1-50](#)
  - [Cisco Network Registrar, page 1-51](#)
  - [Cisco CNS Address and Name Registrar, page 1-51](#)
- [Cisco Resource Manager Essentials, page 1-51](#)

### Cisco Broadband Access Center for Cable

The Cisco Broadband Access Center for Cable (BACC), formerly known as the Cisco Broadband Provisioning Registrar® (BPR), makes it easy for service providers to deploy high-speed data and Voice over IP services over DOCSIS cable modems and media terminal adapters. Cisco BAC for Cable builds intelligence on top of the Cisco CNS Network Registrar® protocol servers to allow cable operators to automate the subscriber-provisioning process.

Performance, scalability, and reliability were the design requirements behind this third-generation Cisco BAC product. In addition, Cisco BAC includes a Java-based provisioning API, ensuring quick integration with customers' existing and next-generation OSSs.

The Cisco BAC includes Cisco CNS Network Registrar, Cisco CNS Address and Name Registrar, and IPfonix Key Distribution Center. Cisco BAC supports PacketCable and DOCSIS standards.

Cisco Broadband Access Center (BAC) is used to provision subscriber data for the MTAs:

1. Broadband Access Center provisions subscriber data into the Cisco BTS 10200 Softswitch.
2. A phone call is placed over the service providers IP network, as shown in [Figure 1-9](#), consisting of the Cisco uBR7246vxx Cable Modem Termination System (CMTS), Cisco BTS 10200 Softswitch, IP backbone, and the Cisco MGX® 8850 Trunk Gateway.
3. The Cisco MGX 8850 routes the IP-based call from the MTA to the PSTN.
4. As the call is processed, RADIUS messages are collected by the Record-Keeping Server (RKS) from the Cisco uBR7246vxx router and the Cisco BTS 10200 Softswitch.
5. The RADIUS messages are mediated into a call detail record (CDR).
6. The CDR is then passed to an external billing system, where the record is rated and posted to the customer's account.

The Cisco NMS/OSS for Broadband Services solution also provides service assurance:

- Alarm notifications from the Cisco uBR7246vxx (CMTS) and Cisco BTS 10200 Softswitch can be viewed on Cisco Information Center.
- Software image management and configuration can be accomplished using CiscoWorks Resource Manager Essentials (RME).
- Diagnostics can be provided on the DOCSIS domain by using the Cisco Broadband Troubleshooter and Cisco Cable Diagnostic Manager.

For additional information on the Cisco Broadband Access Center for Cable application, see [http://www.cisco.com/en/US/products/sw/netmgtsw/ps529/prod\\_technical\\_documentation.html](http://www.cisco.com/en/US/products/sw/netmgtsw/ps529/prod_technical_documentation.html).

## Cisco Network Registrar

Cisco CNS Network Registrar, through its carrier-class performance (in both scalability and reliability) and advanced provisioning, simplifies IP address management. Cisco CNS Network Registrar offers the Dynamic Host Configuration Protocol (DHCP), Domain Name System (DNS), and Trivial File Transfer Protocol (TFTP) server features to help cable operators reduce network infrastructure operating costs via customizable capabilities while increasing return on investment through faster subscriber activation and more reliable and scalable service deliveries.

For additional information on the Cisco Network Registrar application, see [http://www.cisco.com/en/US/products/sw/netmgtsw/ps1982/prod\\_technical\\_documentation.html](http://www.cisco.com/en/US/products/sw/netmgtsw/ps1982/prod_technical_documentation.html).

## Cisco CNS Address and Name Registrar

The Cisco CNS Address and Name Registrar enables cable operators to deploy open access by using customized policies to drive intelligent IP address allocation and reclamation decision. Cisco CNS Address and Name Registrar turns complex IP address utilization data into meaningful management information. Furthermore, it can help cable operators eliminate error-prone tasks by automatically monitoring, tracking, distributing, and managing IP address spaces.

For additional information on the Cisco CNS Address and Name Registrar application, see [http://www.cisco.com/en/US/products/sw/netmgtsw/ps423/prod\\_technical\\_documentation.html](http://www.cisco.com/en/US/products/sw/netmgtsw/ps423/prod_technical_documentation.html).

## Cisco Resource Manager Essentials

Cisco Resource Manager Essentials (RME), one of the major components of CiscoWorks 2000, is a powerful suite of Web-based applications offering network management solutions for Cisco switches, access servers, and routers. Cisco RME enables the deployment, monitoring, and configuration of devices across your network.

Cisco RME is a suite of web-based network management tools integrated into a network desktop that includes web-based tools and web-browser capability. The Cisco RME browser interface allows easy access to information critical to network uptime and simplifies time-consuming administrative tasks.

Cisco RME is based on a client/server network architecture that connects multiple web-based clients to a network server. The Management Connection feature adds Web-level integration of other management tools from Cisco and partner companies, thereby enabling utilization of these tools and applications to create a seamless, central point of network administration.

Cisco Resource Manager Essentials includes the following components:

- Inventory Manager
- Change Audit
- Device Configuration Manager
- Software Image Manager
- Availability Manager
- Syslog Analyzer
- Cisco Management Connection

For additional information on the Cisco Resource Manager Essentials application, see [http://www.cisco.com/en/US/products/sw/cscowork/ps2073/prod\\_technical\\_documentation.html](http://www.cisco.com/en/US/products/sw/cscowork/ps2073/prod_technical_documentation.html).

## Service Assurance Applications

The Cisco NMS/OSS for Broadband Services Service Assurance package helps cable operators monitor and troubleshoot their networks in a proactive manner. The Cisco NMS/OSS Service Assurance package includes the following components.

- [Cisco Information Center, page 1-52](#)
- [Cisco Broadband Troubleshooter, page 1-52](#)
- [Cisco Broadband Configurator, page 1-53](#)
- [Cisco BTS 10200 Element Management System, page 1-53](#)

### Cisco Information Center

Cisco Information Center (CIC) is a service-level alarm monitoring and diagnostics tool that provides network fault and performance monitoring, network trouble isolation, and real-time service-level management for large networks. Cisco Information Center is designed to help operators focus on important network events, offering a combination of alarm processing rules, filtering, customizable alarm viewing, and partitioning. Cisco Information Center provides a highly configurable client-server application that can consolidate, de-duplicate, filter, and correlate fault information from multiple network layers from a wide range of management platforms and technologies in a heterogeneous network.

Cisco Information Center is the fault management component of the Cisco Service Management Applications (SMA) infrastructure that provides end-to-end service management solutions for service provider networks. Operating at the service and network levels, Cisco Information Center interacts with other management tools within the SMA product suite to provide customer-focused, service-level monitoring and network partitioning for customer network management services.

Cisco Information Center works in conjunction with network element management software such as Cisco WAN Manager to provide fault and alarm management across LAN and WAN networks and management software such as CiscoWorks 2000.

Cisco Information Center consists of the Netcool technology from Micromuse at its core, plus notable Cisco enhancements. Cisco enhancements include event classes, policies, automations, rules, and tools that work together to provide out-of-the-box support and integration for Cisco devices, element management systems (EMSs), and domain managers.

For additional information on the Cisco Information Center application, see [http://www.cisco.com/en/US/products/sw/netmgtsw/ps996/prod\\_technical\\_documentation.html](http://www.cisco.com/en/US/products/sw/netmgtsw/ps996/prod_technical_documentation.html).

### Cisco Broadband Troubleshooter

The Cisco Broadband Troubleshooter (CBT) is a best-in-class tool for diagnosing the HFC network. The product enables a radio frequency technician to quickly isolate plant and provisioning problems. Using the Cisco Broadband Troubleshooter, technicians can easily discern and characterize upstream and downstream trouble patterns. The tool dynamically monitors radio frequency characteristics on a per modem or per upstream basis, provides a measurement interface that looks and feels like a spectrum analyzer, decentralizes radio frequency monitoring and analysis, and automatically sorts and categorizes radio frequency problem conditions.

Cisco Broadband Troubleshooter automates the analysis and interpretation of the flap list maintained in the Cisco uBR7100 Series, Cisco uBR7200 Series, and Cisco uBR10012 Universal Broadband Router. This improves staff effectiveness and ensures a stable return path, thereby increasing service and customer satisfaction.

New features added in Cisco Broadband Troubleshooter version 2.0 include:

- A multi-user client-server architecture; it is web-based to allow remote access
- The ability to interrogate CMTS and cable modems for fault isolation
- The ability to perform scheduled captures and provide real-time status on cable modems
- An SQL database for subscriber information
- The ability to pinpoint the geographic location of cable modems through an optional third-party mapping tool

For additional information on the Cisco Broadband Troubleshooter application, see

[http://www.cisco.com/en/US/products/sw/netmgtsw/ps530/prod\\_technical\\_documentation.html](http://www.cisco.com/en/US/products/sw/netmgtsw/ps530/prod_technical_documentation.html).

## Cisco Broadband Configurator

Cisco Broadband Configurator is a UI-based tool designed to collect information needed to generate configuration files for DOCSIS, EuroDOCSIS and PacketCable-based cable modems, set-top boxes, and multi-media terminal adapters. This tool aids in the creation of static configuration files that would otherwise have to be created by hand.

For additional information on the Cisco Broadband Configurator application, see

[http://www.cisco.com/en/US/products/sw/netmgtsw/ps819/prod\\_technical\\_documentation.html](http://www.cisco.com/en/US/products/sw/netmgtsw/ps819/prod_technical_documentation.html).

## Cisco BTS 10200 Element Management System

The Cisco BTS 10200 Element Management System (EMS) manages all of the Cisco BTS 10200 Softswitch components and provides operations, administration, management, and provisioning (OAM&P) interfaces for monitoring and control. It provides the following user OAM&P capabilities:

- Perform system administration and security functions
- Show, add, change, or delete the database information through a local or remote interface
- Display reports of events, alarms, and faults
- Monitor and manage hardware
- Monitor and manage traffic measurements
- Monitor and manage queuing and audit functions
- Display and control the status of a component

The EMS also provides system access security.



### Note

---

For more information on using EMS functions, refer to the *Cisco BTS 10200 Softswitch Operations, Maintenance, and Troubleshooting Guide* and the *Cisco BTS 10200 Softswitch Provisioning Guide*.

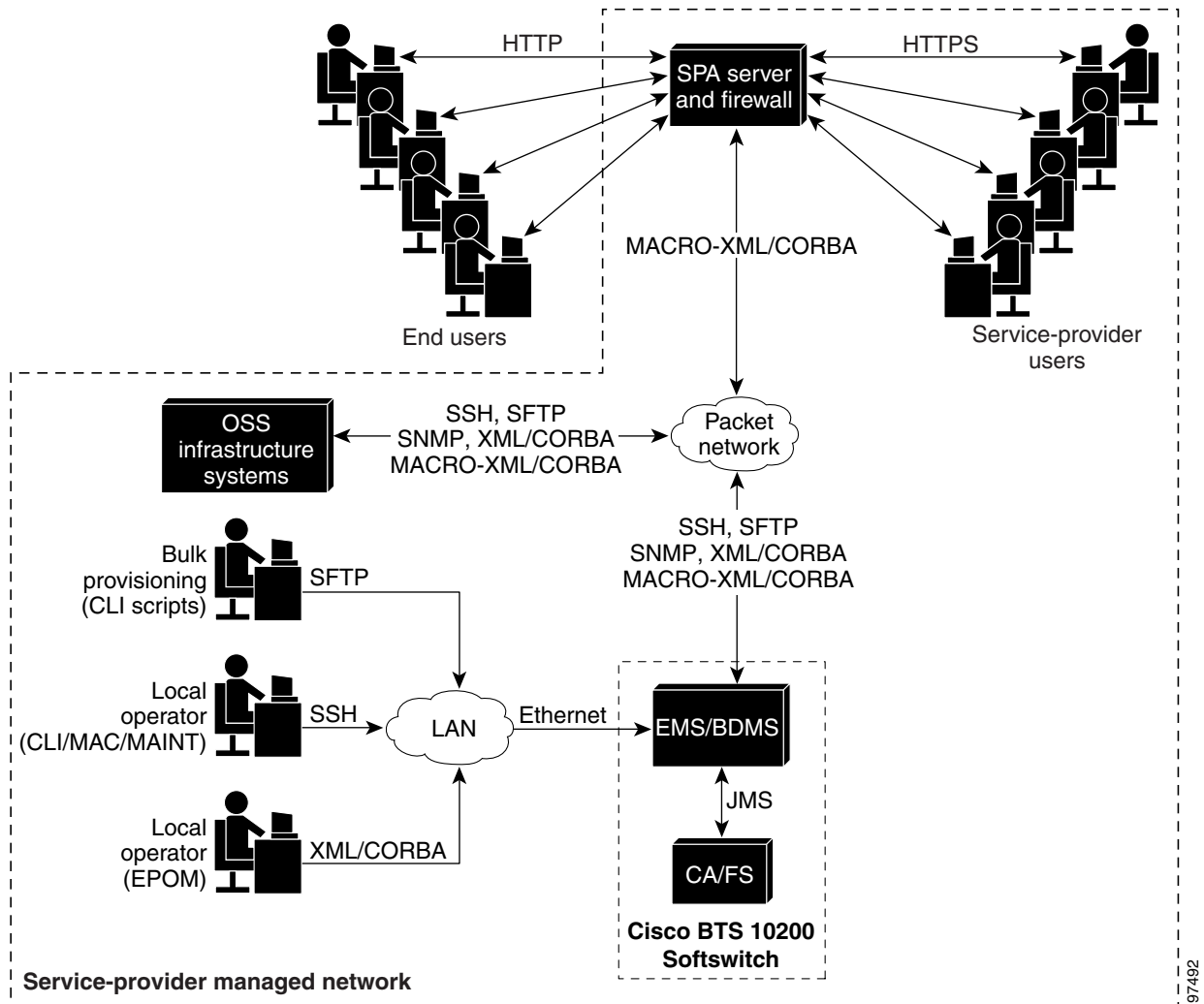
---

The EMS provides a flexible mechanism to transport information over any protocol to any external device. The EMS interface design takes into account that each carrier has its own unique set of Operations Support Systems (OSS). The EMS provides a decoupling layer between the external protocols used within the service provider network and the internal protocols of the Cisco BTS 10200 Softswitch. The core system does not need to interpret the specific data formats used by the other carrier network elements.

## EMS Communications

Operators, network administrators, and end users can communicate with the EMS from their workstation or PC over the interfaces shown in Figure 1-10.

**Figure 1-10 Preferred EMS Management Interfaces for Service Provider and End Users**



The user interfaces include the following:

- **Secure shell (SSH)**—For provisioning via command-line interface (CLI), Menu Assisted Commands (MAC), and Maintenance (MAINT) shells.
  - CLI shell—Used for entering entire commands and their parameters from the command line.
  - MAC shell—Provides a menu for each command for entering all the applicable parameters.
  - MAINT shell—Provides a maintenance interface for CLI commands that does not time out or disconnect on switchover. It supplies a prompt based on the username.



### Note

After software installation, CLI provisioning must be enabled by applying database licenses. You will not be able to run CLI commands until this is done. Your Cisco account team can provide the necessary licenses and procedures.



- **Secure File Transfer Protocol (SFTP)**—For bulk provisioning sessions. SSH and SFTP are always available on the Cisco BTS 10200 Softswitch, and there is no command to turn them off. The user can temporarily enable Telnet or FTP (or both); however, this can create security issues.

**Caution**

Cisco strongly recommends that you use secure interfaces only. Refer to the *Cisco BTS 10200 Command Line Interface Reference Guide* for additional information on these commands.

- **XML/CORBA and MACRO-XML/CORBA:**
  - Supports a CORBA provisioning and monitoring interface
  - Supports provisioning via the Cisco Extensible Provisioning and Operations Manager (EPOM) and the Cisco Self-Service Phone Administration (SPA).

**Note**

MACRO-XML/CORBA is a read-only interface that end users can configure and use to display large sets of data. It is used to streamline data queries and display complex data relationships.

- **Simple Network Management Protocol (SNMP)**—Provides traps, status, control, and measurement functions, and provisionable community strings.

The Cisco BTS 10200 SNMP agent supports SNMPv2c operations defined by the `optical.mib` Management Information Base (MIB). The MIB is located in the directory `/opt/BTSsnmp/etc` on the EMS. The NMS needs to load the main MIB (`optical.mib`), that will in turn import three other MIBs: `IPCELL-TC`, `SNMPv2-TC`, and `SNMPv2-SMI`. The main MIB uses variables from these MIBs.

- **Hypertext Transfer Protocol (HTTP) and Secure Hypertext Transfer Protocol (HTTPS)**—Permits end users and service providers to perform many of the feature provisioning processes via the web-based Cisco SPA system. Access from the user's web browser to the SPA server is via HTTP. Access from the service provider's web browser is via HTTPS.

By default, SFTP sessions are used for file transfers initiated by elements outside the Cisco BTS 10200 Softswitch (and directed toward the Cisco BTS 10200 Softswitch). FTP sessions are used for file transfers initiated by the Cisco BTS 10200 Softswitch.





## Troubleshooting Overview

---

This chapter contains an overview of troubleshooting concepts for the Cisco Broadband Local Integrated Services Solution (BLISS) for Cable 1.5. It provides guidelines for troubleshooting problems on the network, including guidelines for preventing problems before they occur.

- [Troubleshooting Basics, page 2-1](#)
- [Troubleshooting Strategy, page 2-2](#)
- [Troubleshooting Tools, page 2-11](#)

This chapter also includes overall system troubleshooting strategies and describes the wide variety of tools and methods that you can use to troubleshoot your system, including information on using diagnostic commands, using Cisco network management tools, and third-party troubleshooting tools.

## Troubleshooting Basics

System knowledge and planning, supported by up-to-date documentation and communication, is the key to maintaining a problem-free network environment, as well as to providing the ability to isolate and fix a network fault quickly. This requires a framework of procedures and personnel to be in place long before any network changes take place.

The Cisco BLISS for Cable solution supports connections to external switches and to internal components, such as media gateway controllers, signal processors, and trunking gateways. Because the Cisco BTS 10200 functions in a complex environment involving numerous connections, links, and signaling protocols, when connectivity and performance problems occur, this troubleshooting guide can help you isolate and resolve the most common connectivity and performance problems in your network environment.

This section provides a broad look at the topics related to troubleshooting. These topics give you a frame of reference for understanding the various components, interfaces, and tools you will work with when troubleshooting the Cisco Broadband Local Integrated Services Solution.

This section introduces the following topics:

- Where to find information about hardware and software components
- Where to find architecture diagrams and call flows
- Communications protocols used between solution components
- Tools that will aid in troubleshooting, their uses, and how to access them

# Troubleshooting Strategy

Troubleshooting consists of determining the nature of a problem and then isolating the problem to a particular device or component of a device. When a problem has been isolated and identified, troubleshooting also consists of fixing the problem, usually by replacing the device, some component of the device, or changing a setting or variable in the software.

Cisco telephony solutions include connections to external switches and to internal components, such as call agents, signal processors, and trunking gateways. This is a complex environment involving many connections, links, and signaling protocols. Connectivity and performance problems are very difficult to resolve. The goal of this section is to provide you with a general troubleshooting strategy for isolating and resolving connectivity and performance problems.

The cost of a network failure in a telephony environment can mount rapidly. Generally, the average cost of a production network outage---using lost revenue due to loss of calls as the basis of calculation---can be many thousands of dollars per hour. Restoring a network that has failed or has become impaired puts a lot of pressure on network operators and administrators. Given this kind of pressure, the use of special expertise and known shortcuts to rapidly restore network functionality is valuable. If you know how to solve a production network problem directly, do so. Use your expertise. However, this expertise requires a technical depth and a detailed breadth of knowledge about the network that does not result from isolated, scattered, and unsystematic troubleshooting.

Unless you already know how to solve a problem, an unsystematic approach to troubleshooting can result in wasting time lost in the network's maze of symptoms, interdependencies, and contingencies. A systematic troubleshooting method, on the other hand, can help you understand the network's details by going through a process that can help you identify facts, consider possibilities, act on likely causes, and observe the results of your actions.

The general idea of a troubleshooting model is to systematically reduce a large set of possible causes of trouble to a small set of causes or to a single cause. You can then fix the problem and restore network function. After the problem is resolved, a systematic method of documenting the case helps to capture, preserve, and communicate the troubleshooting experience gained while solving the problem.

As more advanced technologies and services are introduced into communication networks, the tasks of designing, managing, and maintaining the resulting networks are also becoming increasingly complex. The use of a systematic troubleshooting model increases the expertise of the organization and reduces the time to solve similar problems in the future. This evolution of improving expertise and collaboration can help mitigate the pressures of supporting crucial, complex networks.

Historically, telephone network architectures were switch-centric. These switch-based architectures have evolved into distributed systems with the emergence of softswitches. New applications such as video, audio, and multimedia are gaining popularity and are feasible due to the increase in processor power on clients and servers.

The troubleshooting procedures provided in this guide assume that your network has been turned up and is operating properly prior to experiencing the problem you are troubleshooting. For problems with incorrect configurations or provisioning refer to the component documentation for procedures.

## Symptoms, Problems, and Solutions

The symptoms of a problem can be general (such as being unable to access the SS7 network) or specific (routes not in routing table). First you need to determine the cause of a symptom by using troubleshooting tools and techniques. After identifying the cause, you can correct the problem.

Attempt to reproduce the reported symptoms if possible. If you cannot reproduce the symptoms, it will be extremely difficult to analyze and solve the problem. If you cannot narrow the troubleshooting scope to a particular subsystem or component, then you will probably be unable to determine how to fix it.

## General Problem-Solving Model

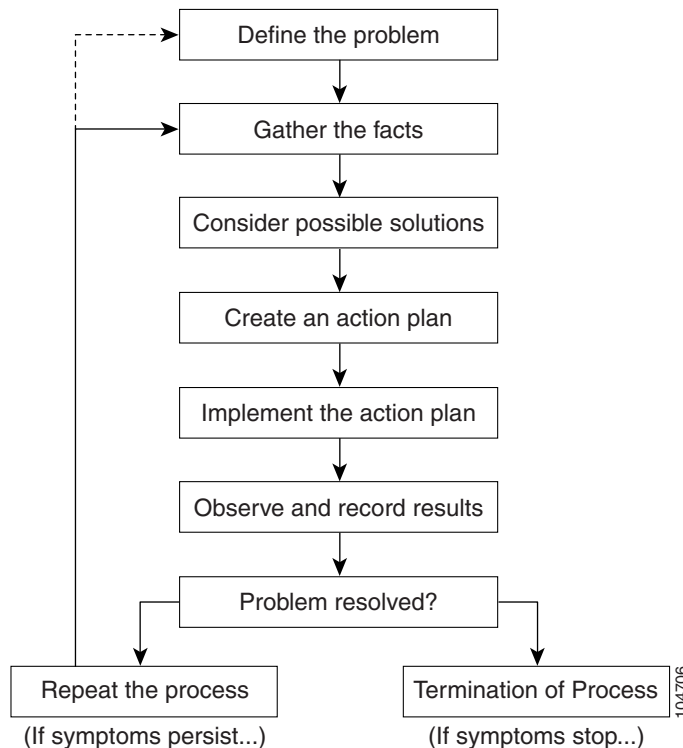
The complexity and crucial uptime requirements of modern telephone networks intensify the pressures to solve configuration, connectivity, and performance problems. The best way to approach a network problem is to develop a standard troubleshooting methodology. The problem-solving model presented in [Figure 2-1](#) is one example of such a methodology. This model is not to be considered a set of rigid rules; it is simply a method you can use to troubleshoot problems. Note that it is an iterative process that should allow you to eliminate possible causes and narrow the focus of your investigation.

Using a systematic approach and an ordered pattern of thought when troubleshooting helps you solve any problems you encounter. It also helps you and your organization improve overall expertise as your organization supports its internetwork. Define the symptoms, identify potential problems that could be causing the symptoms, then you can systematically eliminate each potential problem (from the most likely to the least likely) until you can determine the cause or the symptoms disappear.

If this process does not solve the problem as it was defined, it might be necessary to start over from the beginning (Define the Problem) in another area (dotted line). Remember that most components in the Cisco BLISS for Cable solution must interoperate with several other components in the cable network. A problem that becomes apparent in one component may actually be caused by the information it is receiving from another component. That is why it is imperative that you have normal baseline data, including typical measurement data and normal call flows,

[Figure 2-1](#) shows the sequence of steps necessary to solve a problem.

**Figure 2-1 General Problem-Solving Model**



These steps can be grouped into a small number of troubleshooting phases:

- Make sure you have a clear, sufficient definition of the problem.
- Gather all the relevant facts and consider the likely possibilities.
- Create and implement an action plan for the most likely possibility, then observe the results.
- If the symptoms do not stop, repeat the process and try another action plan (or gather more facts).
- If the symptoms stop, make sure you document how you resolved the problem.

The following steps describe the problem-solving process outlined in [Figure 2-1](#) in more detail:

- 
- Step 1** When analyzing a problem, draft a clear problem statement. Define the problem in terms of a set of symptoms and the potential causes behind those symptoms.
- For example, the symptom might be that the EQPT FAIL alarm has become active. Possible causes might be physical problems, a bad interface card, or the failure of some supporting entity.
- Step 2** Gather the facts you need to help isolate the symptoms and their possible causes.
- Ask questions of affected users, network administrators, managers, and other key people. Collect information from sources such as network management systems, protocol analyzer traces, output from router diagnostic commands, or software release notes.
- Step 3** Consider possible causes based on the facts you have gathered. You can also use these facts to eliminate potential causes from your list.
- For example, depending on the data, you might be able to eliminate hardware as a cause, allowing you to focus on software. At every opportunity, try to narrow the number of potential causes so that you can create an efficient plan of action.
- Step 4** Create an action plan based on the remaining potential causes. Begin with the most likely cause, and devise a plan in which only one variable at a time is manipulated.
- This approach allows you to reproduce the solution to a specific problem. If you alter more than one variable simultaneously, identifying the change that eliminated the symptom becomes more difficult.
- Step 5** Perform each step of the action plan carefully, and test to see if the symptom disappears.
- Step 6** Whenever you change a variable, gather the results. You should use the same method of gathering facts that you used in [Step 2](#).
- Analyze the results to determine if the problem has been resolved. If it has, then the process is complete.
- Step 7** If the problem has not been resolved, you must create an action plan based on the next most likely problem in your list. Return to [Step 2](#) (or possibly [Step 1](#)) and repeat the process until the problem is solved.
- Before trying out a new solution, make sure to undo any "fixes" you made in implementing your previous action plan. Remember that you want to change only one variable at a time.
- If you exhaust all the common causes and actions (either those outlined in this guide or those that you have identified for your environment) and still have not resolved the problem, you should contact the Cisco Technical Assistance Center (TAC). Refer to the preface for more information about contacting the Cisco TAC.
- This problem-solving model is just one of many such models you can use. If you are already using another model (based on an alternative model or learned through experience), you should continue to use it. If, in your past experience, you have not approached problems systematically and have not considered using a problem-solving model, you should adopt a scheme such as the one outlined here.
-

## Detailed Troubleshooting Methodology

The goal of this section is to establish a methodical mindset—an ordered pattern of thought to use when troubleshooting. The model described in this section takes a multistep approach to problem-solving. In the following subsections, we will examine each of these steps in detail to see how it can be used in a troubleshooting example.

### Step 1: Define the Problem

A systematic approach to troubleshooting consists of a sequence of steps. The first grouping of these steps is to make sure you have a clear, sufficient definition of the problem. When analyzing a network problem, make a clear problem statement by defining the problem in terms of a set of symptoms and associated causes. To do this, identify the general symptoms and ascertain what possible causes could result in these symptoms.

At this point in the methodology, you define the problem by identifying associated general symptoms and identifying possible causes. Try to form opinions of possible causes and document them. Many answers might arise, but concentrate on those that could be considered major contributors to the problem. Subsequent steps in the methodology allow you to ask questions (that is, gather facts).

Form problem statements with reference to the baselines you have established for your network. You should know what your network indicators look like when the network is performing as you expect. Also, you must have knowledge of any network changes since the last evidence of baseline performance.

In this group of steps, you should gather the initial diagnosis made by the end users. What the end user reports is important; however, the full definition of the problem may have a broader basis. If possible, proceed from your own knowledge about your network and try to see the problem for yourself.

As part of the systematic approach to troubleshooting, many support teams have developed a set of primary questions and processes to use when getting problem report information from end users. Among the primary questions are "How often has this problem happened?" and "When did it start?" and "Can you readily reproduce the problem condition, and if so, how?"

### Step 2: Gather the Facts

The second step in troubleshooting is to gather the facts you need to help isolate possible causes.

Ask questions of affected users, network administrators, managers, and any other key people involved with the network. Try to ascertain whether anyone is aware of anything that has changed. Thoroughly document all information received.

Depending on the nature of the reported symptoms, collect facts from sources such as network management systems, protocol analyzer traces, output from router diagnostic commands such as debug commands and show commands, or software release notes. It might be necessary to collect this information at discrete times or over extended time periods, such as an overnight data capture.

It is always a good idea to document and keep on record copies of the configurations of switches, routers, servers, and any other configurable network devices to be able to compare configurations and determine whether anything has changed. You need to gather facts in an attempt to focus on the possible causes.

### Step 3: Consider the Possibilities

Using the data you gathered and your knowledge of the systems and devices in your network, you can set the boundaries that help you begin to isolate the problem cause(s). By setting boundaries, you focus on only those portions of the solution that are relevant to the specific problem or failure mode.

One of the most important outcomes of a systematic troubleshooting approach is to narrow possibilities—remove irrelevant details from the set of items that you need to check. You can eliminate entire classes of problems associated with system software and hardware. You can eliminate several possible causes based on the facts gathered for the problem. Consider the possible causes identified earlier and eliminate those that are not relevant to narrow the scope of the problem as much as possible.

## Step 4: Create an Action Plan

You can now devise an action plan based on the set of possibilities that were just created. From these possibilities, you can implement a "divide and conquer" policy. Consider the most likely possibility, and determine a plan in which only one variable is manipulated. This approach allows you to reproduce a given solution to a specific problem. If more than one variable is altered simultaneously and the problem is solved, you cannot identify which variable caused the problem.

- Use a partitioning effect. Split your troubleshooting domain into discrete areas that are logically isolated from each other. This approach allows you to determine which side of the partition (if not both sides) keeps the problem after the partitioning.
- Determine where in the network the problem exists. Use a series of tests to pinpoint where network failure occurs. Begin from a source device and try a sequence of tests to determine whether proper functioning occurs from the source to successively more distant, intermediate network devices. This approach allows you to gradually trace a path from a source along the way to the ultimate destination and possibly isolate the part of the path that contains the problem.
- Collaborate with others and share rules-of-thumb action plan approaches. The more of these logical problem-solving approaches you learn, the more tools you have. Tools help you test a given problem situation. As you gain experience, you improve your ideas on how to relate the given possibilities and your troubleshooting tools to a specific and systematic action plan.

An action plan for a typical cause, for example, is to look at each device's current configuration and determine whether any recent changes were accomplished correctly.

## Step 5: Implement the Action Plan

It is important to be very specific in creating and executing an action plan; the plan must identify a set of steps to be executed, and each step must be carefully implemented. Keep track of exactly what you are testing. Try not to change too many variables at the same time.

As you implement your action plan, also try to

- Make sure what you implement does not make the problems worse or add new problems.
- Limit as much as possible the invasive impact of your action plan on other network users.
- Minimize the extent or duration of potential security lapses during your action plan implementation.

It is important to have a backout plan (for example, a saved configuration file) to return the network to a known previous state. For example, connect to a device's command console to view its configuration. If the configuration is deemed to be incorrect, reconfigure the device or temporarily disable it.

To ensure that not more than one variable is manipulated at a time, the results of the changes made must be observed before any changes are made to the configuration of this device or any other device.



## Step 6: Observe the Results of the Action Plan

After manipulating a variable to find a possible solution to a problem, be sure to gather results based on the action plan. Generally, you should use the same method of gathering facts that you used in step 2 of the methodology.

After you have analyzed the results, you must determine whether the problem has been resolved. If it has, then this is the exit point of the iterative loop in the problem-solving model. If the problem has not been resolved, then you must use these results to fine-tune the action plan until a solution is reached.

## Step 7: Repeat the Problem-Solving Process

To reach a point where you can exit the problem/solution loop, you must make continuous progress toward a smaller set of possibilities until you are left with only one. After narrowing the possibilities as a result of implementing the previous action plan and observing the results, repeat the process, starting with a new action plan based on a new list of possibilities. Continue the process until a solution is found. Problem resolution can involve many iterations of modifications to switch configurations or gateway configurations.

Remember that it is very important to undo any “fixes” you made that did not work. Remember that you want to change only one variable at a time. Also, if too many changes are made at one time in the network, it could result in a degradation of network performance and policy. This is why it is always important to have a backout plan to undo your changes and restore the network to its previous state.

You must now implement the next step of the action plan. Check to see if your work results in a fix that accomplishes the intended operation. Make additional changes as required. The iterations must continue until the problem is solved. Systematically eliminate each of the possible causes until you isolate and confirm the cause or causes so you can fix the problem.

## Step 8: Resolve the Problem

If you have located the true source of the problem, then you can finish up and document the problem. If, however, you have exhausted all common causes and actions for your environment as you attempt to resolve a problem, then your last recourse is to contact your Cisco technical support representative. You should have available all of the necessary information about your problem that might help the support representative determine the possible cause of the problem.

One of the aims of this chapter is to help you develop your own processes for gathering data, resolving problems, and preventing problems from recurring with an absolute minimum of downtime and external intervention. Even though the recursive progression through this model may seem time-consuming, as your troubleshooting skills mature, this process will become more automatic, and you will not need to follow a flow diagram step-by-step.

## Step 9: Document the Solution

As soon as the problem symptoms stop, chances are you have resolved the problem. At all times you need to document your work, which involves the following:

- Maintaining a record of which steps you have already taken (for example, whether you involve others, such as other engineers in your organization or the Cisco Technical Assistance Center).
- Providing a backout trail if it turns out that you must reverse the actions you took (for example, if you solved the problem at hand but inadvertently caused some other problem).
- Establishing an historical record for future reference to help others learn about what occurred and what to do about it). This record can provide a shortcut to solving a similar future problem.

## Preparing Yourself to Troubleshoot

Troubleshooting complex networks, like those implemented in the Cisco BLISS for Cable solution, is somewhat different than troubleshooting other networks. The best way to approach any troubleshooting problem is to isolate the cause, not the symptom. Of course, the only clues you have are the symptoms, but you must use them to synthesize a possible (maybe even probable) cause. You can solve any reproducible problem in any system for which you have the requisite knowledge, training, and experience.

It is always easier to recover from network problems if you are prepared ahead of time. Possibly the most important requirement in any network environment is to accurately document all current information about the network and make it available to support personnel. Having complete network information is critical to making effective network changes, as well as troubleshooting quickly and easily. During the process of troubleshooting the network, it is very important to ensure that this documentation is kept up-to-date.

As you troubleshoot, isolate problem causes, and restore your network to its normal functioning, you apply your expertise about your own network. In order to troubleshoot effectively, you should know your network well and be able to communicate efficiently and effectively with all key people involved in network administration and those people affected by the problem.

Consider the solution architecture shown in Figure 1-1 and ask yourself the following questions to determine whether you are prepared to deal with network problems:

- Do you have accurate physical, functional, and logical maps of your network?  
Does your organization have an up-to-date network map that outlines the physical location of all the devices on the network and how they are connected, as well as a logical map of network addresses, network numbers, subnetworks, and so on?
- Do you have a list of all network protocols implemented in your network?  
For each of the protocols implemented, do you have a list of the network numbers, subnetworks, zones, areas, and so on that are associated with them?  
For each of these protocols do you have a correct, up-to-date set of configuration parameters?
- Do you know all the points of contact to external networks, including any connections to the HFC network, the PSTN, the SS7 network, and the Internet?  
For each external network connection, do you know which signaling/routing protocols are used?
- Do you have an established baseline for all elements of your network?  
Has your organization documented normal network behavior and performance at different times of the day so that you can compare the current problem with a baseline? What constitutes the normal baseline functioning that you expect when your network is running well? What events, new equipment, software, or reconfigurations have been added since the last baseline?
- What specific application characteristics and traffic demands are involved (and which are not involved) in the problem? What past troubleshooting cases (if any) might apply to or assist with the current situation?

A systematic troubleshooting method helps overcome the time that is often wasted trying to work through the maze of complex, interrelated network details. Because networks are strategic tools in your organization, it is a practical reality to look for shortcuts. These shortcuts usually come from prior expertise, which, in turn, probably resulted from systematic troubleshooting.

To communicate what is learned during network problem solving, use a process for documenting your troubleshooting details. Both now and in the future, this documentation step can help you, help others in your team, and help the engineers in Cisco's Technical Assistance Center (TAC).

## Taking Preventive Action

Monitoring the general health of the network helps avoid problems, and makes troubleshooting easier when they do occur. You have to have normal baseline data to identify when problems occur.

Before you do anything that could cause additional problems, take the appropriate precautions. In the Cisco BLISS for Cable solution the prime precaution is to ensure that you have current backups of all component configurations and provisioning data.

In no case should maintenance be attempted before taking the proper precautions.

Here are some guidelines:

- Establish benchmarks when the network is running smoothly. In other words, know what the usual range of values is for the variables you may later examine when investigating a problem.
- When troubleshooting a call processing problem, you will need a normal working call flow for comparison. Generate and save successful call flows for each Call Agent call scenario, such as:
  - On-net to on-net call
  - On-net to off-net call
  - Off-net to on-net call
  - On-net to off-net to on-net call (forwarded call)
  - Off-net to on-net to off-net call (forwarded call)
  - Originating party terminates
  - Terminating party terminates
  - Terminating party busy
  - Terminating announcement (intraswitch)
  - Terminating announcement (interswitch)
  - Incoming call with COT
  - Custom calling features: call forwarding, call waiting, and so on

**Note**

---

Make sure you have a recent version of call flows prior to making any changes in the network, in case the change creates problems. Always make new copies of call flows after successful changes so you always have the most current view of the network.

---

- Trap successful call flows on the SS7 links for later reference.
- Generate reports from different devices to view trends. The reports can be run from either your own scripts or the standard ones.
- Set and review the appropriate alarms and polling mechanisms via the trunking gateway element management system.

## Scope of Troubleshooting

Troubleshooting usually consists of determining the nature of a problem and then isolating the problem to a particular device or component. When a problem has been isolated and identified, maintenance consists of fixing the problem, usually by replacing the device or some component of the device. The goal of this troubleshooting guide is to provide you with a general troubleshooting strategy, as well as information about the tools available for isolating and resolving connectivity and performance problems.

## Fault Analysis

Troubleshooting begins with analyzing the following in the order listed:

1. Alarms and system messages (if present)
2. Call traces and log files (if available)
3. Software and system state(s)
4. Signaling links and destinations
5. Bearer channels and destinations
6. Hardware components (interfaces, cables, indicators)

Troubleshooting usually includes the following tasks for each element of the Cisco Broadband Local Integrated Services Solution, performed in the order listed:

1. Checking equipment status. Determining the current status involves three basic activities:
  - a. Reading LEDs—Most Cisco products include light-emitting diode (LED) indicators on the front or rear panels and, in some cases, on both panels.

These LEDs indicate the status of the equipment. The specific meaning of each LED on each product is described in the maintenance sections for the individual elements of the Cisco Broadband Local Integrated Services Solution.
  - b. Issuing Status Queries—You can query the status of the system using various commands. The commands that can be used to determine the status of the devices in your system are described in the maintenance sections for the individual elements of the Cisco Broadband Local Integrated Services Solution.
  - c. Using a GUI NMS—Using a network management system (NMS) with a graphical user interface (GUI), such as CiscoWorks2000 or Cisco WAN Manager, to determine the operational status of system devices is described in detail in the maintenance sections for the individual elements of the Cisco Broadband Local Integrated Services Solution.
2. Removing the device from the system—Procedures for removing defective devices from the system with as little impact on the system as possible are described in the maintenance sections for the individual elements of the Cisco Broadband Local Integrated Services Solution.
3. Replacing the complete device—Reinstating a device into the system using a new or repaired model, again with as little impact on the system as possible, is described in the maintenance sections for the individual elements of the Cisco Broadband Local Integrated Services Solution.
4. Replacing hardware components—Swapping out components of a device is a maintenance task used for replacing defective components and for upgrading hardware. The maintenance chapters for each element of the Cisco BTS 10200 Softswitch node include sections describing how to replace the field-replaceable components of that device.

# Troubleshooting Tools

There are two types of tools available to troubleshoot problems in the Cisco Broadband Local Integrated Service Solution (BLISS) for Cable:

- [Software Tools, page 2-11](#)
- [Hardware Tools, page 2-15](#)

## Software Tools

This section describes software tools that can help you in troubleshooting.

- Alarms and error messages
- Call traces
- System logs
- CLI queries

## Alarms and Error Messages

The Cisco BTS 10200 Softswitch software generates alarms and error messages to indicate problems with processes, routes, linksets, signaling links, and bearer channels. Refer to the *Cisco BTS 10200 Softswitch Software Release 4.1 Operations Guide* for detailed information on system alarms and error messages.

The Error Message Decoder Tool is available to registered Cisco.com users at <http://www.cisco.com/cgi-bin/Support/Errordecoder/home.pl>

There is also a Messages and Recovery Procedures Guide for every set of CatOS or Cisco IOS LAN Documentation. For example, for CatOS 8.1 use the URL [:http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sw\\_8\\_1/msg\\_gd/emsg.htm](http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sw_8_1/msg_gd/emsg.htm)

The Output Interpreter also now incorporates the functionality of the Error Message Decoder tool <https://www.cisco.com/cgi-bin/Support/OutputInterpreter/home.pl>. Also, you may be interested in the TAC Advanced Search's error message data collection at [http://www.cisco.com/kobayashi/support/tac/s\\_tac.shtml](http://www.cisco.com/kobayashi/support/tac/s_tac.shtml) (when logged in with your registered Cisco.com user ID and password).

To decode error messages, you paste your one- or two-line console error message into the Output Interpreter. Your analysis will include an explanation of the message, any recommended actions to take, and a list of related support resources. The Output Interpreter can decode error messages from devices running Cisco IOS and Catalyst OS.

## Call Traces

The Cisco BTS 10200 Softswitch can generate call traces that capture call-processing activity by following the call from a specified destination through the Cisco BTS 10200 Softswitch to see where it fails. Call failure location is determined using the following information provided in the call trace:

- The protocol data units (PDUs) that the Cisco BTS 10200 Softswitch receives
- How the Cisco BTS 10200 Softswitch decodes the PDU
- The PDUs that the Cisco BTS 10200 Softswitch sends out

The results of call traces are signal flow diagrams that you can use for troubleshooting. Call traces are typically used to capture system activity as part of a procedure to clear an alarm. You should have a trace of all normal call functions to use as a baseline to compare to when problems arise.

## System Logs

The Cisco BTS 10200 Softswitch software continuously generates log files of various system information, including operational measurements (OMs) and alarm records. You can use these logs to obtain statistical information about the calls processed by the system and network events such as delays or service-affecting conditions. The Cisco BTS 10200 Softswitch generates the following types of logs:

**Table 2-1 System Log Types**

Log Type	Description
Platform logs	Contain information useful for tracking configuration errors and signaling link and call instantiation problems.
Command/response logs	Contain CLI command history.
Alarm logs	Contain alarm information.
Measurement logs	Contain system measurements data.
Call record logs	Contain call-processing data.

## Diagnostic Commands

The following integrated IOS command types are also provided to assist you in monitoring and troubleshooting systems:

- Show
- Debug
- Ping
- Trace

## Show Commands

The show commands are powerful monitoring and troubleshooting tools. You can use the show commands to perform a variety of functions:

- Monitoring router behavior during initial installation
- Monitoring normal network operation
- Isolating problem interfaces, nodes, media, or applications
- Determining when a network is congested
- Determining the status of servers, clients, or other neighbors



### Note

It is a good idea to use the trace command when the network is functioning properly under normal conditions so that you have something to compare against when troubleshooting.

## Commonly Used Show Commands

Some of the most commonly used Cisco IOS **show** commands include:

- **show interfaces**—displays statistics for the following network interfaces
  - **show interfaces ethernet**
  - **show interfaces fddi**
  - **show interfaces serial**
- **show controller t1**—Displays statistics for T1 interface card controllers
- **show running-config**—Displays the router configuration currently running
- **show startup-config**—Displays the router configuration stored in nonvolatile RAM (NVRAM)
- **show flash**—Group of commands that display the layout and contents of Flash memory
- **show buffers**—Displays statistics for the buffer pools on the router
- **show memory**—Shows statistics about the router's memory, including free pool statistics
- **show processes**—Displays information about the active processes on the router
- **show stacks**—Displays information about the stack utilization of processes and interrupt routines, as well as the reason for the last system reboot
- **show version**—Displays the configuration of the system hardware, the software version, the names and sources of configuration files, and the boot images

For details on using and interpreting the output of **show** commands, refer to the relevant Cisco IOS command references.

## Debug Commands

The debug privileged EXEC commands can provide a wealth of information about the traffic being seen (or not seen) on an interface, error messages generated by nodes on the network, protocol-specific diagnostic packets, and other useful troubleshooting data.



### Caution

Be very careful when using debug commands. These commands are processor-intensive and can cause serious network problems (degraded performance or loss of connectivity) if they are enabled on an already heavily loaded router. When you finish using a debug command, remember to disable it with its specific **no debug** command, or use the **no debug all** command to turn off all debugging.

Use debug commands to isolate problems, not to monitor normal network operation. Because the high processor overhead of debug commands can disrupt switch operation, you should use them only when you are looking for specific types of traffic or problems and have narrowed your problems to a likely subset of causes.

Output formats vary among debug commands. Some generate a single line of output per packet, and others generate multiple lines of output per packet. Some generate large amounts of output, and others generate only occasional output. Some generate lines of text, and others generate information in field format.



### Note

In many situations, third-party diagnostic tools can be more useful and less intrusive than the use of debug commands. For more information, see the section [Hardware Tools, page 2-15](#).

To minimize the negative impact of using **debug** commands, follow this procedure:

- 
- Step 1** Use the **no logging console** global configuration command on your router. This command disables all logging to the console terminal.
  - Step 2** Telnet to a router port and enter the **enable EXEC** command.
  - Step 3** Use the **terminal monitor** command to copy **debug** command output and system error messages to your current terminal display.

This permits you to view **debug** command output remotely, without being connected through the console port. Following this procedure minimizes the load created by using **debug** commands because the console port no longer has to generate character-by-character processor interrupts.

---

If you intend to keep the output of the **debug** command, spool the output to a file. The procedure for setting up a **debug** output file, as well as complete details regarding the function and output of **debug** commands is provided in Chapter 10, “Debug Command Reference,” in the *Troubleshooting Internetworking Systems* manual.

## Ping Command



### Note

---

It is a good idea to use the ping command when the network is functioning properly under normal conditions so that you have something to compare against when you are troubleshooting.

---

To check host accessibility and network connectivity, use the ping EXEC (user) or privileged EXEC command.

For IP, the ping command sends ICMP Echo messages. If a station receives an ICMP Echo message, it sends an ICMP Echo Reply message back to the source. The extended command mode of the ping command allows you to specify the supported IP header options. This allows the router to perform a more extensive range of test options.

For detailed information on using the ping and extended ping commands, refer to the *Cisco BTS 10200 Softswitch Operations Guide*.

## Trace Command



### Note

---

It is a good idea to use the trace command when the network is functioning properly under normal conditions so that you have something to compare against when troubleshooting.

---

The trace user EXEC command discovers the routes a router's packets follow when traveling to their destinations. The trace privileged EXEC command permits the supported IP header options to be specified, allowing the router to perform a more extensive range of test options. The trace command uses the error message generated by routers when a datagram exceeds its time-to-live (TTL) value. First, probe datagrams are sent with a TTL value of 1. This causes the first router to discard the probe datagrams and send back "time exceeded" error messages. The trace command then sends several probes and displays the round-trip time for each. After every third probe, the TTL is increased by 1.



Each outgoing packet can result in one of two error messages:

- A "time exceeded" error message indicates that an intermediate router has seen and discarded the probe.
- A "port unreachable" error message indicates that the destination node has received the probe and discarded it, because it could not deliver the packet to an application. If the timer goes off before a response comes in, the trace command prints an asterisk (\*).

The trace command terminates when the destination responds, when the maximum TTL is exceeded, or when the user interrupts the trace with the escape sequence.

For detailed information on using the trace and extended trace commands, refer to the *Cisco BTS 10200 Softswitch Operations Guide*.

## Hardware Tools

Most Cisco components include LED indicators on the front or rear panels and, in some cases, on both panels. These LEDs indicate the status of the equipment. The meaning of each LED is described in the component's documentation.

In many situations, third-party diagnostic hardware tools can be more useful than commands that are integrated into the router. For example, enabling a processor-intensive **debug** command can help to overload an environment that is already experiencing excessively high traffic levels. Attaching a network analyzer to the suspect network is less intrusive and is more likely to yield useful information without interrupting the operation of the router.

This section presents an overview of the various tools that are available for troubleshooting cable networks that include Cisco devices. Some typical third-party tools used for troubleshooting include

- Volt-ohm meters (VOM), digital multimeters (DMM), and cable testers
- Breakout boxes, fox boxes, bit error rate testers (BERT), and block error rate testers (BLERT)
- Network analyzers and network monitors
- Time domain reflectometers (TDR) and optical time domain reflectometers (OTDR)
- Low-End Cable Test Equipment
- High-End Cable Testers
- Digital Interface Testing Tools
- Network Management Systems
- Simulation and Modeling Tools

Each of these tools has a specific purpose and works at specific OSI reference model layers.

Understanding what each tool can do and which tool is appropriate for each troubleshooting task will help you become a more efficient network technician.

When troubleshooting, you should start at the physical layer. Use cable testers and other low-level testers to ensure that there are no problems with the media, such as noise, too much attenuation, improper cable lengths, improper connectors, and so forth. If the physical layer seems fine, then move up the layers to the data link layer. You can use a protocol analyzer to check for excessive collisions on Ethernet, beaconing on Token Ring or FDDI networks, excessive soft errors on Token Ring, and other link-layer issues. If the data link layer seems fine, check for routing errors or misconfigurations at the network layer, using a protocol analyzer and Cisco IOS commands. Finally, you can look for upper-layer problems such as misconfigurations, software bugs, and user errors.

## Low-End Cable Test Equipment

At the low-technology end of the spectrum of test equipment are volt-ohm meters and digital multimeters. These devices measure parameters such as AC and DC voltage, current, resistance, capacitance, and cable continuity. They can be used to check physical connectivity.

Cable testers (that is, scanners) can also be used to check physical connectivity. Cable testers give users access to physical-layer information and are available for shielded twisted-pair (STP), unshielded twisted-pair (UTP), 10BaseT, and coaxial and twinax cables.

Cable testers can perform one or more of the following functions:

- Test and report on cable conditions, including near-end crosstalk (NEXT), attenuation, and noise
- Perform time domain reflectometry (TDR), traffic monitoring, and wire map functions
- Display media access control (MAC) layer information about LAN traffic, provide statistics such as network utilization and packet error rates, and perform limited protocol testing (for example, TCP/IP tests such as ping)

Similar testing equipment is available for fiber-optic cable. Due to the relatively high cost of fiber cable and its installation, it is recommended that fiber-optic cable be tested before installation (that is, on-the-reel testing) and after installation. Continuity testing of the fiber requires either a visible light source or a reflectometer. Light sources capable of providing light at the three predominant wavelengths---850 nm, 1300 nm, and 1550 nm---are used with power meters that can measure the same wavelengths and test attenuation and return loss in the fiber.

One of the cable scanners available from Microtest, for example, is the OMNI Scanner. The OMNI Scanner has the functionality to test cables complying with current and upcoming standards with an extremely wide dynamic range of 100 dB and the ability to support up to 300 MHz bandwidth. The OMNI Scanner can test all the way up to 300 MHz on Category 7 cables.

## High-End Cable Testers

At the most technologically advanced end of the cable testing spectrum are time domain reflectometers (TDRs). These devices can quickly locate opens, shorts, crimps, kinks, sharp bends, impedance mismatches, and other defects in metallic cables.

A TDR works by reflecting a signal from the end of the cable. Opens, shorts, and other problems reflect the signal back at different amplitudes, depending on the problem. A TDR measures how much time it takes for the signal to reflect and calculates the distance to a fault in the cable. When a signal reaches the end of a cable, it reflects at a very low amplitude, so TDRs can also be used to measure the length of a cable. Some TDRs can also calculate the propagation rate based on a configured cable length.

Fiber-optic measurement is performed by an optical TDR (OTDR). These devices can accurately measure the length of the fiber, locate cable breaks, measure the fiber attenuation, and measure splice or connector losses by measuring the reflections that occur. Pulse reflections that are generated at breaks or joints, and backscatter reflections that are generated uniformly throughout the cable, are used to measure the fiber attenuation. One way in which the OTDR can be put to good use is to take the signature of a particular installation, noting attenuation and splice losses. This baseline measurement can then be compared with future signatures when a problem in the system is suspected.

## Digital Interface Testing Tools

Several test tools can be used to measure the discrete digital signals that are present at PCs, modems, printers, and other peripheral interfaces. Examples of this type of test equipment include breakout boxes, fox boxes, and bit/block error rate testers (BERTs/BLERTs). These devices can monitor data line conditions, analyze and trap data, and diagnose problems common to data communication systems. Traffic from data terminal equipment (DTE) through data communications equipment (DCE) can be examined to help eliminate problems, identify bit patterns, and ensure that the proper cabling has been installed.

The line-powered Blue Box 100 breakout box from IDS, Inc. is a breakout box and cable tester that is compact, handheld, and fully 100 percent LED. It accesses and monitors all 25 conductors of the RS-232-C, EIA-232-D, CCITT, and V.24, and any other single-ended interface such as the Centronics parallel printer interface. One hundred red and green LEDs monitor and display high, low, off, and signal activity conditions for each of 25 conductors on the DTE and DCE sides of the interface.

## Network Monitors and Analyzers

Network monitors continuously track packets crossing a network, providing an accurate picture of network activity at any moment or a historical record of network activity over a period of time. Monitors collect information such as packet sizes, the number of packets, error packets, overall usage of a connection, the number of hosts and their MAC addresses, and details about communications between hosts and other devices. Correlation of this data allows network administrators to create profiles of their LAN traffic and find traffic overloads, plan for network expansion, detect intruders, establish baseline performance, and distribute traffic more efficiently.

Not only must the monitor collect information about frames, but it must also be able to warn users if any frames are dropped or flag users if certain events such as bad frames, protocol errors, or illegal addresses occur. Visible and audible alarms for the entire network or for individual stations can be set, allowing the network manager to be informed when certain parameters have exceeded predetermined thresholds.

The concept of baselining is becoming very important to network managers. To create a baseline, the activity on a network is sampled over a period of time, and averages, means, and other statistical calculations are used to establish a normal performance profile, or baseline. This baseline can then be used as a reference if any abnormal performance is noted in the network, or it can be used to plan expansion options.

Network monitors further enhance network management by gathering information from remote sites and sending it back to a central management location.

Apart from gathering the standard traffic information, many monitors implement Simple Network Management Protocol (SNMP), Remote Monitoring (RMON), and Management Information Bases (MIBs) to gather information for central management stations. CiscoWorks can also supply network monitoring functions.

The monitor screens of a Sniffer Pro product display charts and graphs that enable you to easily build graphical baseline reports on your network.

## Protocol Analyzers

A protocol analyzer records, interprets, and analyzes how a communication protocol operates in a particular network architecture. It captures frames as they travel across the network. It then decodes the various layers of protocol in the recorded frame contents and presents them as readable abbreviations or summaries, detailing what layer is involved (physical, data link, and some protocol analyzers, right up to the application layer) and what function each byte or byte content serves. With LAN/WAN networks that involve multiple protocols, it is important that a protocol analyzer be able to detect and decode all the protocols used in the network environment.

In capture mode, filters can be set to record only traffic that meets certain criteria; for example, if a particular unit is suspected of inconsistent protocol behavior, then a filter can be configured that captures all traffic to and from that unit. The analyzer should have the capability to timestamp all the captured data. This can be extremely important when determining the effects of peak traffic periods and when analyzing network performance---for example, determining protocol response times by measuring the delta time between frames.

In display mode, an analyzer interprets the captured traffic, presenting the protocol layers in an easily readable form. Filters can be set to allow only those captured frames that meet certain criteria to be displayed.

It is also important that the analyzer be able to generate frames and transmit them onto the network in order to perform capacity planning or load testing of specific devices such as servers, bridges, routers, and switches. The analyzer should be able to send multiple captured frames in succession, as well as allow network managers to tailor the frames by being able to edit the frames prior to generation.

Sniffer Pro analyzers include the Expert System that identifies fault symptoms and provides a diagnosis of the network problems. Sniffer Pro provides decodes for more than 250 protocols. Portability of the analyzer is also an important factor because networks are not physically located in one place, and the analyzer must be moved from segment to segment as problems arise. Several manufacturers provide tools that allow for the remote gathering (and in some cases, analysis) of data and transmission back to a central console or master station.

The ability of the analyzer to use a set of rules and knowledge of the network operation to diagnose network problems is the emergent feature of an expert system. The expert system gleans its knowledge from theoretical databases (that is, from standards information), from network-specific databases (that is, topological information relating to the network), and from users' previous results and experience. From these repositories, the expert system generates a hypothesis about the problem it has detected and offers a plan of action to resolve it.

Protocol analyzers are generally available in three categories:

- Software-based analyzers are software packages that are installed on personal computers (usually portable notebook PCs) that are equipped with appropriate LAN interface adapters.
- General-purpose analyzers offer a wide range of uses, such as traffic monitoring, reasonably extensive protocol capture and decode support, and some network traffic modeling during the network design phase.
- High-end analyzers offer a range of advanced features and can typically capture traffic at higher rates and provide a more comprehensive protocol decode than can the other analyzers. They also support generate-and-capture capabilities, which means you can use them to stress-test parts of the network.

## Network Management Systems

As networks grow larger and more complex, there is a greater chance of network failures that can disable the entire network or degrade performance to an unacceptable level. The complexity of such large networks makes the use of automated network management tools a critical factor in efficient management. It is important that the continued addition of users, interfaces, protocols, and vendor equipment to the network does not result in the network manager losing control of these resources and how they are used. It is also important that as network resources become more critical in an organization's operations, downtime be reduced. To ensure maximum network availability, network managers should include network management in their internetwork designs.

The International Organization for Standardization (ISO) has defined five key functional areas of network management: fault management, configuration management, accounting management, performance management, and security management, commonly called FCAPS.

The functions of fault, performance, and configuration management are most applicable to a troubleshooting environment. To achieve maximum network availability, all individual components of a network must be maintained in working order. A key ingredient to achieving this is having a mechanism in place that reports a fault immediately as it occurs. A fault can be defined as an abnormal network event, usually indicated by network components failing to operate correctly or causing excessive errors. It is therefore important to be able to do the following:

- Determine exactly where the fault has occurred.
- Isolate the failed area from the rest of the network so that the rest of the network can continue operating.
- Reconfigure or modify the network or its configuration to minimize the impact of operating without the failed component or affected portions of the network.
- Repair or replace the failed components to restore normal network operation.

Configuration management involves several functions. The network manager should be able to set up the network by initial configuration of the network components and interactively control these components by changing their configuration in response to performance evaluation or in response to network upgrades or fault recovery.

SNMP is an application-layer protocol that facilitates the exchange of management information between network devices. It is part of the TCP/IP protocol suite. SNMP enables network administrators to manage network performance, find and solve network problems, and plan for network growth. An SNMP network consists of SNMP agents (managed devices) and an SNMP management station (manager).

In a typical SNMP design an SNMP manager queries an SNMP agent on a router to obtain operational statistics from the agent.

## Simulation and Modeling Tools

Simulation/modeling software is useful for purposes such as initial network design, analysis of a network reconfiguration or redesign, and stress-testing a network.

This type of software usually uses object-oriented design to predict the performance of networks, ranging from departmental LANs up to complex, enterprisewide internetworks and WANs.

By selecting numerous objects that represent network topology, protocols in use, traffic, and routing algorithms, Netsys Baseline attempts to simulate the operation of the network. Most types of LAN, MAN, and WAN technologies can be modeled by these tools. The output gives measures of the network performance such as response times; network throughput; node, link, and LAN utilization; packets dropped; and other performance data.

Many analyzer vendors offer the capability to export the data from their analyzers into the simulation/modeling tools, thus providing a source of real network data.

These simulation/modeling tools allow the network manager to see and test network performance before committing to proposed designs or changes.

## Cisco Supplied Tools

The following tools require user registration for access. The registered sites are noted beside the link. To become a registered user, refer to <http://www.cisco.com/register/>.

If you are accessing the tools from Cisco.com, go to the top of the Cisco.com page, and click Log In before clicking the links below. Clicking Log In first will bring you to a login Screen. Clicking the links on the Tools and Utilities page without clicking Log In will not bring up a login screen.

The Tools and Utilities index provides links to tools and utilities such as configuration, installation, software download, troubleshooting, and assessment tools.

The Troubleshooting Tools index includes tools such as:

- Feature Navigator for Cisco IOS
- Cisco Error Message Decoder Tool
- Cisco IOS Upgrade Planner
- Command Lookup Tool
- Field Notice Alert Tool
- Output Interpreter Tool
- Software Advisor
- Software Bug Toolkit

The Output Interpreter can now also help you troubleshoot reloads on Catalyst 6500/6000, Catalyst 5500/5000, and Catalyst 4500/4000 Series switches, and on certain Catalyst 2900 models. Just paste the output from the "show tech-support" command into the tool from a device running Catalyst OS, Cisco IOS(R), or Integrated IOS(R). For a Catalyst 4500/4000 running Catalyst OS, also paste in the output from the "show crashdump 1" command. Your customized analysis will identify the most likely bugs and will show the OS version where these bugs have been fixed.

## Other Troubleshooting Information Websites

These websites are provided to help you find the most current troubleshooting information:

- Search the Cisco TAC assistance website, at <http://www.cisco.com/public/support/tac/home.shtml>
- Use the troubleshooting tools at [http://www.cisco.com/kobayashi/support/tac/tools\\_trouble.shtml](http://www.cisco.com/kobayashi/support/tac/tools_trouble.shtml)
- Search cable products field notices at <http://www.cisco.com/warp/public/770/61.html>
- Find router and IOS architecture technical tips at <http://www.cisco.com/cgi-bin/Support/browse/index.pl?i=Products>
- If your system is still not responding, find help at [http://www.cisco.com/warp/public/63/why\\_hang.html](http://www.cisco.com/warp/public/63/why_hang.html)



## Trouble Isolation Procedures

---

This chapter presents comprehensive trouble isolation procedures for the Cisco Broadband Local Integrated Services Solution (BLISS) for Cable.

Trouble isolation covers the following activities, which are described in the following sections:

- [Finding System Information, page 3-1](#)
  - Information, such as port numbers and IP addresses, are needed to perform troubleshooting tasks
- [Checking Events and Alarms, page 3-2](#)
- Checking device and communications status
  - Aggregation routers (CMTSs)
  - Trunking gateways (TGWs)
  - Trunk groups (TGs)
  - Trunks
  - Subscriber terminations (MTAs)
  - SS7 signaling links
  - Signaling destinations

### Finding System Information

Before you begin troubleshooting the solution, be sure you have the following information:

- IP addresses and port numbers for all components
- Passwords for those components, when necessary
- Physical locations of solution components/contact information
- SS7 point codes, if necessary

This information should be available in your solution documentation if you have followed Cisco's recommendations for implementing the solution.

- See the [Cisco BTS 10200 Site Surveys](#)
- See the [Cisco BTS 10200 Cabling Procedures](#)

## Determining the Source of the Problem

The first step in troubleshooting your system is determining the source of your problem. There are several network elements connected to the Cisco BTS 10200 Softswitch and to the IP management network centered on the Catalyst 6509 switch.

You will usually be notified of system problems by events and alarms. Use the CLI commands described in this chapter to pull event and alarm logs for the Cisco BTS 10200 Softswitch.

If the same alarm originates from the Cisco BTS 10200 and another network element, there is a strong chance that the problem is not with the softswitch. If the alarm originates only on the Cisco BTS 10200, then the problem is probably in the softswitch.

Always begin your investigation by checking all physical connections and indicator lights (wherever physically possible). You can frequently save yourself hours of troubleshooting time by checking the indicator lights and the physical connections of the system.

## Checking Events and Alarms

A wide variety of events and alarms provide vital information about the status of links and components. You can use event and alarm logs to help isolate problems within the system. Each event or alarm on the Cisco BTS 10200, for example, belongs to one of the following eleven categories that describe the type of failure the event or alarm indicates:

- **Audit**—Event or alarm messages generated by the audit subsystem
- **Billing**—Event or alarm messages generated by the billing subsystem
- **Callp**—Event or alarm messages generated by call processing
- **Config**—Event or alarm messages that provide information about system configuration
- **Database**—Event or alarm messages generated by the database
- **Maintenance**—Event or alarm messages that provide information about maintenance
- **OSS**—Event or alarm messages generated by the Operations Support System (OSS)
- **Security**—Event or alarm messages generated by the billing subsystem
- **Signaling**—Event or alarm messages generated by signaling protocols or interfaces
- **Statistics**—Event or alarm messages that provide information about system statistics
- **System**—Event or alarm messages that convey information about system status or trouble

In addition to event and alarm types, events and alarms can have one of the following serverity levels:

- **Critical:** Indicates a fundamental problem with the system. This is an alarm.
- **Major:** Indicates a problem with a significant impact on call handling. This is an alarm.
- **Minor:** Indicates a problem with a minor impact on call handling. This is an alarm.
- **Warning:** Indicates a situation with little or no impact to call handling that might become a problem if it persists. This is an event; it does not generate an alarm.
- **Info:** Indicates an autonomous system event with little or no impact to call handling. While they do not necessarily indicate trouble and do not generate an alarm, informational events can aid in pinpointing sources of failure.



## Managing Event and Alarm Reports

There are two ways to view events and alarms—by subscribing to event and alarm reports (automatic, real-time) and by retrieving event or alarm summaries from the log files by operator query.

Use the following subscribe commands to subscribe to reports of real-time event messages or alarms:

```
subscribe event-report type=all | type=<type>; severity=all | severity=<severity>;
subscribe alarm-report type=all | type=<type>; severity=all | severity=<severity>;
```



### Note

In the **subscribe event-report** or **subscribe alarm-report** commands you can specify "**type=all**" and/or "**severity=all**" or you can specify the types and severities of events and alarms you wish to display.

Cisco recommends that you choose to receive **all** types and **all** severities of all event and alarm reports. This allows you to monitor the system for **all** events and alarms and be alerted quickly if there is trouble.

### Show Alarm Command

Use the **show alarm** command to view real-time alarms. This command does not show events of severity Warn and Info. All of the following tokens are optional.

```
show alarm id=<sn>; type=<type>; number=<num>; severity=<sev>;
component-id=<comp>; origin=<process>; start-time=<yyyy-mm-dd hh:mm:ss>;
end-time=<yyyy-mm-dd hh:mm:ss>
```

Specifying a *type* and a *number* shows only alarms of that type and number. You can specify a *number* without specifying a *type*; and you can specify a *type* without specifying a *number*.



### Note

If the **show alarm** command is issued without any tokens (parameters), **all** alarms of **all** types and **all** severities (CRITICAL, MAJOR, and MINOR) are displayed. Issuing a **show alarm** command with any combination of optional tokens limits the display to the designated subset of alarms.

### Format of Event and Alarm Reports

The general format of an event or alarm report, as displayed on an operator console, is as shown below. An event or alarm summary contains multiple event or alarm reports, selected according to the query that is entered.

For example, the following query produced the result shown here.

```
show alarm type=callp; number=23; component-id=tg1@ca1.carrier.com
```

```
Reply : Success: Request was successfully completed
```

```
ID=123456
TYPE=callp
NUMBER=23
TEXT=Trunk Group Out Of Service
STATUS=ACKNOWLEDGED
SEVERITY=MAJOR
TIME=2004-06-23 10:54:20
COMPONENT ID=tg1@ca1.carrier.com
ORIGIN=bcm@ca146
THREAD=
DATAWORD1= through DATAWORD8=
```

The elements of the reply for an alarm (or an event) are defined as follows:

- **Serial Number (ID)**—All events and alarms have a unique, system-assigned serial number.
- **Type**—Type is the designated category of the report: Audit, Billing, Callp, Config, Database, Maintenance, Oss, Security, Signaling, Statistics, or System.
- **Number**—Event or alarm numbers are preset in the Cisco BTS 10200. They are not user provisionable.
- **Description**—Up to an 80-character description of the event or alarm.
- **Status**—Status for an alarm can be ALARM\_ON, ALARM\_OFF, ALARM\_IGNORE, or ACKNOWLEDGED.
- **Severity**—Severity of the alarm: CRITICAL, MAJOR, MINOR (or event: WARNING, or INFO)
- **Date and Time**—Date and time of report in the format yyyy-mm-dd hh:mm:ss. Year, month, and day plus hours, minutes, and seconds of an alarm or event, displayed in Greenwich Mean Time (GMT).
- **Component ID**—ID for the component reporting the event or alarm.
- **Origin**—ID for the process generating the event or alarm.
- **Thread**—Thread within the BTS process that initially issued the alarm, when applicable.
- **DataWord $n$** —Header for additional data fields to an event or alarm. Up to 8 data fields can be reported, depending on the event or alarm.

## Event Message and Alarm Logs

It is recommended that you manage the event and alarm messages and logs in a manner that permits the operator to access all events and alarms and watch for unexpected events or alarms. For example, if any of the following anomalies are seen, investigate promptly to determine the cause(s) and required action:

- Congestion warnings
- Routing errors
- Termination failures
- Billing errors
- Security warnings
- Diagnostic failures
- Process failovers

### Viewing Event or Alarm Logs

Use the following **show** commands to view event or alarm logs. The event and alarm logs are typically used if the user session is disrupted, or if all events or alarms of one kind are needed in a single report.

```
show event-log id=<sn>; type=<type>; number=<num>; severity=<severity>;
component-id=<comp-id>; origin=<process-id>; start-time=<yyyy-mm-dd hh:mm:ss>;
end-time=<yyyy-mm-dd hh:mm:ss>;
```

```
show alarm-log id=<sn>; type=<type>; number=<num>; severity=<severity>;
component-id=<comp-id>; origin=<process-id>; start-time=<yyyy-mm-dd hh:mm:ss>;
end-time=<yyyy-mm-dd hh:mm:ss>;
```

**Note**

If the **show event-log** or **show alarm-log** commands are issued without any tokens (parameters), *all* events or alarms of *all* types and *all* severities for *all* components are displayed. Issuing the **show event-log** or **show alarm-log** commands with any combination of optional tokens limits the display to the designated subset of events or alarms.

**Event Queue**

The event-queue commands allow you to show, add, or delete an event queue on a Cisco BTS 10200 Call Agent or Feature Server.

```
show event-queue instance=CA146
add event-queue instance=CA146
delete event-queue instance=CA146
```

**Event-queue** commands must include the mandatory **instance** token, which specifies the Call Agent or Feature Server (*CAmmn*, FSPTC, or FSAIN) where the event queue is located. Only one instance can be shown, added, or deleted at a time.

**Saving Events and Alarms to Log Files**

Use the commands in this section to manage the way events and alarms are saved to their respective logs.

**Show Report-Properties**

Use the following **show report-properties** command to view the event or alarm properties currently used to specify which levels, events, and alarms are saved to the event or alarm logs:

```
show report-properties
Reply : Success: Entries 1-3 of 3 returned.

TYPE=EVENT_LOGSIZE
VALUE=30000
TYPE=ALARM_LOGSIZE
VALUE=30000
TYPE=EVENT_LEVEL
VALUE=INFO
```

**Note**

The **show report-properties** command, without any tokens as shown above, returns *all* alarm-logsize, event-logsize, and event-level data.

There are no mandatory tokens (parameters) required for the **show report-properties** command; however, you can optionally use the type and/or value tokens described previously.

**Changing Report-Properties**

Use the following **change report-properties** command to specify the maximum number and/or the severity of event or alarm entries to be saved to the event or alarm logs:

```
change report-properties type=event-logsize|alarm-logsize; value=<logsize>; or
change report-properties type=event-level; value=<severity>
```

The **type** and **value** tokens are both mandatory for the **change report-properties** command.

- If **type=event-logsize** or **alarm-logsize**, then **value** must be an integer between 1 to 30000.

- If **type**=*event-level*, then **value** designates the severity of the events or alarms to include in the log files, which can be CRITICAL, MAJOR, MINOR, WARN, or INFO.  
All events or alarms whose severity is equal to or greater than the event level specified are included in the designated event or alarm log file.

**Tip**

Cisco recommends that you store events of *all* severity levels in the event and alarm log files by entering INFO as the value in this command. This permits the operator to access *all* event and alarm reports.

## Changing Threshold and Throttle Values

The **threshold** and **throttle** values used in event and alarm reporting are user-provisionable. You can use the following **show event-prov** command to display the current threshold and throttle values for any event or alarm message:

```
show event-prov type=callp; number=9;
```

```
Reply : Success: Entry 1 of 1 returned.
```

```
REPORTTYPE=2
REPORTNUMBER=9
REPORTDESCRIPTION=No Route Available for Carrier Dialed
THRESHLIM=100
THROTTLELIM=20
DW1NAME=Orig Type(Trunk or S
DW2NAME=Orig Sub or TG id
DW3NAME=Calling Party Number
DW4NAME=Called Party Number
DW5NAME=Carrier Code Dialed
DW6NAME=n/a
DW7NAME=n/a
DW8NAME=n/a
```

```
CAUSE1=No route is available for the interexchange carrier (IXC) dialed.
ACTION1=The data words in the event report indicate the parameters that need to
be corrected. Refer to office records for the carrier.
```

```
CAUSE2=Parameter(s) in the carrier and/or route-grp table are missing or
incorrect for the carrier.
ACTION2=Determine whether the routing parameters were entered correctly in the
carrier and/or route-grp tables.
```

```
ACTION3=If the carrier-id or route-grp-id are not specified, or are incorrect in
the dial-plan table, enter the correct values. Use the change carrier or change
route-grp command.
```

The command **show event-prov** with no parameters displays *all* events that are provisioned. The command **show event-prov** with only **type** specified displays *all* events of that type.

Use the following **change event-prov** command to specify event **threshold** and **throttle** values:

```
change event-prov type=<type>; number=<n>; threshold=<n>; throttle=<n>;
```

- **threshold**—The maximum number of reports of the designated event or alarm that can be issued in any 30-minute interval. Valid values are 1 to 100.
- **throttle**—The number of occurrences of the designated event or alarm message required to trigger the issuance of one report. Valid values are 1 to 100.

The total number of occurrences of the designated event or alarm message is determined by multiplying these two values (**threshold X throttle**). The system maximum number of occurrences of an event or alarm that can be reported in any 30-minute interval is 100x100 or 10,000.

## Managing and Responding to Events and Alarms

To manage and respond to events and alarms on the Cisco BTS 10200 softswitch, complete these steps:

- 
- Step 1** Set the event-logsize and event-level parameters as desired using the **report-properties** command (see the “[Changing Report-Properties](#)” section on page 3-5).
  - Step 2** Subscribe to events and request event summary reports as needed using the **subscribe** command (see the “[Managing Event and Alarm Reports](#)” section on page 3-3).
  - Step 3** Set the alarm-logsize and event-level parameters as desired using the **report-properties** command (see the “[Changing Report-Properties](#)” section on page 3-5).
  - Step 4** Subscribe to alarms and request alarm summary reports as needed using the **subscribe** command (see the “[Managing Event and Alarm Reports](#)” section on page 3-3).
  - Step 5** Set the threshold and throttle parameters as desired using the **change event-prov** command (see the “[Changing Threshold and Throttle Values](#)” section on page 3-6).
  - Step 6** View event and alarm reports and investigate potential problems.  
Examples of problems to look for include: congestion warnings, routing errors, termination failures, billing errors, diagnostic failures, security warnings, and process failovers.
  - Step 7** Refer to the "Probable Cause" and "Corrective Action" instructions for events and alarms in the "Event Messages and Alarms" chapter of the *Cisco BTS 10200 Softswitch Operations, Maintenance, and Troubleshooting Guide*.
  - Step 8** Take the necessary corrective action; escalate the problem if necessary.  
The **subscribe** command causes the system to display events and alarms as they occur. Opening an alarm subscription in a separate window enables you to see how your actions affect the system.  
The situation that caused an event or alarm must be resolved before the event or alarm can be cleared.
  - Step 9** After the problem is fixed, enter the following command to clear a specific alarm:

```
clear alarm id=<sn>
```

where **id** is the system-assigned serial number (*sn*) of the event or alarm.

Events (severity levels of info or warn) do not need to be cleared.

Examine the display. If there are any MAJOR or CRITICAL alarms, **do not** continue with this procedure. Instead, take the necessary actions to correct the conditions causing the alarm(s). Contact your technical support group if you need assistance. If additional support is needed, contact Cisco TAC.

When you are finished viewing events and alarms, remember to turn off the subscription by entering the following command:

```
CLI > unsubscribe
```

---

# Troubleshooting Hardware Components

Hardware troubleshooting involves making sure all the Cisco BLISS for Cable solution components are powered on, properly connected, and communicating with one another and with the Public Switched Telephone Network (PSTN). The following sections cover procedures for isolating and remedying physical layer problems.

## Trouble Isolation

Hardware-related trouble usually means power system failure or connectivity failure. Since testing for connectivity can uncover power failures, this procedure begins with a connectivity test on each type of physical link in the Cisco Broadband Local Integrated Services Solution. The following list describes the three kinds of physical links that connect the solution components:

- IP links that connect all solution components to the Cisco BTS 10200 management IP network.  
In addition to network cards and cabling terminating in each component, the management IP network can also include switches and/or routers.
- SS7 links from the PSTN that terminate in the Cisco BTS 10200.
- Bearer trunks from the PSTN that terminate in the Cisco MGX 8850 Media Gateway.

Each type of link requires different troubleshooting techniques, which are covered in the following procedure:

---

### Step 1 Test IP connectivity.

Verify that each solution component is connected to the same IP management network. The solution IP management network allows each component to send and receive messages to and from all the other components in the solution that are connected to the IP management network.

Use the ping command to verify IP connectivity among all the solution components. In order to do this, you will need to know the IP address of each solution component. You can attempt to ping each device from any of the following locations:

- A PC or workstation on the same LAN as the solution components
- When you are logged in to the Cisco BTS 10200 EMS
- When you are logged in to the Cisco Media Gateway (MGW)

If you cannot successfully ping one or more devices, troubleshoot that device to ensure that it is operating properly.

### Step 2 Test SS7 link connectivity.

Signaling messages are received from the SS7 signaling network via SS7 links that terminate in the Cisco BTS 10200. After verifying that you can successfully ping other devices from the Cisco BTS 10200, use the following command to verify SS7 link connectivity.

```
CLI> show ss7-cic trunk-id=<id>; tgn-id=<id>; dpc=<num>;
```

where all of the following tokens are optional

- **trunk-id**—is the system generated trunk id
- **tgn-id**—is the user provisioned trunk group id
- **dpc**—is the destination point code of the STP reached via the specified trunk

**Step 3** Test bearer trunk connectivity.

Bearer trunks carry traffic from end-users dialed into the PSTN to cable modems on the CMTS. After you have verified that you can successfully ping the CMTS, verify bearer trunk connectivity between the MGW and the PSTN.

## Trouble Resolution

If your connectivity tests for IP links, SS7 links or Bearer Trunks were unsuccessful, you need to visually inspect the device or devices that have failed. Once you, or someone working with you, can visually inspect the solution components, follow this procedure for resolving hardware-related problems:

**Step 1** **Make sure your test is valid.** If no devices responded to your ping attempt, check first to make sure that the device where you executed the ping command is properly connected to the LAN. If your device appears to be properly connected, and your ping attempts are still unsuccessful, check that the switch or router that provides LAN connectivity for the solution is configured properly, not overwhelmed by heavy traffic, powered on, and connected to the LAN.

**Step 2** **Check Indicator Lights.** Check the power and connectivity indicators of each component you were unable to ping. Power LEDs should be lit, and connectivity LEDs should indicate that all connections are active.

**Note**

For descriptions of power and connectivity indicators on each solution component, see the following sections of this document:

- If you determine there is a power failure, continue with the next step of this procedure.
- If the power is up, but there is a connectivity failure, continue with Step 4 of this procedure.
- If power and connectivity appear to be good, continue with the “Checking Alarms” section.

- a. **Resolving Power Troubles.** If any indicators show the device is not receiving power, you will need to check one of the following:
  1. Check the power supply unit on the device. If it has failed, replace it. Consult the platform documentation to determine the part number for replacement power supplies.
  2. Check the power system of the building where the device is installed. You will need to work with the facilities manager or lab administrator to troubleshooting building power problems.
- b. **Resolving Physical Connectivity Troubles.** If any indicators show that a link is down, check the following to restore connectivity:
  1. Loose cable connection.  
Remedy: re-seat the connection.
  2. Bad or miswired cable.  
Remedy: replace the cable.
  3. Interface card malfunction.  
Remedy: replace or re-seat the card. NOTE: Make sure the device supports hot-swap feature before removing a card from a live system.

## Call Traces

**Traces** are records of the message flows through the Cisco BTS 10200 Softswitch. Traces are useful when problem calls are reaching the Cisco BTS 10200 Softswitch basic call module (BCM). If a trace is empty, the call has not reached the BCM.

A problem call can be readily identified through the presence of non-idle bearer circuits entries in the debug logs. In most cases, the logs need to be operating at debug level to be useful; however, there are performance implications when using this level of logging.

Examination of the debug log file is most useful for tracking down:

- Configuration errors
- Signaling link problems
- Problems with non-established calls

Fault identification up to this point is largely a matter of gathering background information to gain a picture of the platform and signaling states. From this point, however, the decision to attempt a trace or to examine the logs depends on several factors, including the level of personal experience.



### Caution

Contact Cisco TAC before attempting a trace or generating debug level logs.

## Component States

The Cisco BTS 10200 Softswitch can be used to monitor and, to a certain extent, administer the states of some solution components including the following:

- SS7 Signaling Trunks
- SS7 Signaling destinations
- Aggregation routers, which are used as Cable Modem Termination Systems (CMTSS)
- Media gateways (MGWs), which are used as trunking gateways
- Trunk groups (TGs)
- Trunks
- Subscriber terminations (Media Termination Adapters (MTAs))

The following solution components have the following dependencies:

- Allowed subscriber states depend on the current CMTS or MTA state.
- Allowed trunk states depend on the current Trunk Group state, which, in turn, depends on the current Trunking Gateway state.

There are two types of independent service states possible for solution components:

- **Administrative**—The state the Cisco BTS 10200 operator sets for the link to the component
- **Operational**—The physical state of the component itself, or the link to the component

The independence of these two service states is illustrated by the following example:

A Cisco BTS 10200 Softswitch operator executes the command to place a media gateway connection in service. The administrative state of the connection is “In Service” (ADMIN\_INS). However, the link between the Cisco BTS 10200 and the media gateway might be out or the media gateway itself might be placed out of service, so the operational state of the media gateway link is MGW\_STATUS\_DOWN.



A status report for the media gateway lists both the administrative state and operational state of the link to the media gateway as well as the operational state of the gateway.

This section explains how to use status, control, and administrative commands to determine the status of various solution components, including:

- [Signaling Gateway Process](#)
- [Signaling Destinations](#)
- [Destination Point Code Status](#)
- [Aggregation Status](#)
- [Media Gateway](#)
- [Subscriber Termination](#)
- [Trunk Group](#)
- [Trunk Termination](#)

## Signaling Gateway Process

The status command for the signaling gateway process (SGP) returns the state of the SGP.

```
CLI> status sgp-id=sgp1;
```

where **sgp-id** is the ID of the selected signaling gateway process.

## Signaling Destinations

Signaling destinations are endpoints in a time-division multiplex (TDM) network. In SS7, multiple destinations can be served by one or more signaling links. Destination states are similar to the signaling link states, but with fewer possible combinations.

[Table 3-1](#) identifies and defines the possible signaling destination states:

**Table 3-1 Signaling Destination States**

Destination State ID	Name	Definition
IS	In Service	Ideal state—Generally, if signaling links are in service, destinations should be in service as well.
OOS	Out-of-Service	Link is unavailable, often due to a communication problem with the remote end. Requires additional diagnosis.
INB	Installed Busy	Default state of newly installed links. New links must be manually set in service using the <b>set-sc-state</b> command.

Signaling destination problems can result from any of the following:

- SS7 traffic restart handling
- SS7 STP problems
- Configuration problems
- Software problems
- Bearer Channels

Bearer channels are at the core of the solution. The goal is to ensure that a bearer channel successfully communicates between two endpoints. The state of the bearer channels is often a good indicator as to the health of the overall system. In the SS7 network, CICs identify each bearer channel in the network. The state of each channel is maintained by the EMS.

## Destination Point Code Status

This example describes the status command for destination point codes (DPCs).

```
CLI> status dpc id=dpc1;
```

```
Reply : Success:
```

```
DPC ID -> dpc1
OPER STATE -> DPC IN SERVICE
RESULT -> ADM configure result in success
REASON -> ADM executed successful
```

The possible operational states returned by the **status dpc** command are as follows:

- DPC IN SERVICE—the connection to the DPC is up and the DPC is in service.
- DPC OUT OF SERVICE—the connection to the DPC is down and/or the DPC is out of service.



### Note

---

The DPC-ID is not the destination point code (DPC). You must check the DPC-ID entry in the Destination Point Code table to determine the actual DPC value.

---

## Aggregation Status

Aggregation routers are used in the Cisco BLISS for Cable solution as cable modem termination systems (CMTSs).

Use the following command to check the status of an aggregation router (CMTS):

```
CLI> status aggr id=CMTS1
```

```
Reply : Success:
```

```
AGGR ID -> CMTS1
OPER STATE -> AGGR IN SERVICE
RESULT -> ADM configure result in success
REASON -> ADM executed successful
```

The possible operational states returned by the **status aggr** command are as follows:

- AGGR IN SERVICE—the connection to the CMTS is up and the CMTS is in service.
- AGGR OUT OF SERVICE—the connection to the CMTS is down or the CMTS is out of service.

- AGGR CONNECTING—the connection to the CMTS is being set up.
- AGGR INITIALIZING—identifies the initial state of the CMTS before the Call Agent (CA) attempts to connect to it. This is a transitional state, which a user may rarely see.

## Media Gateway

This example describes how to check the status of a media gateway.

```
CLI> status mgw id=c8850_197;
```

Reply : Success:

```
MGW ID -> c8550_197
RESULT -> ADM configure result in success
REASON -> ADM executed successful
ADMIN STATE -> ADMIN_INS
OPER STATE -> Media gateway in working status
```

The administrative states the system can return are as follows:

- ADMIN-INS—the media gateway is in service
- ADMIN-OOS-PENDING—the media gateway is transitioning to out of service
- ADMIN-OOS—the media gateway is out of service
- ADMIN-MAINT-PENDING—the media gateway is transitioning to maintenance mode
- ADMIN-MAINT—the media gateway is in maintenance mode.

The system can also report the following media gateway operational states:

- Media gateway in unknown status
- Media gateway in working status
- Media gateway in down status
- Media gateway cannot be reached

## Control Command

This section shows how to control a media gateway in service. Modes can be either forced or graceful. Forced mode tears down all calls immediately; graceful mode allows calls in progress to complete before teardown.

**Step 1** Use the following example to control a media gateway in service:

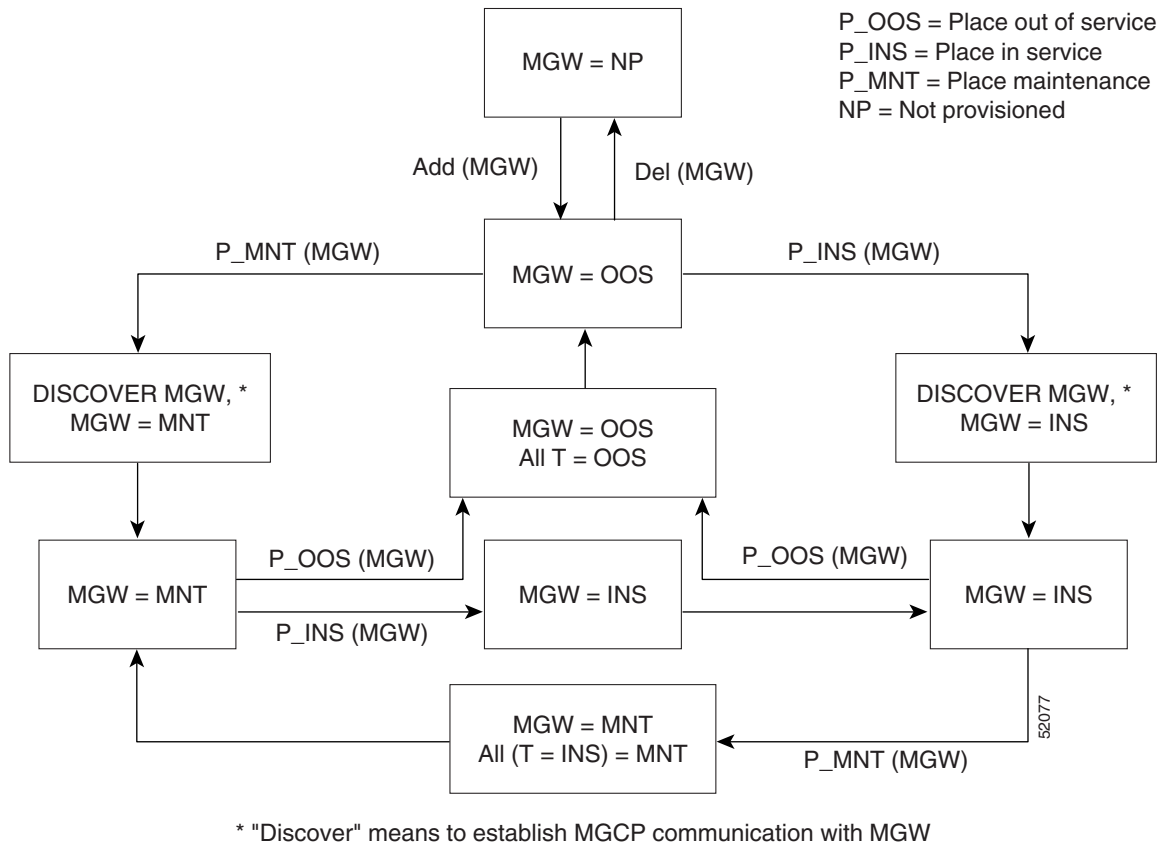
```
CLI> control mgw id=c5300_162; mode=forced; target-state=INS;
```

Reply : Success: CLI change successful

```
MGW ID -> c5300_162
INITIAL STATE -> ADMIN_OOS
REQUEST STATE -> ADMIN_INS
RESULT STATE -> ADMIN_INS
FAIL REASON -> ADM found no failure
REASON -> ADM executed successful
RESULT -> ADM configure result in success
```

The rules for placing an MGW into the OOS, INS, and MAINT states are shown in [Figure 3-1](#).

**Figure 3-1 Administrative and Operational Maintenance States for MGW**



## Subscriber Termination

This section describes the status and control commands for subscriber terminations.



### Note

When first provisioned, all subscriber terminations are in the unequipped (UEQP) state. A subscriber termination must also be in the UEQP state before it can be deleted.

Individual subscriber terminations can be placed into any of three administrative service states: INS, OOS, and MNT. The relationship between subscriber termination states and the CMTS state is provided in [Table 3-2](#).

**Table 3-2 CMTS and Subscriber Termination States**

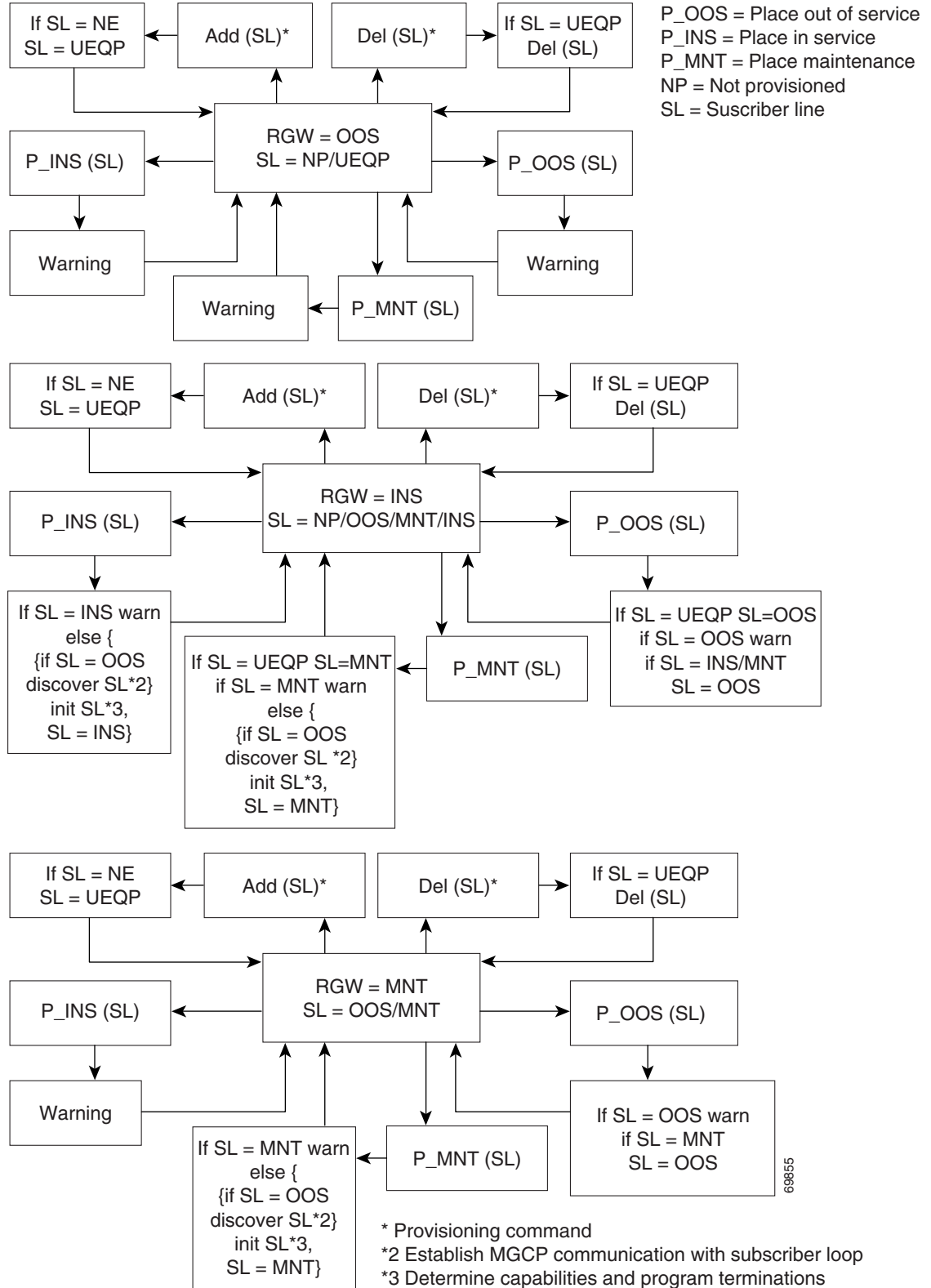
<b>CMTS State</b>	<b>Allowed Subscriber Termination States</b>
OOS	OOS UEQP
INS	OOS MAINT INS UEQP
MAINT	OOS MAINT UEQP

where:

- OOS—out of service
- MAINT—maintenance
- INS—in service
- UEQP—unequipped

The rules for placing subscriber terminations into the OOS, INS, and MAINT states (which depend upon the CMTS state) are shown in [Figure 3-2](#). In this figure the Residential Gateway (RGW) is the CMTS.

Figure 3-2 Administrative and Operational Maintenance States for CMTS



69855

## Status Command

This section describes how to show the status of subscriber terminations. It is organized as follows:

- [Single Subscriber Termination Status](#)
- [All Subscriber Terminations Status](#)
- [Administrative State Token](#)
- [Operating State Token](#)
- [Source Token](#)

### Single Subscriber Termination Status

The following example checks the status of a single subscriber termination:

```
CLI> status subscriber-termination id=ubr204_1;

RESULT -> ADM configure result in success
REASON -> ADM executed successful
ADMIN STATE -> ADMIN_INS
OPER STATE -> Termination is idle
SUBSCRIBER DN -> ubr204_1
FAULT REASON -> No fault reason available
```

The administrative states the system can return are as follows:

- ADMIN-UEQP—Unequipped.
- ADMIN-INS—In Service.
- ADMIN-OOS—Out of Service.
- ADMIN-MAINT—Maintenance Mode.
- ADMIN-OOS-PENDING—Transitioning to Out of Service.
- ADMIN-MAINT-PENDING—Transitioning to Maintenance Mode.

### All Subscriber Terminations Status

The following example shows the status of all subscriber-terminations on a particular gateway:

```
CLI> status subscriber-termination id=*@ubr235;

Reply : Success:

SUBSCRIBER DN -> ubr235_1
ADMIN STATE -> ADMIN_UEQP
OPER STATE -> Termination is unequipped
REASON -> ADM executed successful
RESULT -> ADM configure result in success
FAULT REASON -> No fault reason available
SUBSCRIBER DN -> ubr235_2
ADMIN STATE -> ADMIN_UEQP
OPER STATE -> Termination is unequipped
REASON -> ADM executed successful
RESULT -> ADM configure result in success
FAULT REASON -> No fault reason available
```

## Administrative State Token

The Administrative State (admin-state) token returns the administrative state of the subscriber termination. Valid values are:

- UEQP—Unequipped; resource is not commissioned. Resource is not registered.
- OOS—Termination was manually controlled out of service.
- INSQ—Termination was manually controlled in service, but operationally may be available or unavailable.
- OOS-PENDING—Termination was manually controlled out of service with mode graceful, termination is still involved in a call.
- MAINT—Termination was in maintenance mode, can run diagnostic commands.
- MAINT-PENDING—Termination was manually controlled to MAINT state, but termination is still involved in call.
- ALL—Return all possible states.

The following command example returns only those trunk terminations that are in administrative state OOS (if any), and operating state IDLE (if any):

```
CLI> status trunk-termination tgn-id=12; cic=1-1000; admin-state=OOS;
oper-state=idle
```

## Operating State Token

The Operating State (oper-state) token expands the range of useful information returned by the status subscriber-termination command.

Valid values for the oper-state token are:

- FA—Faulty
- NF—Not faulty
- IDLE—Termination idle
- ACTIVE—Termination active
- DOWN—Termination down
- TERM-FA—Termination fault
- TEMP-DOWN—Termination temporarily down
- UNREACH—Termination unreachable
- INT-MAINT—Termination internal maintenance
- UEQP—Termination unequipped
- ALL—All states, same as executing command without oper-state token

The following example returns only those subscriber terminations that are FA (if any):

```
CLI> status subscriber-termination id=*@ubr235; oper-state=FA;
```



## Source Token

The source token specifies whether to query the Call Agent, or the EMS, for status information. It is an optional token. Valid values for the source token are:

- EMS (Default)—Query the local EMS database for most current status.
- AGENT—Query the remote Call Agent database for most current status.

The following example returns the current status of a Call Agent:

```
CLI> status subscriber-termination id=@ubr235; source=AGENT;
```

## Control Commands

This section describes how to control subscriber terminations on a particular gateway. To control a subscriber termination to the equipped or unequipped state, use the equip or unequip commands in the “Equip Command” section on page 3-20 or the “Unequip Command” section on page 3-20. This section is organized as follows:

- [Control a Single Subscriber Termination](#)
- [Control All Subscriber Terminations](#)
- [Equip Command](#)
- [Unequip Command](#)

### Control a Single Subscriber Termination

The following example controls a single subscriber termination into service:

```
CLI> control subscriber-termination id=@c3810_167; mode=forced;
      target-state=INS;
```

```
Reply : Success: CLI change successful
```

```
ID -> c3810_167
REQUEST STATE -> ADMIN_INS
RESULT STATE -> ADMIN_INS
FAIL REASON -> ADM found no failure
REASON -> ADM executed successful
RESULT -> ADM configure result in success
```

### Control All Subscriber Terminations

The following example controls all subscriber-terminations on a particular gateway to the target state:

```
CLI> control subscriber-termination id=@ubr235; mode=forced; target-state=MAINT
```

```
Reply : Success: CLI change successful
```

```
ID -> ubr235
REASON -> ADM executed successful
RESULT -> ADM configure result in success
REQUEST STATE -> ADMIN_MAINT
RESULT STATE -> ADMIN_MAINT
FAIL REASON -> ADM found no failure
CLI>diag subscriber-termination
Reply : Success: Diagnostic Subscriber Menu.
```

## Equip Command

The equip command changes the administrative state of terminations that are in the UEQP state to OOS state. It ignores the terminations in the states INS, MAINT, or OOS.

**Step 1** Use the following example to equip a subscriber termination:

```
CLI> equip subscriber-termination id=97_8@ipclab.cisco.com;
```

```
Reply : Success: CLI change successful
```

```
ID -> Subscriber ID -> 97_8@ipclab.cisco.com
REASON -> ADM executed successful
RESULT -> ADM configure result in success
FAIL REASON -> ADM found no failure
```

## Unequip Command

The unequip command changes the administrative state of subscriber terminations that are in OOS state into UEQP state. It ignores the terminations in the INS, MAINT, or UEQP states.

**Step 1** Use the following command to unequip a subscriber termination:

```
CLI> unequip subscriber-termination id=97_8@ipclab.cisco.com;
```

```
Reply : Success: CLI change successful
```

```
ID -> Subscriber ID -> 97_8@ipclab.cisco.com
REASON -> ADM executed successful
RESULT -> ADM configure result in success
FAIL REASON -> ADM found no failure
FAIL REASON -> ADM found no failure
```

## Trunk Group

This section describes the status and control commands for trunk groups (TGs). Individual TGs can be placed into any of three administrative service states: INS, OOS, and MAINT. The relationship between TGW and TG state is provided in [Table 3-3](#).

**Table 3-3 TGW/TG State Relationships**

TGW State	Allowed TG States
INS	<ul style="list-style-type: none"> <li>• OOS</li> <li>• MAINT</li> <li>• INS</li> </ul>
MAINT	<ul style="list-style-type: none"> <li>• OOS</li> <li>• MAINT</li> </ul>

## Status Command

The following example shows the status of a single TG ID:

```
CLI> status trunk-grp id=2;

RESULT -> ADM configure result in success
REASON -> ADM executed successful
ADMIN STATE -> ADMIN_INS
OPER STATE -> Trunk group in-service
TGN ID -> 2
```

Table 3-4 lists the administrative states the system can return.

**Table 3-4 Example Returnable Administrative States**

State	Definition
ADMIN-INS	In Service.
ADMIN-OOS	Out of Service.
ADMIN-MAINT	Maintenance Mode.
ADMIN-OOS-Pending	Transitioning to Out of Service.
ADMIN-MAINT-Pending	Transitioning to Maintenance Mode.
ACL	Congestion is at level 1
ACL	Congestion is at level 2
ACL	Congestion is at level 3
TFC	Congestion is at level 1
TFC	Congestion is at level 2
TFC	Congestion is at level 3

The system can return the following operating states:

- Trunk group in-service
- Trunk group out-of-service
- Trunk group manually busy
- Trunk group operate in wait state
- Trunk group operate in standby state
- Trunk group restore session request normal
- Trunk group restore session request switch-over
- Trunk group restore session request maintenance
- Trunk group restore session fail normal
- Trunk group restore session fail switch-over
- Trunk group restore session fail maintenance
- Trunk group restore establish request normal
- Trunk group restore establish request switch-over

- Trunk group restore establish request maintenance
- Trunk group restore establish fail normal
- Trunk group restore establish fail switch-over
- Trunk group restore establish fail maintenance
- Trunk group in maintenance state
- Trunk group down session set fail soft normal
- Trunk group down session set fail hard normal
- Trunk group down session set fail soft maintenance
- Trunk group down session set fail hard maintenance
- Trunk group down establish request soft normal
- Trunk group down establish request hard normal
- Trunk group down establish request soft maintenance
- Trunk group down establish request hard maintenance
- Trunk group down establish fail soft normal
- Trunk group down establish fail hard normal
- Trunk group down establish fail soft maintenance
- Trunk group down establish fail hard maintenance
- Trunk group delete graceful
- Trunk group request remove release
- Trunk group request remove session set
- Trunk group remove graceful in-service and maintenance state
- DPC is inaccessible

## Control Command

The following example controls a single trunk group ID into service:

```
CLI> control trunk-grp id=2; mode=forced; target-state=INS;
```

```
Reply : Success: CLI change successful
```

```
INITIAL STATE -> ADMIN_OOS
REQUEST STATE -> ADMIN_INS
RESULT STATE -> ADMIN_INS
FAIL REASON -> ADM found no failure
REASON -> ADM executed successful
RESULT -> ADM configure result in success
TGN ID -> 2
```



### Note

When performing the following commands in succession, wait at least one second between commands:

```
control trunk-grp tgn-id=129; mode=forced; target-state=oos;
control trunk-grp tgn-id=129; mode=forced; target-state=ins;
```

## Trunk Termination

This section describes the status and control commands for trunk terminations. Either a range (for example, cic=1-24;) or a single value (for example, cic=1;) for the CIC parameter can be specified for the status and control of trunk terminations.

Individual trunks and trunking groups can be placed into any of three administrative service states: INS, OOS, and MAINT. The relationship between trunk/trunk group state and the TGW state is provided in [Table 3-5](#). For all other trunk types, the trunk state and trunk group state are independent.

**Table 3-5 TGW/TG State Relationships**

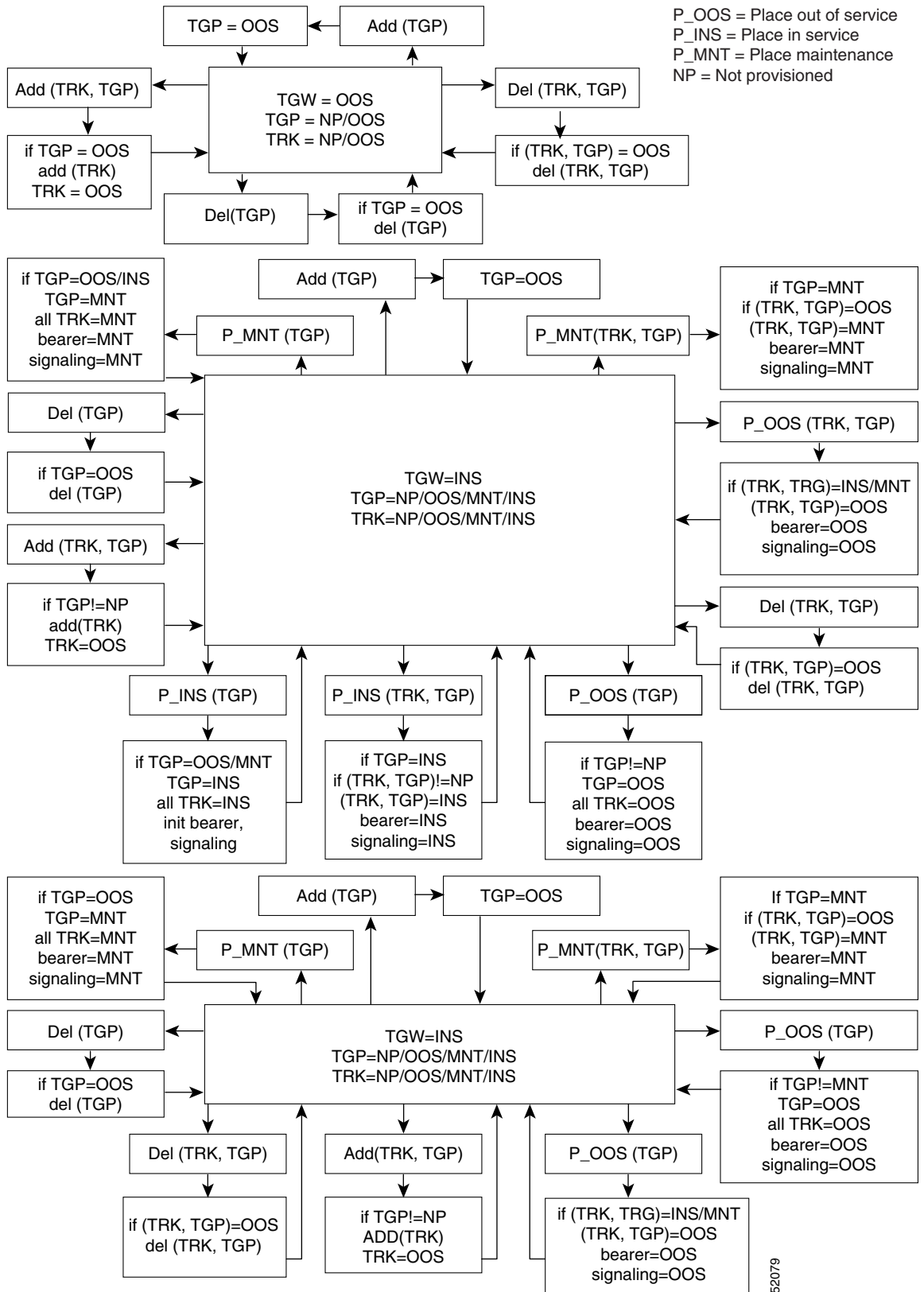
TGW State	Allowed TG States	Allowed Trunk States
INS	OOS	UEQP OOS
	MAINT	UEQP OOS, MAINT
	INS	UEQP OOS, MAINT, INS
MAINT	OOS	UEQP OOS
	MAINT	UEQP OOS, MAINT

where:

- TGW—trunking gateway
- TG—trunk group
- OOS—out of service
- MAINT—maintenance
- INS—in service
- UEQP—unequipped

The rules for placing trunks and TG into the OOS, INS, and MAINT states (which depend upon the TGW state) are shown in [Figure 3-3](#).

Figure 3-3 Administrative and Operational Maintenance States for a Trunking Gateway



52079

## Status Command

This section describes how to check trunk termination status. This section is organized as follows:

- [Trunk Termination Status—Basic Command](#)
- [Trunk Termination Status—Optional Tokens](#)
- [Trunk Termination Status—”status tt” Command](#)

### Trunk Termination Status—Basic Command



#### Note

This command can be executed for one CIC (for example, `cic=1;`), a range of CICs (for example, `cic=1-12;`) or for all CICs (`cic=all;`).

Use the following example to check the status of one trunk termination:

```
CLI> status trunk-termination tgn-id=2; cic=8;
```

```
Reply : Success:
```

```
RESULT -> ADM configure result in success
REASON -> ADM executed successful
TGN ID -> 2
CIC -> 8
TERM ADMIN STATE -> ADMIN_INS
TERM OPER STATE -> Termination is idle
TERM REASON -> No fault reason available
TRUNK STATIC STATE -> ACTV
TRUNK DYNAMIC STATE -> TRNS
TRUNK REASON -> NON_FAULTY
```

[Table 3-6](#) lists the administrative states the system can return for the *term admin status* response.

**Table 3-6 Example Returnable Administrative States**

State	Definition
ADMIN-UNEQP	Unequipped
ADMIN-INS	In Service
ADMIN-OOS	Out of Service
ADMIN-MAINT	Maintenance Mode
ADMIN-OOS-PENDING	Transitioning to Out of Service
ADMIN-MAINT-PENDING	Transitioning to Maintenance Mode
ADMIN-NULL	Resource does not exist

## Trunk Termination Status—Optional Tokens

The following optional tokens can be used with the status trunk-termination command. They expand the range of useful information returned. Either all, or none of the tokens can be used, with the exception of the off-normal token, which must be used by itself (without any other tokens).

- Administrative State (admin-state). Valid values are:
  - UEQP—Unequipped; resource is not commissioned. Resource is not registered.
  - OOS—Termination was manually controlled out of service.
  - INS—Termination was manually controlled in service, but operationally may be available or unavailable.
  - OOS-PENDING—Termination was manually controlled out of service with the graceful mode, termination is still involved in a call.
  - MAINT—Termination was in maintenance mode, can run diagnostic commands.
  - MAINT-PENDING—Termination was manually controlled to the MAINT state, but termination is still involved in call.
  - ALL—Return all possible states.

The following command example returns only those trunk terminations that are in administrative state OOS (if any), and operating state IDLE (if any):

```
CLI> status trunk-termination tgn-id=12; cic=1-1000; admin-state=OOS;
oper-state=idle
```

- Operating State (oper-state). Valid values for the oper-state token are:
  - FA—Includes FAULTY, UNREACH, TEMP-DOWN, and DOWN.
  - FAULTY—The MGCP endpoint returned a permanent error code.
  - UNREACH—The MGCP endpoint was declared as not reachable. This indicates gateway connectivity problems.
  - TEMP-DOWN—The MGCP endpoint is temporarily down.
  - DOWN—MGCP endpoint is down because GW termination has sent an RSIP-down message.
  - NF—Includes INT-MAINT, IDLE, BUSY, and ACTIVE.
  - INT-MAINT—Internal error recovery is in progress.
  - IDLE—Termination is not involved in a call, but is available.
  - BUSY—Termination is involved in transient call.
  - ACTIVE—Termination is involved in stable call.
  - UEQP—Termination is not equipped.
  - ALL—Returns all possible operational states.

The following command example returns only those trunk terminations that are FA (if any):

```
CLI> status trunk-termination tgn-id=12; cic=ALL; oper-state=FA;
```



- Static State (static-state). Valid values for the static-state token are:
  - UEQP—Unequipped resource is not commissioned. Resource is not registered.
  - LBLK—Termination is locally blocked: either manually taken OOS/MAINT (block reason can be MANUAL-OOS, MAINT-OOS), or automatically went out of service.
  - RBLK—Termination is remotely blocked (blocked by remote side).
  - ACTV—Available.
  - All—Returns all possible static states.

The following command example returns only those terminations that are locally blocked (if any):

```
CLI> status trunk-termination tgn-id=101; cic=1-24; static-state=lblk;
```

- Dynamic State (dynamic-state). Valid values for the dynamic-state token are:
  - IBSY—Trunk-termination is involved in an incoming active call.
  - OBSY—Trunk-termination is involved in an outgoing active call.
  - TRNS—Transient maintenance state (sent maintenance signaling message and waiting for response).
  - IDLE—Termination is not involved in a call.
  - IBSY-TRNS—Termination is involved in an incoming transient call.
  - OBSY-TRNS—Termination is involved in an outgoing transient call.
  - ALL—All possible dynamic states.

The following command example returns only those terminations that are idle (if any):

```
CLI> status trunk-termination tgn-id=101; cic=1-24; dynamic-state=idle;
```

- Off-normal State (off-normal)
  - Yes—Return all terminations in off-normal state.
  - No—Return all terminations in normal state.

The following command example returns only those terminations in an off-normal state (if any).

```
CLI> status trunk-termination tgn-id=101; cic=1-24; off-normal=yes;
```

A termination is in an off-normal state when it is *not* in one of the state combinations shown in [Table 3-7](#).

- Source (source)—Specifies whether to query the Call Agent or the Element Management System (EMS) for status information. It is an optional token.
  - EMS (Default)—Query the local EMS database for most current status.
  - AGENT—Query the remote Call Agent database for most current status.

The following command example returns the current status of the Call Agent:

```
CLI> status trunk-termination tgn-id=101; cic=1-24; source=AGENT;
```

Table 3-7 Valid Normal Trunk Termination States

State/Token	ADMIN-STATE	OPER-STATE	STATIC-STATE	DYNAMIC-STATE
UNEQP	UNEQP	ANY	UEQP	IDLE
MANUALLY OOS	OOS	ANY	LBLK	IDLE
MANUALLY MAIN	MAINT	IDLE	LBLK	IDLE
IDLE	INS	IDLE	ACTV	IDLE
ACTIVE INCOMING	INS	IDLE	ACTV	IDLE
ACTIVE OUTGOING	INS	ACTIVE	ACTV	OBSY
TRANSIENT INCOMING	INS	ACTIVE	ACTV	IBY-TRNS
TRANSIENT OUTGOING	INS	BUSY	ACTV	OBSY-TRNS

### Trunk Termination Status—"status tt" Command

The following command example (**status tt**) returns current status in a tabular format.

```
CLI> status tt tgn-id=994; cic=all

994 1  ADMIN_INS  TERM_ACTIVE_IDLE  ACTV  IDLE  NON_FAULTY
994 2  ADMIN_INS  TERM_ACTIVE_IDLE  ACTV  IDLE  NON_FAULTY
994 3  ADMIN_INS  TERM_ACTIVE_IDLE  ACTV  IDLE  NON_FAULTY
994 4  ADMIN_INS  TERM_ACTIVE_IDLE  ACTV  IDLE  NON_FAULTY
994 5  ADMIN_INS  TERM_ACTIVE_IDLE  ACTV  IDLE  NON_FAULTY
994 6  ADMIN_INS  TERM_ACTIVE_IDLE  ACTV  IDLE  NON_FAULTY
994 7  ADMIN_INS  TERM_ACTIVE_IDLE  ACTV  IDLE  NON_FAULTY
994 8  ADMIN_INS  TERM_ACTIVE_IDLE  ACTV  IDLE  NON_FAULTY
994 9  ADMIN_INS  TERM_ACTIVE_IDLE  ACTV  IDLE  NON_FAULTY
994 10 ADMIN_INS  TERM_ACTIVE_IDLE  ACTV  IDLE  NON_FAULTY
994 11 ADMIN_INS  TERM_ACTIVE_IDLE  ACTV  IDLE  NON_FAULTY
994 12 ADMIN_INS  TERM_ACTIVE_IDLE  ACTV  IDLE  NON_FAULTY
994 13 ADMIN_INS  TERM_ACTIVE_IDLE  ACTV  IDLE  NON_FAULTY
994 14 ADMIN_INS  TERM_ACTIVE_IDLE  ACTV  IDLE  NON_FAULTY
994 15 ADMIN_INS  TERM_ACTIVE_IDLE  ACTV  IDLE  NON_FAULTY
994 16 ADMIN_INS  TERM_ACTIVE_IDLE  ACTV  IDLE  NON_FAULTY
994 17 ADMIN_INS  TERM_ACTIVE_IDLE  ACTV  IDLE  NON_FAULTY
994 18 ADMIN_INS  TERM_ACTIVE_IDLE  ACTV  IDLE  NON_FAULTY
994 19 ADMIN_INS  TERM_ACTIVE_IDLE  ACTV  IDLE  NON_FAULTY
994 20 ADMIN_INS  TERM_ACTIVE_IDLE  ACTV  IDLE  NON_FAULTY
994 21 ADMIN_INS  TERM_ACTIVE_IDLE  ACTV  IDLE  NON_FAULTY
994 22 ADMIN_INS  TERM_ACTIVE_IDLE  ACTV  IDLE  NON_FAULTY
994 23 ADMIN_INS  TERM_ACTIVE_IDLE  ACTV  IDLE  NON_FAULTY
994 24 ADMIN_INS  TERM_ACTIVE_IDLE  ACTV  IDLE  NON_FAULTY
```

Reply : Success:

## Control Command

This section describes how to control trunk terminations. The section is organized as follows:

- [Control One Trunk Termination](#)
- [Control All Trunk Terminations](#)

### Control One Trunk Termination

Use the following example to control one trunk termination into OOS:

```
CLI> control trunk-termination tgn-id=22; cic=1; target-state=OOS; mode=forced;
```

```
Reply : Success: CLI change successful
```

```
TGN ID -> 22  
REASON -> ADM executed successful  
RESULT -> ADM configure result in success  
CIC START -> 1  
CIC END -> 1  
FAIL REASON -> ADM found no failure  
REQUEST STATE -> ADMIN_OOS  
RESULT STATE -> ADMIN_OOS
```

### Control All Trunk Terminations

Use the following example to control all trunk terminations for a particular CIC group to OOS:

```
CLI> control trunk-termination tgn-id=17; cic=1-23; target-state=oos;  
mode=forced;
```

```
Reply: Request was successful.  
TGN ID -> 17  
REASON -> ADM executed successful  
RESULT -> ADM configure result in success  
CIC START -> 1  
CIC END -> 24  
FAIL REASON -> ADM found no failure  
REQUEST STATE -> ADMIN_OOS  
RESULT STATE -> ADMIN_OOS
```

## Reset Command

The reset command clears all manual and blocked states as well as any active/transient calls on a trunk termination, with the exception of SS7 trunk terminations. It brings a trunk into INS mode.

This section is organized as follows:

- [Reset a Single CIC](#)
- [Reset a Range of CICs](#)
- [Reset All CICs](#)

### Reset a Single CIC

The following example resets a single CIC on a specific trunk:

```
CLI> reset trunk-termination tgn-id=22; cic=1
```

```
Reply : Success:
```

```
TGN ID -> 22
REASON -> ADM executed successful
RESULT -> ADM configure result in success
CIC START -> 1
CIC END -> 1
FAIL REASON -> ADM found no failure
```

### Reset a Range of CICs

The following example resets a range of CICs on a specific trunk:

```
CLI> reset trunk-termination tgn-id=13; cic=1-6;
```

```
TGN ID -> 13
REASON -> ADM executed successful
RESULT -> ADM configure result in success
CIC START -> 1
CIC END -> 6
FAIL REASON -> ADM found no failure
```

### Reset All CICs

The following example resets all CICs on a specific trunk:

```
CLI> reset trunk-termination tgn-id=13; cic=all;
```

```
TGN ID -> 13
REASON -> ADM executed successful
RESULT -> ADM configure result in success
CIC START -> 1
CIC END -> 24
FAIL REASON -> ADM found no failure
```

## Equip Command

The equip command changes the administrative state of terminations that are in the UEQP state to the OOS state. It ignores the terminations in the INS, MAINT, or OOS states.

Use the equip command or the control trunk-grp command to change the termination state for a subscriber to a trunk. The control trunk-grp command changes all trunks in the specified trunk group to the specified state. Use the equip command to set the subscriber termination state. Thereafter, to change the termination state, use the control command.

A subscriber termination state must be set to unequipped before it can be deleted.

You cannot use the control command to change a termination state to UEQP. Furthermore, you cannot use the control command to change the state of any subscriber termination that is already in the UEQP state.

For example, consider a case in which 24 CICs in a trunk group are in the following initial states:

- CICs 1–10 in OOS state
- 11–15 in UEQP state
- 16–24 in MAINT state

For this case, issuing the control, equip, or unequip commands would affect the initial state of the CICs as follows:

- If a control command is used with target-state = ins, the final states of all the CICs are:
  - CICs 1–10 in INS state
  - CICs 11–15 in UEQP state
  - CICs 16–24 in INS state
- If an equip command is applied to the CICs in the initial states, the final states of all the CICs are:
  - CICs 1–10 in OOS state
  - CICs 11–15 in OOS state
  - CICs 16–24 in MAINT state
- If an unequip command is applied to the CICs in the initial states, the final states of the CICs are:
  - CICs 1–10 in UEQP state
  - CICs 11–15 in UEQP state
  - CICs 16–24 in MAINT state

Use the following example to equip a trunk termination:

```
CLI> equip trunk-termination tgn-id=13; cic=all;
```

```
Reply : Success: CLI change successful
```

```
TGN ID -> 13
REASON -> ADM executed successful
RESULT -> ADM configure result in success
CIC START -> 1
CIC END -> 24
FAIL REASON -> ADM found no failure
```

## Unequip Command

The `unequip` command changes the administrative state of terminations that are in the OOS state into the UEQP state. It ignores the terminations in the INS, MAINT, or UEQP states.

Use the following example to unequip terminations:

```
CLI> unequip trunk-termination tgn-id=13; cic=all;
```

```
Reply : Success: CLI change successful
```

```
TGN ID -> 13  
REASON -> ADM executed successful  
RESULT -> ADM configure result in success  
CIC START -> 1  
CIC END -> 24
```



## Troubleshooting with Call Flows

---

This chapter suggests ways to use call flows to help diagnose network problems. It includes the following sections:

- [Understanding MGCP, page 4-2](#)
- [Understanding SS7, page 4-10](#)
- [Call Flow Analysis, page 4-13](#)
- [Voice Quality Problems, page 4-22](#)

Making a phone call on a VoIP over cable network is a complex process that involves many software and hardware components. The network elements directly involved in call setup include MTAs, CMTSSs, trunk gateways, the Call Agent, and announcement servers, which are all described in [Chapter 1, “Solution Overview”](#). These network elements communicate call setup information to each other using Signaling System 7 (SS7) and the Media Gateway Control Protocol (MGCP). The sequence of messages that must be exchanged to setup and teardown the call is referred to as a call flow.

Call flow analysis can be used to identify which element in the network is not behaving to specification, a procedure known as trouble isolation. It allows you to initially treat each network element as a “black box,” with a known set of inputs and a known set of expected outputs or behavior. Identifying the non-conforming network element can point you in the right direction to further investigate a problem, although it does not always yield the root cause of the problem. Finding the root cause of a problem within a network element usually requires further investigation with element-specific debug tools, logs, or trouble reports.

This chapter includes an overview of the MGCP and SS7 protocols and the key parts that are useful for call flow analysis. The following sections review strategies for collecting MGCP protocol data, and for identifying which MGCP messages are related to a single call attempt. It also includes an overview of SS7 messages for off-net call setup and teardown and guidelines for troubleshooting certain specific call flow-related problems.

# Understanding MGCP

Media Gateway Control Protocol (MGCP) is the protocol used between the Call Agent and the endpoints within the network to establish, manage, and delete connections. Endpoints are defined by the call topology:

- On-net to on-net—both calling and called parties are on the same provider's network. In this case the endpoints are MTAs.
- On-net to off-net (or off-net to on-net) via gateway—one party is on the service provider's network and one is on the PSTN. In this case the endpoints are the MTA and the trunking gateway.

MGCP messages are transmitted over UDP. Requests are sent to one of the IP addresses defined in the DNS for the specified endpoint. Responses are sent back to the source address of the requests. In the absence of a timely response, requests are repeated.

It is the responsibility of the requesting entity to provide suitable time-outs for all outstanding requests, and to retry requests when time-outs have been exceeded. Furthermore, when repeated requests are not acknowledged, it is the responsibility of the requesting entity to seek redundant services or clear existing or pending connections.

When tracing call flows in the course of troubleshooting a problem, these repeated messages are often indications of where the problem is occurring.

## MGCP Transactions

MGCP is implemented as a series of transactions, composed of a request and a mandatory response. All requests and responses are composed of a request header, optionally followed by a session description.

Headers and session descriptions are each encoded as a set of text lines, separated by line feed characters. Headers are separated from session descriptions by an empty line.

The request header is composed of:

- A request line, identifying the command (or verb), the endpoint from which the action is requested, and the MGCP version
- A set of parameter lines, composed of a parameter name followed by a parameter value

The request line is composed of:

- The encoded name of the requested command
- The transaction ID (encoded as a string of up to 9 decimal digits)
- The name of the endpoint that should execute the request (in notifications, the name of the endpoint that is issuing the notification).

Endpoint names are encoded as e-mail addresses, in which the domain name identifies the system where the endpoint is located, while the left side identifies a specific endpoint on that system. For example, *123456@gw23.whatever.net* indicates circuit number 123456 in the Gateway 23 of the Whatever network.

The name of the notified entity is expressed the same way, possibly followed by a port number; for example, *Call-agent@ca.whatever.net:5234*.

- The protocol version



## MGCP Commands

Table 4-1 describes the five commands (also called *verbs*) used by MGCP to make and terminate connections between endpoints. All commands except Notify are sent by the Call Agent to the gateway. Notify is sent from the gateway (which may also send a DeleteConnection).

**Table 4-1 MGCP Commands**

Verb	Code	Used By	Action
Notify	NTFY	Gateway	Notifies the call agent of events.
Notification Request	RQNT	Call Agent	Requests gateway to send notifications on occurrence of specified events in an endpoint, such as off-hook; or to signal the caller, for example, play dial tone.
Create Connection	CRCX	Call Agent	Sets up a new connection at the gateway.
Modify Connection	MDCX	Call Agent	Modifies a gateway's view of a connection, that is, changes established connection parameters.
Delete Connection	DLCX	Call Agent	Terminates a connection.

## MGCP Parameters

Parameter lines are composed of a parameter name (in most cases a single uppercase character), followed by a colon, a space, and the parameter value. Table 4-2 lists parameters that can be present in requests (M=mandatory, O=optional, F=forbidden).

**Table 4-2 MGCP Parameters**

Parameter Name	Code	Association of Parameters with Requests:				
		CRCX	MDCX	DLCX	RQNT	NTFY
Call Identifier	<b>C</b>	M	M	O	F	F
Connection Identifier	<b>I</b>	F	M	O	F	F
Request Identifier	<b>X</b>	O	O	O	M	M
Notified Entity	<b>N</b>	O	O	O	O	O
Local Connection Options	<b>L</b>	O	M	F	F	F
Connection Mode	<b>M</b>	M	M	F	F	F
Requested Events	<b>R</b>	O	O	O	O	F
Signal Requests	<b>S</b>	O	O	O	O	F
Digit Map	<b>D</b>	O	O	O	O	F
Observed Events	<b>O</b>	F	F	F	F	M
Connection Parameters	<b>P</b>	F	F	O	F	F
Reason Code	<b>E</b>	F	F	O	F	F

The parameters are described in more detail in the following sections.

**Call Identifier (C)**

The call ID identifies the call (or session) to which this connection belongs. This parameter is unique within the network of gateways; however, connections that belong to the same call share the same call ID. The call ID can be used to identify calls for reporting and billing purposes.

**Connection Identifier (I)**

The connection ID identifies the connection within the call.

**Request Identifier (X)**

The request ID is used to correlate the request with the notifications that it triggers.

**Notified Entity (N)**

The notified entity is an optional parameter that specifies where the notification should be sent. An example of notification is a disconnect request from the gateway.

**Local Connection Options (L)**

The local connection options describe the operational parameters that the call agent suggests to the gateway. These parameters are:

- The length in time in milliseconds, encoded as the keyword **p**, followed by a colon and a decimal number. If the call agent specifies a range of values, the range is specified as two decimal numbers separated by a hyphen.
- The preferred type of compression algorithm, encoded as the keyword **a**, followed by a character string. If the call agent specifies a list of values, these values are separated by a semicolon.

This is the parameter that specifies the codec. Should the Call Agent request the wrong codec, or should the endpoint be configured incorrectly and respond that it cannot support the correct requested codec, voice quality will be affected (or the call may not succeed, triggering a NAK).

G.711 is specified in the case of fax, mode, and when connecting to the voice-mail system. G.711 samples the analog signal 8000 times/sec, producing an 8-bit pulse code modulation. Thus, G.711 requires 64 kbps of continuous transmission. G.711 provides extremely high-quality speech transmission (often referred to as toll quality), but can tolerate little delay or variation.

- The bandwidth in kilobits per second, encoded as the keyword **b**, followed by a colon and a decimal number. If the call agent specifies a range of values, the range is specified as two decimal numbers separated by an hyphen.
- The echo cancellation parameter, encoded as the keyword **e**, followed by a colon and the value **on** or **off**. By default, telephony gateways always perform echo cancellation. However, for some calls it is necessary to turn it off.

Each of the parameters is optional. When several parameters are present, the values are separated by a comma.

Examples:

L: p:10, a:G.711

L: p:10, a:G.711;G.726-32

L: p:10-20, b: 64

L: b:32-64, e:off

## Connection Mode (M)

Each connection is qualified by a connection mode parameter, which can be set to **send**, **receive**, **send/receive**, **inactive**, **loopback**, or **continuity test**.

The handling of the audio signals received on these connections is determined by the parameters:

- Audio signals incoming from connections in **receive** or **send/receive** mode are mixed and sent to the endpoint.
- Audio signals originating from the endpoint are transmitted over all connections whose mode is **send** or **send/receive**.
- If the mode is set to **loopback**, the gateway is expected to return the incoming signal from the endpoint back to that same endpoint.
- If the mode is set to **continuity test**, the gateway is informed that the other end of the circuit has initiated a continuity test procedure. It is expected to follow the procedure specified for that endpoint, which may require either that the circuit be placed in loopback mode, or to wait for a specific tone and return an appropriate signal.



### Note

There are two types of continuity tests: loopback and two-tone. It is important that the gateway be configured to reply correctly with the requested test signal; otherwise the test fails, the time slot being tested is taken out of service, and the test is repeated on the next available channel, which again fails, and is taken out of service, and so on until the testing threshold is reached. By that time, several time slots are temporarily not available, which can affect service.

Table 4-3 lists possible Connection Mode values

**Table 4-3 Connection Modes**

Connection Mode	Meaning
M: sendonly	The gateway should only send packets.
M: recvonly	The gateway should only receive packets.
M: sendrecv	The gateway should only send and receive packets.
M: inactive	The gateway should neither send nor receive packets.
M: loopback	The gateway should place the circuit in loopback mode.
M: contest	The gateway should place the circuit in test mode.

## Requested Events (R)

The requested events parameter is a list of events that the gateway is requested to detect and report. Each event is identified by a code, as shown in Table 4-4.

These ASCII encodings are not case-sensitive. Values such as “hu”, “Hu”, “HU”, or “hU” are considered equivalent.

**Table 4-4 Requested Events**

Event	Code
Fax tones	ft
Modem tones	mt

**Table 4-4 Requested Events (continued)**

Event	Code
Continuity tone	co
Continuity detected (as a result of a continuity test)	cv
On-hook transition	hu
Off-hook transition	hd
Flash hook	hf
Digit collection	Individual digits (e.g. “#”), timers (“T”), or ranges (e.g. “[0-9]” or “[0-9*#T]”)

Each event can be qualified by a requested action or by a list of actions. The actions, when specified, are encoded as a list of keywords, enclosed in parentheses and separated by commas. The codes for these events are:

- **N** (Notify immediately, with the accumulated list of observed events)
- **A** (Accumulate)
- **D** (treat according to Digit map)
- **S** (Swap audio)
- **I** (Ignore)

When no action is specified, the default action is to notify the event. This means that, for example, ft and ft(N) are equivalent. Events not listed are ignored.

The swap audio action can be used when a gateway handles more than one active connection on an endpoint. This is the case for three-way calling, call waiting, and possibly other features. In order to avoid the round-trip to the call agent when only changing the connection attached to the audio functions of the endpoint, the notification request can map an event (usually hook-flash) to a local function swap audio, which selects the next connection in a round robin fashion. If there is only one connection, this action is effectively no operation.

The digit-map action can be specified only for the digits, letters and timers.

The requested list is encoded on a single line, with event or action groups separated by commas.

Examples:

R: hu(N), hf(S,N)

R: hu(N), [0-9#T](D)

## Signal Requests (S)

The Signal Requests parameter contains the set of actions that the gateway is asked to perform on the endpoint. Each signal is identified by a code, as shown in [Table 4-5](#).

**Table 4-5 Signal Requests**

Signal	Code
Ringing	rg
Distinctive ringing (8 variants numbered 0-7)	r0, r1, r2, r3, r4, r5, r6, or r7
Ring back tone	rt

**Table 4-5 Signal Requests (continued)**

Signal	Code
Dial tone	dl
Intercept tone	it
Network congestion tone	cg
Busy tone	bz
Confirm tone	cf
Answer tone	aw
Call waiting tone	wt
Off hook warning tone	ot
Preemption tone	pt
Continuity tone (default)	co
Continuity tone (single tone)	co1
Continuity test (go tone, in dual tone procedures)	co2
Continuity verified (response tone, in dual tone procedures)	cv
DTMF tones	A string composed of the individual digits that should be played on the endpoint.
ASDI display	The keyword <b>ad</b> , followed by the string to be displayed, in parentheses.  Example: Ad(123456 Your friend)

The action triggered by the signal requests is synchronized with the collection of events specified in the request events parameter. For example, if the notification request mandates “ringing” and the event request asks to look for an “off-hook” event, the ringing should stop as soon as the phone goes off-hook. In order to stop tone generation, the call agent can send a notification request whose signal list is empty.

### Digit Map (D)

Digit map is an optional parameter that allows the call agent to provision the gateways with a digit map that specifies how digits are accumulated. This parameter must be present if the requested events contain a request to “accumulate according to digit map.”

The collection of digits results in a digit string. The digit string is initialized to a null string upon receipt of a request, so that a subsequent request returns only digits that were collected between the two requests.

### Observed Events (O)

Observed events is a list of event detected by the gateway. The event codes are the same as those used in the notification request.

A single notification may report a list of events, which are reported in the order in which they were detected. The list may contain only the events that were requested in the requested events parameter of the triggering request.

The list contains the following:

- Events that were accumulated (but not notified)
- Events that were treated according to the digit map (but not matched yet)
- The final event that triggered the detection or provided a final match in the digit map

Events that have been accumulated according to the digit map are grouped in a single string. Examples of observed actions are:

- hu
- 8295555T
- hf, hf, hu

## Connection Parameters (P)

When the call agent terminates a connection, it collects statistics (connection parameters) on the execution of the connection. In the general case where a connection has two ends, the delete connection command is sent to both gateways involved in the connection, and therefore the statistics are collected from both.

Connection parameters are encoded as a string of *type* and *value* pairs, where the type is a two-letter identifier and the value is a decimal integer. Types are separated from values by an equals sign. Parameters are separated from each other by a comma.

Table 4-6 lists Connection Parameter types.

**Table 4-6** Types of Connection Parameters

Connection Parameter Name	Code	Value
Packets Sent	PS	Total number of RTP data packets transmitted by the sender since starting transmission on this connection. <sup>1</sup>
Octets Sent	OS	Total number of payload octets (not including header or padding) transmitted in RTP data packets by the sender since starting transmission on the connection. <sup>1</sup>
Packets Received	PR	Total number of packets received by the sender since starting reception on the connection. <sup>2</sup>
Octets Received	RO	Total number of payload octets (not including header or padding) received in RTP data packets by the sender since starting transmission on the connection. <sup>2</sup>
Packets Lost	PL	Total number of packets that were not received on the connection, as derived from gaps in the sequence number. The value is zero if the connection was set in “send only” mode.

**Table 4-6** Types of Connection Parameters (continued)

Connection Parameter Name	Code	Value
Jitter	JI	Average inter-packet arrival jitter in milliseconds, expressed as an unsigned integer. Jitter is defined as the mean deviation (smoothed absolute value) of the difference in packet spacing at the receiver compared to the sender for a pair of packets. Detailed computation algorithms are found in RFC 1889. The value is zero if the connection was set in “send only” mode.
Latency	LA	Average network latency expressed in milliseconds. It is the average value of the difference between the sender’s NTP timestamp of the RTCP messages and the receiver’s NTP timestamp, measured when the messages are received.

1. The count is not reset if the sender changes its SSRC identifier, for example, as a result of a modify command. The value is zero if the connection was set in “receive only” mode.
2. The count is not reset if the sender changes its SSRC identifier, for example, as a result of a modify command. The value is zero if the connection was set in “send only” mode.

Example:

P: PS=1245, OS=62345, PR=0, OR=0, PL=0, JI=0, LA=48

### Reason Code (E)

In some circumstances, a gateway may have to clear a connection; for example, it may have lost the resource associated with the connection, or detected that the endpoint no longer is capable or willing to send or receive voice. The gateway terminates the connection using a form of the delete connection request that includes a reason code. The reason code indicates the cause of the disconnection.

### Return Codes and Error Codes

All MGCP requests are acknowledged. The acknowledgment includes a return code that indicates the status of the request. The return code has the follow three ranges of values:

- 200 to 299 indicates a successful completion
- 400 to 499 indicates a transient error
- 500 to 599 indicates a permanent error

Defined values include:

**200**— the requested transaction executed normally

**250**—the connection was deleted

**400**—the transaction could not be executed due to a transient error

**401**—the phone is already off the hook

**402**—the phone is already on the hook

**500**—the transaction could not be executed because the endpoint is unknown

**501**—the transaction could not be executed because the endpoint is not ready

**502**—the transaction could not be executed because the endpoint does not have sufficient resources

**510**—the transaction could not be executed because a protocol error was detected

# Understanding SS7

Connections to the PSTN are done through ISDN user part (ISUP) trunks with a trunk gateway providing the bearer connections, and an SS7 gateway providing the signaling connections into the SS7 network. SS7 provides call setup and teardown, network management, fault resolution, and traffic management services. The SS7 network is used solely for network control, and the only data sent over it is signaling messages.

The Call Agent maps the PSTN and trunk gateway bearer circuits to the SS7 connection. This allows the Call Agent to determine which bearer circuit to use for the outgoing part of a call when a call originates from the PSTN or trunk gateway. Each SS7 connection is identified using the following three codes:

- Originating Point Code (OPC)
- Destination Point Code (DPC)
- Circuit Identification Code (CIC)

The signaling controller uses the SS7 circuit identification information to uniquely identify each bearer circuit, which is identified by:

- Span ID (the trunk ID)
- Timeslot within the trunk

When troubleshooting a call flow, you may need to access the Call Agent mapping table to identify a call.

## Processing a Telephone Call

It helps to understand what happens at an application level when you place a call using VoIP. The general flow of a two-party voice call using VoIP is as follows:

- 
- Step 1** The user picks up the handset. This signals an off-hook condition that is generated by the end-office Service Switching Point (SSP) in the PSTN.
  - Step 2** The SSP provides digit analysis and route determination, then generates dial tone and sends an IAM to the signaling application part of VoIP in the gateway.
  - Step 3** The VoIP issues an alerting/ACM that indicates to the SSP to start the dial tone or busy tone (based on the state of the receiving end).
  - Step 4** Upon dial tone, the user dials the telephone number. Those numbers are accumulated and stored by the session application.
  - Step 5** After enough digits are accumulated to match a configured destination pattern, the telephone number is mapped to an IP host through the dial plan mapper. The IP host has a direct connection to the destination telephone number.
  - Step 6** The session application uses the MGCP protocol to establish a transmission and a reception channel for each direction over the IP network. If the call is being handled by a PBX, the PBX forwards the call to the destination telephone.
  - Step 7** The codecs are enabled for both ends of the connection and the conversation proceeds using RTP/UDP/IP as the protocol stack.



- Step 8** Any call-progress indications (or other signals that can be carried in-band) are cut through the voice path as soon as an end-to-end audio channel is established. Signaling that can be detected by the voice ports (for example, in-band dual tone multifrequency [DTMF] digits after the call setup is complete) is also trapped by the session application at either end of the connection and carried over the IP network encapsulated in RTP Control Protocol (RTCP), using the RTCP APP extension mechanism.
- Step 9** When either end of the call hangs up, session ends. Each end becomes idle, waiting for the next off-hook condition to trigger another call setup.
- 

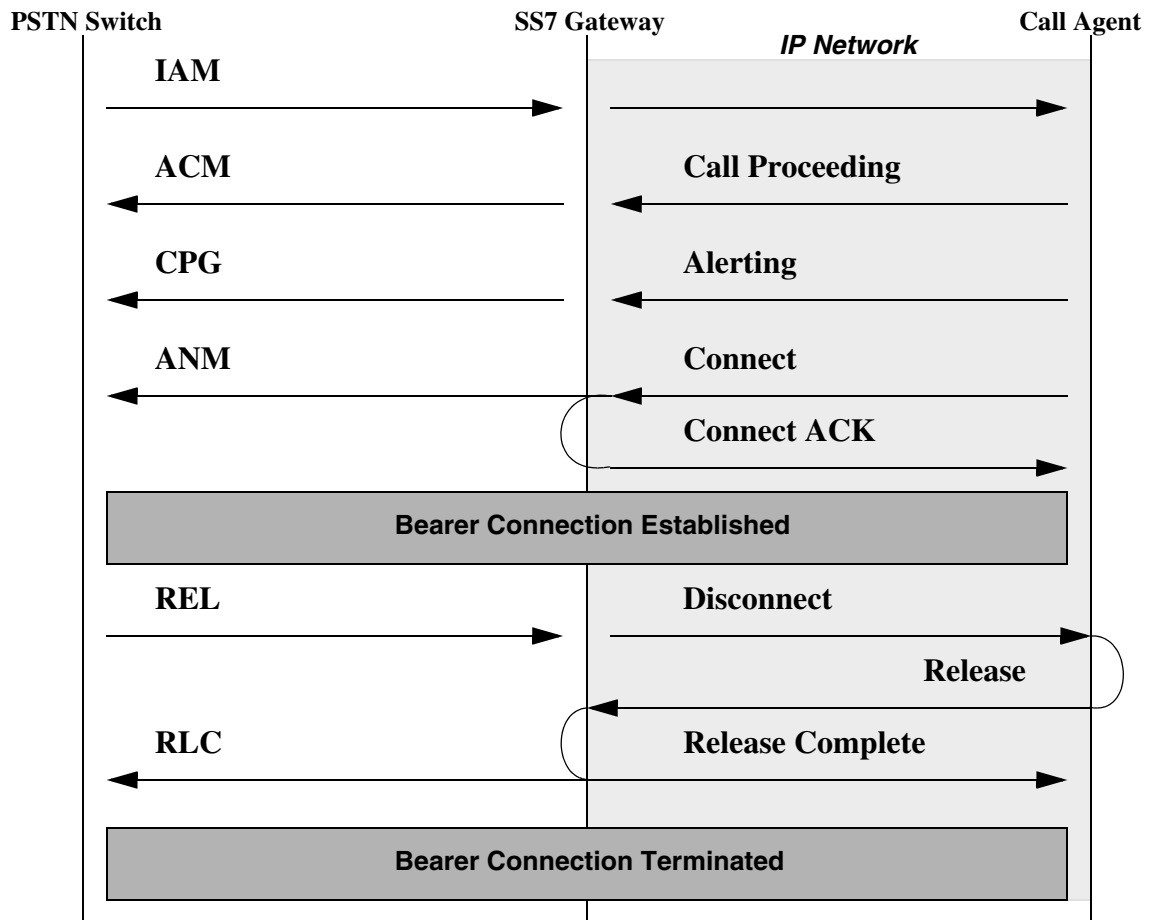
## ISUP Signaling Messages

ISUP defines the protocol used to set up, manage, and release trunk circuits that carry voice and data between terminating line exchanges (for example, between a calling party and a called party). ISUP is used for both ISDN and non-ISDN calls. However, calls that originate and terminate at the same switch do not use ISUP signaling. [Table 4-7](#) displays ISUP messages.

**Table 4-7 ISUP Messages**

Message	Description
IAM	Initial Address Message
ACM	Address Complete Message
SAM	Subsequent Address Message
ANM	Answer Message
REL	Release Message
RLC	Release Complete Message

Here is a sample call flow over the SS7 network:



# Call Flow Analysis

The following sections discuss how to use MGCP and SS7 messages in troubleshooting problems.

## MGCP Key Fields

The first problem in call flow analysis is to identify which messages are associated with a single call attempt. A modest amount of call activity on the network produces a relatively large volume of MGCP messages. You must be able to extract a small subset of messages for analysis, those related to the failed call. Several fields can be used to identify related MGCP messages. [Table 4-8](#) lists the key fields, which are described in more detail in the “[Understanding MGCP](#)” section on page 4-2

**Table 4-8 Key MGCP Fields Used to Identify Messages Related to a Single Call**

Parameter	Purpose	OSI Layer
endpoint ID	Identifies the endpoint involved in the call.	Application
transaction ID	Links an MGCP verb (NTFY, RQNT, CRCX, MDCX, DLCX) with the its associated ACK.  For example, CRCX xsactionID=001, with ACK xsactionID=001	Application
call ID	Identifies the group of connection management messages (CRCX, MDCX, DLCX) associated with a call instance.  Note: you can have multiple call instances associated with a single endpoint.	Application
IP address	Indicates the source/destination IP address of the gateway and/or call agent node	Network

Every MGCP command associated with call setup (RQNT, NTFY, CRCX, MDCX, DLCX) contains the endpoint ID of the gateway voice port and a transaction ID that uniquely identify the instance of a transmitted MGCP message, called an MGCP transaction. A node that receives an MGCP command must respond to the sender with an ACK (or NAK) message. The ACK message does not contain an endpoint ID, making it more difficult to correlate the ACK with its associated MGCP command. However, the ACK message does contain a transaction ID that can be correlated to the original command and the destination IP address, which is the original sender of the MGCP command. It is the combination of both the destination IP address and transaction ID in the ACK that associates it with an MGCP command. The transaction ID by itself is not required to be unique in the network; it is only required to be unique between the Call Agent and a specific gateway.

## MGCP Message Correlation

A major obstacle to tracing call flows in a production network is the sheer volume of MGCP messages that flow through the network at any time. In order to extract a call, you must find a way of linking all the messages in a call setup together. This section on correlation assumes the following:

- All the MGCP traffic has been captured and fully decoded, and is available to you.
- The call is made from an MTA to an off-net location (that is, SS7 messaging is involved).

- The MTA has been successfully provisioned and is ready for use.
- The call attempt is successful (that is, the call flow is complete without errors).
- You know the approximate time that the call was made.

The time of the call is used to find the likely location of the MGCP messages in the LAN analyzer trace. It is important that the analyzer time, which is used to timestamp messages, be synchronized with network time—the time that the trouble is reported. Without accurate time information, it may be more difficult to locate the messaging associated with the call instance in question, especially if the endpoint has made several calls during the day.

The following steps describe how to link call flow messages together:

---

**Step 1** To trace the call, begin by identifying the endpoint ID associated with the troubled phone number. For example, if a caller reports inability to get dial tone, use provisioning records to identify which endpoint ID has been assigned to this customer.

The single most important field in correlating MGCP messages is the endpoint ID. This parameter identifies the logical name of the endpoint being controlled by the Call Agent. Most trouble reports begin by identifying a phone number, such as:

- Which end has trouble; for example, “The customer cannot call from 404-524-1234.”
- Which end cannot be reached; for example, “Caller gets reorder tone when dialing 515-223-1256.”

The endpoint ID is critical because it is always constant. The IP address assigned to the customer’s phone may change, since IP addresses are dynamically assigned by DHCP, but the endpoint ID remains static.

**Step 2** Find the approximate time that the call attempt was made; then locate the NTFY message around that time period with the desired endpoint ID. The NTFY should indicate an off-hook (HU observed event) and should contain a transactionID. Write down the originating IP address from the NTFY. This tells you the IP address currently assigned to the MTA, which should not change during the call setup (although it could change between calls). The originating IP address is necessary to identify ACK messages that come from the MTA.

Identify the source and destination IP addresses of the nodes involved in the call setup (refer to the example in [Step 1](#)). This allows you to find the ACK (or NACK) messages for each MGCP command. The ACKs (or NACKs) are critical for determining if a node has trouble with a requested command.

Here is a sample notify message and a return acknowledge message to demonstrate how values are repeated to connect the two messages:

```
NTFY xsactionID=1 sourceIP=<X> destIP=<Y>
```

```
ACK xsactionID=1 sourceIP=<Y> destIP=<X>
```

**Step 3** The Call Agent responds to the NTFY with an ACK that echoes the transaction ID. Make note of the originating IP address in the ACK. This is the current IP address of the Call Agent, and (in most cases) remains the same over the duration of the call.

At this point, the following information is known: the MTA endpointID involved in the call, the IP address of the MTA, and the IP address of the call agent. The IP address of the egress gateway (in this example, the TGW) is not yet known.

**Step 4** Find the MGCP command messages (and ACKs) associated with call setup at the originating side by looking for MGCP messages that include the MTA endpoint ID, up to and including the CRCX to the MTA.

**Step 5** The first CRCX to the MTA contains the Call ID parameter. The Call ID parameter is used to link connection control messages (CRCXs, MDCXs, and DLCXs) at both ingress and egress endpoints. This is important if the call is off-net, since you do not know from the facts gathered so far which trunk gateway is used to egress the call.

Search the LAN analyzer trace for messages that contains the same Call ID used in the first CRCX to the MTA. This trace enables you to locate the other MGCP messages going to the egress trunk gateway, since they use the same call ID. By noting the transaction ID and destination IP address in the CRCXs to the TGW, you can determine the associated gateway ACKs.

**Step 6** The connection control messages to the egress trunk gateway contain endpoint IDs, which correspond to the voice gateway port being used. This corresponds to a specific PSTN trunk, which is identified by an SS7 Circuit Identification Code (or CIC). Analysis of the dialed digits in the NTFY message from the MTA should indicate the target SS7 node for the call (that is, the SS7 destination point code, or DPC). Provisioning records should show the relationship of a trunk gateway endpoint ID with the PSTN trunk group identifier and CIC that are provisioned to the DPC. This allows you to follow the call flow into the SS7 network.

For example, endpointID DS0-1/24@tgw.cisco.com may correspond to CIC 4015 between SS7 point codes 229-151-023 (the VoIP virtual switch) and 229-151-024 (an adjacent Lucent 5ESS switch). To trace the SS7 messaging associated with this call, the SS7 messaging must first be captured on an SS7 protocol test tool. You must locate all SS7 messaging between the two point codes which have the CIC code 4015. This corresponds to SS7 messaging related to call setup on trunk gateway endpointID DS0-1/24@tgw1.cisco.com.

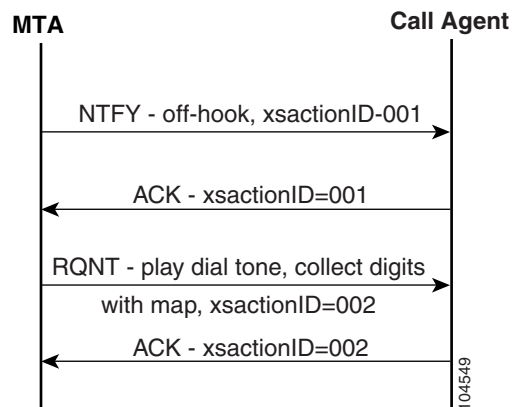
At this point, there is sufficient information to identify all messages associated with the call flow.

## Call Flow Problems

Configuration errors or lack of resources may be revealed in signaling messages to and from the Call Agent. The following sections list the problems encountered in call flows, and some guidelines for diagnosing the causes. For additional information about troubleshooting call flows, see [Chapter 4, “Troubleshooting with Call Flows”](#).

### No Dial Tone

In this scenario, the customer cannot get a dial tone after going off-hook. Normally, in order to get dial tone, the following sequence of messages must be exchanged between the Call Agent and the MTA:



If this is a new service, verify that the line was properly provisioned in the Call Agent, and data was input to DHCP/LDAP. Allow time for the provisioning changes to flow through.

Assuming that the MTA is connected and has been working, you need to trace the call flow. See [Chapter 4, “Troubleshooting with Call Flows,”](#) for the procedure for tracing a call flow.

An analysis of the call flows can reveal one of the following scenarios and narrow your investigation:

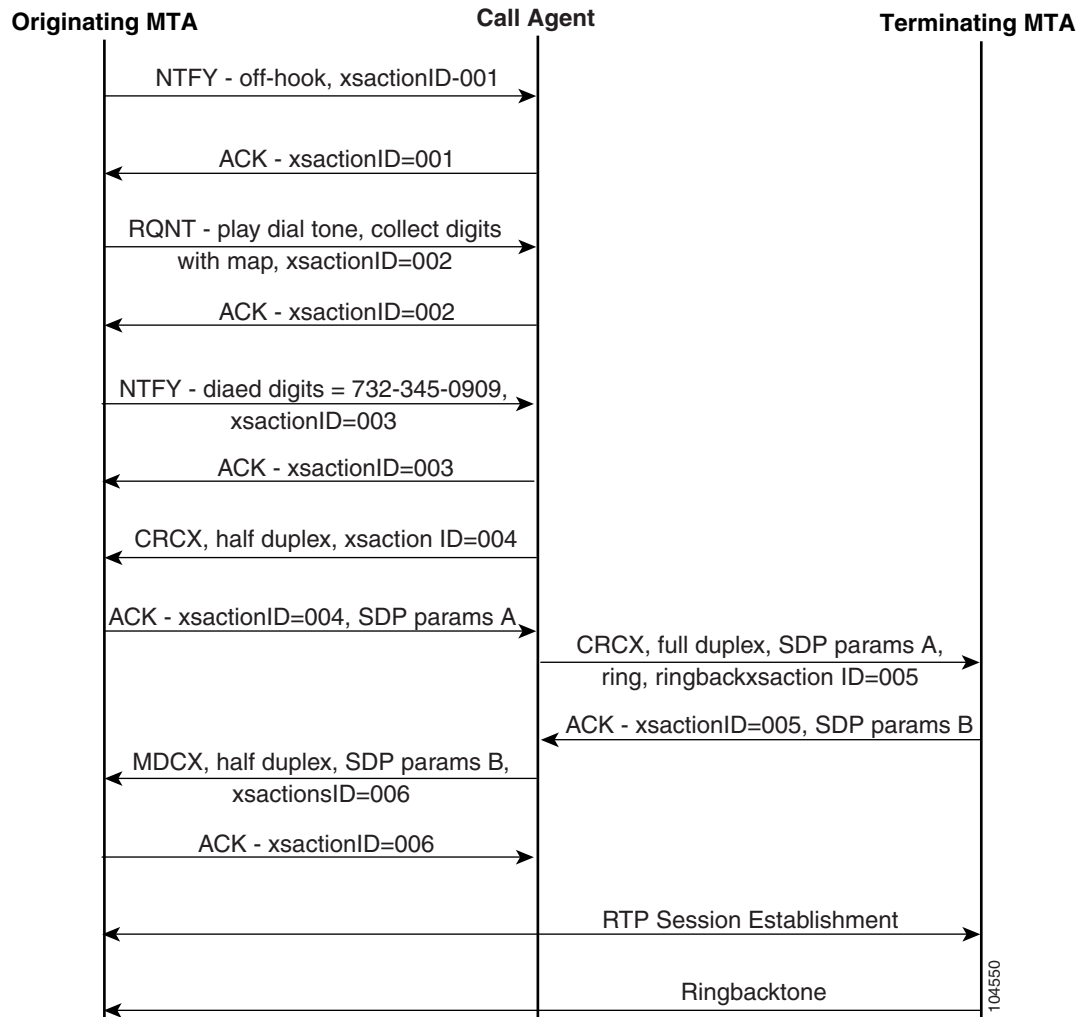
- MTA is not sending a NTFY message on off-hook.
  - Check the MTA configuration file to verify the proper notified entity (Call Agent), DHCP settings, and endpoint settings; then reset the MTA and verify this information again.
- MTA sent a NTFY message, but the Call Agent did not receive it (you can see repeated NTFY messages from the modem).
  - Trace the route to view the hops the packet makes on the way to the Call Agent to isolate where the problem is occurring. If a particular router is causing the problem, more than one customer will be involved and the problem router will be in their common path. Fixing a routing problem may require further investigation into routing tables.
- The Call Agent received the NTFY message, but did not respond (no ACK or RQNT messages seen at Call Agent links).
  - The problem is with the Call Agent.
  - The connection manager cluster may require restart. In this scenario, multiple lines are affected, all belonging to the same cluster.
- The Call Agent sent an ACK message (in response to an initial NTFY message from the MTA), but it was not received by the MTA. Do either of the following:
  - Turn on debug for the MTA to determine the problem.
  - The problem is in the network.
  - Trace the route from the Call Agent to the MTA to see where the route stops.
  - Fixing the problem may require further investigation into routing tables.

## No Post-Dial Cut-Through (No Ringback) — On-Net to On-Net

In this scenario, the customer receives dial tone, dials the number, and then expects to hear ringback (or a network announcement), but instead hears nothing.

If the caller is able to receive dial tone, then the Call Agent and originating MTA were able to exchange messages. This implies that there is no basic network connectivity problem with the originating MTA; however, connectivity problems with the terminating MTA are not ruled out.

The call flow extract below shows the message exchange required to reach the point where ringing is heard. To reach this point, MGCP messages must be exchanged to create VoIP “connections” on the originating and terminating MTAs. Calls fail if they cannot get past this stage; that is, the CRCX to the originating or terminating end is not successful, resulting in a NAK from the gateway instead of an ACK.



The call flow can fail at a number of different points. To troubleshoot this problem, perform the following steps:

**Step 1** Trap the message exchange between the Call Agent and originating or terminating MTAs and compare it to the reference call flow. Determine whether CRCX or MDCX messages are receiving return NAK messages. The MTAs may NAK for the following reasons:

- The Call Agent is attempting to create a connection (CRCX) for a line that already has an RTP session active. This can happen if the Call Agent and MTA get out of sync (less likely to happen with an MTA than a TGW). Somehow, an RTP session from a previous call was not torn down. See the MTA troubleshooting procedures for how to verify active RTP sessions or line state. If the MTA shows an RTP session already active on the terminating line, it may require a reset.
- The SDP parameters are not understood by the MTA. Check the SDP parameters in the trapped message against the reference call flow.

- Step 2** Check to see whether the Call Agent can reach the terminating MTA—that is, are repeated attempts to create the connection (CRCX messages) seen at the terminating side? This may indicate a problem communicating with the terminating MTA.




---

**Note** This failure should normally cause the Call Agent to route the originator to an announcement. Verify L3 connectivity between the Call Agent and the terminating MTA.

---

- Step 3** If the MGCP messaging looks correct, check to see whether the originator can dial another on-net test phone. If the originator can call the test phone and talk successfully, the problem could be with the terminating MTA. Use the test phone to originate a call to the terminating MTA. If the test phone cannot terminate to the MTA, the problem may be in the terminating MTA.

- Step 4** If the CRCX messages are not sent to the originating and terminating MTAs, the Call Agent may not be responding correctly—that is the Call Agent may provide dial tone, but may not continue with the call flow. Contact Cisco technical support.
- 

## No Post-Dial Cut-Through (No Ringback)—On-Net to Off-Net

This scenario is similar to the previous one, except that this call is attempting to reach the PSTN, so SS7 messaging is required. The symptom is the same: the caller receives dial tone and can dial digits, but then receives “dead air.” The call flow is between an originating MTA, the Call Agent, and a trunking gateway (TGW). The call flow is very similar to the previous case, with the following exceptions:

- The CRCX messages to the TGW do not request power ring (ring signal), or ringback tone. These signals are normally generated by the terminating PSTN switch, carried over TDM facilities to the TGW, which digitizes the tone for transport over the VoIP over cable network.



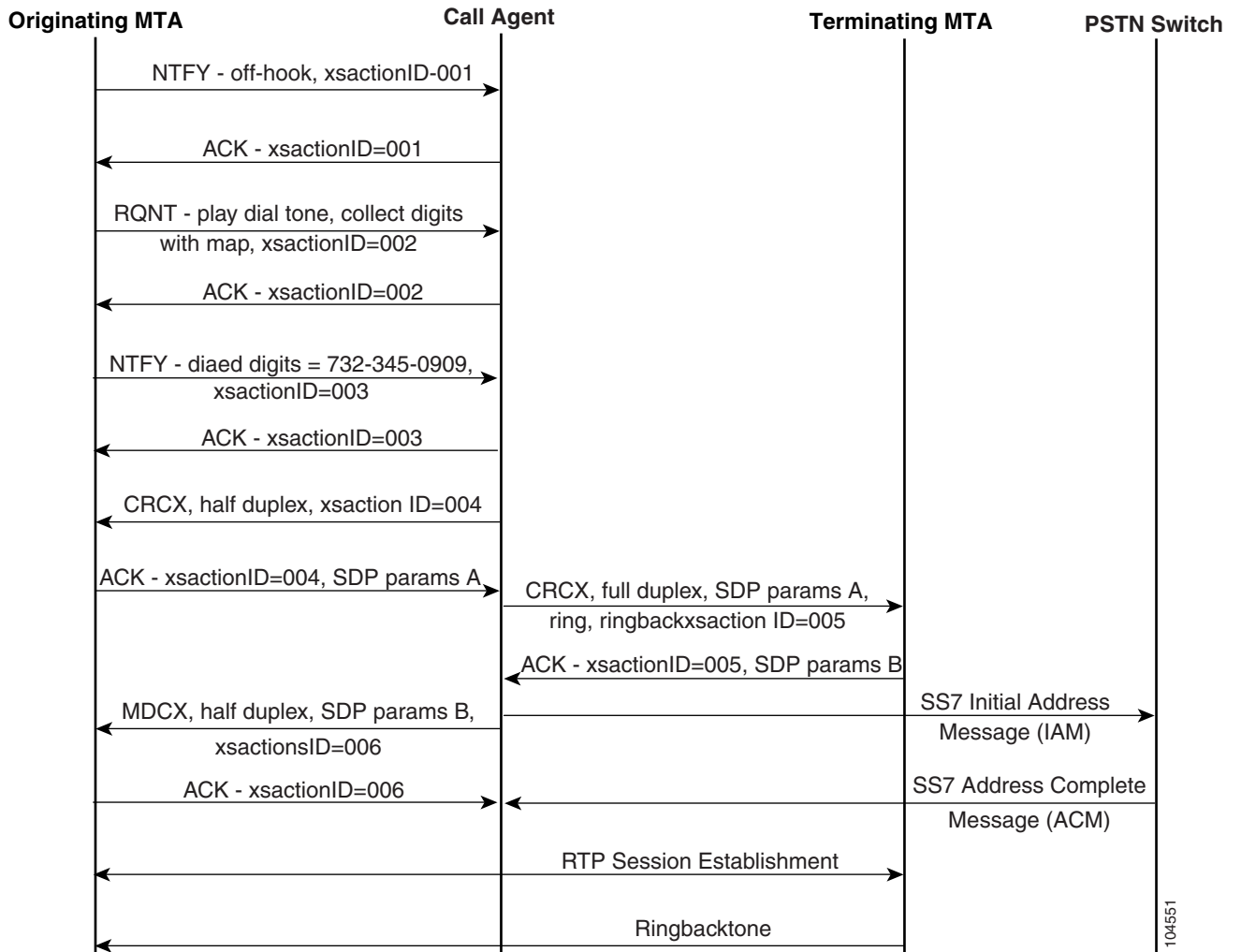

---

**Note** The ringback and ring signals may be included in the TGW CRCX, but are ignored by the TGW. See the reference call flow below.

---

- The call flow includes SS7 messaging to the PSTN switch.





To troubleshoot the problems in this scenario, perform the following steps:

**Step 1** Trap the message exchange between the Call Agent, the originating MTA, and trunk gateway, and verify it against the reference call flow.

Determine whether CRCX or MDCX messages are receiving return NAK messages. The MTAs may NAK for the following reasons:

- The Call Agent is attempting to create a connection (CRCX) for a line that already has an RTP session active. This can happen if the Call Agent and trunk gateway get out of sync. Somehow, an RTP session from a previous call was not torn down, though the Call Agent thinks the trunk endpoint is idle. (See your trunk gateway’s troubleshooting procedures for verifying active RTP sessions or trunk state.) If the trunk gateway that an RTP session already active on the trunk, it may be necessary to reset the individual trunk state.
- The SDP parameters are not understood by the TGW. Check the SDP parameters in the trapped message against the reference call flow.

- Step 2** Check to see whether the Call Agent can reach the terminating TGW—that is, can you see repeated attempts to send CRCX messages to the trunk gateway? This may indicate a problem communicating with the terminating TGW.



---

**Note** This failure should normally cause the Call Agent to route the originator to an announcement. Verify L3 connectivity between the Call Agent and the terminating TGW.

---

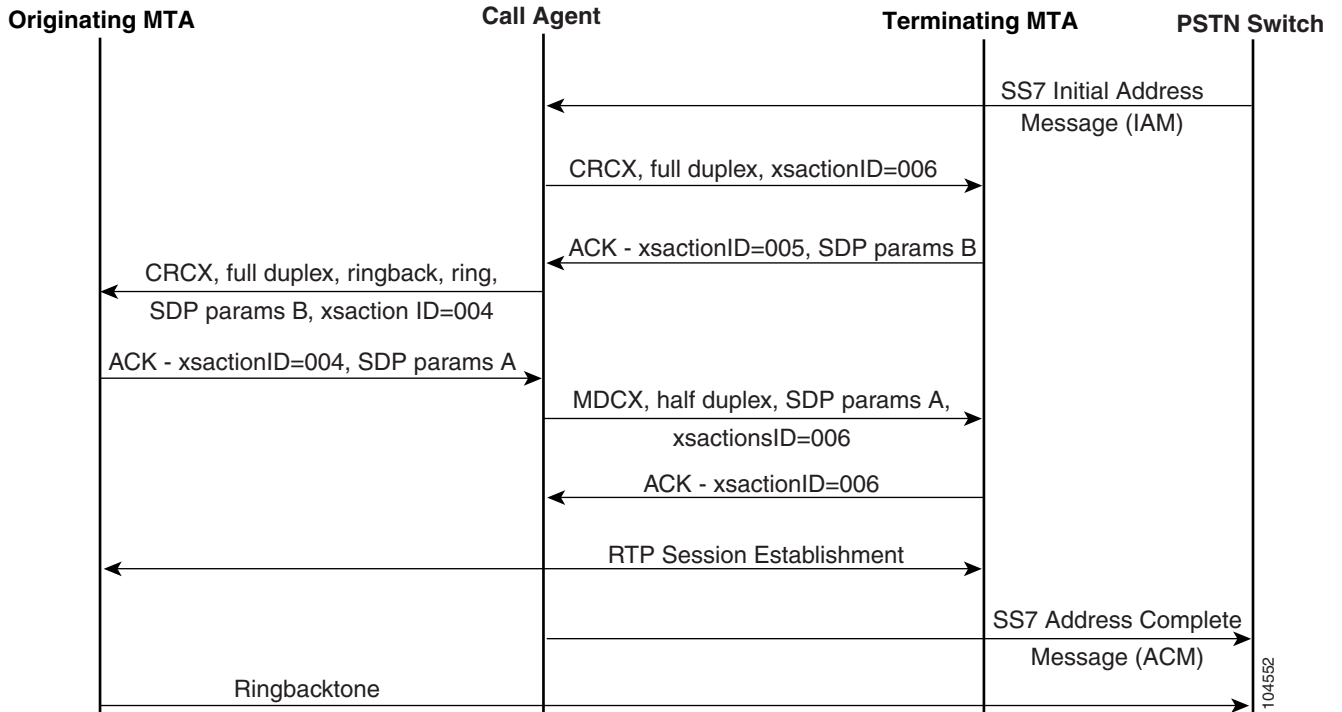
- Step 3** If the MGCP messaging looks correct, check to see whether the Call Agent sent an IAM to the PSTN switch. The PSTN switch should have replied with an ACM. If there are no SS7 messages, check L3 connectivity between the connection manager and SS7 gateway. If there is L3 connectivity, contact Call Agent technical support. The connection manager is not communicating with the SS7 gateway.
- Step 4** If the CRCX messages are not seen by the originating MTA and trunk gateway, the Call Agent may be having a problem. Contact Cisco technical support.
- 

## No Post-Dial Cut-Through (No Ringback)—Off-Net to On-Net

In this scenario, a caller from the PSTN calls a subscriber with an MTA. The PSTN caller reports hearing “dead air.” There is no ringback or network announcement.

All incoming calls from the PSTN start with an SS7 IAM message. The receipt of an IAM causes the Call Agent to send a CRCX message to both the trunking gateway, where the call enters and the terminating MTA, as is shown in the call flow below. When the Call Agent sends the CRCX to the terminating MTA requesting power ring and ringback tone, it also sends an SS7 ACM message back to the PSTN switch. The PSTN caller should hear ringback tone provided by the terminating MTA.

If the Call Agent detects an error in processing the call (for example, the subscriber number is unallocated), it sends an SS7 REL message with the appropriate cause code. This causes the PSTN switch to play a local announcement. The caller’s receiving dead air most likely indicates that the Call Agent proceeded with the call and sent an ACM within the acceptable GR317 time limits, or else the PSTN switch would have routed the caller to reorder tone. When the PSTN switch receives the ACM, it cuts through the backward direction of the call and expects ringback from the terminating MTA. If the caller does not hear ringback tone, there is a problem in making the VoIP connections, or the terminating MTA is having a problem playing ringback tone.



To troubleshoot the problems in this scenario, perform the following steps:

**Step 1** Trap the message exchange between the Call Agent, the originating MTA and trunk gateway, and verify it against the reference call flow.

Determine whether CRCX or MDCX messages are receiving return NAK messages. The MTAs or trunk gateway may NAK for the following reasons:

- The Call Agent is attempting to create a connection (CRCX) for a line or trunk that already has an RTP session active. This can happen if the Call Agent and MTA/trunk gateway get out of sync. Somehow, an RTP session from a previous call was not torn down, though the Call Agent thinks the line or trunk endpoint is idle.

From the trunk gateway, use the **show mgcp** command to compare the channels that the SS7 gateway and the trunk gateway both view as available. If they are out of sync, use the Circuit Group Block feature of Maintenance Block to instruct the SS7 gateway not to route calls to the problem trunk. Wait until all active calls are complete, then delete idle calls, and bring the trunk up again.

- The SDP parameters are not understood by the TGW. Check the SDP parameters in the trapped message against the reference call flow.

**Step 2** Check to see whether the Call Agent can reach the terminating MTA and ingress trunk gateway—that is, can you see repeated attempts to create (CRCX) the MTA or trunk gateway connection? This may indicate a problem communicating with the gateways.



**Note** In this case the Call Agent should send a REL message to the PSTN switch, and route the caller to an announcement.

- Step 3** If the MGCP messaging looks correct, check to see if the Call Agent sent an ACM to the PSTN switch. If the Call Agent appears to have sent the MGCP messaging correctly, but there is no ACM, check L3 connectivity between the connection manager and SS7 gateway. If there is L3 connectivity, the connection manager is not communicating with the SS7 gateway. Contact Cisco technical support.
- Step 4** If the CRCX messages are not seen by the originating MTA and trunk gateway, and the Call Agent did not send a REL message, the Call Agent may be having a problem. Contact Cisco technical support.

## Test Tools

Even in a lightly loaded network, it can be difficult to extract MGCP messages associated with a single call. It is desirable, from an operational perspective, to have test tools capable of automatically correlating the messages in the fashion described above.

Network monitoring provides visibility into the internal operation of the VoIP network. This allows maintenance personnel to understand how well the network is performing and to understand what is happening when a network element fails. Almost all network elements keep information about their current status, which can be reported to a centralized network management system using SNMP. Another method of monitoring is to capture MGCP protocol messages as they traverse the VoIP network. Protocol message capture is the starting point for call flow analysis. A protocol analyzer is an invaluable tool in tracking down the causes of problems in a network.

Remember to keep reference call flows up-to-date. If there are changes to the network or updates to software, update your working call flow references. When you encounter problems, you need to compare problem call flows to the reference call flows.



### Note

In general, errors, packet or cell loss, and latency increase with load. Therefore, you should take your sample of performance during peak load, as well as during normal periods.

## Voice Quality Problems

This section describes several types of voice quality problems and troubleshooting strategies for them.

Voice quality problems include lost or distorted audio during phone calls. Common problems include breaks in the sound that cause the audio to be intermittent (like broken words), the presence of odd noises that distort the audio, echo, or effects that cause spoken words to sound watery or robotic.



### Note

One-way audio, that is, a conversation between two people where only one person can hear anything, is not considered a voice quality problem. A protocol analyzer can help you verify that the phone or gateway is actually sending or receiving packets.

One or more of the following components can cause audio problems:

- Telephone
- Gateway
- Network

To troubleshoot voice quality problems, you must examine the infrastructure and all devices for drops and delays. You may find that all individual devices are working fine, but that you have address sizing and scaling problems (which are discussed in a later chapter).

## Lost or Distorted Audio

One of the most common problems is a *breaking up* of audio, which is often described as garbled speech or a loss of syllables within words or sentences. There are two common causes: packet loss and jitter.

- **Packet loss**—occurs when packets are dropped or arrive at their destination too late to be useful.
- **Jitter**—is the variation in arrival times of successive packets.

Ideally, all VoIP packets from one phone to another would arrive at a constant rate of 1 every 20 ms. Notice that travel time itself does not matter, only the variation in arrival times between packets.

There are many sources of variable delay in a packetized cable network, and it cannot be eliminated entirely. In anticipation of variable delay, digital signal processors (DSPs) on phones and other voice capable devices are designed to buffer some of the audio.

This *dejittering* is done only after the audio packet has reached its destination and is ready to be put into an audio stream (that is, played into the user's ear or sent to the PSTN via a digital PCM stream). The network administrator can minimize the variation in packet arrival times by applying quality-of-service (QoS) and other measures in advance.

When faced with lost or distorted audio, first try to determine the path of the audio. Identify each network device in the path of the call's audio stream. Try to determine whether the problem occurs only between two particular sites, only through a certain gateway, and so on. This will help to isolate the devices to examine.

For troubleshooting, it may be desirable to disable silence suppression (also known as Voice Activation Detection or VAD). This mechanism saves bandwidth by not transmitting audio when there is silence, but may cause noticeable (and unacceptable) clipping at the beginning of words. You can then use a network (or protocol) analyzer to view packet flow.

A call between two phones should have 50 packets per second (or 1 packet every 20 ms) with silence suppression disabled. In a poor quality call (such as a call with a lot of jitter), the difference in arrival times of these packets can vary greatly. With proper filtering, it should be possible to determine whether packets are being lost or delayed excessively.

### Crackling

Another symptom of poor voice quality may be crackling, which is sometimes caused by a defective power supply or strong electrical interference close to the phone. Try swapping the power supply and moving the phone and/or MTA to a different location.

### Echo

*Echo* (also known as talker echo) occurs when a talker's transmitted speech is coupled into the receive path from the far end. Talkers then hear their own voices, delayed by the total echo path delay time. The cause of echo usually lies in analog components and wiring. Exceptions occur when one party is using a speakerphone whose volume is set too high, or in other situations that can create an audio loop.

When troubleshooting echo problems, make sure the phones being tested are not using a speakerphone and they have the headset volume set to reasonable levels (start with 50 percent of the maximum audio level). Most of the time, echo problems occur when attaching to the PSTN through a gateway.

Although the source of the problem is almost always at the far end, it is difficult to change anything in the PSTN. So the first step is to determine which gateway is being used. It might be possible to add additional padding to the gateway in the transmit direction (toward the PSTN) so that the lower signal strength yields less reflected energy.

You can also adjust the receive level so that any reflected audio is reduced. It is very important to make small adjustments at a time. Too much attenuation can make the audio impossible to hear at both ends. Alternatively, you can contact the carrier and ask to have the lines checked. On a typical T1/PRI circuit from the PSTN in North America, the input signal level should be -15 dB at the VoIP trunking gateways for an originating audio source of 0dB, 1001 Hz tone (should expect 3-6 dB audio signal attenuation on a IMT trunk) and a tail circuit limitation of 16ms (64 or 128ms depending on the gateway) for Cisco VoIP trunking gateways echo cancellation. If the signal level is higher, echo can result.

Keep a log of all calls that experience echo. Record the time of the problem, the source phone number, and the number called. Gateways have a fixed 16 ms of echo cancellation. If the delay in reflected audio is longer than 16 ms, the echo canceller will not work properly. This should not be a problem for local calls; long-distance calls should have external echo cancellation built into the network at the central office. This is why it is important to note the external phone number of a call that experiences echo.

## Voice Network Troubleshooting Procedures

Troubleshooting voice problems usually begins at one of the endpoints (either the trunk gateway or the MTA) and works through the network to the other endpoint. Where you begin depends on the problem, but most of the time you will not have access to the PSTN end-point. If customers complain that their voices sound bad to others off the network, start troubleshooting at the MTA. If customers complain that the voice quality they are hearing is poor, start at the trunk gateway.

- First, in order to successfully troubleshoot voice quality issues, you must have accurate information: on-net number, number dialed (on-net or off-net), date and time, type of echo or voice quality issue, and whether this is the first time the problem occurred when dialing this number. If available, the type of phone used at the far end (cell phone, speaker phone, conference bridge, cordless, and so on).
- Second, you need to determine which trunk group/T1 this call used to reach the far end and check the following configured values on the VoIP trunking gateway; input and output levels, echo cancellation coverage (the default is 16 ms). The input and output levels should be 0 dB and the echo cancellation coverage should be at least 32 ms but preferably 64 ms. If echo cancellation coverage is below 32 ms, it needs to be changed to 64 ms. Global verification of all T1's echo cancellation coverage values is recommended since these values are provisioned on a per T1 basis.
- Third, you should verify the CDRs generated by the Cisco BTS 10200 and look for packet loss and jitter values. These could indicate some network related issues that could impact voice quality.

If the customer is still experiencing echo, you should do a case-by-case analysis to determine if there is any call pattern that could isolate the problem to a specific T1. Do not adjust gateway levels or contact the Service Provider before opening a TAC case, unless you can provide them with a full description and documentation of the echo problem. Level adjustments provide limited impact on the echo cancellers ability to converge, so you do not want to fix one echo problem but create 10 new voice quality problems.

### Starting at the MTA

If you are troubleshooting a VoIP over cable problem at the MTA, first determine whether it is an isolated incident or a regular occurrence. If it is a regular occurrence, determine whether there is any pattern—all the time, only at certain times of day, only on certain days, and so on. To do this, track performance of the problem MTA over several days.

Here are some sources of data to review:

- Over at least a 24-hour period, look at the number of times the MTA resets, loss of synchronization data, and time-outs. Regular resets indicate a problem. If they are occurring at a particular time of day, look more closely at what is happening locally or on the network during this period.

If the `LostSyncs` value is high (such as once an hour), there is something physically wrong with the connection. Send a technician to recable the MTA.

If `T3Timeouts` or `T4Timeouts` values are high, it is most likely an upstream problem.

- Look at signal-to-noise ratio, corrected errors, and uncorrectable errors. If the signal-to-noise ratio is higher than normal, you will probably also notice an increasing proportion of corrected and uncorrectable errors. Check for ingress noise, impulse noise, or common path distortion.

## Starting at the Trunking Gateway

If you are starting to troubleshoot a VoIP over cable problem at the trunking gateway, here are some guidelines:

- Look at values for the following objects in the Voice Over IP Call Active Table of **CISCO-VOICE-DIAL-CONTROL-MIB.my**:
  - `cvVoipCallActiveGapFillWithSilence`—duration of the voice signal replaced with signal played out during silence, due to voice data not received on time (or lost) from the voice gateway on this call.
  - `cvVoipCallActiveGapFillWithPrediction`—duration of the voice signal played out with signal synthesized from parameters or samples of data preceding in time, due to voice data not received on time (or lost) from the voice gateway for this call. An example of such playout is frame-erasure or frame-concealment strategies in G.729 and G.723.1 compression algorithms.

Excessive values could indicate codec problems.

- In the same MIB, look at values for these objects:
  - `cvVoipCallActiveHighWaterPlayOutDelay`—provides the high-water mark Voice Playout FIFO (first-in-first-out) Delay during the voice call.
  - `cvVoipCallActiveLowWaterPlayOutDelay`—provides the low-water mark Voice Playout FIFO Delay during the voice call.

Excessive values indicate a jitter problem.

- To determine where jitter is occurring, do the following:
  - Use a sniffer to see where the jitter is occurring. The normal arrival time for packets is about 20 ms; a variation of 5 ms indicates jitter. Also look at the sequence of RTP packets to see where packets are lost.
  - View values for the following objects in the Voice Over IP Call Active Table of **CISCO-VOICE-DIAL-CONTROL-MIB.my**:
    - `cvVoIPCallActiveLostPackets`—number of lost voice packets during the call.
    - `cvVoIPCallActiveLate Packets`—number of received voice packets that arrived too early to store in the jitter buffer during the call.
    - `cvVoIPCallActiveEarlyPackets`—contains the number of received voice packets that arrived too late to playout with CODEC during the call.

Abnormal numbers here can indicate a network problem.

- Use the **show call history voice brief** command to view round-trip delay (last/minimum/maximum) of packets in milliseconds.
- A high degree of processing may be the cause of the problem. Use the **show processes cpu** command to view a graph of the maximum and average trunk gateway CPU to locate what process is interfering with voice transmission quality.

## Dropped Calls

Dropped calls occur when a call is terminated prematurely. Dropped calls can be the result of a gateway resetting or a circuit problem. Use a protocol analyzer to determine which side is hanging up the call, and trace call flows to isolate where the problem is occurring.

## Codec Mismatch

If a customer gets a reorder tone when going off-hook, it could be the result of codec disagreement between endpoints. Verify that both endpoints support at least one common codec (for example, G.711). If not, you need to use transcoders.

## Dial Plans

A Dial Plan is a list of numbers (and groups of numbers) that tells the call agent which devices to send calls to when a certain string of digits is collected. It is analogous to a static routing table in a router. Be sure that your dial plan concepts, basic call routing, and planning have been carefully considered and properly configured before trying to troubleshoot a potential dial plan problem.

Consider the following questions when troubleshooting dial plan problems:

- What Directory Number (DN) is originating the call?
- What is the number that is being dialed? Note if and when callers are receiving a secondary dial tone at any stage. What do callers hear after all the digits have been entered (re-order, fast-busy)? Do they receive progress tones before they expect to hear anything? Make sure callers wait at least 10 seconds after entering the last digit, since they may have to wait for the interdigit timer to expire.





## Troubleshooting DOCSIS Networks

---

DOCSIS provides the bandwidth and latency guarantees needed to provide toll-quality voice, data services, and multimedia applications across a shared HFC network. It is designed to be backward compatible, enabling DOCSIS 1.0 and 1.1 modems to operate in the same spectrum on the same network.

This chapter discusses:

- [DOCSIS 1.0+, page 5-1](#)
- [Understanding Initialization States, page 5-3](#)
- [Radio Frequency \(RF\) Issues, page 5-9](#)
- [Troubleshooting RF Problems, page 5-10](#)
- [Measuring RF Signals, page 5-11](#)
- [Troubleshooting Slow Performance, page 5-17](#)

### DOCSIS 1.0+

The Cisco uBR7246Vxr CMTS supports DOCSIS 1.0+ starting from IOS release 12.1(01)T. DOCSIS 1.0+ is DOCSIS 1.0 with some special QoS extensions for supporting realtime Voice/Fax/Video on the local access network. However, these features are only activated when a DOCSIS 1.0+ MTA solicits these services via new dynamic MAC messages.

The DOCSIS 1.0+ services include the following:

- Two MTA-initiated dynamic MAC messages, DSA and DSD. These messages allow dynamic SIDs to be created/destroyed at run-time on a per Voice/Fax call basis.
- Unsolicited Grant Service (CBR-scheduling) on the upstream. This helps to provide a high quality QoS channel for the upstream constant bit rate (CBR) Voice/Fax packets from the MTA.
- For any given MTA, the ability to provide separate downstream rates based on the IP-precedence value in the packet. This helps in separating Voice/Signaling/Data traffic going to the same MTA for rate-shaping purposes.

Following is an example of how DOCSIS 1.0+ features are applied in an interaction between the uBR and the MTA.

- The MTA downloads theconfig file at the time of registration, and sends the provisioning information to the DOCSIS 1.0+ CMTS.

- When CMTS receives the REG-REQ, it creates a local database entry for the MTA. A static SID is immediately assigned to the MTA for the data service. For the phone line service, the CMTS only creates 2 deferred service flows (for subsequent activation) in the MTA's database entry. No SIDs are assigned for the phone line service during registration.
- Whenever an MTA wants to get a Voice/Fax channel with real time CBR service, it sends a DSA-REQ MAC message to the CMTS, specifying its special CBR scheduling requirements like grant-size, grant-interval (grant-size, grant-interval depend on the codec type G.711/G.729 being used on the MTA).
- When the CMTS receives the DSA-REQ, it first checks in that MTA's database entry if any deferred service flow is available. If a deferred service flow is available, the CMTS assigns a new dynamic SDI for that MTA and triggers unsolicited grants (CBR slots) on that newly assigned dynamic SID. The CMTS informs the MTA of the newly assigned dynamic SDI, using the DSA-RSP.
- Given that the CMTS can accommodate the new CBR connection, that MTA will keep getting unsolicited grants of the correct size (enough to fit the periodic Voice/Fax) packet at correct periodic intervals. The MTA does not have to contend with any other MTA on the upstream for sending these real-time packets. It has a dedicated TDM sub-channel on the upstream in the form of the unsolicited grants. The delay/jitter is well bounded and good voice quality is thus maintained on the upstream path from the MTA to the uBR.
- The MTA colors the precedence bits in the IP header of these voice packets with the predefined value of 0x05 for propagating the preferential local access QoS eventually into the IP backbone.

When the Voice packets arrive at the CMTS in the CBR slots, they are either switched into the WAN (IP cloud), or forwarded to some other MTA on the downstream channel.

In the former case, the backbone routers like the Cisco GSR 12000 need to be configured to recognize and give preferential treatment for these Voice transport packets (precedence value 0x05), as compared to signaling/regular best effort data packets with precedence 0x3, 0x0 respectively.

In the later case, where the upstream packets are switched to the downstream channel of the same uBR, the Voice packets (0x05) are separately handled for rate limiting, as compared to signaling, data packets based on their precedence values.

Even if at the time of the call, the destination MTA is doing a large downstream file transfer, the Voice packets forwarded to it on the same downstream will be unaffected by FTP on the same MTA, due to the use of ip-precedence values in doing downstream bandwidth accounting.

- When the call is torn down, the MTA sends a DSD-REQ to the CMTS to release the dynamic SDI. The CMTS stops the CBR grants, destroys the dynamic SDI indicated in DSD-REQ, frees up one deferred flow for the MTA, and sends a DSD-RSP to the MTA confirming the same.
- The CMTS ensures that a subscriber MTA provisioned for 2 virtual phone lines can only get up to 2 high quality dynamic CBR QoS SIDs at runtime. Every time the MTA sends a DSA-REQ requesting a new dynamic SID, the CMTS first checks to see if that MTA has any unused deferred service flow available before creating a new dynamic SID. If the MTA is already using 2 dynamic SIDs, both its deferred service flows will show up as in-use at the CMTS. So long as a dynamic SID is using the service flow, the service flow will be unavailable for creation of any new dynamic SID from this MTA.


**Note**

Refer to “DOCS-IF-MIB.my” and “CISCO-DOCS-EXT-MIB.my” in Chapter 9 for information on DOCSIS-related SNMP MIBs for monitoring MTA performance.

# Understanding Initialization States

The following sections review each of the initialization states, including any problems that may occur in that state.

Before discussing the initialization process in detail, following is a summary of the process as displayed on a Killerbee RDCM console:

Example output from Killerbee initialization:

```
Found DS frequency (64 QAM): 651000000 Hz
MAC State --->>> 'wait_ucd_state'
    Found US channel: 1 6 5 4 3 2
    MAC State --->>> 'wait_map_state'
    Trying Upstream Channel 6 (41200000 Hz)
    MAC State --->>> 'ranging_broadcast_state'
    MAC State --->>> 'ranging_unicast_state'
    MAC State --->>> 'establish_dhcp_state'
cmWriteFlashFile("CM_MACCONFIG", 0x8313d54, 0x136) by TID 0x82eb558 (tConfigNV)
cmWriteFlashFile("CM_DHCPLEASE", 0x81162c0, 0x24) by TID 0x82d7d90 (tLease-0)
    MAC State --->>> 'establish_tod_state'
    MAC State --->>> 'security_association_state'
    MAC State --->>> 'configuration_file_state'
    MAC State --->>> 'registration_state'
    MAC State --->>> 'establish_privacy_state'
    MAC State --->>> 'operational_state'
cmWriteFlashFile("CM_MACCONFIG", 0x8313d54, 0x136) by TID 0x82eac00 (tConfigNV)
cmWriteFlashFile("CM_BOOT_BK", 0x8313e8a, 0x13e) by TID 0x82eac00 (tConfigNV)
cmWriteFlashFile("CM_BOOT", 0x8313e8a, 0x13e) by TID 0x82eac00 (tConfigNV)
```

## Physical and MAC Configuration

The first few states involve configurations at the Physical and Data Link (Media Access) levels.

### Scanning Downstream Channel

```
Scanning Downstream Channel...
          lower_limit upper_limit step_size  valid
BAND 0: 855000000    855000000    6000000    yes  Trying: 855000000 2
```

The first stage of MTA bring-up is downstream channel acquisition. The tuner scans the downstream spectrum until a digital QAM signal is encountered. When a channel with QAM is found, the receiver listens for SYNC messages from the CMTS (the Cisco uBR7246vxxr). SYNC messages are CMTS timestamps that the MTA needs in order to synchronize with the CMTS to calculate latency — how much time it takes for messages to travel in the HFC network.

If a modem is stuck in this state, or comes back to this state quite frequently, this is an indication of a less than adequate physical setup. Difficulty in acquiring sync can be caused by a weak carrier signal (or lots of noise). Since noise is random, the downstream channel has a carrier signal that must have enough power for the modem to discern the carrier from the noise. This carrier is the QAM symbols representing the bits of the SYNC messages (and all other messages and data). The signal power can also be too strong for the receiver to discern the symbols in the carrier.

Another problem to check for with failure to sync is the center frequency. If the center frequency of the carrier is not a standard channel center frequency, the receiver may not discern all the symbols, or more likely will not achieve QAM lock at all.

To troubleshoot, use a signal or spectrum analyzer off a drop port (the final splitter to which modems are attached) to measure the digital channel power coming from the splitter to the modem. The optimal input power level at the modem is 0 dBmV. The receiver has a range of -15dBmV to +15dBmV.

- If the power is too low, configure the upconverter as per Chapter 4 of the *Cisco uBR7246 Hardware Installation Guide*. This is preferred to removing attenuation because the carrier to noise ratio must remain sufficiently high to reduce the chance of bit errors due to noise.
- If the signal is too strong, add attenuation at the high frequency port on the diplexer. This is preferred to reducing the power output of the upconverter, in order to maintain the carrier to noise ratio. If the frequency is off, adjust the frequency of the upconverter.

A modem that resets back to this state frequently is one that is not maintaining sync or is losing sync with the CMTS. The cause is similar to not acquiring sync (discussed above), and the same troubleshooting methods should apply.

## Wait UCD State

```
Found DS frequency (64 QAM): 855000000 Hz
MAC State --->>> 'wait_ucd_state'
Found US channel: 1
```

After a downstream channel has been acquired and latency has been calculated, the next task is to locate a suitable upstream channel. The modem listens for an upstream channel descriptor (UCD), which contains the physical properties of the upstream channel, such as, frequency, modulation, channel width, and other parameters defined in the burst descriptors discussed in Section 4 of [DOCSIS].

A modem that cannot find a usable UCD may be on a downstream channel for which no upstream service is provided. This is likely to be a headend misconfiguration. The **show controller interface** command is a good place to start.

Another possible reason a modem may not find a usable UCD is that its hardware or MAC may not support the parameters in the burst descriptors. This is likely to be either a headend misconfiguration, or a modem that is not DOCSIS compliant.

## Wait MAP State

Once a usable UCD is found, the modem begins to listen to MAP messages which contain the upstream bandwidth allocation map of time. A section of time is mapped out into mini-slots, and assigned to individual modems. There are also regions in the MAP for broadcast, contention-based initial maintenance (or broadcast) ranging. It is to these regions of the MAP that the modem must send its initial ranging requests until the CMTS responds with a ranging response (RNG-RSP).

If a modem cannot find an initial maintenance region before a T2 timer expiry, there is likely a headend misconfiguration. You should check the insertion-interval for the cable interface.

## Ranging Broadcast State

```
Trying Upstream Channel 1 (41200000 Hz)
MAC State --->>> 'ranging_broadcast_state'
```

At this stage, the modem begins a ranging process to calculate the necessary transmit power level to reach the CMTS at its desired input power level. The MAC sends a ranging request (RNG-REQ) message to the CMTS and waits for a ranging response (RNG-RSP) message, or a T3 timer expiry. If a T3 timeout occurs, the retry count increments. If the retry count is less than the maximum number of retries, the modem transmits another RNG-REQ at a higher power level.

This ranging process occurs in the initial maintenance or broadcast regions of the MAP, because the CMTS has not assigned the modem a service identifier (SID) for unicast transmissions in the MAP. Thus, broadcast ranging is contention based and subject to collisions. To compensate for this the modems have a ranging backoff algorithm to calculate a random backoff time between RNG-REQ transmissions. When the transmit power has reached a sufficient level for the CMTS, it responds to the RNG-REQ with a RNG-RSP containing a temporary SID. This SID is used to identify unicast transmission regions in the MAP for unicast ranging.

If a modem cannot proceed out of `ranging_broadcast_state`, the likely cause is an insufficient transmit power level. Transmit power can be adjusted by adjusting attenuation at the low frequency port of the diplexer. Increased attenuation will result in increased transmit power levels. Roughly 20 - 30 dBmV of attenuation is a good place to start. This can be refined once the modem is reaching `ranging_unicast_state` more reliably.

## Ranging Unicast State

```
MAC State --->>> 'ranging_unicast_state'
```

With help from the CMTS, the goal of unicast ranging is to have the modem configure the transmit timing offset and power level, to insure that transmissions from the modem are received at the correct time and are at an acceptable input power level at the CMTS receiver. This is achieved through a conversation of unicast RNG-REQ and RNG-RSP messages. The RNG-RSP messages contain power and timing offset corrections the modem must make. The modem continues to transmit RNG-REQ and perform adjustments per RNG-RSP, until the RNG-RSP message indicates ranging success.

If a modem cannot proceed out of `ranging_unicast_state`, transmit power needs to be refined. That is what this state is for, so it is a lot easier to find the right attenuation levels for the proper CMTS input power level. A log mask of `0xffff00bf` should be adequate to view ranging messages and power levels.

Use the following command:

```
-> cmSetLogMask 0xffff00bf
```

```
Turning on extensive debugging may severely impact performance and functionality.
Continue? [y|n] y
Full debugging enabled.
cmWriteFlashFile("CM_LOGCONFIG", 0x82f0168, 0x18) by TID 0x82f0400 (tShell)
usrEraseSysFlash(1, 0x1e0000, 0x18) by TID 0x82f0400 (tShell)
.....value = -65473 = 0xffff003f = __func_taskRegsShowRtn + 0xf7ed9d5f
->
```

For Killerbee reference design modems, a reasonably good transmit power is roughly 40 - 50 dBmV (based on a CMTS input power of 0 dBmV.) Other hardware may vary. Like the downstream channel, the carrier in the upstream channel should be sufficiently strong for the CMTS receiver to discern the symbols, yet not too high to prevent increased bit error-rates.

A modem which encounters T4 timeouts in this state is indicative of an upstream frequency error. The IF (intermediate frequency)—the output frequency from the uBR before upconversion—is 44 MHz. With every signal on the cable, there are weaker harmonic products of the signal present on the cable. In most cases, the power-ratio between the signal and the harmonic products should be large enough such that the harmonic products can be dismissed. However, the upstream is more sensitive to harmonic products so an upstream frequency which lies at a harmonic frequency of the IF is a difficult channel to range on. Harmonics of the IF occur at 11 MHz steps on either side of the 44 MHz IF so upstream frequencies of 11, 22, and 33 MHz should be avoided.

Additionally, on linecards with multiple upstreams, the upstream frequencies on a single linecard must be unique if the upstream channels are combined on the same physical trunk. The upstreams may be on the same frequency if the upstream channels are not physically combined.

## Network Layer Configuration And Above

After ranging is successful, the modem needs additional configuration from the operational support servers. The collection of services they provide and configure are called operational support services (OSS).



### Note

At this point, the modem is functional; it could act like a bridge and be a fairly quick transmission device, but there would be nothing in the way of administrator configuration, diagnosis, class of services, security, privacy, or remote software upgrade capability, *and therefore* it would not be DOCSIS compliant.

## Establish DHCP State

```
MAC State --->>> 'establish_dhcp_state'
cmWriteFlashFile("CM_MACCONFIG", 0x8313db6, 0x12e) by TID 0x82eb0f8 (tConfigNV)
usrEraseSysFlash(1, 0x1e0400, 0x12e) by TID 0x82eb0f8 (tConfigNV)
.....cmWriteFlashFile("CM_DHCPLEASE", 0x810ebe4, 0x24) by TID 0x82d825c (tLease-0)
usrEraseSysFlash(1, 0x1e0200, 0x24) by TID 0x82d825c (tLease-0)
```

The first task in configuring the OSS is acquiring network configuration via DHCP. A broadcast DHCP DISCOVER message is issued by the modem. Normally, routers will not forward broadcast messages, but they can be configured to do so for a collection of UDP protocols - one of which is DHCP. If a DHCP server responds to the DISCOVER with an OFFER, the modem may choose to send a REQUEST for the offered configuration. The DHCP server can respond with an ACK (acknowledged) or NAK (not acknowledged). A NAK may be a result of an incompatible IP address and gateway address, which might occur if a modem hopped from one downstream channel to another which resides on a different subnet. When the modem seeks renewal of the lease, the IP address and the gateway address of the DHCP REQUEST message will be different network numbers and the DHCP server will refuse the REQUEST with a NAK. These situations are rare and the modem will simply release the lease and start over with a DHCP DISCOVER message.

Frequently, errors at `establish_dhcp_state` manifest as timeouts rather than NAKs. Troubleshooting practices at this stage, should include:

- start at the lower layers and work up
- start locally and work towards remote possibilities
- look at the modem, before diagnosing the DHCP server via DHCP logs

The log mask `0xffff00bf` used above in ranging can also help you in troubleshooting virtually all the problems a modem might encounter in bring up stage and is a good place to start when troubleshooting a bring-up error. The order of DHCP messages should be DISCOVER, OFFER, REQUEST, ACK. If the modem is transmitting a DISCOVER with no OFFER response from the DHCP server, turn on UDP debugging on the uBR, using the following command:

```
uBR# debug ip udp
```



### Note

If connected to the router via a telnet session or any session other than a console session, the **terminal monitor** command (abbreviated **term mon**) is necessary to view debug messages. To turn off **term mon**, use the **term no mon** command or simply logout.

**Caution**

Running debug commands on a uBR with more than a handful of modems may cause the uBR to halt the system in order to keep up with the debugging. In this case, all the modems may lose sync and debugging will be useless.

If no packets are seen in debug messages, check the configuration of the “ip helper-address” statement on the cable interface to which this modem is attached. If this is configured correctly and a packet trace of the DHCP server subnet also reveals no DHCP packets from the modem, then the next place to look is the output errors of the modem's cable interface, or the input errors of the cable interface of the uBR. It might be a good idea to boost the transmitter power a bit more with more attenuation.

If you can see that packets are being transmitted onto the DHCP server subnet, it would be a good idea to double-check the modem debug messages to see if there are parameter request or assignment errors. This is the stage of troubleshooting where you should investigate the routing between the modem and the DHCP server. It is also advisable to double-check the DHCP server configuration.

## Establish TOD State

```
MAC State --->>> 'establish_tod_state'
```

After a modem has acquired its network parameters, it must request the time of day from a Time Of Day (TOD) server. TOD uses a UTC timestamp (seconds from January 1, 1970) combined with the time offset option value from DHCP to calculate the current time. The time is used for syslog and event log timestamps.

Time of day errors almost always point to a DHCP misconfiguration. Possible misconfigurations that can result in TOD errors are IP address, gateway address misconfigurations, or the wrong TOD server address. Again, start troubleshooting locally by examining the DHCP parameters the modem has stored, using the following command:

```
-> cmShowDhcpParameters
```

or:

```
-> cmAddLogValues ("SEV_ALL FAC_DHCP")
```

The latter will give debug output of DHCP actions and tasks.

Also check the modem routing table with the vxWorks **routeShow** command.

## Security Association State

```
MAC State --->>> 'security_association_state'
```

This is a placeholder for a state yet to be defined. It is envisioned that a security association with a security server will provide IPsec-like security for the modems. Questions about its design and implementation are still being discussed. In the meantime, DOCSIS 1.0 requires modems to support a future definition of this state including the DHCP option for a security server. It is unlikely to find a modem having a problem with this state until it is defined in DOCSIS and implemented on the modem.

## Configuration File State

The main configuration and administration interface to the MTA is the configuration file downloaded from the provisioning server. This configuration file contains downstream channel and upstream channel identification and characteristics, as well as Class of Service settings, Baseline Privacy settings, general operational settings, network management information, software upgrade fields, filters, and vendor specific settings.

Common reasons for failure at this state are missing file, wrong file permissions, TFTP server is unreachable, file is wrong format, file has missing required options, misconfigured required options, or incorrect options - unknown or invalid TLVs. For a description of the required parameters and guidelines for their values, see Appendix C of [DOCSIS].

A debug command for configuration file transactions and parsing is:

```
-> cmAddLogValues ("SEV_ALL FAC_CONFIGFILE")
```

## Registration State

```
MAC State --->>> 'registration_state'
```

After configuration, the modem sends a registration request (REG-REQ) with a required subset of the configuration settings, as well as the CM and CMTS message integrity checks (MIC). The CM MIC is a hashed calculation over the configuration file settings which provides a method for the modem to be sure the configuration file was not tampered with in transit. The CMTS MIC is much the same thing except it also includes a setting for a shared-secret authentication string. This shared secret is known by the CMTS and the provisioning server, and ensures that only modems configured by authenticated provisioning servers will be allowed to register with the CMTS.

Problems with registration state almost always point to a configuration file error. Make sure the modem and the CMTS both support the settings in the configuration file. Make sure the CMTS allows the creation of class of service profiles or use a profile created by the CMTS. Check the authentication strings in the CMTS cable interface configuration and the configuration file.

## Establish Privacy State

```
MAC State --->>> 'establish_privacy_state'
```

The modem must negotiate baseline privacy with the CMTS through the Baseline Privacy Key Management protocol, if all of the following are true:

- the modem software supports baseline privacy,
- the class of service is a privacy enabled profile, and
- baseline privacy settings are present in the configuration file.

If errors occur in this state, the likely causes are configuration file misconfigurations. Be certain that both the CM and the CMTS support baseline privacy and are enabled in the interface configuration for the CMTS and the configuration file for the CM. Also check Appendix A of [BPKM] for valid option values.

Another possible error that can be encountered is that due to encryption export restrictions, some vendor modems may require the following command on the uBR in the interface configuration:

```
uBR(config-if)# cable privacy 40-bit-des
```



## Operational State

```
MAC State --->>> 'operational_state' cmWriteFlashFile("CM_BOOT", 0x8109180, 0x13e) by TID
0x83049b8 (tMACCtrl)
usrEraseSysFlash(1, 0x1e0900, 0x13e) by TID 0x83049b8 (tMACCtrl)
```

If registration and baseline privacy negotiation (if required) succeed, the modem is operational and is ready to pass traffic.

A modem may make it to operational state but not remain in operational state. This could be caused by sync loss or DHCP lease renewal failure, just to name a couple.

## Radio Frequency (RF) Issues

Two-way digital data signals are more susceptible than one-way signals to stresses in the condition of the HFC network. Degradation in video signal quality might not be noticed, but when two-way digital signals share the network with video signals, digital signals might be hampered by the following types of network variations:

- **Impulse and electrical signal ingress**---Noise can enter the network from electrical sources within a home, such as hair dryers, light switches, and thermostats; or from high-voltage lines that run near CATV cabling in the network. Areas of signal ingress can be located and repaired by implementing a signal leakage maintenance program.
- **Amplifier noise**---Amplifiers add noise to the HFC network that usually goes unnoticed in video signals. Improperly configured amplifiers will degrade digital data signals. The larger the network, the higher the probability of amplifier noise affecting the signals.
- **Ingress noise**---There are two types of ingress noise: broadband and narrowband. Broadband noise is generally concentrated below 10 to 15 MHz.

Sources of ingress noise include major appliances and CB and short-wave radios, which can interfere with frequencies anywhere between 3 and 65 MHz. Noise from sources such as amateur radio transmissions, citizen band radios, or high-power shortwave broadcast signals are often picked up by cabling and equipment on the network.



### Note

Some HFC equipment will pass 3-MHz signals, which can overload the return path.

- **Noise funneling**---The upstream data path to the headend is susceptible to picking up noise and interference from the entire network and all upstream noise ultimately ends up at the headend. This effect is known as noise funneling because of the cumulative nature of the noise from anywhere on the network that becomes concentrated at the headend. As a network serviced by a single RF receiver increases in size, the probability of noise funneling also increases.
- **Variable transmit levels**---Signal loss over coaxial cable is affected by temperature. This can cause variations of 6 to 10 dB per year.
- **Clipping**---The lasers in fiber-optic transmitters can stop transmitting light (clipping) when input levels are excessive. Excessive input levels introduce bit errors in both the upstream and downstream transmissions. If a laser is overdriven as briefly as a fraction of a second, clipping can occur.

For example, if your headend overdrives the fiber-optic lasers, in either the upstream or downstream path, clipping can occur. Fiber-optic clipping leads to damaged signal integrity. In minor doses, this signal damage is not immediately visible on an analog video signal, but it can completely disrupt the digital transmission path. (That is, digital signals are more sensitive to clipping than analog signals and will more readily display the negative effects of laser clipping.)

If a digital signal employing forward error correction (FEC) is near its impairment limit, it is very susceptible to changes in signal level---on the order of 0.1 dB. If there is no amplitude margin available in the transmission path between the headend and any one Residential Gateway, the typical signal level variations of a properly functioning cable network (3 to 6 dB) can create intermittent service outages that are difficult to isolate.

Typical CATV measurement equipment, such as digital signal level meters, measure to an accuracy of +/-1 dB. However, some older analog meters only measure to an accuracy of +/-3 dB; therefore, maintaining 6 dB margins above the minimum levels can provide reliable long-term service.

## Troubleshooting RF Problems

Most customer RF problems are caused by wrong configurations in the HFC network, as opposed to a specific modem problem.

The MTAs should be easily installed, providing the following configuration guidelines and monitoring practices are followed:

- Signal levels are configured within the optimal ranges
- RF distortions are minimized or eliminated
- Amplifiers are not being overdriven
- Good HFC monitoring practices are in place
- Regular flap list monitoring is performed

## Troubleshooting Tools

There are several tools, including features of the Cisco uBR7200 series that can help you in troubleshooting RF problems:

- The Cisco uBR7200 series maintains a database of flapping Residential Gateways, known as the “flap list” (refer to [“Monitoring the Cisco uBR7246VXR Flap List”](#) in Chapter 7).
- Various show commands, such as **show cable modem** (refer to [“Troubleshooting the Cable Modem State”](#) in Chapter 7, for information on understanding the online state options of the MTAs, and using show and debug commands to troubleshoot problems)



### Caution

---

Be aware that running debug commands on a uBR (Universal Broadband Router) with more than a handful of modems may cause the uBR to halt the system in order to keep up with the debugging. In this case, all the modems may lose sync and debugging will be useless.

---

- A spectrum analyzer or a digital signal level meter can be used to measure the downstream IF and RF signals, so that you can compare measurements to recommended settings (refer to [“Measuring RF Signals”](#) later in this chapter, which also includes tables listing the recommended frequency settings).

# Measuring RF Signals

You can use a spectrum analyzer or a digital signal level meter to gather measurements of RF signals that can help you in identifying problems and making adjustments.

Measuring downstream IF and RF signals with a spectrum analyzer is normally done at setup time. However, if there are problems detected, it may be necessary to verify the quality of the IF and RF downstream signals. For example, it is possible, that after the initial setup, the uBR or upconverter may start to drift in frequency (because there is some sort of hardware problem), or the output level (that is, the RF power being produced) is too high or too low. The only way to verify these conditions would be with the spectrum analyzer.

## Measuring Downstream IF and RF

The following sections describe how to measure the downstream RF signal using the channel power option on a spectrum analyzer.

### Measuring the Downstream IF Signal at the Cisco uBR7200 Series

To connect a spectrum analyzer and measure the downstream intermediate frequency (IF) signal, perform the following steps:

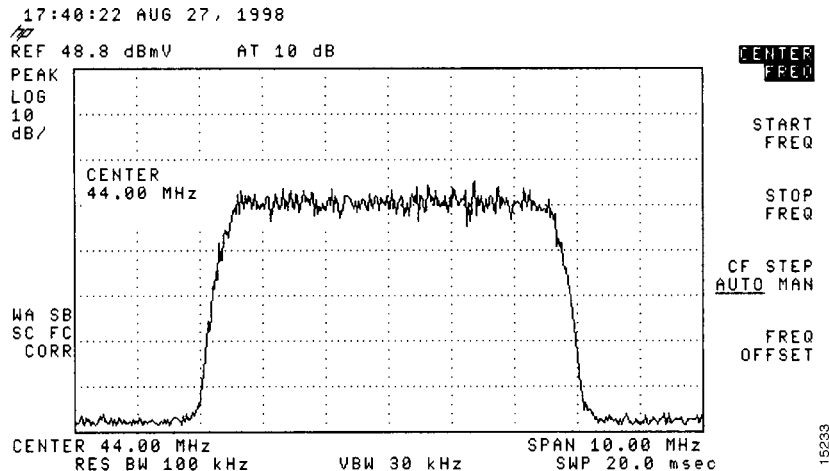


**Note**

Refer to the user guide that accompanied your spectrum analyzer to determine the exact steps required to use your analyzer to perform these measurements.

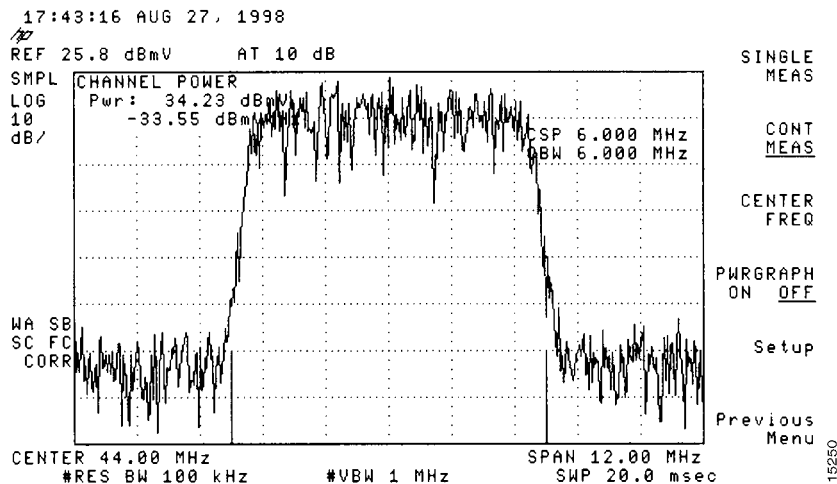
- Step 1** Connect a spectrum analyzer to the downstream connector on a cable modem card in a Cisco uBR7246.
- Step 2** Turn the power switch on the spectrum analyzer to the ON position.
- Step 3** Set the spectrum analyzer to view the downstream intermediate frequency (IF) signal with a center frequency of 44 MHz for a North American headend.
- Step 4** Set the span to 10 MHz. Your analyzer should display a signal similar to the one shown in [Figure 5-1](#).

**Figure 5-1 Viewing the Downstream IF Signal on a Spectrum Analyzer**



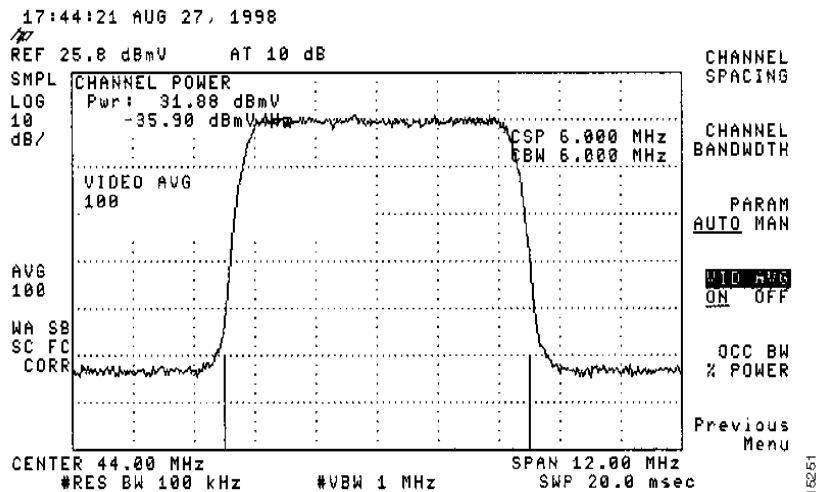
- Step 5** Measure the IF signal using the channel power option on your spectrum analyzer. Set your channel spacing and your channel bandwidth to 6 MHz. Your analyzer should display a signal similar to the one shown in [Figure 5-2](#).

**Figure 5-2 Measuring the IF Channel Power**



- Step 6** Select the video averaging feature. Your spectrum analyzer should display a signal similar to the one shown in [Figure 5-3](#).

**Figure 5-3 Measuring the IF Channel Power Using Video Averaging**



**Note**

The peak-to-valley flatness can be verified using the spectrum analyzer's video averaging feature. Be aware, however, that amplitude values registered while in the video averaging mode are typically around 2.5 dB below the actual channel power.

## Measuring the Downstream RF Signal at the Upconverter Output

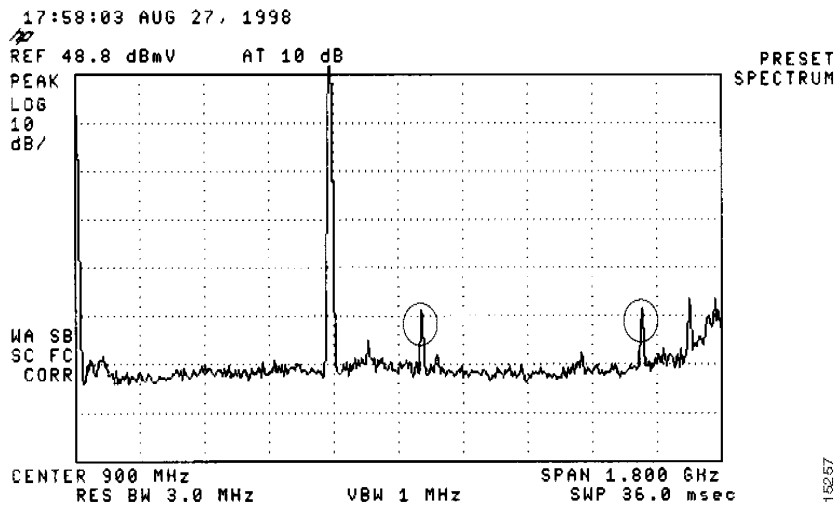
To measure the downstream radio frequency (RF) signal, perform the following steps:

- Step 1** Disconnect the spectrum analyzer from the cable modem card downstream connector. Connect the downstream output of the cable modem card to the upconverter input connector. Connect the spectrum analyzer to the RF output of the upconverter.

If your spectrum analyzer input is overloaded, you might see artifacts that are internally generated by the spectrum analyzer. The artifacts are circled on the analyzer trace shown in Figure 5-4. The sloping of the lines at the sides of the signal indicates a false reading.

Add attenuation to the input to the spectrum analyzer as necessary to correct the overload condition.

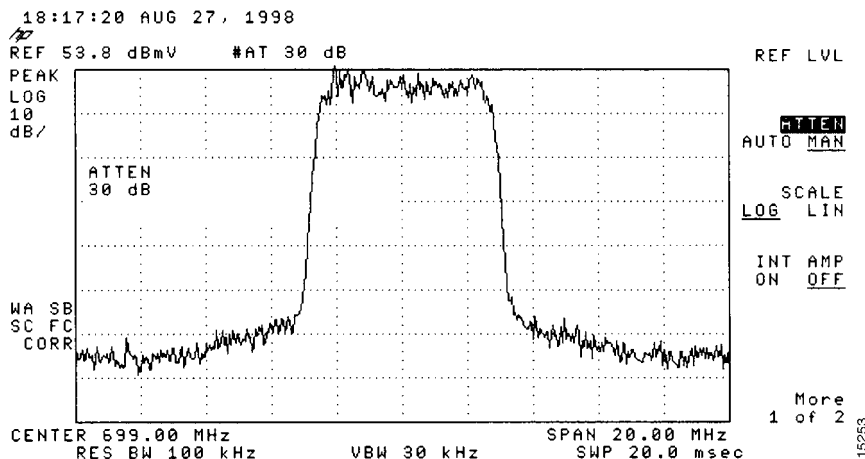
**Figure 5-4 Overloaded Spectrum Analyzer Input**



- Step 2** Set the input of the upconverter to a digital QAM signal and the output level to the manufacturer's recommended settings. Typical output amplitudes range from +50 to +58 dBmV.

- Step 3** Set the spectrum analyzer to view the RF signal at the center frequency you selected for your headend. In this example, the RF center frequency is 699 MHz. Set your span to 20 MHz. Finally, set your channel spacing and your channel bandwidth to 6 MHz. If you still have an overload condition, similar to that shown in Figure 5-4, add more attenuation to the input of the spectrum analyzer.

**Figure 5-5 Measuring the RF Signal at the Upconverter ---Overload Corrected with Attenuation**

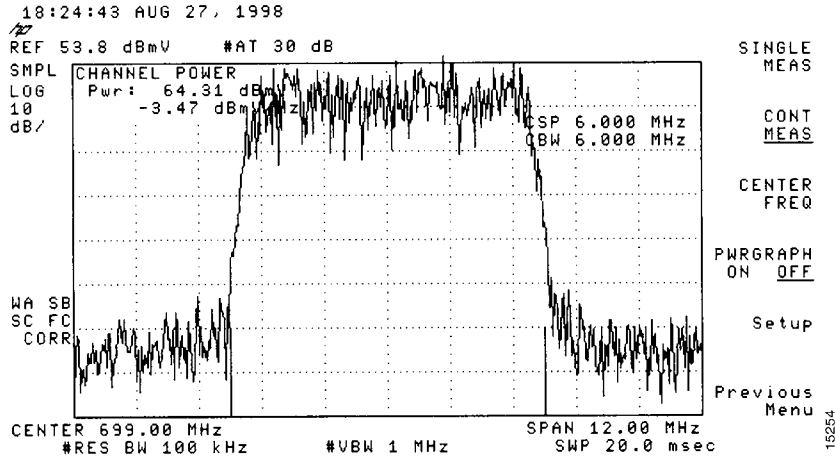


- Step 4** Change the spectrum analyzer settings to view the digital channel power. This setting will enable you to see if there is too much power on the upconverter output. In [Figure 5-6](#), the upconverter output is reading +64.31 dBmV, which is beyond the typical range of +50 to +58 dBmV.

**Note**

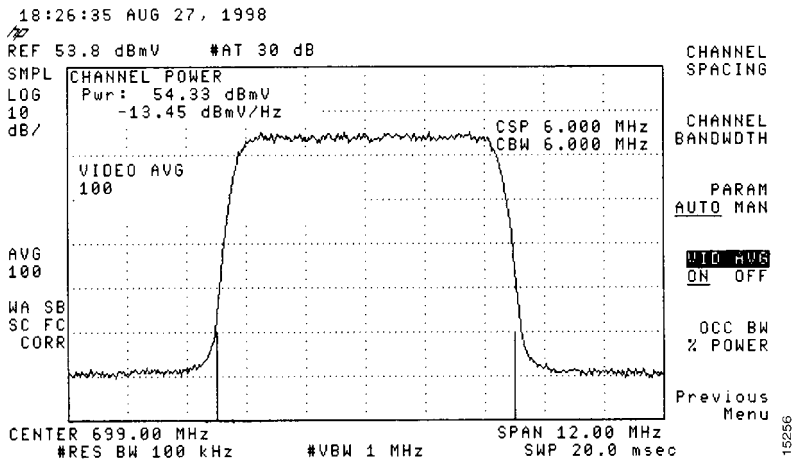
A spectrum analyzer might become overloaded and produce false readings (such as internally generated spurs) when measuring a signal at this amplitude.

**Figure 5-6 Measuring the RF Signal at the Upconverter Output---Upconverter Output Level Too High**



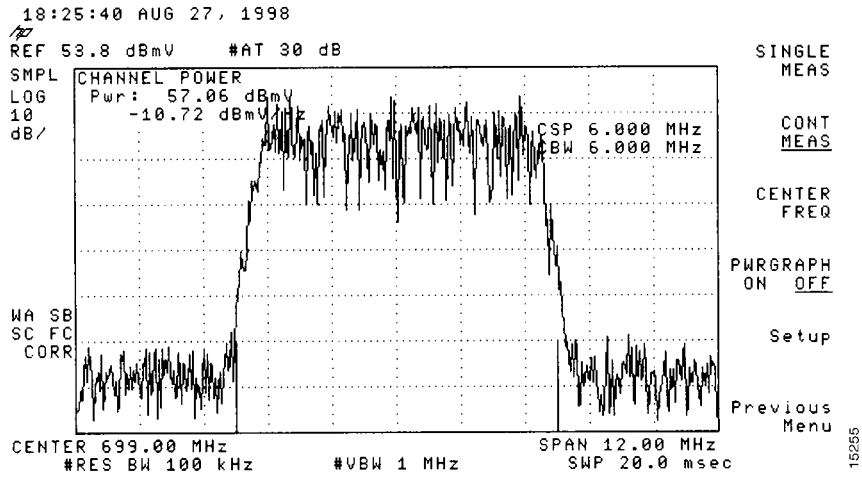
- Step 5** Adjust the power on the upconverter output to ensure that it is between +50 and +58 dBmV. In [Figure 5-7](#), the upconverter output is reading +57.06 dBmV, which is within the correct range.

**Figure 5-7 Measuring the RF Signal at the Upconverter Output Using Video Averaging**



- Step 6** Select the video averaging feature on the spectrum analyzer. The signal will become smoother and frequency response problems might become visible. Your analyzer will now display an RF signal similar to the one shown in [Figure 5-8](#).

Figure 5-8 Measuring the RF Signal at the Upconverter Output---Output Adjusted to Correct Range



**Note**

Any channel frequency response problems at the headend can impair network performance or prevent a cable modem on the HFC network from operating. The specified maximum peak-to-valley measurement from a Cisco cable modem card is +/-1.5 dB across 5.6 MHz. At the output of the upconverter, the maximum tilt should not exceed +/-1.5 dB across 5.6 MHz. If the tilt is greater than +/-1.5 dB across 5.6 MHz when measured, the upconverter might not be compatible with digital QAM signals, or the upconverter might be defective. Remember, however, that when using your spectrum analyzer in “video averaging” mode, amplitude accuracy adjustments must also be taken into consideration.

**Step 7**

Verify that your headend RF measurements match the recommended settings listed in [Table 5-2](#), RF Specifications. Make a copy of the table and record your headend settings in the last column as you verify them. This will assist in troubleshooting the Cisco uBR7246VXR installation later in the process.

## Comparing Measurements to Recommended Settings

The following tables display recommended settings to which you can compare your downstream measurements. [Table 5-1](#) displays typical RF downstream modulation; and [Table 5-2](#) displays DOCSIS cable downstream RF specifications.

**Table 5-1 Typical RF Downstream Modulation**

Downstream Bandwidth	64 QAM Data Throughput	256 QAM Data Throughput
6 MHz	27.0 Mbs	38.0 Mbs
8 MHz	27.0 Mbs	38.0 Mbs

**Table 5-2 DOCSIS Cable Downstream RF Specifications**

Specification	DOCSIS Specifications <sup>1</sup>	Minimum Settings <sup>2</sup>	Your Headend Settings
<b>System/Channel</b>			
RF channel spacing (bandwidth)	6 MHz	6 MHz	
Transit delay <sup>3</sup>	0.800 µsec	0.800 µsec	
Carrier to noise ratio	> 30 dB (64 QAM <sup>4</sup> ) <sup>5</sup> > 35 dB (256 QAM) <sup>5</sup>	>30 dB (64 QAM) <sup>5</sup> > 33 dB (256 QAM) <sup>5</sup>	
Carrier to ingress power ratio	> 35 dB	> 35 dB	
Composite triple beat distortion	< -50 dBc <sup>6</sup>	< -50 dBc	
Carrier to second order	< -50 dBc	< -50 dBc	
Cross-modulation level	< -40 dBc	< -40 dBc	
Amplitude ripple	0.5 dB in 6 MHz	0.5 dB in 6 MHz	
Group delay	75 ns <sup>7</sup> in 6 MHz	75 ns in 6 MHz	
Micro reflections bound for dominant echo	-10 dBc @ < 0.5 µsec -15 dBc @ < 1.0 µsec -20 dBc @ < 1.5 µsec -30 dBc @ < 1.5 µsec	-10 dBc @ < 0.5 µsec -15 dBc @ < 1.0 µsec -20 dBc @ < 1.5 µsec -30 dBc @ < 1.5 µsec	
Carrier hum modulation	< -26 dBc (5%)	< -26 dBc (5%)	
Burst noise	< 25 µsec	< 25 µsec	
Seasonal/diurnal signal level variation	8 dB	8 dB	
Signal level slope (50 to 750 MHz)	16 dB	16 dB	
Maximum analog video carrier level	+17 dBmV	+17 dBmV	
Minimum analog video carrier level	-5 dBmV	-5 dBmV	
<b>Digital Signal Levels</b>			
From headend	-15 to +15 dBmV	-15 to +15 dBmV	
Signal as relative to adjacent video signal	-6 or -10 dBc	-6 or -10 dBc	

<sup>1</sup> DOCSIS specifications are baseline settings for an DOCSIS-compliant, two-way data-over-cable network.

<sup>2</sup> Minimum settings are slightly different than the DOCSIS settings to account for cable network variations over time and temperature. Using these settings should increase the reliability of DOCSIS-compliant, two-way data-over-cable networks.

<sup>3</sup> Transit delay is defined as the “round trip” from the cable headend to the furthest customer and back.

<sup>4</sup> QAM = Quadrature Amplitude Modulation: a method of modulating digital signals onto a radio-frequency carrier signal involving both amplitude and phase coding.

<sup>5</sup> These settings are measured relative to the digital carrier. Add 6 or 10 dB, as determined by your company's policy and derived from the initial cable network setup, relative to the analog video signal.

<sup>6</sup> dBc = decibels relative to carrier.

<sup>7</sup> ns = nanoseconds.



## Measuring Upstream RF Signals

To measure the upstream RF signal, perform the following steps (this procedure is known as the “Zero Span Method”, which is described in greater detail in “Connecting and Configuring the Cable Headend” available on Cisco Connection Online):

- 
- Step 1** Connect the spectrum analyzer to the upstream signal from your cable network at the combiner where all the cable modems connect.
  - Step 2** Set the analyzer to view the upstream with a center frequency to match the configuration on the CMTS.
  - Step 3** Set the span to 0 MHz.
  - Step 4** Set the bandwidth and video channel bandwidth to 3 MHz. Do extended pings.
  - Step 5** Set the sweep value to 80 micro sec. Push the sweep button, manual, 80, then usec.
  - Step 6** Activate the trigger line between the highest and lowest portions of the signal. Do this by pushing the trig button, video button, and turn dial down appropriately.
  - Step 7** Adjust the amplitude so the upper portion of the RF signal is on the top graticule of the display grid and reset the trigger line accordingly.
- 

## Troubleshooting Slow Performance

There are a number of issues that can affect the performance and speed of cable modems in a DOCSIS network. This section addresses the major causes of slow throughput from the perspective of a cable service provider.

This section describes how to accurately determine what kinds of throughput levels an end user is achieving and how to make sure that the performance being measured is that of the cable network, rather than that of the broader Internet.

This section does not discuss troubleshooting a complete loss of connectivity over the cable network or cable modems not coming online.

## Hardware and Software Versions

The information in this document is based on the software and hardware versions below.

- Software Release 12.1(9)EC for the Cisco uBR7246VXR CMTS product
- The information in this document is relevant for all other currently available releases of DOCSIS 1.0 based Cisco IOS® software for Cisco brand CMTS equipment.

## Determining Levels of Performance

The following sections describe how to accurately determine what level of performance is present.

## Measuring the Correct Parts of the Network

There are a number of ways to gauge the speed and performance of a network, however it is important to understand exactly what parts of the network are being tested. In the diagram below there are a number of components:

- The Hybrid Fiber Coax network between the end user and the CMTS
- The local CMTS network segment where the CMTS connects to the cable service provider's network
- The cable service provider's internal network
- The public Internet.

When you perform a speed test between two points, you are measuring the speed of all the network components between the two points.

For example, if you try to perform a speed test between the CPE and Server 3, which is connected to the Internet via a 128Kbps ISDN line, then you will never see speeds of greater than 128Kbps, even if the available bandwidth on the cable segment is greater than 128Kbps.

The most accurate way to measure the performance of the cable segment itself would be to perform a speed test between the CPE and Server 1 which is connected to the same network segment as the CMTS. This is because the only path data needs to travel over is the coaxial cable segment. The data must also travel across the local CMTS Network Segment as well, but it is presumed that this segment is of a high bandwidth (FastEthernet or greater) and does not have a high level of congestion.

If for some reason, no server can be connected to the local CMTS network segment, then the next most accurate way to test the performance of the cable segment would be to perform a speed test between the CPE and Server 2. This will be an accurate measurement as long as there are adequately high speed and uncongested links within the cable service provider's internal network between the CMTS and the CPE.

The most inaccurate way to determine the performance of the cable segment is to perform a speed test between the CPE and a server on the public Internet. This is because there may be congested links in the public Internet between the CPE and the server, or there may be very low speed links in the path between the CPE and the server on the Internet.

## Determining the Download and Upload Rate

It is very important to be able to get an objective measurement of exactly what levels of upload and download throughput are being achieved before any conclusions can be made about whether a performance problem exists in a DOCSIS network.

The easiest way to determine the speed at which uploads and downloads may be occurring is to upload or download a very large file via FTP or HTTP between a CPE device connected to a cable modem, and a server located somewhere behind the CMTS. Most FTP and HTTP clients are able to display the speed at which a download or an upload is occurring either during the transfer or once the transfer is complete. The transfer speed as seen as a result of the FTP or HTTP operation will typically be about 90% of the true total throughput attained. This is because the displayed FTP or HTTP transfer speed does not take into account extra IP and DOCSIS overhead that needs to travel between the CPE device and the CMTS.

There are more accurate methods of measuring throughput, such as using dedicated testing equipment like a Netcom Smartbits or IXIA packet generator, however these systems are not always readily available or easily connected to a production cable network. It is worth noting however that if throughput tests are being carried out in a lab environment then using a dedicated device will reveal much more information than the simple FTP or HTTP download test.

Note that the FTP or HTTP based upload and download test is only reliable for testing speeds of around 3Mbps or less. At higher speeds the processing power of the CPE device, Server or Network Interface Cards may become a limiting factor in the test. For testing speeds higher than about 3Mbps, dedicated data throughput testing equipment should be used.

In the following example, a simple FTP download and upload test is performed between a CPE device connected to a cable modem, and an FTP server on the cable service provider's network. The cable modem has downloaded a DOCSIS configuration file that allows a download speed of up to 256Kbps and an upload speed of up to 64Kbps. In this test a 3 Megabyte file has been placed on the FTP server at IP address 172.17.110.132. The user of the CPE device is given a username and password in order to be able to log into the FTP server so that they can download this file from the FTP server, and then upload it back to the FTP server. The command line FTP utility is used to perform the transfer. This utility is available in virtually all versions of Microsoft Windows and Unix.

A similar test could be conducted by having an http web server set up in the service provider's network and performing an http download.

```
C:\>ftp 172.17.110.132          ! Initiate the FTP session to the Server
Connected to 172.17.110.132.
220 Solaris FTP server (SunOS 5.6) ready.
User (172.17.110.132:(none)): anonymous      ! Enter the FTP server username
331 Guest login ok, send your complete e-mail address as password.
Password: user@samplenetwork.com.au        ! Enter the FTP server password.
230 User anonymous logged in.

ftp> dir                                ! View the contents of the current directory
200 PORT command successful.
150 ASCII data connection for /bin/ls (64.104.207.118,1282) (0 bytes).
total 74932
-rw-r--r--  1 root      other    3276800 Oct 10 19:31 cable.txt
                                     ! A 3M file that you can download.

226 ASCII Transfer complete.
ftp: 105 bytes received in 0.12 Seconds 2.46Kbytes/sec.
ftp> bi                                  ! Turn on Binary File transfer mode
200 Type set to I.
ftp> get cable.txt                       ! Retrieve the file cable.txt and wait for it to download.
200 PORT command successful.
150 Binary data connection for cable.txt (192.168.1.13,3154) (3276800 bytes).
226 Binary Transfer complete.
ftp: 3276800 bytes received in 111.35Seconds 29.43Kbytes/sec.
                                     ! Download complete. It seems that the
                                     ! download occurred at 29.43Kbytes/sec
                                     ! which equals 235Kbits/sec. This is about
                                     ! 90% of the allowed 256Kbps download rate
                                     ! for the modem being tested.

ftp> put cable.txt                        ! Begin uploading the file. You need to make
                                     ! sure you have the correct access in order to
                                     ! upload a file to the FTP server or you may
                                     ! get an access-denied error.

200 PORT command successful.
150 Binary data connection for cable.txt (192.168.1.13,3157).
226 Transfer complete.
ftp: 3276800 bytes sent in 432.49Seconds 7.58Kbytes/sec.
                                     ! Upload Complete. Here you see the upload
                                     ! occurred at 7.58Kbytes/sec which is
                                     ! equivalent to 60.64Kbits/sec. This is
                                     ! about 90% of the allowed 64Kbps upload
                                     ! rate for the modem being tested.

ftp> quit                                ! Exit the FTP client application.
221 Goodbye.
```

While the FTP transfer is occurring, it is possible to monitor the progress of the test on the CMTS using the show interface cable X/Y sid Z counters command where cable X/Y is the cable interface the modem under test is connected to, and Z is the Service ID (SID) number of the modem under test. This command shows how many bytes are being transferred from or to a particular cable modem. Let's say that the CPE you are testing is behind a cable modem with MAC address 0001.9659.4461.

First you need to find the SID number of the modem you're testing by using the show cable modem command. In this case the SID of the cable modem is 5.

```
uBR7246-VXR# show cable modem 0001.9659.4461
Interface   Prim Online   Timing Rec   QoS CPE IP address   MAC address
      Sid  State      Offset Power
Cable3/0/U0 5   online      1996    0.25  5   2   10.1.1.24      0001.9659.4461
```

While the download or upload is progressing you clear all the packet counters on the CMTS back to zero using the clear counters command. At the exact same time as you clear the counters, you start a stopwatch or timer.

```
uBR7246-VXR# clear counters           ! Reset packet counter to zero.
Clear "show interface" counters on all interfaces [confirm]   ! Start the stopwatch when
you hit Enter.
```

After the stopwatch or time reads exactly one minute execute the show interface cable X/Y sid Z counters command. You may wish to type the command first and then hit enter at exactly when your timer indicates one minute. Naturally you can perform the test over a longer or a shorter period. The longer the test period, the more accurate the result, however make sure that the download or upload does not finish before your stopwatch timer reaches the specified time otherwise your measurement will be inaccurate.

```
uBR7246-VXR# show interface cable 3/0 sid 5 counters      ! Hit enter when stopwatch is at
exactly one minute.
Sid  Inpackets  Inoctets  Outpackets  Outoctets  Ratelimit  Ratelimit
      BWReqDrop  DSPktDrop
5    4019      257216   3368        1921488   0          149
uBR7246-VXR#
```

In this case you were testing download speed. The output of the show interface cable X/Y sid Z counter command indicates that over a period of one minute, 1,921,488 bytes were downloaded by the cable modem. Converting 1,921,488 bytes into bits you get:

8 bits per byte \* 1,921,488 bytes = 15,371,904 bits. Then, to find the download rate in bits per second, you divide this total number of bits downloaded by the time it took to download them in seconds.

15,371,904 bits / 60 seconds = 256 Kbps The download rate in this example is shown to be approximately 256 Kbps, which happens to be the allowed download rate for the cable modem under test.

In order to look at the upload speed using the show interface cable X/Y sid Z counter command, the Inoctets column should be used to determine the number of bytes sent in the upstream direction from the cable modem.

See the *Cisco Cable Modem Termination System Command Reference* for more information about the show interface cable X/Y sid <Z> counters command.

## Potential Reasons for Poor Performance

This section describes the common reasons for slow performance and suggested resolutions, including:

- Performance being restricted by the limits in the DOCSIS configuration file
- Bursty or inconstant download performance caused by using a sub-optimal rate limiting scheme on the cable modem termination system (CMTS)
- Upstream and downstream channel congestion
- Backhaul network or Internet congestion
- Noise or errors on the cable plant
- Under powered end user customer premises equipment (CPE) equipment

Each of these individually or in combination can affect throughput and performance in a cable network.

## Restrictions in DOCSIS Configuration File

The first piece of information that needs to be gathered when troubleshooting slow cable modem performance is the prescribed class of service throughput limitations of the cable modem. When a cable modem comes online, it downloads a DOCSIS configuration file that contains operational limits for the cable modem, including the maximum upload and download rates. Under normal circumstances, the cable modem is not allowed to exceed these rates.

Initially you need to identify the MAC address of a cable modem having problems. Let's say you have a modem with MAC address 0050.7366.2223 that is having problems with slow throughput. You need to find out what class of service profile this cable modem is using by executing the show cable modem <mac-address> command as seen in the example below.

```
uBR7246-VXR# show cable modem 0050.7366.2223
Interface  Prim Online   Timing Rec   QoS CPE IP address   MAC address
          Sid  State      Offset Power
Cable3/0/U1 1   online    1548    0.75  5   0   10.1.1.10   0050.7366.2223
```

This cable modem has a QoS profile of 5. In order to find out what downstream and upstream rates this QoS profile corresponds to, you need to use the show cable qos profile <profile-number> command, where <profile-number> is the QoS profile you're interested in.

```
uBR7246-VXR# show cable qos profile 5
ID Prio Max      Guarantee Max      Max      TOS  TOS   Create  B   IP prec.
    upstream upstream downstream tx   mask value by   priv rate
    bandwidth bandwidth bandwidth burst
5   0   64000    0      256000  1600  0x0  0x0  cm    no   no
```

The QoS profile 5 corresponds to a service providing 256Kbps in the downstream and 64Kbps in the upstream. Any CPE connected to cable modems using QoS profile 5 will not be able to exceed these limits. The QoS profile settings are determined by the contents of the DOCSIS configuration files downloaded by cable modems from the provisioning system's TFTP server, therefore QoS profile 5 in your system may not be the same as QoS profile 5 in the example shown above.

If an end user's download and upload performance correlate with the limits shown in their QoS profile, then they are getting the Class of Service and throughput levels that the cable modem has been provisioned and configured for. The only way to increase the upload and download throughput is to change the DOCSIS configuration file being downloaded by the cable modem to one that has higher throughput limits. See the document entitled Building DOCSIS 1.0 Configuration Files Using Cisco DOCSIS Configurator (registered customers only) for detailed instructions on how to create or modify a DOCSIS configuration file.

## Using a Sub-optimal Method for Rate Limiting

When an end user is trying to download data from the Internet at a rate greater than their cable modem's DOCSIS configuration file allows, the CMTS must rate limit the traffic being sent to that user to ensure that the user does not consume more than their allowed share of bandwidth.

Similarly, when an end user tries to upload or send data to the Internet at a rate greater than what the DOCSIS configuration file allows, the cable modem itself should stop the excess traffic from traveling over the cable segment to the CMTS. If the cable modem, for some reason, fails to perform upstream rate limiting properly then the CMTS will explicitly forbid the cable modem from transmitting at higher than the allowed rate. This behavior on the CMTS is to ensure that even a cable modem with "hacked" characteristics is unable to subvert the Service Provider assigned upload rate limits.

The default rate limiting scheme used by the CMTS monitors the rate of traffic to or from each cable modem over every one second period. If the cable modem sends or receives more than its per second quota in less than a second, then the CMTS will not allow any more traffic to flow to that cable modem for the rest of the second.

As an example, let's say you have a cable modem with a QoS profile allowing a download rate of 512Kbps. If the cable modem downloads 512 kilobits (64 kilobytes) within the first half of a second, then for the next half of the second, the cable modem will not be allowed to download anything. This type of rate limiting behavior may have the effect of a bursty download pattern that seems to stop and start every second or two.

The best downstream rate limiting scheme to use is the token bucket rate limiting algorithm with traffic shaping. This rate limiting scheme has been optimized to allow for a smooth web browsing experience at a steady rate, while at the same time ensuring that end users are not allowed to exceed the prescribed download rate as specified in the DOCSIS configuration file.

The way this scheme works is to measure the rate at which a cable modem is downloading or uploading data each time a packet is sent to or from the cable modem. If sending or receiving the packet in question would cause the modem to exceed its allowed transfer rates then the packet is buffered or cached in CMTS memory until the CMTS can send the packet without exceeding the downstream bandwidth limit. It should be noted however that if the downstream traffic rate consistently exceeds the allowed downstream rate for the cable modem, then packets will eventually be dropped.

By using this smoother method of rate limiting and shaping, most TCP based Internet applications such as HTTP web browsing and FTP file transfers will operate much more smoothly and efficiently than when using the default rate limiting scheme.

The token-bucket rate limiting with traffic shaping scheme can be enabled on the downstream path on a cable interface by issuing the following cable interface configuration command:

```
uBR7246-VXR(config-if)# cable downstream rate-limit token-bucket shaping
```



### Note

It is highly recommended that you enable token-bucket shaping on your CMTS. This command is supported as of IOS release 12.0(5)T1 and 12.1(1)EC1.

The token-bucket with traffic shaping scheme can also be applied to upstream ports, however, since it is the responsibility of the cable modems to perform upstream rate limiting, the upstream rate limiting scheme applied to the CMTS will normally not have any impact on the performance of a network.

```
uBR7246-VXR(config-if)# cable upstream 0 rate-limit token-bucket shaping
```

See the *Cisco Cable Modem Termination System Command Reference* for more information about the cable downstream rate-limit and cable upstream Z rate-limit commands.

You can view how severely the CMTS is rate limiting traffic to a particular cable modem by using the `show interface cable X/Y sid <Z> counters` command, where cable X/Y is the cable interface which the cable modem is connected to, and Z is the SID number of the modem being observed. This command shows the number of times the CMTS has dropped a downstream packet or refused to allow an upstream packet due to the modem exceeding its allowed throughput limits. If no value is specified for Z then counter information for all cable modems connected to interface cable X/Y will be displayed.

```
uBR7246-VXR# show interface cable 3/0 sid 5 counters
Sid  Inpackets  Inoctets  Outpackets  Outoctets  Ratelimit  Ratelimit
                                           BWReqDrop  DSPktDrop
5     150927    9662206   126529     72008199  0          5681
```

The `Ratelimit DSPktDrop` field shows how many times the CMTS has dropped packets destined for the cable modem due to the modem trying to exceed its allowed downstream throughput.

The `Ratelimit BWReqDrop` field shows how many times the CMTS has refused to let a cable modem send a packet in the upstream path due to the modem trying to exceed its allowed upstream throughput. In most circumstances this counter should always remain at 0. If it rises significantly above zero then it may be that the cable modem being observed is not performing upstream rate limiting properly.

It should be noted that the values displayed by the `show interface cable X/Y sid Z counters` command may be reset to zero by issuing the `clear counters` command as seen in the example below.

```
uBR7246-VXR# show interface cable 3/0 sid counters
Sid  Inpackets  Inoctets  Outpackets  Outoctets  Ratelimit  Ratelimit
                                           BWReqDrop  DSPktDrop
1     7          1834     7           1300       0          0
2     2052       549150   0           0          0          0
3     2          1244     2           708        0          0
4     2          1244     2           714        0          0
5     160158    10253220 134294     76423270  0          6023
6     2          1244     2           712        0          0
7     9          1906     4           858        0          0
9     6          1076     3           483        0          0
12    616       165424   0           0          0          0
uBR7246-VXR# clear counters
Clear "show interface" counters on all interfaces [confirm] <press enter here>
uBR7246-VXR# show interface cable 3/0 sid counters
Sid  Inpackets  Inoctets  Outpackets  Outoctets  Ratelimit  Ratelimit
                                           BWReqDrop  DSPktDrop
1     0          0         0           0          0          0
2     0          0         0           0          0          0
3     0          0         0           0          0          0
4     0          0         0           0          0          0
5     111       7104     92          52728     0          6
6     0          0         0           0          0          0
7     0          0         0           0          0          0
9     0          0         0           0          0          0
12    0          0         0           0          0          0
```

See the *Cisco Cable Modem Termination System Command Reference* for more information about the `show interface cable X/Y sid <Z> counters` command.

## Upstream Channel Congestion



### Note

The measures discussed in this section will not significantly increase the performance of an already uncongested network.

The upstream channel is normally the most precious resource in a cable network. At present, most cable service providers use a 1.6MHz channel width and Quadrature Phase Shift Keying (QPSK) modulation in the upstream path. This equates to approximately 2.5Mbps in total available upstream bandwidth for all users connected to the one upstream channel. It is important to ensure that the upstream channel does not become over utilized or congested, otherwise all users on that upstream segment will suffer poor performance.

The upstream utilization for a particular upstream port can be obtained by executing the CMTS command `show interface cable X/Y upstream <Z>`, where cable X/Y is the downstream interface number and Z is the upstream port number. If Z is omitted then information for all upstreams on interface cable X/Y will be displayed.

See the *Cisco Cable Modem Termination System Command Reference* for more information about the `show interface cable X/Y upstream <Z>` command.

```
uBR7246-VXR# show interface cable 6/0 upstream 0
Cable6/0: Upstream 0 is up
Received 71941 broadcasts, 27234 multicasts, 8987489 unicasts
0 discards, 140354 errors, 0 unknown protocol
9086664 packets input, 4394 uncorrectable
122628 noise, 0 microreflections
Total Modems On This Upstream Channel : 359 (354 active)
Default MAC scheduler
Queue[Rng Polls] 0/64, fifo queueing, 0 drops
Queue[Cont Mslots] 0/104, fifo queueing, 0 drops
Queue[CIR Grants] 0/64, fair queueing, 0 drops
Queue[BE Grants] 0/64, fair queueing, 0 drops
Queue[Grant Shpr] 0/64, calendar queueing, 0 drops
Reserved slot table currently has 0 CBR entries
Req IEs 64609697, Req/Data IEs 0
Init Mtn IEs 521851, Stn Mtn IEs 569985
Long Grant IEs 2781600, Short Grant IEs 2067668
Avg upstream channel utilization : 18%
Avg percent contention slots : 77%
Avg percent initial ranging slots : 2%
Avg percent minislots lost on late MAPs : 0%
Total channel bw reserved 37858000 bps
CIR admission control not enforced
Admission requests rejected 0
Current minislot count : 7301855 Flag: 0
Scheduled minislot count : 7301952 Flag: 0
```

On the upstream port seen in the example, the upstream utilization is currently 18% and there are 359 modems connected to this upstream.

If upstream channel utilization is consistently above 75% during the peak usage time then end users will begin to suffer issues like latency, slower "ping" times and a generally slower Internet experience. If upstream channel utilization is constantly above 90% during the peak usage time then end users will be experiencing an extremely poor level of service because a large portion of end user's upstream data will have to be delayed or discarded.

Upstream channel utilization will change during the day as different users have an opportunity to use their cable modem, so it is important to monitor the upstream utilization during the busiest times of the day rather than at low usage times.



Ways of relieving upstream congestion include:

- Reducing the number of cable modems per upstream - If there are too many cable modems connected to a particular upstream, or if users on a particular upstream are heavy users of upstream bandwidth, then the best solution is to move some users on the congested upstream port to an under utilized upstream port, or to a completely new upstream port. This would typically be accomplished by moving a fiber node from one upstream combining group to another, or splitting an upstream combining group into two separate combining groups. For more information refer to *What is the Maximum Number of Users per CMTS*.
- Increasing the upstream channel width - This involves a rigorous and thorough analysis of your upstream spectrum in order to find a wide enough band with adequate Signal to Noise Ratio characteristics to support the increased channel width. The upstream channel width should not be changed without careful planning because this change can potentially affect other services in your cable network. The upstream channel width may be changed by using the cable interface command cable upstream Z channel-width <new-channel-width> where Z is the upstream port number and new-channel-width is one of 200000, 400000, 800000, 1600000 (the default) or 3200000.

```
uBR7246-VXR(config-if)# cable upstream 0 channel-width 3200000
```

See the *Cisco Cable Modem Termination System Command Reference* for more information about the show interface cable X/Y upstream <Z> command.

- Changing the upstream digital modulation scheme to 16-QAM - Once again, this requires a rigorous and thorough analysis of the upstream spectrum in order to verify whether there is a frequency band in the upstream available that can support 16-QAM modulation. If this analysis is not performed properly then there is a risk that performance will be further decreased or a complete upstream outage may occur. The upstream modulation scheme may be changed by creating an upstream modulation profile that uses 16-QAM modulation and then applying that to an upstream port. An example follows

```
uBR7246-VXR(config)# cable modulation-profile 2 mix      ! Create an optimized
                                                         ! 16-qam/qpsk modulation
                                                         ! profile.

uBR7246-VXR(config)# interface cable 6/0
uBR7246-VXR(config-if)# cable upstream 0 modulation-profile 2
```

See the *Cisco Cable Modem Termination System Command Reference* for more information about the cable modulation-profile and cable upstream Z modulation-profile commands. See also *Configuring Cable Modulation Profiles* on Cisco's Cable Modem Termination Systems.

- Reducing the allowed upstream throughput per cable modem - By reducing the Maximum Upstream Transmit Rate in the appropriate DOCSIS configuration files, cable modem users will not be able to transmit at as high a rate in the upstream direction and upstream congestion will be relieved. The negative aspect of this course of action is obviously that cable modem users would be limited to a slower class of service.

See *Building DOCSIS 1.0 Configuration Files Using Cisco DOCSIS Configurator* (registered customers only).

## Downstream Channel Congestion

The downstream channel has significantly more bandwidth to share than an individual upstream channel, therefore the downstream is not usually as subject to congestion as the upstream. However more users will typically be sharing a downstream channel than any single upstream channel so if the downstream channel becomes congested then all users connected to the downstream segment will experience reduced performance.

Table 5-3 shows the total available downstream bandwidth associated with the four possible downstream modulation schemes available in DOCSIS networks.

**Table 5-3 Available Downstream Bandwidth for Selected Modulation Schemes**

Downstream Modulation Scheme	Available Downstream Bandwidth
64-QAM North American DOCSIS	27 Mbps
256-QAM North American DOCSIS	38 Mbps
64-QAM Euro DOCSIS	38 Mbps
256-QAM Euro DOCSIS	54 Mbps

The majority of DOCSIS cable networks currently deploy 64-QAM North American DOCSIS and therefore have 27Mbps available per downstream channel.

Downstream channel utilization can be determined by executing the show interface cable X/Y command, where cable X/Y is the cable interface being observed. The displayed output rate in bits per second should be compared to the available downstream bandwidth as seen in the table above.

In the following example, an interface using North American DOCSIS and 64-QAM digital modulation is analyzed.

```
uBR7246-VXR# show interface cable 3/0
Cable3/0 is up, line protocol is up
  Hardware is BCM3210 ASIC, address is 0005.5fed.dca4 (bia 0005.5fed.dca4)
  Internet address is 10.1.1.1/24
  MTU 1500 bytes, BW 27000 Kbit, DLY 1000 usec,
    reliability 255/255, txload 9/255, rxload 5/255
  Encapsulation MCNS, loopback not set
  Keepalive not set
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters 00:45:01
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 587000 bits/sec, 228 packets/sec
  5 minute output rate 996000 bits/sec, 239 packets/sec
    85560 packets input, 8402862 bytes, 0 no buffer
    Received 1013 broadcasts, 0 runts, 0 giants, 0 throttles
    247 input errors, 35 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
    65912 packets output, 38168842 bytes, 0 underruns
    0 output errors, 0 collisions, 0 interface resets
    0 output buffer failures, 0 output buffers swapped out
```

The first component of this output to note is the Bandwidth of the interface indicated by the BW parameter. In IOS releases 12.1(8)EC and later, this value is automatically adjusted according to the downstream modulation scheme and version of DOCSIS being used. In revisions earlier than 12.1(8)EC, this value must be manually configured using the cable interface command bandwidth <bandwidth-in-kilo-bits-per-second> otherwise it will remain at the default value of 27000 Kbps.

The second component to note is the transmission load as indicated by the txload parameter. This parameter gives a metric out of 255 where 0/255 means that no traffic is flowing in the downstream direction to 255/255 which means that data is traveling in the downstream at the maximum possible rate (in this case at 27000 Kbps). If this parameter is consistently running at greater than approximately 75% during the peak usage time (for example, greater than 191/255) then end users will start to experience slower Internet access and higher latency.

The third component to note is the output rate which shows the average downstream throughput rate in bits per second. If this number consistently exceeds approximately 75% of the available downstream bandwidth during the peak usage time then end users will start to experience slower Internet access and higher latency.

By default, these statistics are calculated over a five minute moving average. (See Definition of 'bits/sec' from 'sh int' for details of how the average is calculated.) The period over which this average is calculated can be reduced to as little as 30 seconds by issuing the cable interface command `load-interval 30`. By lowering this period to 30 seconds, a more accurate and up to date value will be calculated for each of the parameters discussed in this section.

Downstream channel utilization will change during the day as different users have an opportunity to use their cable modem so it is important to monitor the downstream utilization during the busiest times of the day rather than at low usage times.

Ways of relieving downstream congestion include

- Reducing the number of cable modems per downstream - If there are too many cable modems connected to a particular downstream, or if users on a particular downstream are heavy users of downstream bandwidth, then the best solution is to move some users on the congested downstream channel to another downstream channel. This would typically be accomplished by splitting a group of downstream fiber nodes associated with the downstream into two separate groups and assigning each of the new groups separate downstream channels. See also [What is the Maximum Number of Users per CMTS](#).
- Changing the downstream digital modulation scheme to 256-QAM - This action requires a rigorous and thorough analysis of the downstream spectrum in order to verify whether your network can support a 256-QAM signal. If this analysis is not performed properly then there is a risk that performance will be further decreased or a complete downstream outage may occur. The downstream modulation scheme may be changed by issuing the cable interface command as seen below.

```
uBR7246-VXR(config-if)# cable downstream modulation 256qam
```

See the *Cisco Cable Modem Termination System Command Reference* for more information about the cable downstream modulation command.

- Reducing the allowed downstream throughput per cable modem - By reducing the Maximum Downstream Transmit Rate in the appropriate DOCSIS configuration files, cable modem users will not be able to download at as high a rate in the downstream direction and downstream congestion will be relieved. The negative aspect of this course of action is obviously that cable modem users would be limited to a slower class of service. See [Building DOCSIS 1.0 Configuration Files Using Cisco DOCSIS Configurator](#) (registered customers only).

**Note**

The measures discussed in this section will not significantly increase the performance of an already uncongested network.

## Backhaul Network or Internet Congestion

In some cases, performance problems may not be a result of issues on the cable plant or the CMTS, but may be related to congestion or problems in the backhaul network that the CMTS uses to connect to the Internet, or within parts of the Internet itself.

The easiest way to determine if backhaul network congestion is a problem is to connect a workstation to the same network segment as the CMTS and try to browse the same web sites as end users behind cable modems are trying to reach.

If performance is still slow, then there is a performance problem in the network that is not related to the CMTS or the cable segment. If performance from the Local CMTS network segment is significantly better than for users connected to cable modems then you should focus your efforts back on the CMTS and the cable segment.

**Figure 5-9**

In the above network, if Server 1, which is connected to the same network segment as the CMTS, is getting slow performance when browsing the Internet, then the source of the problem is not the CMTS. Instead, the bottleneck or performance issue will be somewhere else. In order to determine where the problem is, performance tests would have to be carried out between Server 1 and various other servers within the Internet Service Provider network and the public Internet.

## Noise and Errors on the Cable Plant

If there is an excessive amount of noise or ingress in a cable network then packets between cable modems and the CMTS can be corrupted and lost. This can lead to a significant degradation in performance.

Aside from a degradation in performance and throughput, some of the prime indicators of noise or RF issues include

- Cable modems sporadically dropping offline or getting stuck in the init(r1) or init(r2) states.
- A low estimated SNR as seen in the output of a show controller cable X/Y upstream Z, where cable X/Y is the cable interface being observed and Z is the upstream port being observed. The DOCSIS specification requires a CNR of at least 25dB for all upstream signals. This equates to an SNR of approximately 29dB. The Cisco CMTS is able to coherently detect QPSK upstream signals at much worse SNR levels, however all cable service providers should strive to meet the DOCSIS CNR requirements in their network. A sample show controller cable X/Y upstream Z output is shown below.

```
uBR7246-VXR# show controller cable 6/0 upstream 0
Cable6/0 Upstream 0 is up
Frequency 25.200 MHz, Channel Width 1.600 MHz, QPSK Symbol Rate 1.280 Msps
Spectrum Group is overridden
SNR 28.6280 dB
Nominal Input Power Level 0 dBmV, Tx Timing Offset 6446
Ranging Backoff automatic (Start 0, End 3)
Ranging Insertion Interval automatic (102 ms)
Tx Backoff Start 0, Tx Backoff End 4
Modulation Profile Group 1
Concatenation is enabled
part_id=0x3137, rev_id=0x03, rev2_id=0xFF
nb_agc_thr=0x0000, nb_agc_nom=0x0000
Range Load Reg Size=0x58
Request Load Reg Size=0x0E
Minislot Size in number of Timebase Ticks is = 8
Minislot Size in Symbols = 64
Bandwidth Requests = 0x37EB54
Piggyback Requests = 0x11D75E
```

```

Invalid BW Requests= 0x102
Minislots Requested= 0x65B74A2
Minislots Granted = 0x65B74A2
Minislot Size in Bytes = 16
Map Advance (Dynamic) : 2809 usecs
UCD Count = 23068

```

In the example above, the estimated SNR reading is 28.628dB. This is adequate for QPSK upstream operation. Note that the SNR figure given in the output of this command is only an estimate and is no substitute for an SNR figure derived from a Spectrum Analyzer or other appropriate testing equipment.

See the *Cisco Cable Modem Termination System Command Reference* for more information about the show controller cable X/Y upstream Z command.

- A quickly incrementing number of Corr FEC and Uncorr FEC errors in the output of a show cable hop command. Corr FEC errors indicates data that was corrupted by upstream noise but was able to be recovered. Uncorr FEC errors indicate data that was corrupted by upstream noise and was not able to be recovered resulting in lost data and slower performance.

A sample output from the show cable hop command is show below.

```

uBR7246-VXR# show cable hop cable 3/0
Upstream      Port      Poll Missed Min      Missed Hop      Hop      Corr      Uncorr
Port          Status    Rate Poll   Poll   Poll   Thres Period  FEC      FEC
(ms) Count   Sample Pcnt  Pcnt  (sec)  Errors Errors
Cable3/0/U0  25.200 Mhz 34   * * * set to fixed frequency * * * 196      55
Cable3/0/U1  25.200 Mhz 34   * * * set to fixed frequency * * * 1655     160
Cable3/0/U2  25.200 Mhz 34   * * * set to fixed frequency * * * 76525   9790
Cable3/0/U3  25.200 Mhz 34   * * * set to fixed frequency * * * 501      77
Cable3/0/U4  admin down 34   * * * interface is down        * * * 0         0
Cable3/0/U5  admin down 34   * * * interface is down        * * * 0         0

```

In the example above, each active upstream port on cable 3/0 seems to have experienced packet loss due to noise. Upstream port 0 seems to be the least affected and upstream port 2 seems to be the most heavily affected. The important factor to note is how quickly the FEC Errors are incrementing rather than the total number of errors.

See the *Cisco Cable Modem Termination System Command Reference* for more information about the show cable hop command.

- A high number of "flap" events in the output of a show cable flap-list. The flap statistics that are most pertinent to possible RF or noise problems are the Miss column, which indicates missed ranging requests, and the P-Adj column which indicates rapidly varying upstream power levels.

A sample output from the show cable flap-list command is shown below.

```

uBR7246-VXR# show cable flap-list
MAC Address      Upstream      Ins  Hit  Miss  CRC  P-Adj  Flap  Time
0000.d025.1b99  Cable3/0/U0  23   58   30   0    *27    77   Oct 23 03:08:23
0002.ddfa.0aa5  Cable3/0/U1  5    518  1260 0    0      131  Oct 23 03:09:43
0001.e659.43bd  Cable3/0/U1  541  342  1467 0    0      746  Oct 23 03:09:17
0001.7659.44c7  Cable3/0/U1  0    694  0     0    1      1    Oct 23 01:44:23
0050.9366.22d3  Cable3/0/U1  0    708  0     0    1      1    Oct 23 01:38:14
0001.f659.44e7  Cable3/0/U1  0    701  0     0    1      1    Oct 23 02:25:11

```

In the example seen above, the cable modem with MAC Address 0000.d025.1b99 has had a number of P-Adj events. This would typically indicate a bad connection or a faulty reverse path amplifier. The cable modem with MAC Address 0002.ddfa.0aa5 has a large number of misses as compared to hits and therefore may be suffering from either downstream or upstream noise issues. The cable modem with MAC Address 0001.e659.43bd has a high number of insertions, which typically indicates a severe RF problem, or more likely a provisioning problem.

See the *Cisco Cable Modem Termination System Command Reference* for more information about the show cable flap-list command.

- Cable modems displaying a \* or a ! in the output of a show cable modem or show cable flap-list. A \* indicates a cable modem that is rapidly varying its upstream power levels. This is indicative of a poor connection to the cable plant, a faulty reverse path amplifier or rapidly changing cable plant attenuation due to temperature or other environmental effects. A ! indicates a cable modem that has reached its maximum upstream power level. This is indicative of too much attenuation between the cable modem and the CMTS, or a poor connection between the cable modem and the cable plant.

A sample output from the show cable modem command is shown below.

```
uBR7246-VXR# show cable modem
      Interface  Prim Online   Timing Rec   QoS CPE IP address   MAC address
              Sid  State   Offset Power
Cable3/0/U1  1   online  1549  !-1.00  5   0   10.1.1.10   005a.73f6.2213
Cable3/0/U0  2   online  1980   0.75  5   0   10.1.1.16   009b.96e7.3820
Cable3/0/U0  3   online  1981   *0.75  5   0   10.1.1.18   009c.96d7.3831
Cable3/0/U1  4   online  1924   0.25  5   0   10.1.1.24   000d.96c9.4441
Cable3/0/U1  5   online  1925   0.50  5   0   10.1.1.13   000e.96b9.4457
```

In the example seen above, the cable modem with MAC address 005a.73f6.2213 is transmitting at its maximum output power. This would result in that modem not being able to transmit at the correct level. Consequently this modem's upstream transmissions will not be heard as clearly as transmissions from other modems. The cable modem with MAC address 009c.96d7.3831 has a rapidly varying power output due to varying cable network attenuation.

See the *Cisco Cable Modem Termination System Command Reference* for more information about the show cable modem and show cable flap-list commands.

More details about identifying and resolving RF noise issues can be found in *Determining RF or Configuration Issues On the CMTS* and *Connecting and Configuring the Cable Headend*.

## High CPU Utilization on the CMTS

In some circumstances a Cisco CMTS can become overloaded due to a sub-optimal configuration, over utilization of certain management functions, or a very high number of packets being routed by the CMTS.

The best way to determine the CPU utilization of a Cisco CMTS is to execute the show process cpu command. The current CPU utilization is indicated on the first line of the output of the command.

In the lines of output shown below the first line, each process running on the CMTS is shown along with the portion of the CPU being used by that process. This section of the show process cpu output is useful for determining if one particular process or function is the cause of high CMTS CPU.

```
uBR7246-VXR# show process cpu
CPU utilization for five seconds: 45%/21%; one minute: 45%; five minutes: 31%
PID  Runtime(ms)  Invoked  uSecs   5Sec   1Min   5Min  TTY  Process
  1         12        9220     1     0.00%  0.00%  0.00%  0  Load Meter
  2      69816   18276677  3    21.79% 22.10%  9.58%  2  Virtual Exec
  3     36368     5556   6545     0.00%  0.06%  0.05%  0  Check heaps
  4         0         1         0     0.00%  0.00%  0.00%  0  Chunk Manager
  5         96      1436     66     0.00%  0.00%  0.00%  0  Pool Manager
  6         0         2         0     0.00%  0.00%  0.00%  0  Timers
  7         0         2         0     0.00%  0.00%  0.00%  0  Serial Backgroun
  8         0         1         0     0.00%  0.00%  0.00%  0  CMTS ping
  9     17020   101889   167     0.00%  0.00%  0.00%  0  EnvMon
 10         0         1         0     0.00%  0.00%  0.00%  0  OIR Handler
. . . . .
```

```

<snip>
. . . . .
89      3304      81013      40  0.00%  0.00%  0.00%  0 PIM Process
90       12       769       15  0.00%  0.00%  0.00%  0 CEF Scanner
92        0       385        0  0.00%  0.00%  0.00%  0 DHCPD Timer
93       40     13058        3  0.00%  0.00%  0.00%  0 DHCPD Database

```

In the example show above, the current CPU load on the CMTS is 45%/21%. This means that the total CPU utilization is at 45% of the capacity of the system. In addition 21% of the CPU is being used to service interrupts. This second figure typically equates to the portion of the CPU being used to route packets and switch traffic through the CMTS.

If the five minutes CPU utilization is consistently above 80% during the peak usage time in your system then end users may start to experience slower performance and increased latency. If the five minutes CPU utilization is constantly above 95% during the peak usage time in your network then you need to take urgent action to ensure that the CMTS will remain in a stable state.

Common strategies for reducing high CPU utilization on your CMTS include:

- Upgrading to release 12.1(9)EC or later, activating the global configuration command `ip cef`, and making sure that no interfaces on the CMTS have the command `no ip route-cache` configured. This typically leads to a 10 to 15 percent reduction in traffic related CPU utilization. Make sure that all of these steps are taken in conjunction.
- Making sure that SNMP management stations are not being too aggressive in polling the CMTS. This leads to a high CPU utilization in the IP SNMP process.
- Not running the `show tech` command several times in succession. This leads to an artificially high CPU utilization in the Virtual Exec Process.
- Making sure that no debugs are running on the CMTS.

For more information about High CPU utilization on Cisco Routers, including Cisco CMTS products, please refer to *Troubleshooting High CPU Utilization on Cisco Routers*.

## Under Powered or Misconfigured CPE Equipment

In many cases, the cause of slow access to a cable network is a problem in the end user's CPE equipment. If only one or a handful of users are experiencing slow throughput, and the rest of the user population are experiencing no problem, then this is a strong indication that there may be a unique problem within that user's environment.

- Under powered or overloaded CPE - If the end users complaining of difficulties are using antiquated CPE equipment, or equipment that may not be powerful enough to run their chosen operating system or Internet access software, then clearly, this end user will have difficulties. The only resolution if this is the case is for the end user to upgrade their CPE equipment.
- Firewall or performance measurement software - If the end user is running any firewall, network performance measurement or other similar software, then it would be a good troubleshooting step to have the user turn this software off to see if it has any effect on performance. Quite often these kinds of software can have a negative impact on performance.
- Misconfigured TCP/IP settings - Most service providers require that end users have their CPE equipment acquire an IP address, network mask, default gateway and DNS servers via DHCP. Check to make sure that any end users experiencing problems have their CPE devices configured to use DHCP to acquire all of these parameters.

If an end user claims to have none of the problems listed above then you should confirm that the end user is not exceeding their maximum download or upload rate as per the sections above.

## Conclusion

A DOCSIS cable network is a sophisticated network that requires proper planning and maintenance. Most performance issues in DOCSIS cable networks are a direct result of the proper planning and maintenance not being performed. In today's Internet access market, where there are a variety of broadband Internet access alternatives, it is vitally important that cable service providers quickly address any performance or congestion issues in their network before they become significant enough for end users to be noticeably affected and consequently consider an alternative means of broadband access.





## Troubleshooting MTAs

---

### Troubleshooting EMTA Provisioning

Provisioning PacketCable Embedded Media Terminal Adapters (EMTAs) is a relatively complex process; however, with the right tools and ‘tricks of the trade,’ getting EMTAs operational is a fairly straightforward process.

This chapter assumes that the Cisco Network Registrar (CNR) and Broadband Access Center for Cable (BACC) are both in use; however, much of the information would also apply for other deployments. Basic knowledge of CNR (scopes, policies, basic DNS zone setup, and record entry) and BACC (class of service, DHCP criteria, external files, and BACC directory structure) is also assumed.

For more information on the Cisco CNR, refer to [http://www.cisco.com/en/US/products/sw/netmgts/ps1982/prod\\_technical\\_documentation.html](http://www.cisco.com/en/US/products/sw/netmgts/ps1982/prod_technical_documentation.html).

For more information on the BACC, refer to <http://www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/baccable/cable26/index.htm>.

### Know The Basics

The PacketCable EMTA provisioning process consists of 25 steps, with several additional steps if secure NCS call signaling is to be used. To troubleshoot EMTAs, knowledge of these 25 steps, or having the ‘cheat sheet’ from the PacketCable provisioning specification (see below) is absolutely essential.

### The Architectural Elements

Before we get into the troubleshooting of EMTAs, you should be familiar with the following system components as described in the subsections that follow.

- [Embedded Media Terminal Adapter](#)
- [DHCP Server](#)
- [DNS Server](#)
- [Key Distribution Center](#)
- [PacketCable Provisioning Server](#)
- [Call Management Server](#)

## Embedded Media Terminal Adapter

The EMTA is a cable modem (CM) and a Media Terminal Adapter (MTA) in one box, with a common software image. The CM and MTA each has its own MAC-address and each performs DHCP to get its own IP address. The EMTA contains, at minimum, 2 certificates. One certificate is a unique MTA certificate, sent by the MTA to authenticate itself to the key distribution center (KDC). The other is a telephony root certificate used to verify the certificate sent by the KDC to the MTA. The KDC's certificate will be chained from the telephony root, therefore the telephony root must reside on the MTA to validate the authenticity of the KDC certificate. The MTA portion receives its own configuration file, which it uses to identify its controlling call agent, among other things.

## DHCP Server

The DOCSIS specifications mandate that cable modems negotiate their IP address using the Dynamic Host Configuration Protocol (DHCP). The MTA, like most CPE on a DOCSIS network, must use DHCP to obtain its IP address and other crucial information (DNS servers, PacketCable option 122 for Kerberos realm name of KDC, provisioning server FQDN).



### Note

---

The CM portion, in addition to its normally required DHCP options, also requests, and must receive, Option 122 suboption 1, which it passes to the MTA portion as the IP address of the correct DHCP server from which to accept offers.

---

When using BACC with PacketCable support, be aware that BACC will automatically populate the ToD server, DNS servers, TFTP server, as well as the Option 122 (or 177) fields; these do not need to be explicitly set in the CNR policy.

## DNS Server

The Domain Name System (DNS) server is fundamental in PacketCable provisioning. The PacketCable provisioning server, the device provisioning engine (DPE) in a BACC architecture, must have an address (A) record in the appropriate zone, as its fully qualified domain name (FQDN) is provided to the MTA in Option 122 by the DHCP server. The KDC realm must have a zone of the same name as the realm name, containing a server (SRV) record that contains the FQDN of the Kerberos server.

The Kerberos server identified in the SRV record must itself have an A record in the appropriate zone. The call management server (CMS) identified in the MTA config file must also have an A record in the appropriate zone. Lastly, the MTAs themselves must have A records in the appropriate zone, since the CMS reaches the MTA by resolving its FQDN. Dynamic DNS (DDNS) is the preferred method of creating A records for the MTA; refer to [configuring and troubleshooting DDNS on CNR](#).

## Key Distribution Center

A key distribution center (KDC) is included in the BACC with PacketCable support. The KDC is responsible for authenticating MTAs. As such, it must check the MTA's certificate, and provide its own certificate so the MTA can authenticate the KDC. It also communicates with the Provisioning Server (DPE in the BACC architecture) to validate that the MTA is, in fact, provisioned on the network.

## PacketCable Provisioning Server

The PacketCable provisioning server is responsible for communicating the location of the MTA configuration file to the MTA, and/or, provisioning MTA parameters via SNMP. SNMPv3 is used for all communication between the MTA and the provisioning server. The keys used to initiate SNMPv3 communication are obtained by the MTA during its authentication phase with the KDC. Provisioning server functionality is provided by the DPE in a BACC architecture.

## Call Management Server

The CMS is essentially a softswitch, or call-agent, with additional PacketCable functionality to control QoS on a cable network, among other things. The MTA sends a network call signaling (NCS) restart in progress (RSIP) message to the CMS upon successful PacketCable provisioning.

## Key Variables

This section describes the key variables that you need to know to provision an EMTA correctly.

- [Certificates](#)
- [Scope Selection Tag\(s\)](#)
- [MTA Configuration File](#)

## Certificates

The MTA\_Root.cer file contains the MTA root certificate. This has not changed in some time, and all MTA vendors now contain certs rooted in official PacketCable MTA root. The MTA\_Root.cer will not likely cause you problems.

You must know in advance what telephony root certificate is required for the MTAs you are trying to provision. In most cases, you should be using telephony certs rooted in the PacketCable test root. Deployments in production networks may use telephony certs rooted in the PacketCable real root. The KDC cert used by the KDC to authenticate itself to the MTA must be rooted in the same telephony root that is stored on the MTA. Most MTA vendors support test images that have telnet and/or http login capabilities such that you can determine which telephony root is enabled, and change the root used (in most cases, you can only select between the PacketCable real or test root).

The most common scenario would have the KDC loaded with certificates (from the \$BPR\_HOME/kdc/solaris/packetcable/certificates dir) as follows:

- CableLabs\_Service\_Provider\_Root.cer
- Service\_Provider.cer
- Local\_System.cer
- KDC.cer
- MTA\_Root .cer

The first 4 certificates comprise the telephony certificate chain, the MTA\_Root.cer file contains the MTA root, so that the KDC can authenticate MTAs.

To determine if you are using PacketCable test root, open the CableLabs\_Service\_Provider\_Root.cer file in Windows, and validate that the Subject OrgName entry is “O = CableLabs”, and/or check the Subject Alternative name reads “CN=CABLELABS GENERATED TEST ROOT FOR EQUIPMENT TEST PURPOSES ONLY,” as seen below.

The KDC certificate (KDC.cer) has the realm name to use embedded in it. The realm name that BACC (and the corresponding DNS zone) is configured to use must match this realm name. Additionally, the MTA config file realm org name must match the organization name as seen in the telephony root .

The KDC certificate has a corresponding private key that must be installed in the \$BPR\_HOME/kdc/solaris directory. Usually it is named kdc\_private\_key\_proprietary or kdc\_private\_key.pkcs8. When changing certificates, you must also change the private key.

## Scope Selection Tag(s)

In most scenarios, the BACC will be involved in processing all DHCP requests from scopes which have scope selection tags that match the selection criteria as specified in the DHCP criteria configuration tab in the BACC GUI. Client Class can also be used to tie scopes to BACC processing. Make sure you make this association before you attempt to provision devices.

## MTA Configuration File

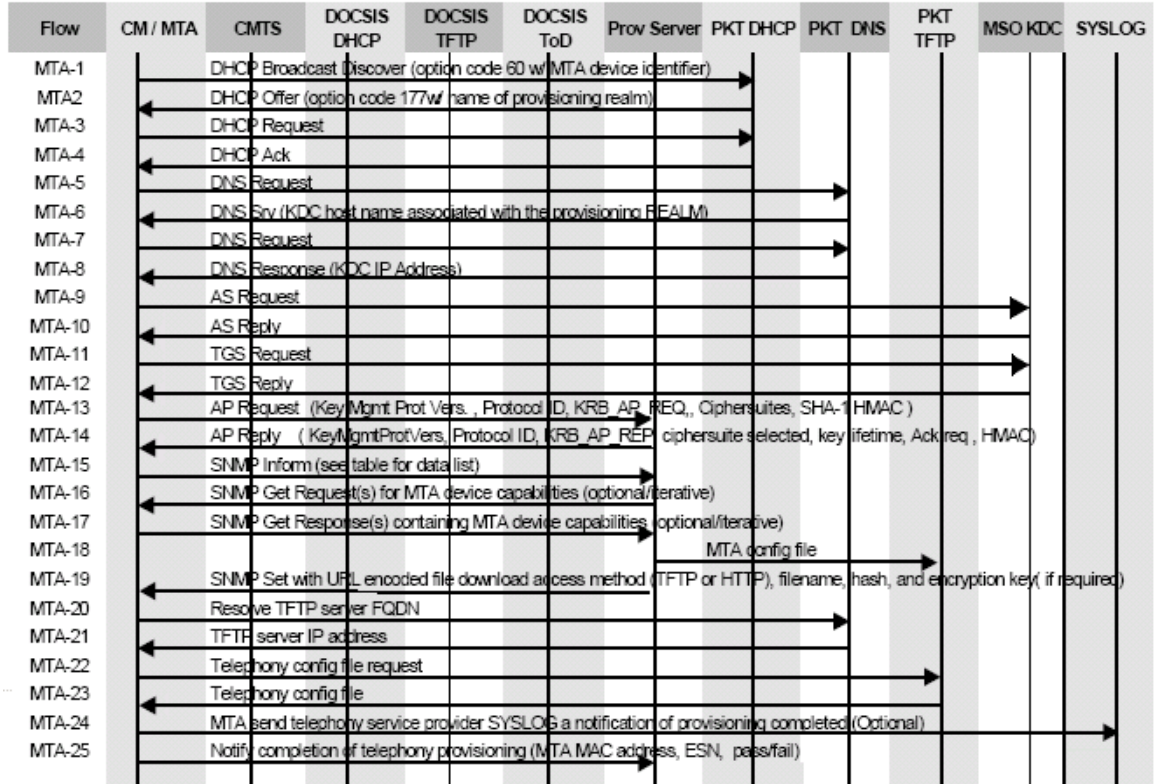
The MTA config file will most importantly contain the location of the CMS. Additionally, it must contain an entry for Realm Org Name. This value must match that of the certificate chain in use.

Certain entries must be indexed by the realm name, as delivered to the MTA in Option 122. The realm name used to index must match that delivered in Option 122. For example, if “DEF.COM” was the realm name delivered in Option 122, MTA config file entries in the pktcMtaDevRealm table would be indexed with a suffix made up of the ASCII-coded character values (in dot delimited decimal format when using the Cisco Broadband Configurator) of the realm name, for example 68.69.70.46.67.79.77. There are many free ASCII conversion pages available on the web to make this conversion easier.

## Troubleshooting Tools

The 25 EMTA provisioning steps contained in PacketCable EMTA Provisioning Specification (PKT-SP-PROV-I03-011221), are as shown in [Figure 6-1](#).

**Figure 6-1 Embedded-MTA Power-on Provisioning Flow**



## Logs

The following log files contain information as listed:

- CNR logs name\_dhcp\_1\_log and name\_dns\_1\_log contain the most recent logging entries from CNR. Look here for DHCP or DNS related problems.
- \$BPR\_HOME/kdc/logs/KDC.log shows all KDC interactions with MTAs, and KDC interactions with the provisioning server (BACC DPE).
- \$BPR\_HOME/dpe.log (or view log from CLI, if using DPE appliance) shows the major steps related to SNMPv3 interaction with MTA. See the [BACC documentation](#) for instructions on how to turn up trace levels.

## Ethereal, SnifferPro, or Other Packet Capture Tools

A packet capture tool is indispensable when troubleshooting the EMTAs. The Ethereal version, as packaged by CableLabs, includes numerous packet decoders specific to PacketCable, including Kerberos AS and AP packets.

If a failure is believed to be DHCP related, you will need to capture packets while filtering on packets sourced from or destined to the CMTS cable interface IP address and the DHCP server IP address.

If a failure is believed to be related to any of the 25 steps occurring after DHCP, merely filter all packets to/from the EMTA IP address. This gives a very concise, easy-to-follow trace of provisioning steps 5-25.

## Troubleshooting Scenarios

The scenarios listed in [Table 6-1](#) are possible failures involving embedded MTAs.

**Table 6-1** Troubleshooting Scenarios

Problem	Possible Causes	Remedies
<b>KDC will not start</b>	<ol style="list-style-type: none"> <li>KDC cert private does not correspond to private key</li> <li>KDC license expired or missing</li> </ol>	<ol style="list-style-type: none"> <li>Ensure that you have matching certs and private key</li> <li>restore KDC license to \$BPR_HOME/kdc directory</li> </ol>
<b>MTA device does not show up in BACC 'Devices' tab</b>	<ol style="list-style-type: none"> <li>Incorrect cable helper address</li> <li>Scope selection tags don't match DHCPCriteria</li> <li>CNR Extension point not properly installed</li> <li>CM portion did not receive Option 122</li> </ol>	<ol style="list-style-type: none"> <li>Fix helper address</li> <li>Make sure MTA scope tags match those in the PacketCable DHCP criteria created in BACC for the MTA(s) in question</li> <li>Re-install extension point</li> <li>Make sure tags on scope of CM portion match the DOCSIS DHCP criteria in use on BACC</li> </ol>

Table 6-1 Troubleshooting Scenarios (continued)


Problem	Possible Causes	Remedies
<b>MTA does not accept DHCP offer</b> (continually cycles thru DHCP steps)	<ol style="list-style-type: none"> <li>a. Invalid DHCP options configured</li> <li>b. Offer came from DHCP server other than indicated in CM portion's Option 122 suboption 1</li> </ol>	<ol style="list-style-type: none"> <li>a. Check that scope policy includes DNS server option, and/or check <code>cnr_ep.properties</code> file includes entry for primary and secondary dns servers</li> <li>b. Check <code>cnr_ep.properties</code> - ensure that primary and secondary dhcp servers are set correctly</li> </ol>
<b>MTA never contacts KDC</b> (as indicated by <code>KDC.log</code> , or etheral trace)	<ol style="list-style-type: none"> <li>a. Incorrect DNS server is specified in <code>cnr_ep.properties</code> and/or MTA scope policy</li> <li>b. Missing or incorrect setup of zone for Kerberos realm</li> <li>c. Missing or incorrect 'A' record entry for KDC</li> <li>d. Cannot resolve FQDN of provisioning server</li> </ol>	<ol style="list-style-type: none"> <li>a. Check /correct <code>cnr_ep.properties</code> dns servers</li> <li>b. Make sure zone with same name as realm is created and contains an 'SRV' record of format '<code>_kerberos._udp 0 0 88 &lt;KDC FQDN&gt;</code>'</li> <li>c. Ensure that an 'A' record exists for the FQDN contained in the Kerberos zone's 'SRV' record</li> <li>d. Ensure that <code>dpe.properties</code> <code>provFQDNs</code> entry has correct FQDN and IP of provisioning server (DPE)</li> </ol>
<b>KDC reports failure at Step 9</b> (Kerberos AS-Request)	<ol style="list-style-type: none"> <li>a. MTA cert mismatch with MTA root used by KDC</li> <li>b. FQDN lookup by KDC to Prov Server failed</li> <li>c. Clock Skew error</li> <li>d. Keys mismatch between KDC and provisioning server.</li> </ol>	<ol style="list-style-type: none"> <li>a. Check that <code>MTA_Root.cer</code> is correct – compare against that used on a working system. If correct, then MTA itself could have a cert problem (which is very rare); contact the manufacturer.</li> <li>b. Device may not yet be provisioned in BACC. Make sure device shows up and is given a Class of Service and DHCP criteria.</li> <li>c. Ensure that all BACC network elements are clock synced via NTP.</li> <li>d. Check that <code>\$BPR_HOME/kdc/solaris/keys</code> directory contains at least the following 3 entries: <ul style="list-style-type: none"> <li>• <code>mtafqdnmap,dpe.abc.com@DEF.COM</code></li> <li>• <code>mtaprovsrvr,dpe.abc.com@DEF.COM</code></li> <li>• <code>krbtgt,DEF.COM@DEF.COM</code></li> </ul> <p>Your system will have the DPE FQDN, and Realname different from this example. Contents of these entries must match the entry in <code>dpe.properties</code> 'KDCServiceKey' entry, or the keys generated using the keygen utility.</p> </li> </ol>
	 <p><b>Note</b> If other devices are provisioning correctly, d is not likely the cause of the problem.</p>	

Table 6-1 Troubleshooting Scenarios (continued)


Problem	Possible Causes	Remedies
<b>KDC reports success at step 9 (AS-Request/Reply), but MTA never moves past step 9, and continually reprovisions up to that step</b>	<p>a. Telephony cert mismatch between telephony root loaded/enabled on MTA, and that loaded on KDC</p> <p>b. Corrupted telephony cert chain (unlikely)</p>	<p>a. Check certs on MTA and KDC.</p> <p>b. Ensure correct cert is loaded/enabled on MTA. If no devices can be provisioned correctly, try different certs on KDC.</p>
	<p> <b>Note</b> If other devices are provisioning correctly, b is not the cause of the problem.</p>	
<b>Failure at AP Request/Reply</b>	<p>a. Clock skew error</p> <p>b. Cannot resolve Prov Server FQDN</p> <p>c. no route from MTA to provisioning server</p>	<p>a. Ensure that all BACC network elements are clock synced via NTP</p> <p>b. Make sure that the provisioning server (DPE) has a correct DNS entry. Ensure that dpe.properties provFQDNs entry has correct FQDN and IP of provisioning server (DPE)</p> <p>c. correct routing problem</p>
<b>MTA never issues TFTP request for config file</b>	<p>a. No route to TFTP server (DPE in a BACC scenario)</p>	<p>a. correct routing problem</p>
<b>MTA never receives TFTP config file</b>	<p>a. File not cached at DPE</p> <p>b. Conflicting tftp-server option included as part of MTA scope policy in CNR</p>	<p>a. Wait until next provisioning attempt, at which time file should be cached, or simply reset the device</p> <p>b. BACC will insert dpe address for tftp-server, one can safely remove that option from the policy</p>
<b>MTA receives config file but fails at step 25 (SNMP Inform to provisioning server as seen in DPE.log)</b>	<p>a. Config file has an internal conflict, or a conflict with Realm Org of telephony cert chain, or a conflict with Realm Name provided in Option 122</p>	<p>a. Ensure that MTA config file is consistent.</p>
<b>MTA reports success at step 25, but no RSIP is sent</b>	<p>a. MTA cannot resolve IP address of CMS FQDN given in MTA config file.</p> <p>b. MTA cannot reach IP addr(s) of CMS – no route</p>	<p>a. Ensure a DNS entry exists for the CMS</p> <p>b. Resolve routing problem</p>

Table 6-1 Troubleshooting Scenarios (continued)

Problem	Possible Causes	Remedies
MTA reports success at step 25, but proceeds to contact KDC again for 'cms' service	<ol style="list-style-type: none"> <li>a. MTA config file points to incorrect CMS</li> <li>b. MTA config file has pktcMtaDevCmsIPsecCtrl value missing or set to '1', meaning do secure NCS call signaling, or uses an ascii suffix that does not match that of CMS FQDN</li> </ol>	<ol style="list-style-type: none"> <li>a. Correct config file, or reconfigure BTS to use FQDN listed in the config file</li> <li>b. Correct config file. If intention is to do secure signaling, take necessary steps to configure KDC and BTS for support (out of scope of this doc).</li> </ol>
MTA reports success at step 25, RSIPs, but gets no response or gets an errored response from the softswitch	<ol style="list-style-type: none"> <li>a. MTA is unprovisioned or incorrectly provisioned on the Cisco BTS 10200</li> <li>b. No DNS entry exists for the EMTA</li> </ol>	<ol style="list-style-type: none"> <li>a. Provision MTA on the Cisco BTS 10200</li> <li>b. Place an entry in correct DNS zone for EMTA (DDNS preferred method – see CNR documentation on how to enable DDNS)</li> </ol>

## Motorola Surfboard

Although the Motorola Surfboard is not a Cisco product, a certain amount of data concerning how to troubleshoot this cable modem has been acquired during solution testing; however, your primary source for troubleshooting information should be the documentation provided by the manufacturer, Motorola.

The Motorola SBV4502 uses a DOCSIS 1.1 and PacketCable™ compliant cable modem to transfer high speed data and digital voice. The Motorola SBV4502 provides high-speed, bi-directional data access in a two-way broadband cable system with Radio Frequency (RF) downstream transfer rates up to 38 Mbps and RF upstream rates up to 10 Mbps.

## Major Features

The major features of the SBV4502 are as follows:

- Voice and data over a single coaxial cable network
- Standard telephone features and CLASS features such as caller ID, call waiting, and call forwarding. Detects tones, such as dual tone multi-frequency (DTMF). Generates tones such as busy and dial tones. Eliminates echoes generated in the loop between the subscriber line interface and the telephone.
- Remote management through SNMP
- Automatic configuration and address assignment
- Software upgrades over the network
- Transport Control Protocol/Internet Protocol (TCP/IP)
- Complies with industry standards (DOCSIS, Packet Cable, etc.).



## Physical Interfaces

Motorola Surfboard SBV4502 contains the following interfaces:

- Type-F female connector for connectivity to HFC cable system.
- One RJ-45 connectors for Ethernet 10BaseT connectivity
- Two FXS voice ports.
- An access-port for the reset button.

## Voice Features

The voice features of the SBV4502 are as follows:

- Voice Encoding
- G.711 (A-law, Mu-law), G.726 (32kbps), G.728, and G.729A codecs.
- 5 Ringer Equivalent Numbers (REN) per POTS lines .
- Basic LD calling (NA dial plan) (includes IP to IP calls; IP to PSTN calls; PSTN to IP calls; and PSTN to IP to PSTN calls)
- Basic local calls (includes IP to IP calls; IP to PSTN calls; PSTN to IP calls; and PSTN to IP to PSTN calls)
- Caller ID, Caller ID with Name, Caller ID on Call Waiting, Calling Name Delivery
- Call Forwarding (Busy/No Answer, Selective), Call Return (\*69), Call Trace, Call Waiting
- Automatic Callback on Busy (\*66), Call Blocking/Call Blocking Toll Restriction
- 3-Way Calling, BLV-Operator interrupt (available 4th quarter 2001)
- Digit Pass Through, DTMF Detection/Dialing, DTMF Relay FRF Format,
- Echo Cancellation, Fast Busy
- Jitter Buffer Mangement in Passthrough, Redundancy
- Message Waiting Indicator (Audible & Visual)
- Fax and Modem Auto Detect
- 56 Kbps V.90 Analog Data Modem Calls
- Up to 14.4 Kbps Fax Data Rate (V.25 & V.21)
- TDD Support per V.18
- Real-time fax (G.711) and dial-up modems (min 33.6kbs)

## Signaling, Data, Routing Features

The signaling, data, and routing features of the SBV4502 are as follows:

- NCS
- DOCSIS 1.0, DOCSIS1.0+, DOCSIS1.1
- Unsolicited Grant Service (??)
- Multiple grades of service (min=3)

- Upstream Channel Change (DCC supported for DOCSIS1.1 certification)
- Upstream Packet Classification
- DHCP Client
- Guaranteed bandwidth delivery (CIR)
- Setting & Policing of IP Precedence for signaling & Voice

## Security Features

The security features of the SBV4502 are as follows:

- BPI, BPI+ (4th Quarter 2001)
- Centrally provisioned
- Centrally upgraded (software)
- DHCP

## Management Features

The management features of the SBV4502 are as follows:

- HTTP Diagnostics
- LEDs (power, port usage)
- SNMP v3 MIB Support
- XGCP/DOCSIS MIB(Moto supports DOCSIS MIB and Moto CM proprietary MIB)
- Centrally provisioned
- Centrally upgraded (software)

## Arris MTAs

To collect logs from the Arris MTAs, complete the following steps:

---

**Step 1** Log on to the call agent using Telnet

```
secca01# telnet nnn.nnn.nnn.nnn
Trying nnn.nnn.nnn.nnn...
Connected to nnn.nnn.nnn.nnn.
Escape character is '^]'.
```

**Step 2** The system should respond with a CLI prompt and request your password. Enter your password.

```
-> CLI_init
Enter password> arristi
```

The system should respond with the following message:

```
Arris console is active
Type 'help' for available commands
```

The Arris console prompt is a line number enclosed in square brackets.

**Step 3** At the Arris console prompt, enter the following command:

```
[ 1] Console> callp m 1
```

The Arris MTA repeats the command you entered and displays the result.

```
callp m 1  
MGCP message trace enabled
```

**Step 4**

```
[ 2] What was this command/response ??
```

```
[ 3] Call Processing> / (back to last directory)
```

```
[ 4] Console> callp m 0  
callp m 0  
MGCP message trace disabled  
Return Status: 0  
[ 5] Call Processing> /  
-> logout
```





## Troubleshooting the CMTS

---

The Cisco Universal Broadband Router (uBR7246VXR, [Figure 7-1](#)) is a modular, standards-based Cable Modem Termination System (CMTS), as defined in the DOCSIS 1.1 specification, with an integrated router that offers carrier-class availability and advanced IP routing capabilities for mid to large cable headends or distribution hubs.

Connectivity to the service provider (SP) for PSTN access is through a CMTS. In the BLISS for Cable solution the Cisco uBR7246VXR is a CMTS with features that enable it to connect cable modems on the Hybrid Fiber Coaxial (HFC) Cable network via a Cisco MCxx cable modem card. The cable modem card provides the interface between the Cisco uBR protocol control information (PCI) bus and the radio frequency (RF) signal on the DOCSIS HFC network, terminating IP packets on its network interface. It is used for aggregating traffic in the cable access portion of the network.

The Cisco uBR7246VXR integrates a CMTS system with a 7200 series router. The 7200 router portion of the unit is based on the NPE-300 Network Processing Engine. The Cisco uBR7246VXR supports multiprotocol, multimedia routing and bridging with a wide variety of protocols and port adapter combinations available. The Cisco uBR7246VXR has up to six slots for port adapters, one slot for an input/output (I/O) controller, and one slot for a network processing engine. You can place the port adapters in any of the available slots. The chassis is fully radio frequency (RF) hardened to ensure noise-free transmission, and all major components are hot swappable to guarantee maximum reliability.

The Cisco uBR7246VXR supports the complete Cisco line of DOCSIS 1.0-qualified and DOCSIS 1.1 based modem cards, including cable and wireless cards that are available now. The Cisco uBR7246VXR supports 1+1 and N+1 redundancy of the cable modem cards. A range of network interfaces is also available, including the newest line of Cisco Dynamic Packet Transport (DPT) port adapters, which provide direct, high-speed optical connectivity combined with add-drop multiplexer capability.

Designed for large cable deployments with tens of thousands of subscriber modems, telephones, and other IP-enabled devices, the Cisco uBR7246VXR offers flexible expansion of DOCSIS infrastructures. The Cisco uBR7246VXR supports a broad set of residential and commercial service offerings, including IP telephony, multicast, streaming media, and Virtual Private Network (VPN) applications. Although the Cisco uBR7246VXR can filter on higher-layer TCP or UDP protocols, these protocols are typically passed transparently.

For complete technical documentation on the Cisco uBR7246VXR Universal Broadband Router see [http://www.cisco.com/en/US/products/hw/cable/ps2217/prod\\_technical\\_documentation.html](http://www.cisco.com/en/US/products/hw/cable/ps2217/prod_technical_documentation.html).

Figure 7-1 Cisco uBR7246VXR—Front View

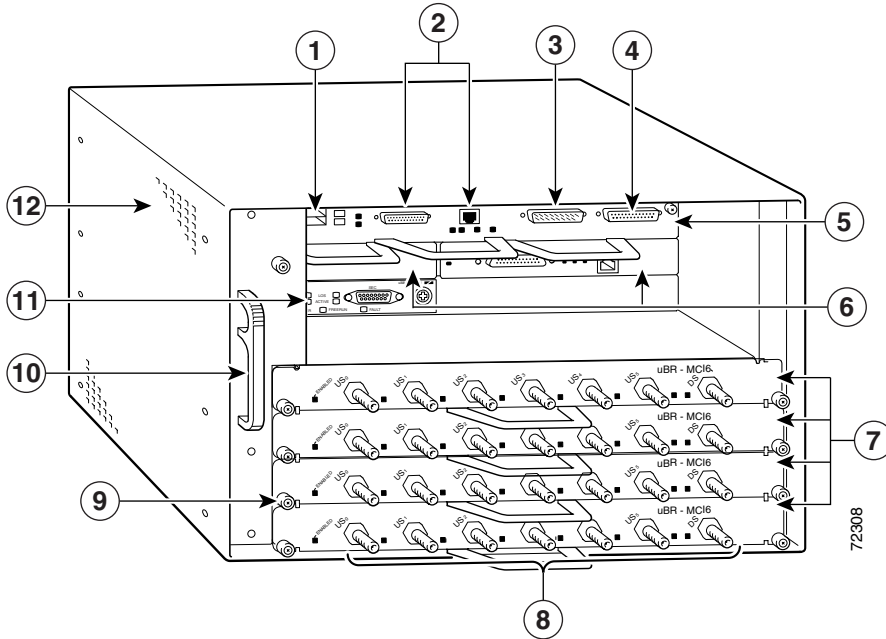
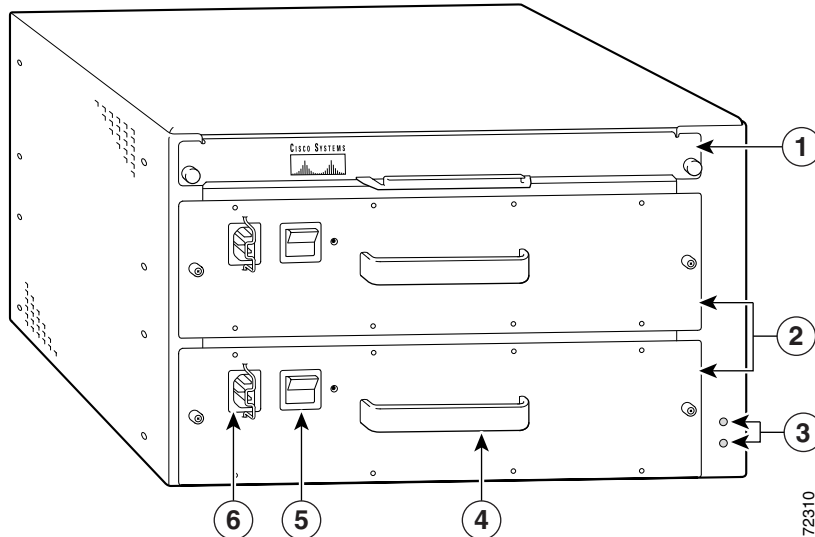


Figure 7-2 Cisco uBR7246VXR—Rear View



## Console Connections

You can use an ASCII terminal or a PC to configure or troubleshoot a Cisco uBR7246VXR. The configuration or troubleshooting can be performed:

- Locally, with a direct connection through the console port
- Remotely, with a connection through the auxiliary port and a cable modem
- Through Telnet or TFTP

## Physical Interfaces

HFC interfaces are provided by up to 4 plug-in modem cards. A variety of modem cards are supported, including UBR-MC11C, UBR-MC12C, UBR-MC14C, UBR-MC16C, and UBR-MC16S. All the cable modem cards have one downstream cable port. The number of upstream cable ports vary with the type of card. For example MC16C has 6 upstream ports.

The MC16S has spectrum management support. The spectrum manager continuously monitors the noise in unused upstream channels. If the signal-to-noise ratio reaches an unacceptable level on a particular channel, the spectrum manager will automatically assign a new upstream channel to the cable modem using that channel (frequency agility).

The Cisco uBR 7246VXR comes equipped with one 100 Base-T Ethernet interface built into the I/O board. Another RJ-45 100 Base-T Ethernet card can be installed via a plug-in port adapter.

- Gigabit Ethernet
- Multi-port Ethernet/Fast Ethernet
- Packet Over Sonet (POS) interfaces (long reach, intermediate reach, multimode)
- 2 port OC-12 DPT ports (long reach, intermediate reach, multimode)
- High-speed backplane (622 Mbps)

## Features

The operating system for the Cisco uBR7246VXR is the Cisco IOS software that resides in Flash memory. The unit includes the following features:

### Management Features

The Cisco uBR7246VXR enables easy setup and service using the following:

- HTML based management tool
- Web browser can be used to navigate through CLI commands
- Simple Network Management Protocol (SNMP) v3
- Works with configuration tools, such as Cisco Network Registrar (CNR), and Cisco Subscriber Registration Center (CSRC)
- MIB support—RF interface MIB, DOCSIS extensions MIB
- Redundancy provided by n+m configuration

### Routing, Security, and QoS Features

The Cisco uBR7246VXR provides support for the following:

- HSRP
- Network Address Translation (NAT), Access Control Lists (ACLs), and Committed Access Rate (CAR)
- Traffic shaping
- VPNs, GRE tunnels
- TAG switching support on cable interfaces (VPN)

- Integrated Time Of Day server
- Integrated DHCP server
- Per SID Bandwidth Request /Grant counters
- QoS for voice: LLQ, TOS
- Point to Point Protocol (PPP)

## Performance Redundancy/Availability/Compatibility Features

The Cisco uBR7246VXR has a carrier class architecture with redundant components, modular design and hardening facilitates maximum performance and uptime in mission critical applications.

- Enhanced processor performance with NPE-300
- Higher packet throughput - supports high speed connections to carrier class backbone fiber rings.
- Built on Cisco 7200 platform with proven reliability in complex environments
- Expandable, High Density Design - scalable to track subscriber demands - support for denser subscriber connections for head end
- Interoperable with Cisco uBR7200 series - investment protection for installed CMTS equipment
- Accepts uBR7200 series plugins - investment protection
- DPT support - direct optical interconnection - eliminates the need for add drop multiplexers - maximum network efficiency via spatial reuse protocol
- Hot Swappable Components - maximum reliability and minimum downtime in the event of an outage
- Online insertion and removal of plugin adapters - interfaces can be added/removed without service interruption.
- Spectrum Management capability with optional modem card - improved reliability and scalability of services through intelligent use of limited upstream bandwidth - even in noisy plant environments.
- HSRP facilitates fast cut over to a backup router
- Dynamic ranging - Cisco patent pending feature that supports quick restoration of service following a catastrophic plant failure.
- Modem Power Enhancement adjustments for low SNR failures
- Clock synchronization for voice applications.
- Baseline Privacy Interface (BPI)

## Classes of Service

The Cisco uBR7246VXR also provides multiple classes of service to include:

- QoS- CAR, Cisco Express Forwarding (CEF), Weighted Random Early Detection (WRED), TAG/Netflow switching, Weighted Fair Queuing, Resource Reservation Protocol (RSVP)
- Spectrum Management Phases 1 and 2
- DOCSIS 1.0 QoS, DOCSIS 1.0 QoS extensions, Multi-SID support (QoS)
- Rate Shaping (includes ToS)
- QoS profile enforcement



- Weighted Fair Drop (WFD) enhancements
- DOCSIS 1.0 CBR
- Per Modem filters
- ISL bridging for non cable interfaces (VLANs)
- IPSec security
- 3DES encryption
- Firewall, CBAC, and intrusion detection
- Cable Modem Multicast authentication (RADIUS)
- Basic lawful intercept support (CALEA) facility based on MAC address, so it can be used for voice or data connections
- Upstream address verification (security)
- 40-bit and 56-bit baseline private data encryption standard (DES)
- Encrypted Baseline Privacy Key Exchange (security)

## Standards

- Modular standards based architecture.  
Complete interoperability and forward compatibility to support future DOCSIS, PacketCable, OpenCable, and other relevant standards.
- DOCSIS 1.0 qualified
- DOCSIS 1.1 based
- Baseline Privacy Interface (BPI)

## Reference Documentation

For additional details, refer to the following documents:

- [Cisco 7200 Series Quick Start Guide](#)
- [Cisco 7200 Series VXR Installation and Configuration Guide](#)
- [Cisco 7200 Series VXR Port Adapter Hardware Configuration Guidelines](#)
- [Regulatory Compliance and Safety Information for Cisco 7200 Series Routers](#)
- [Cisco 7200 Series Routers Troubleshooting Documentation Roadmap](#)

# Troubleshooting the Cisco uBR7246VXR

This section provides information and procedures to help you diagnose problems from the Cisco uBR7246VXR.

For the latest troubleshooting information available for the Cisco uBR7246VXR see [http://www.cisco.com/en/US/products/hw/cable/ps2217/prod\\_alerts\\_troubleshooting.html](http://www.cisco.com/en/US/products/hw/cable/ps2217/prod_alerts_troubleshooting.html).

The CMTS and DOCSIS error messages, their cause, and recommended actions are available at [http://www.cisco.com/en/US/products/hw/cable/ps2217/prod\\_error\\_message09186a0080134033.html](http://www.cisco.com/en/US/products/hw/cable/ps2217/prod_error_message09186a0080134033.html).

The Cisco uBR7246VXR software provides commands to help diagnose problems with:

- Media Terminal Adapters (MTAs) and the cable plant—Cisco uBR7246VXR software includes a flap list that helps isolate problems between the cable plant (such as ingress noise or incorrect power levels) and specific MTAs.

A “flap” is defined as an MTA being registered on the Cisco uBR7246VXR, de-registering, and then immediately reregistering. With the flap list, you can quickly learn how to characterize trouble patterns in the network, determine which amplifier or feeder line is faulty, distinguish an upstream path problem from a downstream path problem, and isolate an ingress noise impairment from a plant equipment problem.

Additional **show** commands are also available to help you diagnosis problems with cable modems.

- TCP/IP and provisioning problems—the system supports tracing and debugging DHCP related messages on an administrator-specified uBR network interface, tracing and debugging all MAC-layer DOCSIS messages for an administrator-defined MAC address, as well as other debugging commands to monitor specific processes.

## Troubleshooting the Cable Modem State

This section provides information on understanding the *online state* of the cable modem, and troubleshooting problems indicated by this state, including RF problems.



### Note

Many but not all of the problems addressed in this section are RF-related. You should review this section to generally understand troubleshooting the problems between the Cisco uBR7246VXR and the MTAs in its domain.

The first and most useful command to use at the Cisco uBR7246VXR is **show cable modem**:

```
#show cable modem
```

Interface Prim Sid	Online State	Timing Offset	Rec Power	QoS	CPE	IP address	MAC address
Cable2/0/U0 5	online(pt)	2290	-0.25	5	0	10.1.1.25	0050.7366.2223
Cable2/0/U0 6	offline	2287	-0.25	2	0	10.1.1.26	0050.7366.2221

The *Online State* field shows what status the MTA is in.

[Table 7-1](#) displays the possible values for the state.

**Table 7-1 State Values**

State Value	Description
offline	Cable modem considered offline
init (r1)	Cable modem sent initial ranging
init (r2)	Cable modem is ranging
init (rc)	Cable modem ranging complete
init (d)	Dhcp request received
init (i)	Dhcp reply received; IP address assigned

**Table 7-1 State Values (continued)**

State Value	Description
init (t)	TOD exchange started
init(o)	Option file transfer started
online	Cable modem registered, enabled for data
online(d)	Cable modem registered, but network access for the cable modem is disabled
online(pk)	Cable modem registered, BPI enabled and KEK assigned
online(pt)	Cable modem registered, BPI enabled and TEK assigned
reject (pk)	KEK modem key assignment rejected
reject (pt)	TEK modem key assignment rejected
reject (m)	Cable modem did attempt to register; registration was refused due to bad MIC (Message Integrity Check)
reject (c)	Cable modem did attempt to register; registration was refused due to bad COS (Class of Service)

**Note**

At the MTA side a good command to use is **show controllers cable-modem 0 mac state** and look at the *MAC State* field.

The following sections discuss each *State* value, what the possible causes are, and what steps can be taken to arrive at the correct state (online).

## Offline State

In some cases the cable modem may cycle through other states then back to offline. The following list gives the most common reasons for a cable modem not to achieve QAM lock:

- Weak carrier signal (too much noise)
- Incorrect downstream center frequency
- Incorrect frequency specified in the DOCSIS file
- Absence of downstream digital QAM modulated signal
- Incorrect frequency specified in **cable modem change-frequency** on the Cisco uBR7246VXR

The following is a portion of the output from **show controllers cable-modem 0** entered at the router end:

```
#sh cont c 0

BCM Cable interface 0:
CM unit 0, idb 0x8086C88C, ds 0x8086E460, regaddr = 0x2700000, reset_mask 0x80
station address 0030.96f9.65d9 default station address 0030.96f9.65d9
PLD VERSION: 1
Concatenation: ON Max bytes Q0: 2000 Q1: 2000 Q2: 2000 Q3: 2000

MAC State is ds_channel_scanning_state, Prev States = 3
MAC mcfilter 01E02F00 data mcfilter 00000000

MAC extended header ON
DS: BCM 3300 Receiver: Chip id = BCM3300
US: BCM 3300 Transmitter: Chip id = 3300
```

```
Tuner: status=0x00
Rx: tuner_freq 529776400, symbol_rate 5361000, local_freq 11520000
    snr_estimate 166(TenthdB), ber_estimate 0, lock_threshold 26000
    QAM not in lock, FEC not in lock, qam_mode QAM_64 (Annex B)
Tx: tx_freq 27984000, symbol_rate 8 (12800000 sym/sec)
    power_level: 6.0 dBmV (commanded)
                7 (gain in US AMP units)
                63 (BCM3300 attenuation in .4 dB units)
...[Rest of the displayed output is omitted]
```

Note in the above output that the Signal to Noise ratio (SNR) estimate is 16.6 dB. Ideally this should be at least 30dB in order for the MTA to operate properly for 64 QAM. See the RF specifications for DOCSIS Downstream and Upstream signals. In some cases you may have a good SNR (of say 34dB) but still have noise present, such as impulse noise. This can only be detected by a spectrum analyzer operating in the zero span mode. One indication of impulse noise is the uncorrectable errors seen in the output of **show interfaces cable 2/0 upstream 0** as shown in the following output:

```
#show interfaces cable 2/0 upstream 0

Cable2/0: Upstream 0 is up
Received 46942 broadcasts, 0 multicasts, 205903 unicasts
0 discards, 12874 errors, 0 unknown protocol
```



**Note** If a value is greater than 1 in 10,000, most likley impulse noise is present.

```
252845 packets input, 1 uncorrectable
12871 noise, 0 microreflections Total Modems On This Upstream Channel : 3 (3 active)
Default MAC scheduler
Queue[Rng Polls] 0/64, fifo queueing, 0 drops
Queue[Cont Mslots] 0/104, fifo queueing, 0 drops
Queue[CIR Grants] 0/64, fair queueing, 0 drops
Queue[BE Grants] 0/64, fair queueing, 0 drops
Queue[Grant Shpr] 0/64, calendar queueing, 0 drops
Reserved slot table currently has 0 CBR entries
Req IEs 77057520, Req/Data IEs 0
Init Mtn IEs 1194343, Stn Mtn IEs 117174
Long Grant IEs 46953, Short Grant IEs 70448
Avg upstream channel utilization : 1%
Avg percent contention slots : 96%
Avg percent initial ranging slots : 4%
Avg percent minislots lost on late MAPs : 0%
Total channel bw reserved 0 bps
CIR admission control not enforced
Current minislot count : 7192093 Flag: 0
Scheduled minislot count : 7192182 Flag: 0
```

The optimal input power level at the MTA is 0dBmV; the receiver has a range of -15dBmV to +15dBmV. This can be measured by the spectrum analyzer. If the power is too low you may need to configure the upconverter per the *Cisco uBR 7246 Hardware Installation Guide*. If the signal is too strong, then you may need to add more attenuation at the high frequency port connection. If a particular frequency has too much noise present, you may need to select another frequency in the spectrum.

To confirm that the MTA has not been able to achieve QAM lock, turn on **debug cable-modem mac log verbose**. You should see output similar to the following:

```
2d18h: 239198.516 CMAC_LOG_LINK_DOWN
2d18h: 239198.516 CMAC_LOG_LINK_UP
2d18h: 239198.516 CMAC_LOG_STATE_CHANGE ds_channel_scanning_state
2d18h: 239198.520 CMAC_LOG_WILL_SEARCH_DS_FREQUENCY_BAND 99/805790200/99770
2d18h: 239198.520 CMAC_LOG_WILL_SEARCH_DS_FREQUENCY_BAND 98/601780000/79970
2d18h: 239198.520 CMAC_LOG_WILL_SEARCH_DS_FREQUENCY_BAND 97/403770100/59570
2d18h: 239198.524 CMAC_LOG_WILL_SEARCH_DS_FREQUENCY_BAND 96/73753600/115750
```

```

2d18h: 239198.524 CMAC_LOG_WILL_SEARCH_DS_FREQUENCY_BAND 95/217760800/39770
2d18h: 239198.528 CMAC_LOG_WILL_SEARCH_DS_FREQUENCY_BAND 94/121756000/16970
2d18h: 239198.528 CMAC_LOG_WILL_SEARCH_DS_FREQUENCY_BAND 93/175758700/21170
2d18h: 239198.528 CMAC_LOG_WILL_SEARCH_DS_FREQUENCY_BAND 92/79753900/857540
2d18h: 239198.532 CMAC_LOG_WILL_SEARCH_DS_FREQUENCY_BAND 91/55752700/677530
2d18h: 239198.532 CMAC_LOG_WILL_SEARCH_DS_FREQUENCY_BAND 90/177000000/21300
2d18h: 239198.532 CMAC_LOG_WILL_SEARCH_DS_FREQUENCY_BAND 89/219000000/22500
2d18h: 239198.536 CMAC_LOG_WILL_SEARCH_DS_FREQUENCY_BAND 88/141000000/17100
2d18h: 239198.536 CMAC_LOG_WILL_SEARCH_DS_FREQUENCY_BAND 87/135012500/13500
2d18h: 239198.540 CMAC_LOG_WILL_SEARCH_DS_FREQUENCY_BAND 86/123012500/12900
2d18h: 239198.540 CMAC_LOG_WILL_SEARCH_DS_FREQUENCY_BAND 85/405000000/44700
2d18h: 239198.540 CMAC_LOG_WILL_SEARCH_DS_FREQUENCY_BAND 84/339012500/39900
2d18h: 239198.544 CMAC_LOG_WILL_SEARCH_DS_FREQUENCY_BAND 83/333025000/33300
2d18h: 239198.544 CMAC_LOG_WILL_SEARCH_DS_FREQUENCY_BAND 82/231012500/32700
2d18h: 239198.544 CMAC_LOG_WILL_SEARCH_DS_FREQUENCY_BAND 81/111025000/11700
2d18h: 239198.548 CMAC_LOG_WILL_SEARCH_DS_FREQUENCY_BAND 80/93000000/105000
2d18h: 239198.548 CMAC_LOG_WILL_SEARCH_DS_FREQUENCY_BAND 79/453000000/85500
NOTE—unable to lock on:
2d18h: 239198.552 CMAC_LOG_WILL_SEARCH_SAVED_DS_FREQUENCY 453000000
2d18h: 239199.672 CMAC_LOG_DS_NO_QAM_FEC_LOCK 453000000
2d18h: 239200.788 CMAC_LOG_DS_NO_QAM_FEC_LOCK 453000000
2d18h: 239201.904 CMAC_LOG_DS_NO_QAM_FEC_LOCK 453000000
2d18h: 239203.020 CMAC_LOG_DS_NO_QAM_FEC_LOCK 459000000

```

Another reason for the MTA not achieving QAM lock is incorrect downstream center frequency being configured on the upconverter. For example, on the NTSC frequency map for standard 6-MHz channel bands in North America, channel 100-100 uses 648.0-654.0 with a center frequency of 651 MHz.

However, if you are using an upconverter that is designed to work off the video carrier frequency (for example, GI C6U which is 1.75MHz below the center frequency), then you need to set a frequency of 649.25 MHz for Channel 100-100.

Another common mistake is to specify an incorrect frequency value in the *Downstream Frequency* field under the Radio Frequency Info in the DOCSIS CPE Configurator. Usually there is no need to specify a frequency value under this option, however, if there is a need (such as when certain modems need to lock on a different frequency), then proper frequency values should be selected, as explained previously. The following debug output illustrates this: an MTA locks on initially at 453MHz and then at 535.25MHz (which was specified in the DOCSIS configuration file), thus causing the cable modem to reset and cycle through this process indefinitely:

```

4d00h: 345773.916 CMAC_LOG_WILL_SEARCH_SAVED_DS_FREQUENCY 453000000
4d00h: 345774.956 CMAC_LOG_UCD_MSG_RCVD 1
4d00h: 345775.788 CMAC_LOG_DS_64QAM_LOCK_ACQUIRED 453000000
4d00h: 345775.792 CMAC_LOG_DS_CHANNEL_SCAN_COMPLETED
4d00h: 345775.794 CMAC_LOG_STATE_CHANGE wait_ucd_state
4d00h: 345776.946 CMAC_LOG_UCD_MSG_RCVD 1
4d00h: 345778.960 CMAC_LOG_UCD_MSG_RCVD 1
4d00h: 345778.962 CMAC_LOG_ALL_UCDS_FOUND
4d00h: 345778.966 CMAC_LOG_STATE_CHANGE wait_map_state
4d00h: 345778.968 CMAC_LOG_FOUND_US_CHANNEL 1
4d00h: 345780.996 CMAC_LOG_UCD_MSG_RCVD 1
4d00h: 345781.000 CMAC_LOG_UCD_NEW_US_FREQUENCY 27984000
4d00h: 345781.004 CMAC_LOG_SLOT_SIZE_CHANGED 8
4d00h: 345781.084 CMAC_LOG_UCD_UPDATED
4d00h: 345781.210 CMAC_LOG_MAP_MSG_RCVD
4d00h: 345781.212 CMAC_LOG_INITIAL_RANGING_MINISLOTS 40
4d00h: 345781.216 CMAC_LOG_STATE_CHANGE ranging_1_state
4d00h: 345781.220 CMAC_LOG_RANGING_OFFSET_SET_TO 9610
4d00h: 345781.222 CMAC_LOG_POWER_LEVEL_IS 22.0 dBmV (comma)
4d00h: 345781.226 CMAC_LOG_STARTING_RANGING
4d00h: 345781.228 CMAC_LOG_RANGING_BACKOFF_SET 0
4d00h: 345781.232 CMAC_LOG_RNG_REQ_QUEUED 0
4d00h: 345781.272 CMAC_LOG_RNG_REQ_TRANSMITTED

```

```

4d00h: 345781.280 CMAC_LOG_RNG_RSP_MSG_RCVD
4d00h: 345781.282 CMAC_LOG_RNG_RSP_SID_ASSIGNED 3
4d00h: 345781.284 CMAC_LOG_ADJUST_RANGING_OFFSET 2288
4d00h: 345781.288 CMAC_LOG_RANGING_OFFSET_SET_TO 11898
4d00h: 345781.292 CMAC_LOG_ADJUST_TX_POWER 7
4d00h: 345781.294 CMAC_LOG_POWER_LEVEL_IS 24.0 dBmV (comma)
4d00h: 345781.298 CMAC_LOG_STATE_CHANGE ranging_2_state
4d00h: 345781.302 CMAC_LOG_RNG_REQ_QUEUED 3
4d00h: 345782.298 CMAC_LOG_RNG_REQ_TRANSMITTED
4d00h: 345782.300 CMAC_LOG_RNG_RSP_MSG_RCVD
4d00h: 345782.304 CMAC_LOG_RANGING_SUCCESS
4d00h: 345782.316 CMAC_LOG_STATE_CHANGE dhcp_state
4d00h: 345782.450 CMAC_LOG_DHCP_ASSIGNED_IP_ADDRESS 10.1.1.25
4d00h: 345782.452 CMAC_LOG_DHCP_TFTP_SERVER_ADDRESS 172.17.110.136
4d00h: 345782.456 CMAC_LOG_DHCP_TOD_SERVER_ADDRESS 172.17.110.136
4d00h: 345782.460 CMAC_LOG_DHCP_SET_GATEWAY_ADDRESS
4d00h: 345782.464 CMAC_LOG_DHCP_TZ_OFFSET 0
4d00h: 345782.466 CMAC_LOG_DHCP_CONFIG_FILE_NAME frequency.cm
4d00h: 345782.470 CMAC_LOG_DHCP_ERROR_ACQUIRING_SEC_SVR_ADDR
4d00h: 345782.474 CMAC_LOG_DHCP_COMPLETE
4d00h: 345782.598 CMAC_LOG_STATE_CHANGE establish_tod_state
4d00h: 345782.606 CMAC_LOG_TOD_REQUEST_SENT
4d00h: 345782.620 CMAC_LOG_TOD_REPLY_RECEIVED 3178880491
4d00h: 345782.628 CMAC_LOG_TOD_COMPLETE
4d00h: 345782.630 CMAC_LOG_STATE_CHANGE security_associate_state
4d00h: 345782.634 CMAC_LOG_SECURITY_BYPASSED
4d00h: 345782.636 CMAC_LOG_STATE_CHANGE configuration_file
4d00h: 345782.640 CMAC_LOG_LOADING_CONFIG_FILE frequency.cm
4d00h: %LINEPROTO-5-UPDOWN: Line protocol on Interface cable-modem0, changed state to up
4d00h: 345783.678 CMAC_LOG_CONFIG_FILE_PROCESS_COMPLETE
NOTE—frequency override:
4d00h: 345783.682 CMAC_LOG_DS_FREQ_OVERRIDE 535250000
4d00h: 345783.686 CMAC_LOG_STATE_CHANGE reset_hardware_state
4d00h: 345784.048 CMAC_LOG_STATE_CHANGE wait_for_link_up_state
4d00h: 345784.052 CMAC_LOG_DRIVER_INIT_IDB_RESET 0x082A5226
4d00h: 345784.054 CMAC_LOG_LINK_DOWN
4d00h: 345784.056 CMAC_LOG_LINK_UP
4d00h: 345784.062 CMAC_LOG_STATE_CHANGE ds_channel_scanning_state
4d00h: 345785.198 CMAC_LOG_DS_NO_QAM_FEC_LOCK 535250000
4d00h: 345785.212 CMAC_LOG_DS_TUNER_KEEPALIVE
4d00h: 345787.018 CMAC_LOG_UCD_MSG_RCVD 1
4d00h: 345787.022 CMAC_LOG_DS_64QAM_LOCK_ACQUIRED 453000000

```

Incorrect frequency specified in **cable modem change-frequency** on the Cisco uBR7246VXR can also cause the MTA to switch frequencies, and if the frequency configured on the router is not chosen carefully, then you will see results similar to that above. The **cable modem change-frequency** command on the Cisco uBR7246VXR is optional and is typically left out by default.

After a downstream channel has been acquired and latency has been calculated, the next task is to locate a suitable upstream channel. The cable modem listens for an upstream channel descriptor (UCD) which contains the physical properties of the upstream channel, such as frequency, modulation, channel width, and other parameters defined in the burst descriptors.

A cable modem that cannot find a usable upstream channel descriptor may be on a downstream channel for which no upstream service is provided. This is likely to be a faulty configuration of the router. The **show controller cable x** command is a good place to start. Another possible reason a cable modem may not find a usable UCD is that its hardware or MAC may not support the parameters in the burst descriptors. This is likely to be either a faulty configuration of the Cisco uBR7246VXR or an MTA that is not DOCSIS-compliant.

Once a usable UCD is found, the cable modem will begin to listen to MAP (Bandwidth Allocation Map) messages which contain the upstream bandwidth allocation map of time. A section of time is mapped out into mini-slots and assigned to individual modems. There are also regions in the MAP for broadcast, contention based initial maintenance (or broadcast) ranging. It is these regions of the MAP that the cable modem must send its initial ranging requests until the Cisco uBR7246VXR responds with a ranging response (RNG-RSP).

If an MTA cannot find an initial maintenance region before a T2 timer expires, most likely the Cisco uBR7246VXR has a faulty configuration. You should also check the **insertion-interval** for the cable interface on the router.

## Ranging Process - init(r1),init(r2), and init(rc) state

At this stage, the MTA begins a ranging process to calculate the necessary transmit power level to reach the Cisco uBR7246VXR at its desired input power level. A reasonably good transmit power is roughly 40 - 50 dBmV (based on a uBR input power of 0 dBmV.) Other hardware may vary. Like the downstream channel, the carrier in the upstream channel should be sufficiently strong for the Cisco uBR7246VXR receiver to discern the symbols yet not too high to prevent increased bit error-rates.

The MTA sends a ranging request (RNG-REQ) message to the Cisco uBR7246VXR and waits for a ranging response (RNG-RSP) message or a T3 timer expiry. If a T3 timeout occurs, the retry count increments. If the retry count is less than the maximum number of retries, the cable modem transmits another RNG-REQ at a higher power level. This ranging process occurs in the initial maintenance or broadcast regions of the MAP because the Cisco uBR7246VXR has not assigned the cable modem a service identifier (SID) for unicast transmissions in the MAP. Thus, broadcast ranging is contention based and subject to collisions. To compensate for this the cable modems have a ranging backoff algorithm to calculate a random backoff time between RNG-REQ transmissions. This can be configured using **cable upstream range-backoff** command. When the transmit power has reached a sufficient level for the Cisco uBR7246VXR, it will respond to the RNG-REQ with a RNG-RSP containing a temporary SID. This SID will be used to identify unicast transmission regions in the MAP for unicast ranging.

Below output shows an MTA in init(r1) state indicating the MTA cannot get past the initial ranging stage:

```
r#show cable modem
```

Interface Prim Sid	Online State	Timing Offset	Rec Power	QoS	CPE	IP address	MAC address
Cable2/0/U0 6	init(r1)	2813	12.00	2	0	10.1.1.22	0050.7366.1e01

The debug below shows how the MTA fails to complete the ranging process and resets after a T3 timer expiry. Note the **CMAC\_LOG\_ADJUST\_TX\_POWER** messages coming from the Cisco uBR7246VXR asking the MTA to adjust its power:

```
1w3d: 871160.618 CMAC_LOG_STATE_CHANGE ranging_1_state
1w3d: 871160.618 CMAC_LOG_RANGING_OFFSET_SET_TO 9610
1w3d: 871160.622 CMAC_LOG_POWER_LEVEL_IS 19.0 dBmV (comman)
1w3d: 871160.622 CMAC_LOG_STARTING_RANGING
1w3d: 871160.622 CMAC_LOG_RANGING_BACKOFF_SET 0
1w3d: 871160.622 CMAC_LOG_RNG_REQ_QUEUED 0
1w3d: 871160.678 CMAC_LOG_RNG_REQ_TRANSMITTED
1w3d: 871160.682 CMAC_LOG_RNG_RSP_MSG_RCVD
1w3d: 871160.682 CMAC_LOG_RNG_RSP_SID_ASSIGNED 6
1w3d: 871160.682 CMAC_LOG_ADJUST_RANGING_OFFSET 2813
1w3d: 871160.682 CMAC_LOG_RANGING_OFFSET_SET_TO 12423
1w3d: 871160.686 CMAC_LOG_ADJUST_TX_POWER -48
1w3d: 871160.686 CMAC_LOG_STATE_CHANGE ranging_2_state
```

```

1w3d: 871160.686 CMAC_LOG_RNG_REQ_QUEUED 6
1w3d: 871161.690 CMAC_LOG_RNG_REQ_TRANSMITTED
1w3d: 871161.690 CMAC_LOG_RNG_RSP_MSG_RCVD
1w3d: 871161.694 CMAC_LOG_ADJUST_TX_POWER -36
1w3d: 871161.694 CMAC_LOG_RANGING_CONTINUE
1w3d: 871162.698 CMAC_LOG_RNG_REQ_TRANSMITTED
1w3d: 871162.898 CMAC_LOG_T3_TIMER
1w3d: 871163.734 CMAC_LOG_RNG_REQ_TRANSMITTED
1w3d: 871163.934 CMAC_LOG_T3_TIMER
1w3d: 871164.766 CMAC_LOG_RNG_REQ_TRANSMITTED
1w3d: 871164.966 CMAC_LOG_T3_TIMER
131.CABLEMODEM.CISCO: 1w3d: %UBR900-3-RESET_T3_RETRIES_EXHAUSTED: R03.0 Ranging
1w3d: 871164.966 CMAC_LOG_RESET_T3_RETRIES_EXHAUSTED
1w3d: 871164.966 CMAC_LOG_STATE_CHANGE reset_interface_state
1w3d: 871164.966 CMAC_LOG_STATE_CHANGE reset_hardware_state
Note: init(r1) is ranging_1_state and init(r2) is ranging_2_state

```

You can get an indication of the Transmit power on the MTA by displaying the following command:

```

#sh cont cable-modem 0
BCM Cable interface 0:
CM unit 0, idb 0x2010AC, ds 0x86213E0, regaddr = 0x800000, reset_mask 0x80
station address 0050.7366.2223 default station address 0050.7366.2223
PLD VERSION: 32

MAC State is wait_for_link_up_state, Prev States = 2
MAC mcfilter 00000000 data mcfilter 00000000

MAC extended header ON
DS: BCM 3116 Receiver: Chip id = 2
US: BCM 3037 Transmitter: Chip id = 30AC

Tuner: status=0x00
Rx: tuner_freq 0, symbol_rate 5055932, local_freq 11520000
    snr_estimate 30640, ber_estimate 0, lock_threshold 26000
    QAM not in lock, FEC not in lock, gam_mode QAM_64
Tx: tx_freq 27984000, power_level 0x20 (8.0 dBmV), symbol_rate 8 (1280000 sym/s)

```

If a cable modem cannot proceed out of ranging state, the likely cause is an insufficient transmit power level. Transmit power can be adjusted by adjusting attenuation at the low frequency port. Increased attenuation will result in increased transmit power levels. Roughly 20 - 30 dBmV of attenuation is a good place to start.

After initial ranging init(r1) the cable modem proceeds onto init(r2) which is where the cable modem must configure the transmit timing offset and power level to ensure that transmissions from the modem are received at the correct time and are at an acceptable input power level at the Cisco uBR7246VXR receiver. This is performed through a conversation of unicast RNG-REQ and RNG-RSP messages. The RNG-RSP messages contain power and timing offset corrections the cable modem must make.

the cable modem continues to transmit RNG-REQ and perform adjustments per RNG-RSP until the RNG-RSP message indicates ranging success or ranging complete by reaching the init(rc) state. If a cable modem cannot proceed out of init (r2) the transmit power needs to be refined. Below is an output display of an MTA in init(r2) state. Note the asterisk (\*) symbol next to the Rec Power column indicating that the noise power adjustment method is active for this modem. If you see an exclamation point (!) this means the cable modem has reached its maximum transmit power.

**#show cable modem**

Interface Prim Sid	Online State	Timing Offset	Rec Power	QoS	CPE	IP address	MAC address
Cable2/0/U0 5	init(r2)	2289	*4.00	2	0	10.1.1.25	0050.7366.2223



## DHCP - init(d) state

The next stage after successful ranging is acquiring network configuration via DHCP.

Below is a an output display of **show cable modem** showing a cable modem in init(d), which indicates that the DHCP request was received from the MTA:

**#show cable modem**

Interface Prim Sid	Online State	Timing Offset	Rec Power	QoS	CPE	IP address	MAC address
Cable2/0/U0 7	init(d)	2811	0.25	2	0	10.1.1.20	0030.96f9.65d9

Note that the MTA can cycle through init(r1) to init(d) indefinitely. Following are some possible causes:

- IP connectivity issue from the Cisco uBR7246VXR to the DHCP server
- DHCP server down
- Wrong default gateway configured at the DHCP server
- Low transmit power at the MTA



### Note

Although you can ping the DHCP server from the Cisco uBR7246VXR, the problem could be that the DHCP has the incorrect gateway set since it may be able to respond to the primary IP address of the Cisco uBR7246VXR cable interface, but not the secondary IP address which is used as the source IP address during the DHCP discovery phase.

Frequently, errors at DHCP state manifest themselves as timeouts rather than NAK's. The order of DHCP messages should be DISCOVER, OFFER, REQUEST, ACK. If the cable modem is transmitting a DISCOVER with no OFFER response from the DHCP server, turn on UDP debugging on the Cisco uBR7246VXR.

This can be done with the following command:

**# debug ip udp**

```
4d01h: UDP: rcvd src=0.0.0.0(68), dst=255.255.255.255(67), length=584
4d01h: BOOTP: opcode 1 from host 0.0.0.0 on Cable2/0, 0 secs, 0 hops
4d01h: UDP: forwarded broadcast 67 from 10.1.1.10 to 172.17.110.136 on Ethernet0
4d01h: UDP: rcvd src=0.0.0.0(68), dst=255.255.255.255(67), length=584
4d01h: BOOTP: opcode 1 from host 0.0.0.0 on Cable2/0, 0 secs, 0 hops
4d01h: UDP: forwarded broadcast 67 from 10.1.1.10 to 172.17.110.136 on Ethernet0
4d01h: UDP: rcvd src=172.17.110.136(67), dst=10.1.1.10(67), length=314
4d01h: BOOTP: opcode 2 from host 172.17.110.136 on Ethernet1/0, 0 secs, 0 hops
4d01h: BOOTP: Broadcasting response 172.17.110.136 -> 10.1.1.20 (Cable2/0)
4d01h: UDP: forwarded broadcast 68 from 172.17.110.136 to 255.255.255.255 on Ca0
4d01h: UDP: rcvd src=0.0.0.0(68), dst=255.255.255.255(67), length=584
4d01h: BOOTP: opcode 1 from host 0.0.0.0 on Cable2/0, 0 secs, 0 hops
4d01h: UDP: forwarded broadcast 67 from 10.1.1.10 to 172.17.110.136 on Ethernet0
4d01h: UDP: rcvd src=172.17.110.136(67), dst=10.1.1.10(67), length=314
4d01h: BOOTP: opcode 2 from host 172.17.110.136 on Ethernet1/0, 0 secs, 0 hops
4d01h: BOOTP: Broadcasting response 172.17.110.136 -> 10.1.1.20 (Cable2/0)
4d01h: UDP: forwarded broadcunast 68 from 172.17.110.136 to 255.255.255.255 on 1
All possible debugging has been turned off
```

**Caution**

Running debug commands on a uBR (Universal Broadband Router) with more than a handful of modems may cause the Cisco uBR7246VXR to halt the system in order to keep up with the debugging. In this case, all the cable modems may lose sync and debugging will be useless.

If no packets are seen through debug messages, check the configuration of the **cable helper-address** statement on the cable interface to which this modem is attached. If this is configured correctly and a packet trace of the DHCP server subnet also reveals no DHCP packets from the cable modem, then a good place to look is the output errors of the cable modem's cable interface or the input errors of the cable interface of the Cisco uBR7246VXR. It might be a good idea to boost the transmitter power of the MTA a bit more with more attenuation.

If packets are seen to be transmitted onto the DHCP server subnet, it would be a good idea to double check the cable modem debug messages to see if there are parameter request or assignment errors. This would be the stage of troubleshooting where you should investigate the routing between the MTA and the DHCP server. It would also be advisable to double-check the DHCP server configuration and the DHCP logs.

Below is a sample debug taken at the MTA by running the **debug cable-modem mac log verbose** command:

```
1w3d: 865015.920 CMAC_LOG_RANGING_SUCCESS
1w3d: 865015.920 CMAC_LOG_STATE_CHANGE                               dhcp_state
1w3d: 865053.580 CMAC_LOG_RNG_REQ_TRANSMITTED
1w3d: 865053.584 CMAC_LOG_RNG_RSP_MSG_RCVD
1w3d: 865055.924 CMAC_LOG_WATCHDOG_TIMER
131.CABLEMODEM.CISCO: 1w3d: %UBR900-3-RESET_DHCP_WATCHDOG_EXPIRED:
Cable Interface Reset due to DHCP watchdog timer expiration
1w3d: 865055.924 CMAC_LOG_RESET_DHCP_WATCHDOG_EXPIRED
1w3d: 865055.924 CMAC_LOG_STATE_CHANGE                               reset_interface_state
1w3d: 865055.924 CMAC_LOG_DHCP_PROCESS_KILLED
1w3d: 865055.924 CMAC_LOG_STATE_CHANGE                               reset_hardware_state
```

As you can see, the above the DHCP process failed and the cable modem was reset.

## DHCP - init(i) state

Once a reply to the DHCP request has been received and an IP address assigned to the cable modem the next **show cable modem** command gives its state as init(i):

**#show cable modem**

Interface Prim Sid	Online State	Timing Offset	Rec Power	QoS	CPE	IP address	MAC address
Cable2/0/U0 7	init(i)	2815	-0.25	2	0	10.1.1.20	0030.96f9.65d9

In the output above, the MTA never gets beyond state init(i). Repetitive **show cable modem** displays will usually show the cable modem cycling between init(r1), init(r2), init(rc), init(d) and init(i) indefinitely.

Following is a list of the more common reasons for a cable modem not getting further than init(i):

- Incorrect or invalid DOCSIS file specified in the DHCP server
- TFTP server issues, for example: incorrect IP address, TFTP server unreachable
- Problems getting TOD or Timing Offset
- Incorrect Router setting in the DHCP configuration

Since the Cable Modem has reached as far as `init(i)` we know that it has got as far as obtaining an IP address. This can be clearly shown in the output display of the `debug cable-modem mac log verbose` command from the cable modem below:

```

3d20h: 334402.548 CMAC_LOG_RANGING_SUCCESS
3d20h: 334402.548 CMAC_LOG_STATE_CHANGE                dhcp_state
NOTE-IP address Assigned to CM:
3d20h: 334415.492 CMAC_LOG_DHCP_ASSIGNED_IP_ADDRESS    10.1.1.20
3d20h: 334415.492 CMAC_LOG_DHCP_TFTP_SERVER_ADDRESS    172.17.110.136
3d20h: 334415.492 CMAC_LOG_DHCP_TOD_SERVER_ADDRESS    172.17.110.136
3d20h: 334415.492 CMAC_LOG_DHCP_SET_GATEWAY_ADDRESS
3d20h: 334415.492 CMAC_LOG_DHCP_TZ_OFFSET              0
NOTE-DOCSIS file CM is trying to load:
3d20h: 334415.496 CMAC_LOG_DHCP_CONFIG_FILE_NAME      nofile
3d20h: 334415.496 CMAC_LOG_DHCP_ERROR_ACQUIRING_SEC_SVR_ADDR
3d20h: 334415.496 CMAC_LOG_DHCP_ERROR_ACQUIRING_LOG_ADDRESS
3d20h: 334415.496 CMAC_LOG_DHCP_COMPLETE
3d20h: 334415.508 CMAC_LOG_STATE_CHANGE                establish_tod_state
3d20h: 334415.512 CMAC_LOG_TOD_REQUEST_SENT           172.17.110.136
3d20h: 334415.524 CMAC_LOG_TOD_REPLY_RECEIVED         3178343318
3d20h: 334415.524 CMAC_LOG_TOD_COMPLETE
3d20h: 334415.528 CMAC_LOG_STATE_CHANGE                security_association_state
3d20h: 334415.528 CMAC_LOG_SECURITY_BYPASSED
3d20h: 334415.528 CMAC_LOG_STATE_CHANGE                configuration_file
NOTE-DOCSIS file name:
3d20h: 334415.528 CMAC_LOG_LOADING_CONFIG_FILE        nofile
133.CABLEMODEM.CISCO: 3d20h: %LINEPROTO-5-UPDOWN: Line protocol on Interface cap
3d20h: 334416.544 CMAC_LOG_CONFIG_FILE_TFTP_FAILED     -1
3d20h: 334416.548 CMAC_LOG_CONFIG_FILE_PROCESS_COMPLETE
3d20h: 334416.548 CMAC_LOG_RESET_CONFIG_FILE_READ_FAILED

```

Similarly, TFTP server issues would give similar errors resulting in the cable modem resetting and cycling through the same process indefinitely:

```

3d21h: 336136.520 CMAC_LOG_STATE_CHANGE                dhcp_state
3d21h: 336149.404 CMAC_LOG_DHCP_ASSIGNED_IP_ADDRESS    10.1.1.20
NOTE-TFTP Server address
3d21h: 336149.404 CMAC_LOG_DHCP_TFTP_SERVER_ADDRESS    172.17.110.100
3d21h: 336149.404 CMAC_LOG_DHCP_TOD_SERVER_ADDRESS    172.17.110.136
3d21h: 336149.404 CMAC_LOG_DHCP_SET_GATEWAY_ADDRESS
3d21h: 336149.404 CMAC_LOG_DHCP_TZ_OFFSET              0
3d21h: 336149.408 CMAC_LOG_DHCP_CONFIG_FILE_NAME      platinum.cm
3d21h: 336149.408 CMAC_LOG_DHCP_ERROR_ACQUIRING_SEC_SVR_ADDR
3d21h: 336149.408 CMAC_LOG_DHCP_ERROR_ACQUIRING_LOG_ADDRESS
3d21h: 336149.408 CMAC_LOG_DHCP_COMPLETE
3d21h: 336149.420 CMAC_LOG_STATE_CHANGE                establish_tod_state
3d21h: 336149.424 CMAC_LOG_TOD_REQUEST_SENT           172.17.110.136
3d21h: 336149.436 CMAC_LOG_TOD_REPLY_RECEIVED         3178345052
3d21h: 336149.436 CMAC_LOG_TOD_COMPLETE
3d21h: 336149.440 CMAC_LOG_STATE_CHANGE                security_association_state
3d21h: 336149.440 CMAC_LOG_SECURITY_BYPASSED
3d21h: 336149.440 CMAC_LOG_STATE_CHANGE                configuration_file
3d21h: 336149.440 CMAC_LOG_LOADING_CONFIG_FILE        platinum.cm
133.CABLEMODEM.CISCO: 3d21h: %LINEPROTO-5-UPDOWN: Line protocol on Interface cap
3d21h: 336163.252 CMAC_LOG_RNG_REQ_TRANSMITTED
3d21h: 336163.252 CMAC_LOG_RNG_RSP_MSG_RCVD
NOTE-TFTP process failing:
3d21h: 336165.448 CMAC_LOG_CONFIG_FILE_TFTP_FAILED     -1
3d21h: 336165.448 CMAC_LOG_CONFIG_FILE_PROCESS_COMPLETE
3d21h: 336165.452 CMAC_LOG_RESET_CONFIG_FILE_READ_FAILED
3d21h: 336165.452 CMAC_LOG_STATE_CHANGE                reset_interface_state

```

Problems getting TOD (Time of Day) or Timing Offset would also result in the cable modem not achieving online status:

```

3d21h: 338322.500 CMAC_LOG_STATE_CHANGE dhcp_state
3d21h: 338334.260 CMAC_LOG_RNG_REQ_TRANSMITTED
3d21h: 338334.260 CMAC_LOG_RNG_RSP_MSG_RCVD
3d21h: 338335.424 CMAC_LOG_DHCP_ASSIGNED_IP_ADDRESS 10.1.1.20
3d21h: 338335.424 CMAC_LOG_DHCP_TFTP_SERVER_ADDRESS 172.17.110.136
3d21h: 338335.424 CMAC_LOG_DHCP_ERROR_ACQUIRING_TOD_ADDRESS
3d21h: 338335.424 CMAC_LOG_DHCP_SET_GATEWAY_ADDRESS
3d21h: 338335.424 CMAC_LOG_DHCP_ERROR_ACQUIRING_TZ_OFFSET
3d21h: 338335.424 CMAC_LOG_DHCP_CONFIG_FILE_NAME platinum.cm
3d21h: 338335.428 CMAC_LOG_DHCP_ERROR_ACQUIRING_SEC_SVR_ADDR
3d21h: 338335.428 CMAC_LOG_DHCP_ERROR_ACQUIRING_LOG_ADDRESS
3d21h: 338335.428 CMAC_LOG_DHCP_COMPLETE
3d21h: 338335.428 CMAC_LOG_RESET_DHCP_FAILED
3d21h: 338335.432 CMAC_LOG_STATE_CHANGE reset_interface_state
3d21h: 338335.432 CMAC_LOG_STATE_CHANGE reset_hardware_state
3d21h: 338336.016 CMAC_LOG_STATE_CHANGE wait_for_link_up_state

```

Note: prior to IOS version 12.1(1) TOD needed to be specified in the DHCP server in order for the cable modem to go online, however, after 12.1(1) TOD is not required but the cable modem still needs to get the timing offset, as shown in the following debugs:

```

344374.528 CMAC_LOG_STATE_CHANGE dhcp_state
344377.292 CMAC_LOG_RNG_REQ_TRANSMITTED
344377.292 CMAC_LOG_RNG_RSP_MSG_RCVD
344387.412 CMAC_LOG_DHCP_ASSIGNED_IP_ADDRESS 10.1.1.20
344387.412 CMAC_LOG_DHCP_TFTP_SERVER_ADDRESS 172.17.110.136
NOTE- TOD server IP address obtained:
344387.412 CMAC_LOG_DHCP_TOD_SERVER_ADDRESS 172.17.110.136
344387.412 CMAC_LOG_DHCP_SET_GATEWAY_ADDRESS
NOTE- Timing offset not specified in DHCP server:
344387.412 CMAC_LOG_DHCP_ERROR_ACQUIRING_TZ_OFFSET
344387.412 CMAC_LOG_DHCP_CONFIG_FILE_NAME platinum.cm
344387.412 CMAC_LOG_DHCP_ERROR_ACQUIRING_SEC_SVR_ADDR
344387.412 CMAC_LOG_DHCP_ERROR_ACQUIRING_LOG_ADDRESS
344387.412 CMAC_LOG_DHCP_COMPLETE
344387.412 CMAC_LOG_RESET_DHCP_FAILED
NOTE-Modem resetting:
344387.412 CMAC_LOG_STATE_CHANGE reset_interface_state

```

In the debug below there is no time-server specified, but there is a timing offset configured in the DHCP server, and therefore the cable modem goes online:

```

3d23h: 345297.516 CMAC_LOG_DHCP_ASSIGNED_IP_ADDRESS 10.1.1.20
3d23h: 345297.516 CMAC_LOG_DHCP_TFTP_SERVER_ADDRESS 172.17.110.136
3d23h: 345297.516 CMAC_LOG_DHCP_ERROR_ACQUIRING_TOD_ADDRESS
3d23h: 345297.516 CMAC_LOG_DHCP_SET_GATEWAY_ADDRESS
3d23h: 345297.516 CMAC_LOG_DHCP_TZ_OFFSET 0
3d23h: 345297.516 CMAC_LOG_DHCP_CONFIG_FILE_NAME platinum.cm
3d23h: 345297.520 CMAC_LOG_DHCP_ERROR_ACQUIRING_SEC_SVR_ADDR
3d23h: 345297.520 CMAC_LOG_DHCP_ERROR_ACQUIRING_LOG_ADDRESS
3d23h: 345297.520 CMAC_LOG_DHCP_COMPLETE
3d23h: 345297.532 CMAC_LOG_STATE_CHANGE establish_tod_state
3d23h: 345297.532 CMAC_LOG_TOD_NOT_REQUESTED_NO_TIME_ADDR
3d23h: 345297.532 CMAC_LOG_STATE_CHANGE security_association_state
3d23h: 345297.536 CMAC_LOG_SECURITY_BYPASSED
3d23h: 345297.536 CMAC_LOG_STATE_CHANGE configuration_file
3d23h: 345297.536 CMAC_LOG_LOADING_CONFIG_FILE platinum.cm
3d23h: 345297.568 CMAC_LOG_CONFIG_FILE_PROCESS_COMPLETE
3d23h: 345297.568 CMAC_LOG_STATE_CHANGE registration_state
3d23h: 345297.592 CMAC_LOG_REG_RSP_MSG_RCVD
3d23h: 345297.592 CMAC_LOG_COS_ASSIGNED_SID 1/7

```

```

3d23h: 345297.596 CMAC_LOG_RNG_REQ_QUEUED 7
3d23h: 345297.596 CMAC_LOG_REGISTRATION_OK
3d23h: 345297.596 CMAC_LOG_STATE_CHANGE establish_privacy_state
3d23h: 345297.596 CMAC_LOG_PRIVACY_NOT_CONFIGURED
3d23h: 345297.596 CMAC_LOG_STATE_CHANGE maintenance_state
133.CABLEMODEM.CISCO: 3d23h: %LINEPROTO-5-UPDOWN: Line protocol on Interface changed state
to up

```

Not including a Router option setting in the DHCP server or specifying an invalid IP address in the Router option field also results in a cable modem not getting beyond init(i) state, as can be seen in the output from **debug cable-modem mac log verbose** below:

```

1d16h: 146585.940 CMAC_LOG_CONFIG_FILE_TFTP_FAILED -1
1d16h: 146585.940 CMAC_LOG_CONFIG_FILE_PROCESS_COMPLETE
1d16h: 146585.944 CMAC_LOG_RESET_CONFIG_FILE_READ_FAILED
1d16h: 146585.944 CMAC_LOG_STATE_CHANGE reset_interface_state
1d16h: 146585.944 CMAC_LOG_STATE_CHANGE reset_hardware_state

```

## TOD exchange- init(t) state

After a cable modem has acquired its network parameters, it must request the time of day from a Time Of Day (TOD) server. TOD uses a UTC timestamp (seconds from January 1, 1970) which when combined with the time offset option value from DHCP, the current time can be calculated. The time is used for syslog and event log timestamps.

Below we have modems with SID 1 and 2 in init(t). Note that with recent IOS, later than 12.1(1) the cable modem still comes online even though the TOD exchange failed, as you can see in the following output from the **show cable modem** command:

**#show cable modem**

Interface Prim Sid	Online State	Timing Offset	Rec Power	QoS	CPE	IP address	MAC address
Cable2/0/U0 1	init(t)	2808	0.00	2	0	10.1.1.20	0030.96f9.65d9
Cable2/0/U0 2	init(t)	2809	0.25	2	0	10.1.1.21	0030.96f9.6605
Cable2/0/U0 3	init(i)	2810	-0.25	2	0	10.1.1.22	0050.7366.1e01

```

2d01h: 177933.712 CMAC_LOG_STATE_CHANGE dhcp_state
2d01h: 177933.716 CMAC_LOG_RNG_REQ_TRANSMITTED
2d01h: 177933.716 CMAC_LOG_RNG_RSP_MSG_RCVD
2d01h: 177946.596 CMAC_LOG_DHCP_ASSIGNED_IP_ADDRESS 10.1.1.20
2d01h: 177946.596 CMAC_LOG_DHCP_TFTP_SERVER_ADDRESS 172.17.110.136
2d01h: 177946.596 CMAC_LOG_DHCP_TOD_SERVER_ADDRESS 172.17.110.130
2d01h: 177946.596 CMAC_LOG_DHCP_SET_GATEWAY_ADDRESS
2d01h: 177946.596 CMAC_LOG_DHCP_TZ_OFFSET 0
2d01h: 177946.600 CMAC_LOG_DHCP_CONFIG_FILE_NAME platinum.cm
2d01h: 177946.600 CMAC_LOG_DHCP_ERROR_ACQUIRING_SEC_SVR_ADDR
2d01h: 177946.600 CMAC_LOG_DHCP_ERROR_ACQUIRING_LOG_ADDRESS
2d01h: 177946.600 CMAC_LOG_DHCP_COMPLETE
2d01h: 177946.612 CMAC_LOG_STATE_CHANGE establish_tod_state
2d01h: 177946.716 CMAC_LOG_RNG_REQ_TRANSMITTED
2d01h: 177946.716 CMAC_LOG_RNG_RSP_MSG_RCVD
133.CABLEMODEM.CISCO: 2d01h: %LINEPROTO-5-UPDOWN: Line protocol on Interface cap
2d01h: 177947.716 CMAC_LOG_RNG_REQ_TRANSMITTED
2d01h: 177947.716 CMAC_LOG_RNG_RSP_MSG_RCVD
2d01h: 177948.616 CMAC_LOG_TOD_REQUEST_SENT 172.17.110.130
2d01h: 177948.716 CMAC_LOG_RNG_REQ_TRANSMITTED
2d01h: 177954.616 CMAC_LOG_TOD_REQUEST_SENT 172.17.110.130
2d01h: 177954.716 CMAC_LOG_RNG_REQ_TRANSMITTED
2d01h: 177954.716 CMAC_LOG_RNG_RSP_MSG_RCVD

```

```

2d01h: 177960.616 CMAC_LOG_TOD_REQUEST_SENT 172.17.110.130
2d01h: 177960.712 CMAC_LOG_RNG_REQ_TRANSMITTED
2d01h: 177960.716 CMAC_LOG_RNG_RSP_MSG_RCVD
2d01h: 177961.716 CMAC_LOG_RNG_REQ_TRANSMITTED
131.CABLEMODEM.CISCO: 2d01h: %UBR900-3-TOD_FAILED_TIMER_EXPIRED:TOD failed, but Cable
Interface proceeding to operational state
2d01h: 177986.616 CMAC_LOG_TOD_WATCHDOG_EXPIRED
2d01h: 177986.616 CMAC_LOG_STATE_CHANGE security_association_state
2d01h: 177986.616 CMAC_LOG_SECURITY_BYPASSED
2d01h: 177986.616 CMAC_LOG_STATE_CHANGE configuration_file
2d01h: 177986.620 CMAC_LOG_LOADING_CONFIG_FILE platinum.cm
2d01h: 177986.644 CMAC_LOG_CONFIG_FILE_PROCESS_COMPLETE
2d01h: 177986.644 CMAC_LOG_STATE_CHANGE registration_state
2d01h: 177986.644 CMAC_LOG_REG_REQ_MSG_QUEUED
2d01h: 177986.648 CMAC_LOG_REG_REQ_TRANSMITTED
2d01h: 177986.652 CMAC_LOG_REG_RSP_MSG_RCVD
2d01h: 177986.652 CMAC_LOG_COS_ASSIGNED_SID 1/1
2d01h: 177986.656 CMAC_LOG_RNG_REQ_QUEUED 1
NOTE- Modem online:
2d01h: 177986.656 CMAC_LOG_REGISTRATION_OK
2d01h: 177986.656 CMAC_LOG_STATE_CHANGE establish_privacy_statee
2d01h: 177986.656 CMAC_LOG_PRIVACY_NOT_CONFIGURED
2d01h: 177986.656 CMAC_LOG_STATE_CHANGE maintenance_state
2d01h: 177988.716 CMAC_LOG_RNG_REQ_TRANSMITTED

```

Time of day errors almost always point to a DHCP misconfiguration. Possible misconfigurations that can result in TOD errors include the following:

- gateway address misconfigurations
- wrong TOD server address

Make sure you can ping the time-server to rule out IP connectivity issues and to make sure the time-server is available.

## Option File Transfer Started-init(o) State

The main configuration and administration interface to the cable modem is the configuration file downloaded from the provisioning server. This configuration file contains downstream channel and upstream channel identification and characteristics as well as Class of Service settings, Baseline Privacy settings, general operational settings, network management information, software upgrade fields, filters, and vendor specific settings.

A cable modem stuck in init(o) state usually indicates that the cable modem has started or is ready to start downloading the configuration file, but was unsuccessful due to the following possible reasons:

- Incorrect, corrupt, or missing DOCSIS configuration file
- Unable to reach the TFTP server, either is unavailable or no IP connectivity
- Invalid or missing Configuration Parameters in DOCSIS file
- Wrong file permissions on the TFTP server

Note that you may not always see init(o), instead you might see init(i) and then cycling through from init(r1) to init(i). A more accurate state can be derived by displaying the output of **show controller cable-modem 0 mac state**.

Following is an abbreviated display of that output:

```

#show controller cable-modem 0 mac state

MAC State: configuration_file_state
Ranging SID: 4

```

```
Registered:                FALSE
Privacy Established:       FALSE
```

When you see `init(o)` in the `show cable modem` output, running the **debug cable-modem mac log verbose** will not tell you if it is a corrupt configuration file or a TFTP server failure that is the cause. The debug point to both of them.

An example of invalid Configuration Parameters in the DOCSIS CPE Configurator is invalid or missing Vendor ID or Vendor Specific Information. The result is similar to the following output display:

```
w3d: 880748.992 CMAC_LOG_STATE_CHANGE                dhcp_state
1w3d: 880751.652 CMAC_LOG_RNG_REQ_TRANSMITTED
1w3d: 880751.656 CMAC_LOG_RNG_RSP_MSG_RCVD
1w3d: 880761.876 CMAC_LOG_DHCP_ASSIGNED_IP_ADDRESS    10.1.1.20
1w3d: 880761.876 CMAC_LOG_DHCP_TFTP_SERVER_ADDRESS    172.17.110.136
1w3d: 880761.876 CMAC_LOG_DHCP_TOD_SERVER_ADDRESS    172.17.110.136
1w3d: 880761.876 CMAC_LOG_DHCP_SET_GATEWAY_ADDRESS
1w3d: 880761.876 CMAC_LOG_DHCP_TZ_OFFSET            0
NOTE—Corrupt configuration file:
1w3d: 880761.880 CMAC_LOG_DHCP_CONFIG_FILE_NAME      data.cm
1w3d: 880761.880 CMAC_LOG_DHCP_ERROR_ACQUIRING_SEC_SVR_ADDR
1w3d: 880761.880 CMAC_LOG_DHCP_ERROR_ACQUIRING_LOG_ADDRESS
1w3d: 880761.880 CMAC_LOG_DHCP_COMPLETE
1w3d: 880761.892 CMAC_LOG_STATE_CHANGE                establish_tod_state
1w3d: 880761.896 CMAC_LOG_TOD_REQUEST_SENT          172.17.110.136
1w3d: 880761.904 CMAC_LOG_TOD_REPLY_RECEIVED        3180091733
1w3d: 880761.908 CMAC_LOG_TOD_COMPLETE
1w3d: 880761.908 CMAC_LOG_STATE_CHANGE                security_association_state
1w3d: 880761.908 CMAC_LOG_SECURITY_BYPASSED
1w3d: 880761.912 CMAC_LOG_STATE_CHANGE                configuration_file_state
1w3d: 880761.912 CMAC_LOG_LOADING_CONFIG_FILE      data.cm
1w3d: 880762.652 CMAC_LOG_RNG_REQ_TRANSMITTED
1w3d: 880762.652 CMAC_LOG_RNG_RSP_MSG_RCVD
133.CABLEMODEM.CISCO: 00:13:07: %LINEPROTO-5-UPDOWN: Line protocol on Interface
cable-modem0, changed state to up
00:13:08: 788.004 CMAC_LOG_CONFIG_FILE_CISCO_BAD_TYPE 155
00:13:08: 788.004 CMAC_LOG_CONFIG_FILE_CISCO_BAD_TYPE 115
00:13:08: 788.004 CMAC_LOG_CONFIG_FILE_CISCO_BAD_TYPE 116
00:13:08: 788.004 CMAC_LOG_CONFIG_FILE_CISCO_BAD_ATTR_MAX LENG128
00:13:08: 788.008 CMAC_LOG_CONFIG_FILE_PROCESS_COMPLETE
00:13:08: 788.008 CMAC_LOG_RESET_CONFIG_FILE_READ_FAILED
```

## Online, Online(d), Online(pk), Online(pt) state

The following states indicate that the cable modem has achieved online status and is able to transmit and receive data:

- online
- online(pk)
- online(pt)

Online(d), however indicates that the cable modem has come online but has been denied network access.

**#show cable modem**

Interface Prim Sid	Online State	Timing Offset	Rec Power	QoS	CPE	IP address	MAC address
Cable2/0/U0 4	online	2810	-0.75	6	0	10.1.1.20	0030.96f9.65d9





```

Assigned SID:          4
Max Downstream Rate:  10000000
Max Upstream Rate:    1024000
Upstream Priority:     7
Min Upstream Rate:    0
Max Upstream Burst:   0
Privacy Enable:       FALSE

```

*[Rest of display been omitted]*

Online means the cable modem has come online and is able to communicate with the Cisco uBR7246VXR. If BPI (Baseline Privacy Interface) is not enabled then the online status is the default state (assuming the cable modem initialization was successful). If BPI is configured then you will see a status of online(pk), followed shortly by online(pt). Following is a debug output display taken on the cable modem side using the **debug cable-modem mac log verbose** command, showing only the registration part:

```

5d03h: 445197.804 CMAC_LOG_STATE_CHANGE                registration_state
5d03h: 445197.804 CMAC_LOG_REG_REQ_MSG_QUEUED
5d03h: 445197.812 CMAC_LOG_REG_REQ_TRANSMITTED
5d03h: 445197.816 CMAC_LOG_REG_RSP_MSG_RCVD
5d03h: 445197.816 CMAC_LOG_COS_ASSIGNED_SID            1/4
5d03h: 445197.816 CMAC_LOG_RNG_REQ_QUEUED              4
5d03h: 445197.816 CMAC_LOG_REGISTRATION_OK
5d03h: 445197.816 CMAC_LOG_STATE_CHANGE                establish_privacy_state
5d03h: 445197.820 CMAC_LOG_PRIVACY_FSM_STATE_CHANGE
  machine: KEK, event/state: EVENT_1_PROVISIONED/STATE_A_START, new state:
STATE_B_AUTH_WAIT
5d03h: 445197.828 CMAC_LOG_BPKM_REQ_TRANSMITTED
5d03h: 445197.848 CMAC_LOG_BPKM_RSP_MSG_RCVD
5d03h: 445197.848 CMAC_LOG_PRIVACY_FSM_STATE_CHANGE
  machine: KEK, event/state: EVENT_3_AUTH_REPLY/STATE_B_AUTH_WAIT, new state:
STATE_C_AUTHORIZED
5d03h: 445198.524 CMAC_LOG_PRIVACY_FSM_STATE_CHANGE
machine: TEK, event/state: EVENT_2_AUTHORIZED/STATE_A_START, new state: STATE_B_OP_WAIT
5d03h: 445198.536 CMAC_LOG_RNG_REQ_TRANSMITTED
5d03h: 445198.536 CMAC_LOG_RNG_RSP_MSG_RCVD
5d03h: 445198.536 CMAC_LOG_BPKM_REQ_TRANSMITTED
5d03h: 445198.536 CMAC_LOG_BPKM_RSP_MSG_RCVD
5d03h: 445198.540 CMAC_LOG_PRIVACY_FSM_STATE_CHANGE
  machine: TEK, event/state: EVENT_8_KEY_REPLY/STATE_B_OP_WAIT, new state:
STATE_D_OPERATIONAL
5d03h: 445198.548 CMAC_LOG_PRIVACY_INSTALLED_KEY_FOR_SID 4
5d03h: 445198.548 CMAC_LOG_PRIVACY_ESTABLISHED
5d03h: 445198.552 CMAC_LOG_STATE_CHANGE                maintenance_state
5d03h: 445201.484 CMAC_LOG_RNG_REQ_TRANSMITTED
5d03h: 445201.484 CMAC_LOG_RNG_RSP_MSG_RCVD

```

If there is a problem with BPI in general you will see reject(pk), meaning it could not get through the key authentication stage. This state is covered in the reject(pk) and reject (pt) section.

For correct BPI operation ensure that the Cisco uBR7246VXR and the cable modem are both running a BPI enabled image, which is signified by the symbol **K1** in the image name.

Also ensure that the field **Baseline Privacy Enable** is set to 1 under the Class of Service option in the DOCSIS CPE Configurator. If the Cisco uBR7246VXR is running a BPI enabled image while the cable modem is not, and we have BPI enabled in the DOCSIS CPE Configurator, then you will observe the cable modem cycling between online and offline.

## Reject(pk) and Reject(pt) state

The following display of output from **show cable modem** on the Cisco uBR7246VXR shows a reject(pk) state:

**#show cable modem**

Interface Prim Sid	Online State	Timing Offset	Rec Power	QoS	CPE	IP address	MAC address
Cable2/0/U0 2	reject(pk)	2812	0.00	6	0	10.1.1.20	0030.96f9.65d9

```
01:58:51: %UBR7200-5-UNAUTHSIDTIMEOUT: CMTS deleted BPI unauthorized Cable Modem
0030.96f9.65d9
```

In most cases where there is a problem with the BPI configuration you will see a reject(pk) state. This state is typically caused by the following:

- Corrupt public key by the CM in the auth request, refer to sample debug cable privacy for proper sequence of events
- Presence of cable privacy authenticate-modem configuration command on the CMTS router but no Radius server present
- Improperly configured Radius server

Reject(pt) is typically caused by an invalid TEK or traffic encryption key. Following is output display using **debug cable privacy** on the Cisco uBR7246VXR:

```
02:32:08: CMTS Received AUTH REQ.
02:32:08: Created a new CM key for 0030.96f9.65d9.
02:32:08: CMTS generated AUTH_KEY.
02:32:08: Input : 70D158F106B0B75
02:32:08: Public Key:
02:32:08: 0x0000: 30 68 02 61 00 DA BA 93 3C E5 41 7C 20 2C D1 87
02:32:08: 0x0010: 3B 93 56 E1 35 7A FC 5E B7 E1 72 BA E6 A7 71 91
02:32:08: 0x0020: F4 68 CB 86 A8 18 FB A9 B4 DD 5F 21 B3 6A BE CE
02:32:08: 0x0030: 6A BE E1 32 A8 67 9A 34 E2 33 4A A4 0F 8C DB BD
02:32:08: 0x0040: D0 BB DE 54 39 05 B0 E0 F7 19 29 20 8C F9 3A 69
02:32:08: 0x0050: E4 51 C6 89 FB 8A 8E C6 01 22 02 34 C5 1F 87 F6
02:32:08: 0x0060: A3 1C 7E 67 9B 02 03 01 00 01
02:32:08: RSA public Key subject:
02:32:08: 0x0000: 30 7C 30 0D 06 09 2A 86 48 86 F7 0D 01 01 01 05
02:32:08: 0x0010: 00 03 6B 00 30 68 02 61 00 DA BA 93 3C E5 41 7C
02:32:08: 0x0020: 20 2C D1 87 3B 93 56 E1 35 7A FC 5E B7 E1 72 BA
02:32:08: 0x0030: E6 A7 71 91 F4 68 CB 86 A8 18 FB A9 B4 DD 5F 21
02:32:08: 0x0040: B3 6A BE CE 6A BE E1 32 A8 67 9A 34 E2 33 4A A4
02:32:08: 0x0050: 0F 8C DB BD D0 BB DE 54 39 05 B0 E0 F7 19 29 20
02:32:08: 0x0060: 8C F9 3A 69 E4 51 C6 89 FB 8A 8E C6 01 22 02 34
02:32:08: 0x0070: C5 1F 87 F6 A3 1C 7E 67 9B 02 03 01 00 01
02:32:08: RSA encryption result = 0
02:32:08: RSA encrypted output:
02:32:08: 0x0000: B6 CA 09 93 BF 2C 05 66 9D C5 AF 67 0F 64 2E 31
02:32:08: 0x0010: 67 E4 2A EA 82 3E F7 63 8F 01 73 10 14 4A 24 ED
02:32:08: 0x0020: 65 8F 59 D8 23 BC F3 A8 48 7D 1A 08 09 BF A3 A8
02:32:08: 0x0030: D6 D2 5B C4 A7 36 C4 A9 28 F0 6C 5D A1 3B 92 A2
02:32:08: 0x0040: BC 99 CC 1F C9 74 F9 FA 76 83 ED D5 26 B4 92 EE
02:32:08: 0x0050: DD EA 50 81 C6 29 43 4F 73 DA 56 C2 29 AF 05 53
02:32:08: CMTS sent AUTH response.
02:32:08: CMTS Received TEK REQ.
02:32:08: Created a new key for SID 2.
02:32:08: CMTS sent KEY response.
```

Below is a sample debug output on the cable modem when there is an authorization failure:

```
6d02h: 527617.480 CMAC_LOG_CONFIG_FILE_PROCESS_COMPLETE
6d02h: 527617.480 CMAC_LOG_STATE_CHANGE registration_state
6d02h: 527617.484 CMAC_LOG_REG_REQ_MSG_QUEUED
6d02h: 527617.488 CMAC_LOG_REG_REQ_TRANSMITTED
6d02h: 527617.492 CMAC_LOG_REG_RSP_MSG_RCVD
6d02h: 527617.492 CMAC_LOG_COS_ASSIGNED_SID 1/2
6d02h: 527617.492 CMAC_LOG_RNG_REQ_QUEUED 2
6d02h: 527617.492 CMAC_LOG_REGISTRATION_OK
6d02h: 527617.496 CMAC_LOG_STATE_CHANGE establish_privacy_state
6d02h: 527617.496 CMAC_LOG_PRIVACY_FSM_STATE_CHANGE
machine: KEK, event/state: EVENT_1_PROVISIONED/STATE_A_START, new state:
STATE_B_AUTH_WAIT
6d02h: 527617.504 CMAC_LOG BPKM_REQ_TRANSMITTED
6d02h: 527617.504 CMAC_LOG BPKM_RSP_MSG_RCVD
6d02h: 527617.508 CMAC_LOG_PRIVACY_FSM_STATE_CHANGE
machine: KEK, event/state: EVENT_2_AUTH_REJECT/STATE_B_AUTH_WAIT, new state:
STATE_E_AUTH_REJ_WAIT
129.CABLEMODEM.CISCO: 6d02h: %CMBPKM-1-AUTHREJECT: Authorization request rejected by CMTS:
Unauthorized CM
6d02h: 527618.588 CMAC_LOG_RNG_REQ_TRANSMITTED
6d02h: 527618.592 CMAC_LOG_RNG_RSP_MSG_RCVD
```

Similarly, a **debug cable privacy** on the Cisco uBR7246VXR provides the following errors:

```
02:47:00: CMTS Received AUTH REQ.
02:47:00: Sending KEK REJECT.
02:47:05: %UBR7200-5-UNAUTHSIDTIMEOUT: CMTS deleted BPI unauthorized Cable Modem
0030.96f9.65d9
```



#### Note

The cable modem keeps cycling from reject(pk) to init(r1) indefinitely.

Another possible error that can be encountered is that due to encryption export restrictions, some vendor modems may require the following command on the Cisco uBR7246VXR in the interface configuration:

```
(config-if)#cable privacy 40-bit-des
```

## Registration - reject (m) state

After configuration, the cable modem sends a registration request (REG-REQ) with a required subset of the configuration settings as well as the cable modem and uBR message integrity checks (MIC). The cable modem MIC is a hashed calculation over the configuration file settings which provides a method for the cable modem to be sure the configuration file was not tampered with in transit. The Cisco uBR7246VXR MIC is similar except it also includes a setting for a cable shared-secret authentication string. This shared secret is known by the Cisco uBR7246VXR and the provisioning server and ensures that only cable modems authenticated by provisioning servers will be allowed to register with the router.

A cable modem in reject(m) state has a bad Message Integrity Check (MIC), typically caused by:

- Mismatch between cable shared-secret under the cable interface and CMTS Authentication value under Miscellaneous option in the DOCSIS CPE Configurator
- Corrupt configuration file (DOCSIS file)

To rectify the problem, verify that you have a valid configuration file and an identical value under **CMTS Authentication** to what is configured in **cable shared-secret <line>** under the cable interface. Also verify that the Cisco uBR7246VXR allows the creation of class of service profiles, or use a profile created by the Cisco uBR7246VXR.

## Registration - reject (c) state

A cable modem that fails registration due to bad class of service (COS) has a state of reject(c). Typically this is caused by:

- uBR is unable or unwilling to grant a particular requested COS
- Misconfigured parameter(s) in Class of Service option in DOCSIS CPE Configurator, such as having two classes of service with the same ID

Following is output from **debug cable-modem mac log verbose** taken on the cable modem side showing failure due to bad COS:

```

1w3d: 885643.820 CMAC_LOG_STATE_CHANGE                registration_state
1w3d: 885643.820 CMAC_LOG_REG_REQ_MSG_QUEUED
1w3d: 885643.824 CMAC_LOG_REG_REQ_TRANSMITTED
1w3d: 885643.828 CMAC_LOG_REG_RSP_MSG_RCVD
1w3d: 885643.828 CMAC_LOG_SERVICE_NOT_AVAILABLE      0x01, 0x01, 0x01
1w3d: 885643.828 CMAC_LOG_RESET_SERVICE_NOT_AVAILABLE
1w3d: 885643.828 CMAC_LOG_STATE_CHANGE                reset_interface_state
1w3d: 885643.832 CMAC_LOG_STATE_CHANGE                reset_hardware_state
1w3d: 885644.416 CMAC_LOG_STATE_CHANGE                wait_for_link_up_state
1w3d: 885644.420 CMAC_LOG_DRIVER_INIT_IDB_RESET      0x8039E23C
1w3d: 885644.420 CMAC_LOG_LINK_DOWN
1w3d: 885644.420 CMAC_LOG_LINK_UP
1w3d: 885644.420 CMAC_LOG_STATE_CHANGE                ds_channel_scanning_state
133.CABLEMODEM.CISCO: 1w3d: %LINEPROTO-5-UPDOWN: Line protocol on Interface cable-modem0,
changed state to down
1w3d: 885645.528 CMAC_LOG_UCD_MSG_RCVD                1
1w3d: 885646.828 CMAC_LOG_DS_64QAM_LOCK_ACQUIRED     453000000

```

Similarly, **debug cable registration** on the Cisco uBR7246VXR gives the following output:

```

sniper#debug cable registration
CMTS registration debugging is on
sniper#
1d04h: %UBR7200-5-CLASSFAIL: Registration failed for Cable Modem 0001.9659.4461 on
interface Cable2/0/U0:
Bad/Missing Class of Service Config in REG-REQ

```

Note how the cable modem eventually resets and starts all over again.

## Monitoring the Cisco uBR7246VXR Flap List

The Cisco uBR7200 series maintains a database of flapping cable modems to assist in locating cable plant problems. The flapping cable modem detector tracks the upstream and downstream performance of all cable modems on the network, without impacting throughput and performance, or creating additional packet overhead on the broadband network. The cable modem flap list keeps track of the cable modems MAC address, up and down transitions, registration events, missed periodic ranging packets, upstream power adjustments and the physical interface on the Cisco uBR7200 series.

The flap list feature is compatible with all DOCSIS-compliant cable modems. Unlike SNMP, the flap list uses zero bandwidth.

The flap list collects the following station maintenance statistics:

- Detects interface up/down flap

The reinsertion counter counts the number of times a cable modem comes up and inserts into the network. This helps identify potential problems in the downstream because improperly provisioned cable modems tend to try to reestablish a link repeatedly.

- Detects intermittent upstream

The keepalive hits versus misses is the number of times cable modems don't respond or don't respond to the MAC layer keepalive messages. If there are a number of misses, this points to a potential problem in the upstream.

- Lists cable modem MAC addresses sorted by flap rate or most recent flap time.

- Shows power adjustment statistics during station maintenance polling

This represents the number of times the Cisco uBR7246VXR tells a cable modem to adjust the transmit power more than 3 dB. If constant power adjustments are detected, this usually indicates a problem with an amplifier. By looking at the cable modems in front and behind various amplifiers, you can find the source of failure.

The cable system administrator typically:

- Sets up a script to periodically poll the flap list, for example, every 15 minutes
- Uses the resulting data to perform trend analysis to identify the cable modems that are consistently in the flap list
- Queries the billing and administrative database for cable modem MAC address-to-street address translation and generates a report

Using these reports, you can quickly discern how characteristic patterns of flapping cable modems, street addresses, and flap statistics can indicate which amplifier or feeder lines are faulty. The reports also help you quickly discern whether problems exist in your downstream or upstream path, and whether the problem is ingress noise or equipment related.

Default values for the following flap-list configuration commands are:

- **cable flap-list miss-threshold**—6 seconds
- **cable flap-list power-adjust**—2 dB
- **cable flap-list insertion-time**—180 seconds



### Note

Since the cable flap list was originally developed, polling mechanisms have been enhanced to have an increased rate of 1/sec when polls are missed. Cable modems go offline faster than the frequency hop period. This can cause the frequency to stay fixed while cable modems go offline. To compensate for this, as appropriate, you can reduce the hop period to 10 seconds.

**Tips**

In Cisco IOS Release 12.0(7)XR2, Cisco IOS Release 12.1(1a)T1, and higher, the system supports automatic power adjustments. The **show cable flap-list** and **show cable modem** commands now indicate when the Cisco uBR7200 series has detected an unstable return path for a particular modem and has compensated with a power adjustment. An asterisk (\*) appears in the power adjustment field for a cable modem when a power adjustment has been made; an exclamation point (!) appears when the cable modem has reached its maximum power transmit level.

The following tips and scenarios allow you to use the flap list in the most effective way:

- If a subscriber's cable modem shows a lot of flap list activity, it is having communication problems.
- If a subscriber's cable modem shows little or no flap list activity, it is communicating reliably; the problem is probably in the subscriber's computer equipment or in the connection to the cable modem.
- The top 10% most active cable modems in the flap list are most likely to have difficulties communicating with the headend.
- Cable modems with more than 50 power adjustments per day have a suspect upstream path.
- Cable modems with approximately the same number of hits and misses and with a lot of insertions have a suspect downstream path (for example, low level into the cable modem).
- All cable modems incrementing the insertion at the same time indicates a provisioning server failure.
- Cable modems with high CRC errors have bad upstream paths or in-home wiring problems.
- Correlating cable modems on the same physical upstream port with similar flap list statistics can quickly resolve outside plant problems to a particular node or geography.
- Monitoring the flap list cannot affect cable modem communications.
- The flap list should be saved to a database computer and cleared at least once a day.
- Important upstream performance data can be obtained by tracking flap list trend data.
- Important installation quality control and performance data is directly available from the flap list.

## Displaying the Flap List

The flap list can be queried using either the standard Simple Network Management (SNMP) API or the CLI. Using any third party SNMP Management Information Base (MIB) browser, you can query the **ccsFlapTable** in the CISCO-CABLE-SPECTRUM-MIB, a proprietary extension to the DOCSIS MIBs.

To display the cable flap list on a Cisco uBR7200 series cable router, use the **show cable flap-list** command in privileged EXEC mode.

**Command:**

```
show cable flap-list [sort-flap | sort-time]
```

No default behavior or values.

**Syntax Description:**

**sort-flap**

(Optional) Sort by the number of times the cable modem has flapped.

**sort-time**

(Optional) Sort by the most recent time the cable modem is detected to have flapped.

**Sample:**

```

      MAC ID___ CableIF   Ins _Hit_   Miss   CRC   P-Adj   Flap   ___Time___
0010.7b6b.60ad C3/0 U0      0 14386  1390    1    38     41   Nov 24 21:34:24
0010.7b6b.65a3 C3/0 U0      0 14503  1264    1    33     37   Nov 24 21:28:09
0010.7b6b.6b9d C3/0 U0      0 14060  1726    3    40     43   Nov 24 21:18:36

```

**Table 7-2 Flap List Statistics Description**

Statistic	Description
MAC ID	This is the MAC-layer address of a cable modem. The first six digits indicate the vendor ID of the cable modem manufacturer, followed by six digits indicating a unique host address. Each cable modem's MAC address is unique.
Cable IF	This is the physical upstream interface on the Cisco uBR7200. It denotes the cable modem card slot number, the downstream port number on the RF line card and the upstream port number on the same cable modem card. The flap list data can be sorted based on the upstream port number which is useful when isolating reverse path problems unique to certain combining groups.
Insertions	<p>Link insertion is the initial maintenance procedure of a cable modem establishing link with the Cisco uBR7246VXR. The <b>Ins</b> column is the flapping modem's insertion count and indicates the number of times the RF link was abnormally re-established. An abnormality is detected when the time between link re-establishment attempts is less than the user-configured parameter.</p> <p>Normal modem activity follows the sequence below:</p> <ul style="list-style-type: none"> <li>• The initial link insertion is followed by a keepalive loop between the Cisco uBR7246VXR and cable modem and is called station maintenance.</li> <li>• Power-on</li> <li>• Initial maintenance</li> <li>• Station maintenance</li> <li>• Power-off</li> </ul> <p>When the link is broken, initial maintenance is repeated to re-establish the link.</p> <ul style="list-style-type: none"> <li>• Initial maintenance @ Time T1</li> <li>• Station maintenance</li> <li>• Init maintenance @ Time T2</li> </ul> <p>The <b>Ins</b> and <b>Flap</b> counters in the flap list are increased whenever <math>T2 - T1 &lt; N</math> where N is the insertion-time parameter configured in <code>&lt;cable flap-list insertion-time&gt;</code>. Default value for this parameter is TBD seconds.</p> <p>A high <b>Ins</b> number indicates:</p> <ul style="list-style-type: none"> <li>• Intermittent downstream sync loss</li> <li>• DHCP or modem registration problems</li> </ul>

Table 7-2 Flap List Statistics Description (continued)

Statistic	Description
Hit and Miss	<p>The <b>HIT</b> and <b>MISS</b> columns are keepalive polling statistics between the Cisco uBR7200 series and the cable modem. The station maintenance process occurs for every modem approximately every 25 seconds. When the router receives a response from the cable modem, the event is counted as a <b>Hit</b>. If the router does not receive a response from the cable modem, the event is counted as a <b>Miss</b>. A cable modem will fail to respond either because of noise or if it is down. Modems which only log <b>Misses</b> and zero <b>Hits</b> are assumed to be powered off.</p> <p><b>Misses</b> are not desirable since this is usually an indication of a return path problem; however, having a small number of misses is normal. The flap count is increased if there are <i>M</i> consecutive misses where <i>M</i> is configured in the <i>cable flap miss-threshold parameter</i>. The parameter value ranges from 1 to 12 with a default of 6.</p> <p>Ideally, the <b>HIT</b> count should be much greater than the <b>Miss</b> counts. If a cable modem has a <b>HIT</b> count much less than its <b>MISS</b> count, then registration is failing. Noisy links cause the <b>MISS/HIT</b> ratio to deviate from a nominal 1% or less. High <b>Miss</b> counts can indicate:</p> <ul style="list-style-type: none"> <li>• Intermittent upstream, possibly due to noise</li> <li>• Laser clipping</li> <li>• Common-path distortion</li> <li>• Ingress or interference</li> <li>• Too much or too little upstream attenuation</li> </ul>
Cyclical Redundancy Check (CRC)	<p>This statistic tracks the <b>CRC</b> error counter per modem. <b>CRC</b> errors are usually an indication of noise on a plant.</p> <p>A low count can be always be expected but a high <b>CRC</b> number calls for some the plant troubleshooting. The <b>CRC</b> counter indicates:</p> <ul style="list-style-type: none"> <li>• Intermittent upstream</li> <li>• Laser clipping</li> <li>• Common-path distortion</li> <li>• Impulsive noise or interference</li> </ul>



Table 7-2 Flap List Statistics Description (continued)

Statistic	Description
Power Adjustments (P-Adj)	<p>The station maintenance poll in the Cisco uBR7246VXR constantly adjusts the cable modem transmit power, frequency, and timing. The <b>P-Adj</b> column indicates the number of times the router instructs the cable modem to adjust transmit power more than 3dB. The power adjustment threshold may be set using the <i>cable flap power threshold</i> command with a value range of 0 to 10 dB and a default value of 2 dB. Tuning this threshold is recommended to decrease irrelevant entries in the flap list. Power Adjustment values of 2 dB and below will continuously increment the <b>P-Adj</b> counter. the cable modem transmitter step size is 1.5 dB, whereas the headend may command 0.25 dB step sizes. Power adjustment flap strongly suggests upstream plant problems such as:</p> <ul style="list-style-type: none"> <li>• Amplifier degradation</li> <li>• Poor connections</li> <li>• Thermal sensitivity</li> <li>• Attenuation problem</li> </ul>
Flap	<p>The <b>Flap</b> counter indicates the number of times the cable modem has flapped. This counter is increased when one of the following events is detected:</p> <p>Unusual modem insertion or re-registration attempts—The <b>Flap</b> and the <b>Ins</b> counters are increased when the cable modem tries to reestablish the RF link with the Cisco uBR7246VXR within a period of time that is less than the user-configured insertion interval value.</p> <p>Abnormal <b>Miss/Hit</b> ratio—The <b>Flap</b> counter is increased when <i>N</i> consecutive <b>Misses</b> are detected after a <b>Hit</b> here <i>N</i> can be configured with a default value of 6.</p> <p>Unusual power adjustment—The <b>Flap</b> and <b>P-adj</b> counters are increased when the cable modem's upstream power is adjusted beyond a configured power level.</p>
Time	<p><b>Time</b> is the timestamp indicating the last time the cable modem dropped the connection (flapped). The value is based on the clock configured on the local Cisco uBR7200 series. If no time is configured, this value is based on the current uptime of the Cisco uBR7200 series. When a cable modem meets one of the three flap list criteria, the <b>Flap</b> counter is increased and <b>Time</b> is set to the current time.</p>

## Troubleshooting with the Flap List

This section includes suggestions on how to interpret different network conditions based on the flap list statistics:

- **Condition 1:** Low miss/hit ratio (< 10% for MC11 card, < 2% for MC16 card), low insertion, low P-adj, low flap counter and old timestamp.  
**Analysis:** This exhibits an optimal network situation.
- **Condition 2:** High ratio of misses over hits (> 10%)  
**Analysis:** Hit/miss analysis should be done after the **Ins** count stops incrementing. In general, if the hit and miss counts are about the same order of magnitude, then the upstream may be experiencing noise. If the miss count is greater, then the cable modem is probably dropping out frequently and not completing registration. The upstream or downstream is perhaps not stable enough for reliable link establishment. Very low hits and miss counters and high insertion counters indicate provisioning problems.

- Condition 3:** Relatively high power adjustment counter.  
**Analysis:** Indicates the power adjustment threshold is probably set at default value of 2 dB adjustment. the cable modem transmitter step size is 1.5 dB, whereas the headend may command 0.25 dB step sizes. Tuning your power threshold to 6 dB is recommended to decrease irrelevant entries in the flap list. The power adjustment threshold may be set using <code><code>cable flap power threshold <0-10 dB></code></code> from the Cisco IOS global configuration mode. A properly operating HFC network with short amplifier cascades can use a 2-3 dB threshold.
- Condition 4:** High P-Adj and CRC errors.  
**Analysis:** This condition can indicate that the fiber node is clipping the upstream return laser. Evaluate the cable modems with the highest CRC count first. If the cable modems are not going offline (Ins = 0), this will not be noticed by the subscriber. However, they could receive slower service due to dropped IP packets in the upstream. This condition will also result in input errors on the Cisco uBR7200 series cable interface.
- Condition 5:** High insertion rate.  
**Analysis:** If link re-establishment happens too frequently, then the cable modem is usually having a registration problem. This is indicated by a high **Ins** counter which tracks the **Flap** counter.

## Configuring Flap List Parameters

You can set certain flap list parameters by using the commands described in the following sections.

### Setting Cable Flap List Aging

To specify the number of days to keep a cable modem in the flap-list table before aging it out of the table, use the **cable flap-list aging** command in global configuration mode. To disable this feature, use the **no** form of this command.

#### Command:

```
[no] cable flap-list aging number-of-days
```

#### Syntax Description:

*number-of-days*

Specifies how many days of cable modem performance is retained in the flap list. Valid values are from 1 to 60 days.

No default behavior or values.

The following example shows how to specify that the flap-list table retain two days of performance for this cable modem:

```
router(config)# cable flap-list aging 2
```

### Verifying Cable Flap List Aging

To verify that cable flap list aging is set, enter the following command and note the dates in the Time column:

```
show cable flap list
```

Mac Addr	CableIF	Ins	Hit	Miss	CRC	P-Adj	Flap	Time
0010.7b6b.5d1d	C3/0 U0	0	688	169	0	0	3 Nov 5	12:28:50
0010.7b6b.5e15	C3/0 U0	1	707	185	0	0	5 Nov 5	12:29:52
0010.7b6b.5e27	C3/0 U0	1	707	198	0	0	5 Nov 5	12:29:55
0010.7b6b.5d29	C3/0 U0	1	709	205	0	0	5 Nov 5	12:29:52
0010.7b6b.5e2b	C3/0 U0	1	710	204	0	0	7 Nov 5	12:30:16

## Setting Cable Flap List Insertion Time

You can set the cable flap list insertion time. When a cable modem makes an insertion request more frequently than the amount of insertion time defined by this command, the cable modem is placed in the flap list. The valid range is from 60 to 86400 seconds. A cable modem will not “flap” more than once in each insertion time interval.

To set the cable flap list insertion time interval, use the **cable flap-list insertion-time** command in global configuration mode. To disable insertion time, use the **no** form of this command.

### Command:

**[no] cable flap-list insertion-time** *seconds*

### Syntax Description:

*seconds*

Insertion time interval in seconds. Valid values are from 60 to 86,400 seconds.

No default behavior or values.

The following example shows how to set the insertion time interval to 62 seconds:

```
router(config)# cable flap-list insertion-time 62
```

## Verifying Cable Flap List Insertion Time

To verify cable flap list insertion time, enter the following command, and note the Time column:

```
show cable flap list
```

Mac Addr	CableIF	Ins	Hit	Miss	CRC	P-Adj	Flap	Time
0010.7b6b.5d1d	C3/0 U0	0	688	169	0	0	3 Nov 5	12:28:50
0010.7b6b.5e15	C3/0 U0	1	707	185	0	0	5 Nov 5	12:29:52
0010.7b6b.5e27	C3/0 U0	1	707	198	0	0	5 Nov 5	12:29:55
0010.7b6b.5d29	C3/0 U0	1	709	205	0	0	5 Nov 5	12:29:52
0010.7b6b.5e2b	C3/0 U0	1	710	204	0	0	7 Nov 5	12:30:16

## Setting Cable Flap List Power Adjustment Threshold

You can specify the minimum power adjustment threshold that will cause a flap-list event to be recorded. When the power adjustment of a cable modem meets or exceeds the threshold, the cable modem is placed in the flap list. The valid range is from 1 to 10 dBmV.



### Note

A power adjustment threshold of less than 2 dB might cause excessive flap list event recording. Cisco recommends setting this threshold value to 3 dB or higher.

To specify the power-adjust threshold for recording a flap list event, use the **cable flap-list power-adjust threshold** command in global configuration mode. To disable power-adjust thresholds, use the **no** form of this command.

### Command:

**[no] cable flap-list power-adjust threshold** *dB*

### Syntax Description:

*dB*—Specifies the minimum power adjustment, in decibels, that results in a flap-list event. Valid values are from 1 to 10 dB. The default value is 2 dB.

**Note**

For underground HFC networks with 4 amplifier cascade length, a typical threshold value should be 3 dB. For overhead HFC networks with 4 amplifier cascade length, a typical threshold value should be 4 dB. Longer coax cascades without return path thermal gain control and sites with extreme daily temperatures will have larger threshold ranges.

The following example shows the power-adjust threshold being set to 5 dB:

```
router(config)# cable flap-list power-adjust threshold 5
```

## Verifying Cable Flap List Power Adjustment Threshold

To verify the cable flap list power adjustment threshold, enter the following command, and note the values in the **P-Adj** column:

```
show cable flap list
```

Mac Addr	CableIF	Ins	Hit	Miss	CRC	P-Adj	Flap	Time
0010.7b6b.5d1d	C3/0 U0	0	688	169	0	0	3 Nov 5	12:28:50
0010.7b6b.5e15	C3/0 U0	1	707	185	0	0	5 Nov 5	12:29:52
0010.7b6b.5e27	C3/0 U0	1	707	198	0	0	5 Nov 5	12:29:55
0010.7b6b.5d29	C3/0 U0	1	709	205	0	0	5 Nov 5	12:29:52
0010.7b6b.5e2b	C3/0 U0	1	710	204	0	0	7 Nov 5	12:30:16

## Setting Cable Flap List Miss Threshold

You can specify the miss threshold for recording a flap-list event. A miss is the number of times a cable modem does not acknowledge a MAC layer keepalive message from a cable modem card. An 8% miss rate is normal for the Cisco cable modem cards. When the number of misses exceeds the threshold, the cable modem is placed in the flap list.

**Note**

A high miss rate can indicate intermittent upstream problems, fiber laser clipping, or common-path distortion.

To set the miss threshold for recording a flap list event, use the **cable flap-list miss-threshold** command in global configuration mode. To disable this function, use the **no** form of this command.

**Command:**

```
[no] cable flap-list miss-threshold misses
```

**Syntax Description:**

*misses*

Specifies the number of MAC-layer keepalive misses that results in the cable modems being placed in the flap list. Valid values are 1 to 12.

No default behavior or values.

The following example shows how to set the miss threshold to 5:

```
router(config)# cable flap-list miss-threshold 5
```

## Verifying Cable Flap List Miss Threshold

To verify the cable flap list miss threshold, enter the `show cable flap list` command and note the values in the **Miss** column:

**show cable flap list**

Mac Addr	CableIF	Ins	Hit	Miss	CRC	P-Adj	Flap	Time
0010.7b6b.5d1d	C3/0 U0	0	688	169	0	0	3 Nov 5	12:28:50
0010.7b6b.5e15	C3/0 U0	1	707	185	0	0	5 Nov 5	12:29:52
0010.7b6b.5e27	C3/0 U0	1	707	198	0	0	5 Nov 5	12:29:55
0010.7b6b.5d29	C3/0 U0	1	709	205	0	0	5 Nov 5	12:29:52
0010.7b6b.5e2b	C3/0 U0	1	710	204	0	0	7 Nov 5	12:30:16

## Setting Cable Flap List Size

You can specify the maximum number of cable modems that can be listed in the cable flap list tables. The valid range is from 1 to 8192 cable modems. The default is 8192 cable modems.

To specify the maximum number of cable modems that can be listed in the flap list, use the **cable flap-list size** command in global configuration mode. To specify the default flap-list table size, use the **no** form of this command.

**Command:**

**[no] cable flap-list size number**

**Syntax Description**

*number*

Specifies the maximum number of cable modems that will report flap performance to the flap-list table. Valid values are from 1 to 8192. The default value is 8192.

The following example shows how to limit the flap-list table size to no more than 200 modems:

```
router(config)# cable flap-list size 200
```

## Verifying Cable Flap List Size

To verify the cable flap list size, enter the `show cable flap list` command, and note the number of modems in the list:

**show cable flap list**

Mac Addr	CableIF	Ins	Hit	Miss	CRC	P-Adj	Flap	Time
0010.7b6b.5d1d	C3/0 U0	0	688	169	0	0	3 Nov 5	12:28:50
0010.7b6b.5e15	C3/0 U0	1	707	185	0	0	5 Nov 5	12:29:52
0010.7b6b.5e27	C3/0 U0	1	707	198	0	0	5 Nov 5	12:29:55
0010.7b6b.5d29	C3/0 U0	1	709	205	0	0	5 Nov 5	12:29:52
0010.7b6b.5e2b	C3/0 U0	1	710	204	0	0	7 Nov 5	12:30:16

## Clearing Cable Flap List

To remove a single cable modem from the flap list or to remove all cable modems from the flap list, use the **clear cable flap-list** command in privileged EXEC mode.

**Command:**

**clear cable flap-list [mac-addr | all]**

**Syntax Description:***mac-addr*

(Optional) MAC address. Specify the 48-bit hardware address of an individual cable modem.

**all**

(Optional) Remove all cable modems from the flap-list table.

No default behavior or values.

Cable modems are removed from the flap list table after the number of days (between 1 and 60) specified by the **cable flap-list aging** global configuration command. Use the **clear cable flap-list** command to remove individual cable modems from the flap list while retaining flapping activity for other cable modems, or to clear the entire flap list table.

The following example shows how to remove all the cable modems from the flap list table:

```
router# clear cable flap-list all
```

**Performing Amplitude Averaging**

The Cisco uBR7200 series uses an averaging algorithm to determine the optimum power level for a cable modem with low carrier-to-noise ratio that is making excessive power adjustments (flapping). To avoid dropping flapping cable modems, the Cisco uBR7200 series universal broadband router averages a configured number of RNG-REQ messages before it makes power adjustments. By compensating for a potentially unstable return path, the Cisco uBR7200 series router maintains connectivity with affected cable modems. You can interpret these power adjustments, however, as indicating unstable return path connections.

The **show cable flap-list** and **show cable modem** commands are expanded to indicate which paths the Cisco uBR7200 series is making power adjustments and which modems have reached maximum transmit power settings. These conditions indicate unstable paths that should be serviced.

The following example shows the output of the **show cable flap-list** command:

```
router# show cable flap-list
```

MAC Address	Upstream	Ins	Hit	Miss	CRC	P-Adj	Flap	Time
0010.7bb3.fd19	Cable5/0/U1	0	2792	281	0	*45	58	Jul 27 16:54:50
0010.7bb3.fcfc	Cable5/0/U1	0	19	4	0	!43	43	Jul 27 16:55:01
0010.7bb3.fcdd	Cable5/0/U1	0	19	4	0	*3	3	Jul 27 16:55:01

The \* symbol indicates that the CMTS is using the power adjustment method on this modem. The ! symbol indicates that the cable modem has reached maximum transmit power.

The following example shows the output of the **show cable modem** command:

```
router# show cable modem
```

Interface	Prim	Online	Timing	Rec	QoS	CPE	IP address	MAC address	Sid
Cable3/0/U0 1		online	2257	0.00	3	0	10.30.128.142	0090.8330.0217	
Cable3/0/U0 2		online	2262	*-0.50	3	0	10.30.128.145	0090.8330.020f	
Cable3/0/U0 3		online	2260	0.25	3	0	10.30.128.146	0090.8330.0211	
Cable3/0/U0 4		online	2256	*0.75	3	0	10.30.128.143	0090.8330.0216	
Cable3/0/U0 5		online	2265	*0.50	3	0	10.30.128.140	0090.8330.0214	
Cable3/0/U0 6		online	2256	0.00	3	0	10.30.128.141	0090.8330.0215	
Cable3/0/U0 7		online	4138	!-1.00	3	1	10.30.128.182	0050.7366.124d	
Cable3/0/U0 8		online	4142	!-3.25	3	1	10.30.128.164	0050.7366.1245	
Cable3/0/U0 9		online	4141	!-3.00	3	1	10.30.128.185	0050.7366.17e3	
Cable3/0/U0 10		online	4142	!-2.75	3	0	10.30.128.181	0050.7366.17ab	
Cable3/0/U0 11		online	4142	!-3.25	3	1	10.30.128.169	0050.7366.17ef	

Similar to the **show cable flap-list** display, the \* symbol in the **show cable modem** output indicates that the Cisco uBR7246VXR is using the power adjustment method on this modem. The ! symbol indicates that the cable modem has reached maximum transmit power.

The following commands pertaining to amplitude averaging, and are discussed in more detail in the following sections:

**cable upstream power-adjust noise**

**cable upstream frequency-adjust averaging**

## Enabling or Disabling Power Adjustment

To enable or disable the power adjustment capability, use the following commands:

**cable upstream *n* power-adjust [ threshold *threshold #* | continue *tolerable value* | noise % of power adjustment ]**

**no cable upstream power-adjust**

Table 7-3 displays descriptions of the arguments in the **cable upstream power-adjust** command.

**Table 7-3 Cable Upstream Power Adjust Syntax Descriptions**

Syntax	Valid Values
<i>n</i>	Specifies the upstream port number.
<i>threshold #</i>	Specifies the power adjustment threshold. The threshold range is from 0 through 10 dB. The default is 1 dB.
<i>tolerable value</i>	Determines if the status of the RNG-RSP should be set to CONTINUE or SUCCESS. The range is from 2 through 15 dB. The default is 2 dB.
<i>% of power adjustment</i>	Specifies the percentage of power adjustment packets required to switch from the regular power adjustment method to the noise power adjustment method. Range is from 10 through 100 percent. The default is 30 percent.



### Note

The threshold default is 1 dB. The tolerable value default is 2 dB. The power adjustment is 30 percent.



### Caution

Default settings are adequate for system operation. Amplitude averaging is an automatic procedure. In general, Cisco does not recommend you adjust values. Cisco does recommend, however, that you clean up your cable plant should you encounter flapping cable modems.



### Note

In some instances, you might adjust certain values:

If cable modems cannot complete ranging because they have reached maximum power levels, you might try to set the tolerable value CONTINUE field to a larger value than the default of 2 dB. Values larger than 10 dB on “C” versions of cable modem cards, or 5 dB on FPGA versions, are not recommended.

If the flap list shows modems with a large number of power adjustments, but the cable modems are not detected as “noisy,” you might try to decrease the percentage for “noisy”. If you think too many modems are unnecessarily detected as “noisy,” you might try to increase it.

## Setting Frequency Threshold to Affect Power Adjustment

To control power adjustment methods by setting the frequency threshold, use the **cable upstream freq-adj averaging** interface configuration command. To disable power adjustments, use the **no** form of this command.

**cable upstream *n* freq-adj averaging *% of frequency adjustment***

**no cable upstream freq-adj averaging**

Table 7-4 displays descriptions of the arguments in the **cable upstream freq-adj averaging** command.

**Table 7-4 Cable Upstream Power Adjust Syntax Descriptions**

Syntax	Valid Values
<i>n</i>	Specifies the upstream port number.
<b>averaging</b>	Specifies that a percentage of frequency adjustment packets is required to change the adjustment method from the regular power adjustment method to the noise power adjustment method.
<i>% of frequency adjustment</i>	Specifies the percentage of frequency adjustment packets required to switch from the regular power adjustment method to the noise power adjustment method. Valid range is from 10 through 100 percent.

The following example shows how to change the power adjustment method when the frequency adjustment packet count reaches 50 percent:

```
router(config-if)# cable upstream 0 freq-adj averaging 50
```

## Additional Diagnostic Commands

The commands described in the following are used in addition to the flap list commands to help you in troubleshooting uBR and cable modem problems.

### Pinging Unresponsive Cable Modems

Ping DOCSIS allows you to quickly diagnose the health of a channel between the Cisco uBR7200 series universal broadband router and the cable modem. The technology uses 1/64—the bandwidth of IP ping—and works with cable modems that don't have an IP address. This allows you to ping cable modems that are unable to complete registration, have internal bugs, or that are unresponsive due to a crash.

The Ping DOCSIS feature provides a real-time view and plot of requested power adjustments, as well as a measure of optimal headend reception power. This gives you the ability to solicit a configured number of periodic ranging requests from a cable modem.

To ping a specific cable modem to determine if it is online, use the following command (with a specific MAC address) in privileged EXEC mode:

**ping docsis *addr***



The following example confirms that the cable modem at 0050.7366.2223 is connected to the network and is operational:

```
# ping docsis 0050.7366.2223
```

```
Queueing 5 MAC-layer station maintenance intervals, timeout is 25 msec:
```

```
!!!!
```

```
Success rate is 100 percent (5/5)
```

Following are the keys used for the ping response messages:

<b>f</b>	The ping message failed.
<b>.</b>	The ping message timed out without getting a response.
<b>!</b>	The ping message was successfully sent and a reply is received.



#### Tips

If you are having trouble, make sure you are using a valid MAC address for the cable modem you want to ping.

## Setting Downstream Test Signals

This section provides configuration commands that allow you to create downstream test signals. Both Pseudo Random Bit Stream (PRBS) and unmodulated carrier test signals are supported.

A PRBS test signal is a random data pattern that has been modulated to look like a real data stream. An unmodulated test signal is a continuous sine wave that looks like a carrier wave on the downstream transmission.

### Generating Unmodulated Test Signals

To generate unmodulated test signals, perform the steps in Table 7-5 in the configure interface mode.

**Table 7-5 Procedure to Generate Unmodulated Test Signals**

Step	Command	Description
1	Router(config-if)# <b>cable downstream if-output continuous-wave</b>	Generates an unmodulated continuous-wave signal on the downstream channel. The interface is shut down.
2	Router(config-if)# <b>no cable downstream if-output</b>	Stops sending test signals. <b>Note</b> Remember to re-enable the interface to resume normal operations.

## Generating PRBS Test Signals

To configure Pseudo Random Bit Stream (PRBS) test signals, perform the steps in Table 7-6 in the configure interface mode.

**Table 7-6 Procedure to Generate PRBS Test Signals**

Step	Command	Description
1	Router(config-if)# <b>cable downstream if-output prbs</b>	Generates a PRBS test signal on the downstream channel. The interface is shut down.
2	Router(config-if)# <b>no cable downstream if-output</b>	Stops sending test signals. <b>Note</b> Remember to re-enable the interface to resume normal operations.

## Verifying Test Signal Output

To verify the output of a continuous-wave test signal or the output of a PRBS test signal, use a spectrum analyzer on the downstream channel. The downstream carrier is enabled as a default.

The standard mode of operation is modulated signal output and the interface is active. For PRBS and continuous wave output, the selected interface will be shut down.

The functioning of the **no cable downstream if-output** command has not changed. The interface is shut down.

## Displaying Per-SID Counters for Bandwidth Requests

Data transport over the RF link uses the registered SID address, rather than the Ethernet address. This allows multiple hosts to access the network by using a single cable modem.

To display per-SID counters for bandwidth requests, use the following command in the privileged EXEC mode:

```
show interface cable interface sid sid counters verbose
```

The **show int cx/y sid** command displays more complete Service ID (SID) status information.

Sample outputs:

The following command displays sample output for the verbose keyword extension for SID 1 on interface cable slot 3, port 0:

```
router# show interface c3/0 sid 1 counters verbose
```

```
Sid : 1
Input packets : 39
Input octets : 15964
Output packets : 30
Output octets : 8796
BW requests received : 40
Grants issued : 40
Rate exceeded BW request drops : 0
Rate exceeded DS packet drops : 0
```

The following command displays output for the verbose keyword extension for all SIDs on the specified interface:

```
router# show interface c3/0 sid counters verbose
```

```

Sid : 1
Input packets : 39
Input octets : 15964
Output packets : 30
Output octets : 8796
BW requests received : 40
Grants issued : 40
Rate exceeded BW request drops : 0
Rate exceeded DS packet drops : 0
Sid : 2
Input packets : 0
Input octets : 0
Output packets : 0
Output octets : 0
BW requests received : 0
Grants issued : 0
Rate exceeded BW request drops : 0
Rate exceeded DS packet drops : 0
Sid : 3
Input packets : 0
Input octets : 0
Output packets : 0
Output octets : 0
BW requests received : 0
Grants issued : 0
Rate exceeded BW request drops : 0
Rate exceeded DS packet drops : 0

```

The following command displays data for the SIDs connected to the specified interface:

```
router# show inter cab 3/0 sid
```

Sid	Prim Sid	Type	Online State	Admin Status	QoS	Create Time	IP Address	MAC Address
23		stat	init(d)	enable	2	04:00:54	209.165.200.0	0050.7366.17ab
24		stat	init(d)	enable	2	04:00:58	209.165.200.0	0050.7366.1803
25		stat	init(rc)	enable	2	04:01:05	209.165.200.0	00d0.bad3.c459
26		stat	init(d)	enable	2	04:01:10	209.165.200.0	0050.7366.1801
27		stat	offline	enable	2	04:01:31	209.165.200.225	0090.8330.0213
28		stat	offline	enable	2	04:01:59	209.165.200.226	0090.8330.0211
29		stat	offline	enable	2	04:02:07	209.165.200.227	0090.8330.0214
30		dyn	init(o)	enable	2	04:03:09	209.165.200.228	0090.833

The following command displays connection information for all SIDs on the specified interface:

```
router# show interface c3/0 sid connectivity
```

Sid	1st time	Times Online	%online	Online time			Offline time		
	online			min	avg	max	min	avg	max
1	15:37:24	1	99.73	00:00	1h45m	1h45m	00:17	00:17	00:17
2	15:37:24	1	99.73	00:00	1h45m	1h45m	00:17	00:17	00:17
3	15:37:24	1	99.73	00:00	1h45m	1h45m	00:17	00:17	00:17

The following command displays connection information for SID 1 on the specified interface:

```
router# show interface c3/0 sid 1 connectivity
```

Sid	1st time	Times Online	%online	Online time			Offline time		
	online			min	avg	max	min	avg	max
1	15:37:24	1	99.72	00:00	1h41m	1h41m	00:17	00:17	00:17

The following command displays the counters of the SIDs connected to the specified interface:

```
router# show interface c3/0 sid counters
  Sid  Inpackets  Inoctets  Outpackets  Outoctets  Ratelimit  Ratelimit
      1     40      16586     31         9160      BWReqDrop  DSPktDrop
      2     0         0         0           0         0          0
      3     0         0         0           0         0          0
```

Table 7-7 describes the fields shown in the output for the **show interface cable sid** displays.

**Table 7-7** *show interface cable sid Command Field Descriptions*

Field	Description
Sid	Service identification number.
Prim Sid	The primary service identifier assigned to the cable modem.
Type	Indicates this SID was created statically at time of registration or dynamically by the exchange of dynamic service messages between the cable modem and the Cisco uBR7246VXR.
Online State	“Online” means the cable modem owning this SID is processing traffic. “Offline” means the cable modem owning this SID is not processing traffic.
Admin Status	“Disable” means that the SID has been turned off. “Enable” is the normal state.
QoS	Quality of service.
Create time	When SID was created, number of seconds since system booted.
Input octets (Inoctets)	Number of octets received by using this SID.
Input packets (Inpackets)	Number of packets received by using this SID.
Output octets (Outoctets)	Number of octets sent from this SID.
Output packets (Outpackets)	Number of packets sent from this SID.
IP address	IP address of the cable modem owning this SID.
MAC address	MAC address of the cable modem owning this SID.
BW requests received	Number of bandwidth requests received by this SID.
Grants issued	Number of bandwidth requests granted by this SID.
Rate exceeded BW request drops	Number of bandwidth requests not granted by this SID.
Rate exceeded DS packet drops	Number of downstream packets lost by this SID.
Ratelimit BWReqDrop	Number of bandwidth requests not granted by this SID.
Ratelimit DSPktDrop	Number of downstream packets lost by this SID.
1st time online	Time at which the cable modem with this SID connected.
Times online	Number of times the cable modem with this SID has connected.
% online	Percentage of time the cable modem with this SID has been connected.
Online time	The minimum, average, and maximum number of hours and minutes the cable modem with this SID has been connected.
Offline time	The minimum, average, and maximum number of hours and minutes the cable modem with this SID has been disconnected.

## Displaying Type of Service (ToS) Specifications

The following command displays ToS specifications:

```
uBR7200#show cable qos profile
```

Service class	Prio	Max upstream bandwidth	Guarantee upstream bandwidth	Max downstream bandwidth	Max tx burst	TOS mask	TOS value	Create by	B priv enab
1	0	0	0	0	0	0x0	0x0	cmts(r)	no
2	0	64000	0	1000000	0	0x0	0x0	cmts(r)	no
3	0	1000	0	1000	0	0x0	0x0	cmts	no
4	3	256000	0	512000	0	0x0	0x0	cm	no
5	5	1000000	0	10000000	0	0x0	0x0	cm	no
6	3	256000	0	512000	0	0x0	0x0	cm	yes

Note: The “r” in the “Create by” column means the first two classes of service the Cisco uBR7246VXR creates are reserved for cable modems that are not online.

## Displaying Cable Interface Data

To display cable interface information, use the following command in privileged EXEC mode:

```
show interface cable slot/port [downstream | upstream] port
```

The following command displays output for a cable modem located in slot 3/port 0 with detailed MAC scheduler state information for the upstream port:

```
router# show interface cable 3/0 upstream 0
```

```
Cable3/0: Upstream 0 is up
  Received 16873 broadcasts, 0 multicasts, 73310 unicasts
  0 discards, 89053 errors, 0 unknown protocol
  90183 packets input, 1 uncorrectable
  89042 noise, 0 microreflections
  Total Modems On This Upstream Channel : 8 (4 active)
  Default MAC scheduler
  Queue[Rng Polls] 0/20, fifo queueing, 0 drops
  Queue[Cont Mslots] 0/104, fifo queueing, 0 drops
  Queue[CIR Grants] 0/20, fair queueing, 0 drops
  Queue[BE Grants] 0/30, fair queueing, 0 drops
  Queue[Grant Shpr] 0/30, calendar queueing, 0 drops
  Reserved slot table currently has 0 CBR entries
  Req IEs 134469315, Req/Data IEs 0
  Init Mtn IEs 385879, Stn Mtn IEs 131059
  Long Grant IEs 10766, Short Grant IEs 15895
  Avg upstream channel utilization : 1%
  Avg percent contention slots : 97%
  Avg percent initial ranging slots : 0%
  Avg percent minislots lost on late MAPs : 0%
  Total channel bw reserved 0 bps
  CIR admission control not enforced
  Current minislot count : 6676390 Flag: 0
  Scheduled minislot count : 6676545 Flag: 0
```

Table 7-8 describes the fields shown in the **show interface cable upstream** display.

**Table 7-8 Show Interface Cable Upstream Command Field Descriptions**

Field	Description
Cable	Indicates the location of the upstream interface.
Upstream is up/...administratively down	Indicates the administrative state of the upstream interface.
Received broadcasts	Number of broadcast packets received through this upstream interface.
Multicasts	Number of multicast packets received through this upstream interface.
Unicasts	Number of unicast packets received through this interface.
Discards	Number of packets discarded by this interface.
Errors	Sum of all errors that prevented upstream transmission of packets through this interface.
Unknown protocol	Number of packets received that were generated using a protocol unknown to the Cisco uBR.
Packets input	Number of packets received through this upstream interface that were free from errors.
Corrected	Number of error packets received through this upstream interface that were corrected.
Uncorrectable	Number of error packets received through this upstream interface that could not be corrected.
Noise	Number of upstream packets corrupted by line noise.
Microreflections	Number of upstream packets corrupted by microreflections.
Guaranteed-rate service queue depth	Number of bandwidth requests queued up in the Guarantee-rate queue. This queue is only available to modems that have a reserved minimum upstream rate in their Class of Service.
Best-effort service queue depth	Number of bandwidth requests queued up in the Best-effort queue. This queue is available to all modems that do not have any reserved rate on the upstream.
Total Modems On This Upstream Channel	Number of cable modems currently sharing this upstream channel. This field also shows how many of these modems are active.

**Table 7-8 Show Interface Cable Upstream Command Field Descriptions (continued)**

Field	Description
Current Total Bandwidth Reserved	Total amount of bandwidth reserved by all modems sharing this upstream channel that require bandwidth reservation. The Class of Service for these modems specifies some non-zero value for the guaranteed-upstream rate. When one of these modems is admitted on the upstream, this field value is increased by this guaranteed-upstream rate value.
CIR admission control (formerly: Current Admission Control Status)	Indicates the status of admission control on the upstream channel.  ENFORCED status allows users to enable admission control on a per port basis. This controls how limited bandwidth is allocated. NOT ENFORCED status indicates that there is no admission control. Every modem that registers with a class of service specifying a minimum upstream rate will be admitted by the Cisco uBR7246VXR regardless of how much aggregate bandwidth is actually available.  Users enable admission control by using the admission control CLI.
Default MAC scheduler	Indicates the status of the MAC scheduler as being in default mode as opposed to Automated Test Procedure (ATP).
Queue[Rng Polls]	The MAC scheduler queue showing the number of ranging polls.
Queue[Cont Mslos]	The MAC scheduler queue showing the number of forced contention request slots in MAPS.
Queue[CIR Grants]	The MAC scheduler queue showing the number of CIR grants pending.  For example, "Queue [CIR Grants] 0/20, fair queueing, 0 drops" means that the queue for CIR-service grants has a current depth of 0, a maximum depth of 20. Weighted fair queueing shows grants in this queue.
Queue[BE Grants]	The MAC scheduler queue showing the number of BE grants pending.
Queue[Grant Shpr]	The MAC scheduler queue showing the number of grants that have been buffered for traffic shaping.
Drops	Number of packets dropped.
Reserved slot table currently has 0 CBR entries	Number of CBR sessions active on an upstream channel at any given time.
Req IEs	The running counter of request IEs sent in MAPS.
Req/Data IEs	The counter of request/data IEs sent in MAPS.

**Table 7-8 Show Interface Cable Upstream Command Field Descriptions (continued)**

Field	Description
Init Mtn IEs	The counter of Initial Maintenance IEs; that is, counters for each type of upstream slot scheduled in the MAPs for this upstream channel.  For example, “Init Mtn IEs 800” means that the MAC scheduler has added 800 initial maintenance information elements (slots) at the time the show command was issued.
Stn Mtn IEs	Number of station maintenance (ranging poll) IEs.
Long Grant IEs	Number of long grant IEs.
Short Grant IEs	Number of short grant IEs.
Avg upstream channel utilization	Indicates on average what percent of the upstream channel bandwidth is being used.
Avg percent contention slots	Indicates on average what percent of slots are in contention state.
Avg percent initial ranging slots	Indicates on average what percent of slots are in initial ranging state.
Avg percent minislots lost on late MAPs	Indicates on average what percent of slots are lost because a MAP interrupt was too late.
Current minislot count (formerly: Last Minislot Stamp (current_time_base))	Indicates the current minislot count at the CMTS. FLAG indicates the timebase reference. This field is used only by developers.
Scheduled minislot count (formerly: Last Minislot Stamp (scheduler_time_base))	Indicates the furthest minislot count allocated at the indicated time. FLAG indicates the timebase reference. This field is used only by developers.

The following command displays output for the downstream cable interface of slot 6 on port 0:

```
router# show interface cable 6/0 downstream

Cable6/0: Downstream is up
      111947771 packets output, 1579682655 bytes, 0 discarded
      0 output errors
```

## Upstream and Downstream Traffic Shaping

The Cisco uBR7200 series universal broadband router supports buffering both upstream and downstream grants to cable modems that are exceeding their allocated bandwidth. This strategy helps to avoid the TCP timeouts and the retransmission of the associated packets which would further degrade overall throughput.

The **cable downstream *port number* rate-limit token-bucket shaping** and **cable upstream *port number* rate-limit token-bucket shaping** commands configure the Cisco uBR7200 series universal broadband router to perform rate shaping by buffering the grants for rate-exceeded modems.



## Using uBR MIBs

Refer to [Chapter 11, “Element Management and MIBs,”](#) for a description of useful MIBs for uBRs.

Also refer to [Chapter 3, “Trouble Isolation Procedures,”](#) for suggestions on using specific MIB objects in troubleshooting.

## Using Debug Commands

Using CMTS debug commands on a large, in-service network is not recommended. These commands can generate large amounts of output, and dramatically affect router performance. Therefore, we have not included any debug commands for the Cisco uBR7200 series in this guide.

For information on debug commands, go to [Cisco Connection Online \(http://www.cisco.com\)](http://www.cisco.com).

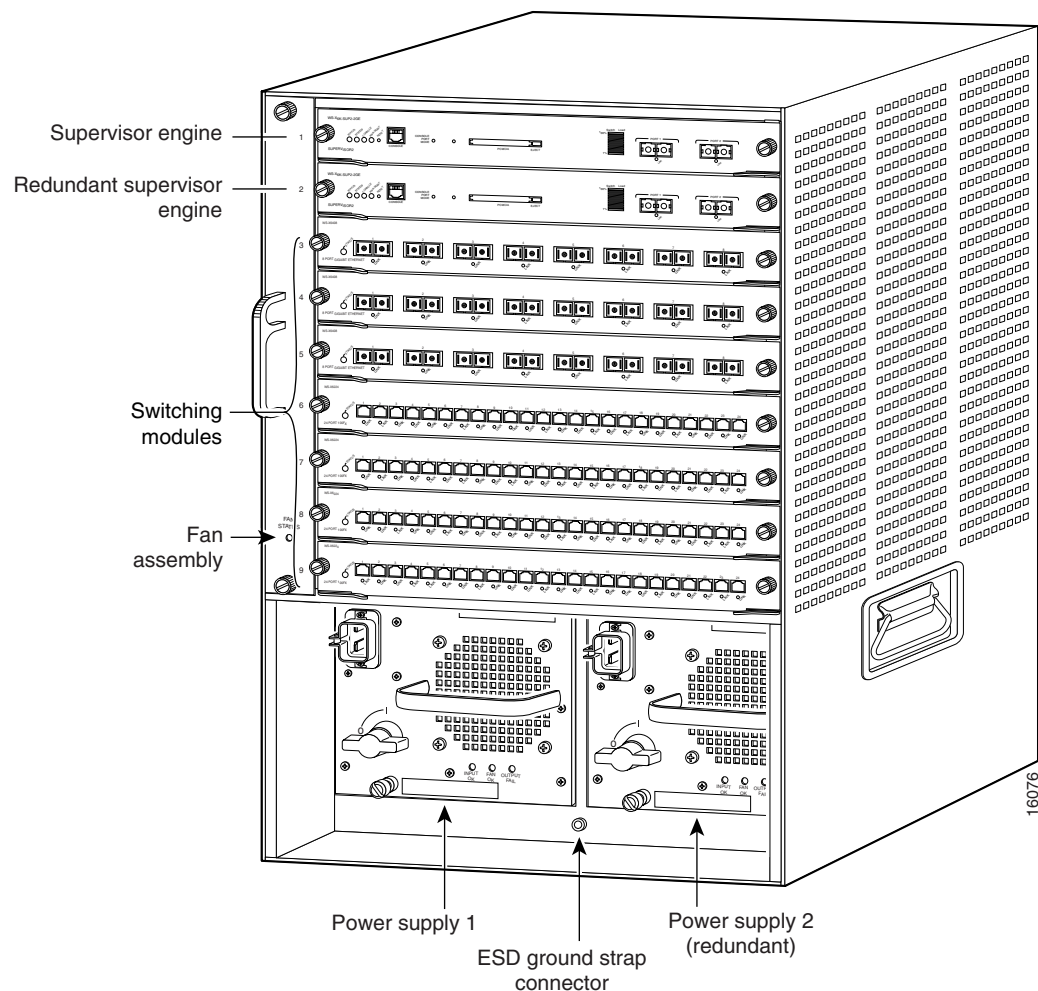




## Troubleshooting the Cisco Catalyst 6509

Cisco Catalyst 6509 Ethernet switches, deployed in a redundant configuration to provide high reliability, are used in the BLISS for Cable solution to provide Layer 2 connectivity for the Cisco BTS 10200, Layer 3 functionality for routing signaling packets to edge and trunking gateways, and to interconnect all servers within the SuperPOP. Each switch is configured with redundant processors, switch fabric, internal clock, power supply and fans to provide high level redundancy with redundant router modules.

**Figure 8-1** Cisco Catalyst 6509 Ethernet LAN Switch



Catalyst 6509 Ethernet switches are used to aggregate traffic from Trunk Gateways, Network Servers, Call Agent and the NMS server. The connections are Fast Ethernets. The key features of the Catalyst 6500 IP switch router include wirespeed Layer 3 IP, IP multicast, and forwarding across Ethernet, Fast EtherChannel (FEC), and Gigabit EtherChannel (GEC) capability. The switch router supports virtual LANs between switches via the Inter-Switch Link (ISL) trunk protocol and the 802.1q standard. The switch router also provides high quality of service (QoS) capabilities, including support for four queues per port and flow classification based on IP precedence bits.

The Catalyst 6509 is a multi-layer internal LAN switching component. It can provide high port density Ethernet/Fast Ethernet and Gigabit switching functions. The Catalyst 6509 switch is a NEBS level-3 compliant product. It supports a wide range of interface types and densities including support for up to 384 10/100 Ethernet ports, 192 100 FX Fast Ethernet ports, and up to 130 Gigabit Ethernet ports.

The Catalyst 6509 switch also provides seamless LAN/WAN convergence in a single multi-layer switching platform using a FlexWAN module. A wide variety of WAN interfaces, including T1/E1, T3/E3, OC-3 ATM, and Packet over SONET (POS) functionality are supported via the port adapter technology from Cisco 7200/7500 series platforms.

The Catalyst 6509 supports both 6 slot and 9 slot versions, providing a wide range of configuration and price/performance options. The architecture of the Catalyst 6500 Series supports scalable switching bandwidth up to 256 Gbps and scalable multilayer switching up to 150 Mpps.

The Ethernet switches connect into the Cisco GSR12000 or ESR10000 via Gigabit Ethernet. The routing protocol between the CAT switches and the Call Agent is IRDP and it is OSPF in the rest of the core network. The 6509s run HSRP so that they appear to have a single virtual IP and MAC address for the call agent that operate best in a single LAN environment. Multiple 100Base T (Fast Ether Channel) links between the Catalyst switches are used to maintain the throughput in case of a Gigabit Ethernet link failure between CSR and GSR (card fail, fiber cut, and so on).

### Interfaces

- 130 ports of Gigabit Ethernet (SX LX/LH, and ZX interfaces via GBICs) are supported
- 192 ports of 100BaseFX MMF (MT-RJ)
- 384 ports 10/100BaseTX (RJ-45 and RJ-21 Options)
- ATM OC12 (Single mode and Multimode Options)

### Features

- All components are hot swappable
- Hot Standby Routing Protocol (HSRP)
- QoS for voice: LLQ, TOS

### Other Data Features

- Routing: static routing, RIP, OSPF
- QoS: WRED, CBWFQ
- IP Security: access lists (ACL)

### Management Features

- SNMP v2, FTP, Telnet, CLI, DHCP
- Domain Name System (DNS), and dynamic VLAN services

### Signaling

- Point to Point Protocol (PPP)

**Redundancy**

- Redundant Switch Fabrics (Catalyst 6500 Series only)
- Redundant power supply and cooling
- Redundant System Clocks
- Redundant Supervisors
- Redundant Uplinks

## Troubleshooting the Switch

There are many ways to troubleshoot a switch. As the features of switches grow, the possible things that can break also increase. If you develop an approach or test plan for troubleshooting, you will be better off in the long run than if you just try a hit-and-miss approach. Here are some general suggestions for making your troubleshooting more effective:

- Take the time to become familiar with normal switch operation. Cisco's web site has a tremendous amount of technical information describing how their switches work, as mentioned in the previous section. The configuration guides in particular are very helpful. Many cases are opened with Cisco's TAC (Technical Assistance Center) that are solved with information from the product configuration guides.
- For the more complex situations, have an accurate physical and logical map of your network. A physical map shows how the devices and cables are connected. A logical map shows what segments (VLANs) exist in your network, and which routers provide routing services to these segments. A spanning tree map is highly useful for troubleshooting complex issues. Because of a switch's ability to create different segments by implementing VLANs, the physical connections alone do not tell the whole story; one has to know how the switches are configured to determine which segments (VLANs) exist, and to know how they are logically connected.
- Have a plan. Some problems and solutions are obvious, some are not. The symptoms that you see in your network may be the result of problems in another area or layer. Before jumping to conclusions, try to verify in a structured way what is working and what is not. Since networks can be complex, it is helpful to isolate possible problem domains. One way of doing this is by using the OSI seven-layer model. For example: check the physical connections involved (layer 1), check connectivity issues within the VLAN (layer 2), check connectivity issues across different VLANs (layer 3), etc. Assuming a correct configuration on the switch, many of the problems you encounter will be related to physical layer issues (physical ports and cabling). Today, switches are involved in layer 3 and 4 issues, incorporating intelligence to switch packets based on information derived from routers, or by actually having routers living inside the switch (layer three or layer four switching).
- Do not assume a component is working without checking it first. This can save you a lot of wasted time. For example, if a PC is not able to log in to a server across your network, there are many things that could be wrong. Don't skip the basic things and assume something works - someone might have changed something without telling you. It only takes a minute to check some of the basic things (for example, that the ports involved are connected to the right place and active), which could save you many wasted hours.

## Troubleshooting Port Connectivity

If the port doesn't work, nothing works! Ports are the foundation of your switching network. Some ports have special significance because of their location in the network, and the amount of traffic they carry. These ports would include connections to other switches, routers, and servers. These ports can be more

complicated to troubleshoot because they often take advantage of special features like trunking and EtherChannel. The rest of the ports are significant as well because they connect the actual users of the network.

Many things can cause a port to be non-functional: hardware issues, configuration issues, and traffic issues. Let's look at these categories a little deeper.

## Hardware Issues

Port functionality requires two working ports connected by a working cable (assuming it is of the correct type). Most Cisco switches default to having a port in "notconnect" state, which means it is currently not connected to anything but it is willing to connect. If you connect a good cable to two switch ports in the "notconnect" state, the link light should become green for both ports and the port status should say "connected", which means the port is up as far as layer 1 is concerned. The following paragraphs point out items for which to check if layer 1 is not up

Check the port status for both ports involved. Make sure that neither port involved in the link is shutdown. The administrator could have manually shut down one or both ports. Software inside the switch could have shut the port down because of configuration error conditions (we will expand on this later). If one side is shutdown and the other is not, the status on the enabled side will be "notconnect" (because it does not sense a neighbor on the other side of the wire). The status on the shutdown side would say something like "disable" or "errDisable" (depending on what actually shut the port down). The link will not come up unless both ports are enabled.

When you hook up a good cable (again, assuming it is of the correct type) between two enabled ports they should show a green link light within a few seconds. Also, the port state should show "connected" in the command line interface (CLI). At this point, if you do not have link, your problem is limited to three things: the port on one side, the port on the other side, or the cable in the middle. In some cases there are other devices involved: media converters (fiber to copper, etc.), or on Gigabit links you may have gigabit interface connectors (GBICs). Still, this is a reasonably limited area to search.

Media converters can add noise to a connection or weaken the signal if they are not functioning correctly. They also add extra connectors that can cause problems, and are also another component to debug.

Check for loose connections. Sometimes a cable appears to be seated in the jack, but it actually isn't; unplug the cable and re-insert it. You should also look for dirt or broken or missing pins. Do this for both ports involved in the connection.

The cable could be plugged in to the wrong port, which commonly happens. Make sure both ends of the cable are plugged in to the ports where you really want them.

You can have link on one side and not on the other. Check both sides for link. A single broken wire can cause this type of problem.

A link light does not guarantee that the cable is fully functional. It may have encountered physical stress that causes it to be functional at a marginal level. Usually you will notice this by the port having lots of packet errors.

To determine if the cable is the problem, swap it with a known good cable. Don't just swap it with any other cable; make sure that you swap it with a cable that you know is good, and is of the correct type. If this is a very long cable run (underground, across a large campus, for example) then it would be nice to have a sophisticated cable tester. If you do not have a cable tester, you might consider:

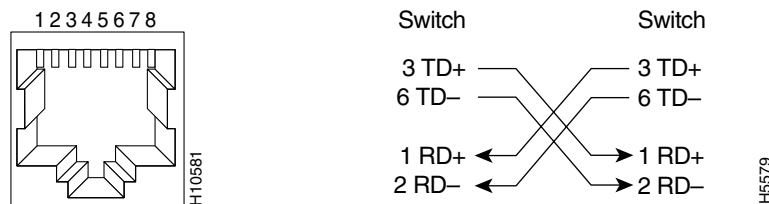
- Trying different ports to see if they come up using this long cable.
- Connecting the port in question to another port in the same switch just to see if the port will link up locally.
- Temporarily relocating the switches near each other so you can try out a known good cable

## Copper

Make sure you have the correct cable for the type of connection you are making. Category 3 cable can be used for 10MB UTP connections, but category 5 should be used for 10/100 connections.

A straight-through RJ-45 cable is used for end-stations, routers or servers to connect to a switch or hub. An Ethernet crossover cable is used for switch to switch, or hub to switch connections. Below is the pin-out for an Ethernet crossover cable. Maximum distances for Ethernet or Fast Ethernet copper wires are 100 meters. A good general rule of thumb is that when crossing an OSI layer, like between a switch and a router, use a straight-through cable; when connecting two devices in the same OSI layer, like between two routers or two switches, use a cross over cable. For purposes of this rule only, treat a workstation like a router.

The following two graphics show the pin-outs required for a switch-to-switch crossover cable.



## Fiber

For fiber, make sure you have the correct cable for the distances involved and the type of fiber ports being used (single mode, multi mode). Make sure the ports being connected together are both single mode, or both multimode ports. Single mode fiber generally reaches 10 kilometers, multimode fiber can usually reach 2 kilometers, but there is the special case of 100BaseFX multimode used in half duplex mode which can only go 400 meters.

For fiber connections, make sure the transmit lead of one port is connected to the receive lead of the other port, and vice versa; transmit to transmit, receive to receive, will not work.

For gigabit connections, GBICs need to be matched on each side of the connection. There are different types of GBICs depending on the cable and distances involved: Short wavelength (SX), long wavelength/long haul (LX/LH), and extended distance (ZX).

For gigabit connections, GBICs need to be matched on each side of the connection. There are different types of GBICs depending on the cable and distances involved: short wavelength (SX), long wavelength/long haul (LX/LH), and extended distance (ZX). An SX GBIC needs to connect with an SX GBIC; an SX GBIC will not link with an LX GBIC. Also, some gigabit connections require conditioning cables depending on the lengths involved. Please refer to the GBIC installation notes.

If your gigabit link will not come up, check to make sure the flow control and port negotiation settings are consistent on both sides of the link. There could be incompatibilities in the implementation of these features if the switches being connected are from different vendors. If in doubt, turn these features off on both switches.

## Configuration Issues

Another cause of port connectivity issues is incorrect software configuration of the switch. If a port has a solid orange light, that means that software inside the switch shut down the port, either by way of the user interface or by internal processes.

Make sure that the administrator has not shut down the ports involved (as mentioned earlier). The administrator could have manually shut down the port on one side of the link or the other. This link will not come up until you re-enable the port; check the port status.

Some switches, such as the Catalyst 4000/5000/6000, may shut down the port if software processes inside the switch detect an error. When you look at the port status, it will read "errDisable". You must fix the configuration problem and then manually take the port out of errDisable state. Some newer software versions (CatOS 5.4(1) and later) have the ability to automatically re-enable a port after a configurable amount of time spent in the errDisable state. Some of the causes for this errDisable state are:

- **EtherChannel Mis-configuration:** If one side is configured for EtherChannel and the other is not, it can cause the spanning tree process to shut down the port on the side configured for EtherChannel. If you try to configure EtherChannel but the ports involved do not have the same settings (speed, duplex, trunking mode, etc.) as their neighbor ports across the link, then it could cause the errDisable state. It is best to set each side for the EtherChannel "desirable" mode if you want to use EtherChannel. Sections later on talk in depth about configuring EtherChannel.
- **Duplex Mismatch:** If the switch port receives a lot of late collisions, this usually indicates a duplex mismatch problem. There are other causes for late collisions: a bad NIC, cable segments that are too long, but the most common reason today is a duplex mismatch. The full duplex side thinks it can send whenever it wants to. The half duplex side is only expecting packets at certain times - not at "any" time.
- **BPDU Port-guard:** Some newer versions of switch software can monitor if portfast is enabled on a port. A port using portfast should be connected to an end-station, not to devices that generate spanning tree packets called BPDUs. If the switch notices a BPDU coming in a port that has portfast enabled, it will put the port in errDisable mode.
- **UDLD:** Unidirectional Link Detection is a protocol on some new versions of software that discovers if communication over a link is one-way only. A broken fiber cable or other cabling/port issues could cause this one-way only communication. These partially functional links can cause problems when the switches involved do not know that link is partially broken. Spanning tree loops can occur with this problem. UDLD can be configured to put a port in errDisable state when it detects a unidirectional link.
- **Native VLAN mismatch:** Before a port has trunking turned on, it belongs to a single VLAN. When trunking is turned on, the port can carry traffic for many VLANs. The port will still remember the VLAN it was in before trunking was turned on, which is called the native VLAN. The native VLAN is central to 802.1q trunking. If the native VLAN on each end of the link does not match, a port will go into the errDisable state.
- **Other:** Any process within the switch that recognizes a problem with the port can place it in the "errDisable" state.

Another cause of inactive ports is when the VLAN they belong to disappears. Each port in a switch belongs to a VLAN. If that VLAN is deleted, then the port will become inactive. Some switches show a steady orange light on each port where this has happened. If you come in to work one day and see hundreds of orange lights don't panic; it could be that all the ports belonged to the same VLAN and someone accidentally deleted the VLAN that the ports belonged to. When you add the VLAN back into the VLAN table, the ports will become active again. A port remembers its assigned VLAN.



If you have link and the ports show connected, but you cannot communicate with another device, this can be particularly perplexing. It usually indicates a problem above the physical layer: layer 2 or layer 3. Try the following things.

- Check the trunking mode on each side of the link. Make sure both sides are in the same mode. If you turn the trunking mode to "on" (as opposed to "auto" or "desirable") for one port, and the other port has the trunking mode set to "off", they will not be able to communicate. Trunking changes the formatting of the packet; the ports need to be in agreement as to what format they are using on the link or they will not understand each other.
- Make sure all devices are in the same VLAN. If they are not in the same VLAN, then a router must be configured to allow the devices to communicate.
- Make sure your layer three addressing is correctly configured.

## Traffic Issues

In this section we will describe some of the things you can learn by looking at a port's traffic information. Most switches have some way to track the packets going in and out of a port. Commands that generate this type of output on the Catalyst 4000/5000/6000 switches are **show port** and **show mac**. Output from these commands on the 4000/5000/6000 switches is described in the switch command references.

Some of these port traffic fields show how much data is being transmitted and received on the port. Other fields show how many error frames are being encountered on the port. If you have a large amount of alignment errors, FCS errors, or late collisions, this may indicate a duplex mismatch on the wire. Other causes for these types of errors may be bad network interface cards, or cable problems. If you have a large number of deferred frames, it is a sign that your segment has too much traffic; the switch is not able to send enough traffic on the wire to empty its buffers. Consider removing some devices to another segment.

## Switch Hardware Failure

If you have tried everything you can think of and the port will not work, then there might be faulty hardware.

Sometimes ports are damaged by Electro-Static Discharge (ESD). You may or may not see any indication of this.

Look at the power-on self-test (POST) results from the switch to see if there were any failures indicated for any part of the switch.

If you see behavior that can only be considered "strange" then this could indicate hardware problems, but it could also indicate software problems. It is usually easier to reload the software than it is to get new hardware. Try working with the switch software first.

The operating system might have a bug. Loading a newer operating system could fix this. You can research known bugs by reading the release notes for the version of code you are using or by using Cisco's Bug Navigator tool (<http://www.cisco.com/support/bugtools/>).

The operating system could have somehow become corrupted. Reloading the same version of the operating system could fix the problem.

If the status light on the switch is flashing orange, this usually means there is some kind of hardware problem with the port or the module or the switch. The same thing is true if the port or module status indicates "faulty."

Before exchanging the switch hardware you might try a few things:

- Reseat the module in the switch. If you do this with the power on, make sure the module is hot swappable. If in doubt, turn the switch off before reseating the module or refer to the hardware installation guide. If the port is built in to the switch, ignore this step.
- Reboot the switch. Sometimes this causes the problem to disappear; this is a workaround, not a fix.
- Check the switch software. If this is a new installation, remember that some components may only work with certain releases of software. Check the release notes or the hardware installation and configuration guide for the component you are installing.
- If you are reasonably certain that you have a hardware problem, then replace the faulty component.

## Before Calling the Cisco Systems TAC Team

Before calling the Cisco Systems Technical Assistance Center (TAC), make sure you have read through this chapter and completed the actions suggested for your system's problem. Additionally, do the following and document the results so that TAC personnel can better assist you:

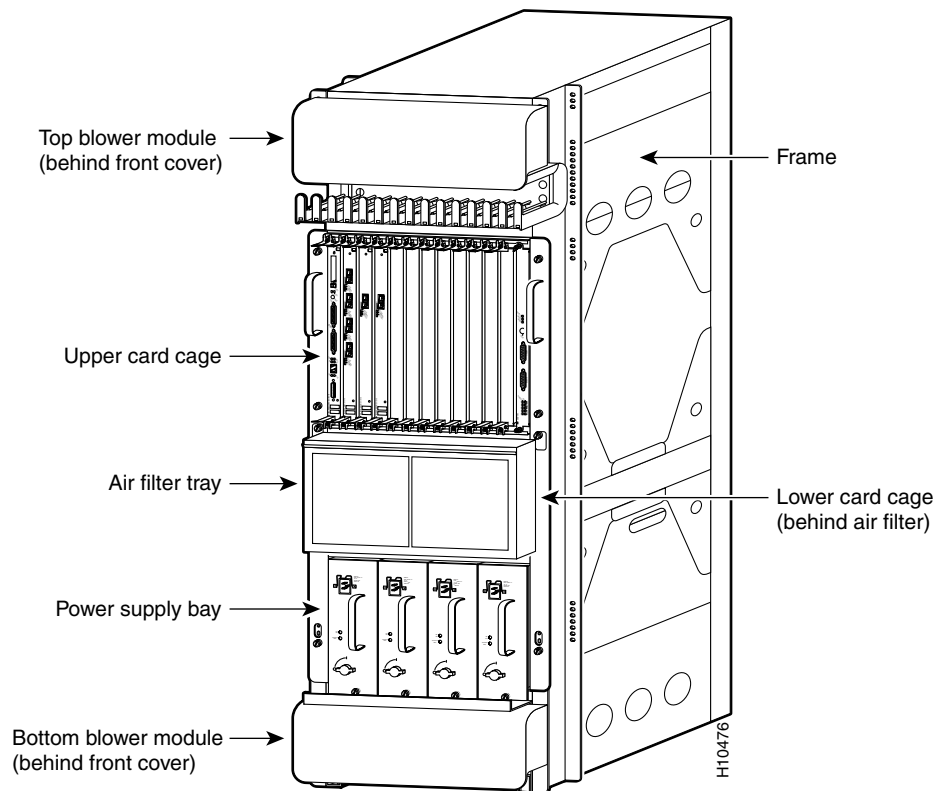
- Capture the output of **show version** from all of the affected switches.
- Capture the output of **show vtp domain** from all of the affected switches.
- Capture the output of **show trunk mod\_num/port\_num** from all of the affected ports.
- Capture the output of **show port mod\_num/port\_num capabilities** from all of the affected ports.

## Cisco GSR-12000 Series Gigabit Switch Router

The Cisco GSR-12000 Series Gigabit Switch Router (GSR) is a data aggregation point that passes packet streams on to, and receives packet streams from, the local IP backbone network in the Cisco BLISS for Cable solution.

The Cisco 12000 Series unique, modular, distributed system architecture delivers the capacity, performance, and service-enablers service providers require to deliver value-added services while offering operational efficiencies, and the industry's only proven investment protection to help control costs. In the Cisco BLISS for cable solution, the Cisco 12000 router will provide Gigabit Ethernet, Packet over SONET (POS) or Dynamid Packet Transport (DPT) access to the core network from the aggregation networks.

**Figure 8-2** Cisco GSR-12000 Series Gigabit Switch Router



## Cisco 12000 Series IP Services Engine (ISE)

For service providers who face the challenge of building scalable, high-speed edge networks to meet increasing demand and deliver value-added services without compromising density and line-rate performance, The Cisco 12000 Series IP Services Engine (ISE) revolutionizes the edge market by combining the power of the Cisco 12000 Series distributed system architecture with to 10G-enable the high-speed provider edge:

- Only 10G-enabled high-speed provider edge
- Only edge solution to eliminate the tradeoff between density and performance
- The only edge solution with dynamic, multi-speed channelization

## Gigabit/Fast Ethernet (GE/FE)

As bandwidth demands increase in the Internet, service providers must cost effectively scale their networks and maintain network simplicity. Ethernet interfaces on the Cisco 12000 Series help meet this critical requirement. The Cisco 12000 Series offers both Fast and Gigabit Ethernet line cards in a variety of port densities, including a high-density, 10-Port Gigabit Ethernet line card compatible with 10G-enabled Cisco 12400 Internet Routers.

## Packet Over SONET/Synchronous Digital Hierarchy (POS/SDH)

POS enables Internet routers to send native IP packets directly over SONET/SDH frames. POS provides lower packet overhead and lower cost per Mbit than any other data transport method. These efficiencies, along with the increasing evolution of the optical network, enable POS to efficiently support increases in IP traffic over existing and new fiber networks.

POS is a SONET/SDH compliant interface that supports SONET/SDH level alarm processing, performance monitoring, synchronization, and protection switching (through APS/MSP). This support enables Cisco 12000 Series Internet Routers to seamlessly interoperate with existing infrastructures and/or migrate to packet-based optical networks, thus eliminating the need for expensive "forklift" upgrades to existing equipment as demand for services escalates. In addition to backbone applications, POS is often used for customer access and intra-pop connectivity. As the inventor of POS, Cisco offers a range of Cisco 12000 Series POS line cards that can be interconnected over SONET/SDH infrastructures, dark fiber connections or DWDM gear.

## Dynamic Packet Transport (DPT)

DPT is a resilient packet ring (RPR) technology designed to deliver scalable Internet service, reliable IP-aware optical transport, and simplified network operations. Principally for metropolitan area applications, DPT-based solutions allow Service Providers to cost effectively scale and distribute their Internet and IP services across a reliable optical packet ring infrastructure. DPT is based on Spatial Reuse Protocol (SRP), a Cisco-developed MAC-layer protocol for ring-based packet internetworking. Cisco has submitted SRP to the IEEE 802.17 Resilient Packet Ring (RPR) Working Group for consideration as a standard.

DPT technology enables a set of carrier-class IP solutions, which leverage existing and emerging technologies. These solutions include ISP internetworking, Regional Metro IP internetworking, and Metro Internet Access.

## Troubleshooting Serial Lines

This section describes methods for detecting and correcting data errors on the Cisco 10000's serial interfaces.

## Optical Signal Input/Output Problems

Signal input and output problems can occur at any point in the network and can be caused by mechanical defects in cables or fiber, poor connections, or loss of signal caused by other equipment failures.

Refer to your site log and other facility records to isolate signal connections for your facility.

## Fiber-Optic Connections

An optical signal I/O problem can be caused by

- Incorrect type of fiber
- Defective fiber
- Transmit (TX) and Receive (RX) fibers reversed
- Insufficient power budget on the optical link
- Receiver overload on the optical link

Be sure to use single-mode fiber for a single-mode interface and multimode fiber for a multimode interface. [Table 8-1](#) describes fiber types appropriate for each Cisco 10000 ESR line card.

**Table 8-1 Optical Fiber Types for Cisco 10000 ESR Line Cards**

Card Type	Fiber Type
OC-12 Packet over SONET line card	Single mode
Gigabit Ethernet line card	Depends on installed GBIC: <ol style="list-style-type: none"> <li>1. 1000BaseSX, multimode</li> <li>2. 1000BaseLX/LH, single mode and multimode<sup>1</sup></li> <li>3. 1000BaseZX, single mode</li> </ol>

1. A mode-conditioning patch cord (CAB-GELX-625 or equivalent) is required. If you use an ordinary patch cord with MMF, 1000BaseLX/LH GBICs, and a short link distance (tens of meters), you can cause transceiver saturation, resulting in an elevated bit error rate (BER). In addition, if you use the LX/LH GBIC with 62.5-micron diameter MMF, you must install a mode-conditioning patch cord between the GBIC and the MMF cable on both transmit and receive ends of the link. The mode-conditioning patch cord is required for link distances greater than 1000 ft (300 m).

## Evaluating the Power Budget

Proper operation of an optical data link depends on modulated light reaching the receiver with enough power to be demodulated. The power budget (PB) is the difference between transmitter power (PT) and receiver sensitivity (PR). For instance, if transmitter power is -20 dB and receiver sensitivity is -30 dB, the power budget is 10 dB:

$$PB = PT - PR$$

$$PB = -20 \text{ dB} - (-30 \text{ dB})$$

$$PB = 10 \text{ dB}$$

The SONET specification requires the signal to meet the worst-case requirements listed in [Table 8-2](#).

**Table 8-2 SONET Signal Requirements**

	MM	SMI	SML
Transmitter power	-20 dBm	-15 dBm	-5 dBm
Receiver sensitivity	-30 dBm	-31 dBm	-34 dBm
Power budget	10 dB	16 dB	29 dBm

The difference between the power budget and the link loss (LL) is called the power margin (PM). If the power margin is zero or positive, the link should work. If it is negative, the signal may not arrive with enough power to operate the receiver.

Power loss over a fiber-optic link arises from the following causes:

- Attenuation caused by passive components (cables, cable splices, and connectors) is common to both multimode and single-mode transmission. Attenuation is significantly lower for optical fiber than for other media.
- The signal spreads in time because of differing speeds of the different wavelengths of light (chromatic dispersion).
- In multimode fiber, the signal spreads in time because of the different propagation modes (modal dispersion).
- Higher-order mode loss (HOL) results from light radiated into the fiber cladding.
- Clock recovery at the receiver consumes a small amount of power.

The power lost over the data link is the sum of all these losses. [Table 8-3](#) gives an estimate of the amount of loss attributable to each cause.

**Table 8-3 Link Loss Causes and Values**

Cause	Amount of Loss
Fiber attenuation	0.5 dB/km (SM), 1 dB/km (MM)
Splice	0.5 dB
Connector	0.5 dB
Modal and chromatic dispersion	Depends on fiber and wavelength <sup>1</sup>
Higher-order mode losses	0.5 dB
Clock recovery	1 dB

1. Dispersion is usually negligible for single-mode fiber. For multimode fiber, the product of bandwidth and distance should be less than 500 MHz-km.



**Note**

These are typical values; refer to the manufacturer for actual values.

## Managing Receiver Overload

The maximum receive power for SML is  $-10$  dBm, and the maximum transmit power is  $0$  dBm. The SML receiver can therefore be overloaded when using short lengths of fiber. Overloading the receiver does not damage it, but can cause unreliable operation. To prevent overloading an SML receiver, insert a minimum 10-dB attenuator on the link between any SML transmitter and the receiver.



**Note**

For the gigabit Ethernet line card,  $PR_{\max}$  is greater than or equal to  $PT_{\max}$ , so an attenuator is unnecessary.

## Using Bit Error Rate Tests

This section discusses problem isolation using bit error rate (BER) tests. The topics discussed are:

- [Configuring a BER Test on a T1 Line, page 8-13](#)
- [Sending a BER Test Pattern on a T1 Line, page 8-13](#)
- [Viewing the Results of a BER Test, page 8-14](#)
- [Terminating a BER test, page 8-16](#)

### Configuring a BER Test on a T1 Line

BER test circuitry is built into the CT3 line card. With BER tests, you can test cables and signal problems in the field. You can configure individual T1 lines to run BER tests, but only one BER test circuit exists for all 28 T1 lines. Hence, only one BER test can be run at once on a single T3 port.

The onboard BER test circuitry can generate two categories of test patterns: pseudorandom and repetitive. Pseudorandom test patterns are exponential numbers and conform to CCITT/ITU O.151 and O.153 specifications; repetitive test patterns are all zeros, all ones, or alternating zeros and ones.

Here is a description of each type of test pattern:

- Pseudorandom test patterns:
  - $2^{11}$  (per CCITT/ITU O.151)
  - $2^{15}$  (per CCITT/ITU O.151)
  - $2^{20}$  (per CCITT/ITU O.153)
  - $2^{20}$  QRSS (per CCITT/ITU O.151)
  - $2^{23}$  (per CCITT/ITU O.151)
- Repetitive test patterns:
  - All zeros (0s)
  - All ones (1s)
  - Alternating zeros (0s) and ones (1s)

Both the total number of error bits received and the total number of bits received are available for analysis. You can set the testing period from 1 minute to 14,400 minutes (240 hours), and you can also retrieve error statistics anytime during the BER test.

When running a BER test, your router expects to receive the same pattern that it is transmitting. To help ensure this:

- Use a loopback at a location of your choice in the link or network.
- Configure remote testing equipment to transmit the same BER test pattern at the same time.

### Sending a BER Test Pattern on a T1 Line

You can send a BER test pattern on a T1 line with the controller command. The *unframed* option causes the BER test pattern to use the entire T1 bandwidth, including the T1 framing as well as payload bits. If *unframed* is omitted, then the T1 is either SF or ESF framed, as configured by the **T1 framing** command, and the BER test pattern occupies only the T1 payload bits.

```
t1 t1-line-number bert pattern pattern interval time [unframed]
```

where:

- *t1-line-number* is 1–28.
- *time* is 1–14400 minutes.
- *pattern* is:
  - 0s, repetitive test pattern of all zeros (as 00000...)
  - 1s, repetitive test pattern of all ones (as 11111...)
  - 2<sup>11</sup>, pseudorandom test pattern (2,048 bits long)
  - 2<sup>15</sup>, pseudorandom O.151 test pattern (32,768 bits long).
  - 2<sup>20</sup>-O153, pseudorandom O.153 test pattern (1,048,575 bits long)
  - 2<sup>20</sup>-QRSS, pseudorandom QRSS O.151 test pattern (1,048,575 bits long)
  - 2<sup>23</sup>, pseudorandom O.151 test pattern (8,388,607 bits long)
  - alt-0-1, repetitive alternating test pattern of zeros (0s) and ones (1s), as 01010101

Examples:

- Send a BER test pseudorandom pattern of 2<sup>20</sup> through T1 line 10 for 5 minutes.

This example is for a T1, numbered 10, on a CT3 line card in slot 1:

```
Router(config)# controller T3 1/0/0
Router(config-controller)# t1 10 bert pattern 2^20 interval 5 unframed
```

- Send a repetitive pattern of all ones through T1 line 10 for 14400 minutes (240 hours).

This example is for a T1, numbered 10, on a CT3 line card in slot 1:

```
Router(config)# controller T3 1/0/0
Router(config-controller)# t1 10 bert pattern 1s interval 14400 unframed
```



**Note**

You can terminate a BER test during the specified test period with the **no t1 bert** command.

## Viewing the Results of a BER Test

You can view the results of a BER test using the **controller** command:

```
show controllers T3 slot/port-adapter/port/t1-line-number
```

where *t1-line-number* is 1–28.

You can view the results of a BER test at the following times:

- After you terminate the test using the **no t1 bert** command
- After the test runs completely
- Anytime during the test (in real time)

You can view information about a BER test using the **controller** command:

```
show controllers T3 slot/subslot/port
```

where *t1-line-number* is 1–28.



Examples:

- This example is for a CT3 line card:

```
Router# show controllers T3 1/0/0
T3 1/0/0 is up.
C2T3 H/W Version : 3, C2T3 ROM Version : 0.79, C2T3 F/W Version : 0.29.0
T3 1/0/0 T1 1
No alarms detected.
Clock Source is internal.
```

```
→ BERT test result (running)
   Test Pattern : 2^11, Status : Sync, Sync Detected : 1
   Interval : 5 minute(s), Time Remain : 5 minute(s)
   Bit Errors(Since BERT Started): 6 bits,
   Bits Received(Since BERT start): 8113 Kbits
   Bit Errors(Since last sync): 6 bits
   Bits Received(Since last sync): 8113 Kbits
```

Table 8-4 explains the output of the preceding command, starting at the arrow:

**Table 8-4 Interpreting BER Test Results**

Output Display Line	Explanation
BERT test result (running)	Current state of the test. In this case, running indicates that the BER test is still in progress. After a test is completed, done is displayed.
Test Pattern : 2^11, Status : Sync, Sync Detected : 1	The test pattern you selected for the test (2^11), the current synchronization state (sync), and the number of times synchronization has been detected during this test (1).
Interval : 5 minute(s), Time Remain : 5 minute(s)	The time the test takes to run and the time remaining for the test to run.  If you terminate a BER test, you receive a message similar to the following:  Interval : 5 minute(s), Time Remain : 2 minute(s) (unable to complete)  “Interval: 5 minutes” indicates the configured run time for the test. “Time Remain : 2 minutes” indicates the time remaining in the test prior to termination. “(Unable to complete)” means that you interrupted the test.
Bit Errors(Since BERT Started): 6 bits, Bits Received(Since BERT start): 8113 Kbits Bit Errors(Since last sync): 6 bits Bits Received(Since last sync): 8113 Kbits	These four lines show the bit errors that have been detected versus the total number of test bits that have been received since the test started and since the last synchronization was detected.



**Note**

Unless *unframed* is selected, the BER test runs over the configured framing option for the specified T1 line (ESF or SF). Before running a BER test, you should configure the framing option appropriate to your application.

## Terminating a BER test

To terminate a BER test, type

```
no t1 t1-line-number bert
```

where *t1-line-number* is 1–28.

Example:

- Terminate the BER test running on T1 line 10 on the CT3 line card.

```
Router(config)# controller T3 1/0/0
Router(config-controller)# no t1 10 bert
```

## Using Loopback Tests

The following sections describe the configuration and use of loopback tests in problem isolation:

- [Configuring the Loopback Mode for a T3 Controller, page 8-16](#)
- [Configuring a T3 Controller to Respond to Remote Loopback Commands, page 8-17](#)
- [Configuring the Loopback Mode for a Gigabit Ethernet Interface, page 8-17](#)
- [Configuring the Loopback Mode for an OC-12 POS Interface, page 8-17](#)

### Configuring the Loopback Mode for a T3 Controller

You can configure the loopback modes for a T3 controller by using the **loopback** command:

```
loopback [local | network | remote]
```

The default loopback mode for the T3 controller is **no loopback**.

To return the T3 controller to its default condition, use the **no** form of the command.

Examples:

- Configure a T3 controller for local loopback:

```
Router(config)# controller T3 1/0/0
Router(config-controller)# loopback local
```

Local loopback simultaneously loops all channels toward the router and transmits a T3 AIS to the network. You can use local loopback to diagnose problems with the port when isolated from the network cables.

- Configure a T3 port for network loopback:

```
Router(config)# controller T3 1/0/0
Router(config-controller)# loopback network
```

Network loopback loops the T3 line back towards the network and can be used to diagnose problems with cables from the central switching office to the port.

- Configure a T3 port for remote loopback:

```
Router(config)# controller T3 1/0/0
Router(config-controller)# loopback remote
```

Remote loopback sends a command to loop the T3 line at the far end (central office). It can be used to diagnose problems with cables from the port adapter to the switching office.

## Configuring a T3 Controller to Respond to Remote Loopback Commands

The **equipment customer loopback** command allows a port to respond to loopback commands from remote T3 equipment. The **equipment network loopback** causes a controller to ignore remote T3 loopback commands.

Syntax:

```
equipment [customer | network] loopback
```

Example:

To enable the controller's ability to respond to remote loopback requests, type:

```
Router(config)# controller T3 1/0/0
Router(config-controller)#equipment customer loopback
```

To prevent a controller from responding to remote loopback commands, type:

```
Router(config)# controller T3 1/0/0
Router(config-controller)#equipment network loopback
```



**Note**

---

Remote loopbacks are available only when you use c-bit parity framing.

---

## Configuring the Loopback Mode for a Gigabit Ethernet Interface

To set loopback mode on a gigabit Ethernet interface, use the **loopback** command in interface configuration mode.

```
loopback [internal | external]
[no] loopback [internal | external]
```

where:

- **external** runs a loopback that requires a loopback connector.
- **internal** runs a loopback at the MAC controller using a serializing/deserializing method (SERDES).

Use the **no** form of the command to stop the loopback.

In the following example, an internal loopback mode is defined for a gigabit Ethernet interface:

```
router(config)# interface GigabitEthernet 1/0/0
router(config-if)# loopback internal
```



**Tip**

---

If you are performing a hard plug loopback test on a gigabit Ethernet interface, be sure to set the loopback type for the interface to external. Otherwise, no packets are transmitted onto the fiber optic cable.

---

## Configuring the Loopback Mode for an OC-12 POS Interface

To enable loopback testing of data transmitted from the Cisco 10000 ESR PRE card to the OC-12 POS card and back, use the **loopback** command in interface configuration mode:

```
loopback [line | internal]
[no] loopback [line | internal]
```

Both **line** and **internal** do the following

- Loop any data received at the OC-12 POS card's network interface back into the network
- Loop any data received at the OC-12 POS card's network interface back into the PRE card

Use the **no** form of the command to stop the loopback test.

In the following example, a loopback is set for the OC-12 POS line card in slot 5:

```
Router(config)# interface pos 5/0/0  
Router(config-if)# loopback line
```



# Troubleshooting Cisco Media Gateways

## Media Gateway Management

The Cisco IOS software installed on the media gateways provides an array of network management capabilities, including:

- **SNMP and RMON Support**—The media gateways are fully manageable using the Simple Network Management Protocol (SNMP) and imbedded Remote Monitoring (RMON) capabilities:

SNMP provides for the collection of information about each controller and interface, which can be polled through any SNMP-compatible network management system.

RMON acts as a remote protocol analyzer and LAN probe.

Using the Alarm RMON group, you can set a threshold on any integer-valued Management Information Base (MIB) variable. When the threshold is crossed, an event, defined in the Event RMON group, is triggered. With these capabilities, the system can detect and analyze overloaded conditions and congestion in real-time.

- **Network Management Systems**—The media gateways support both CLI and the CiscoView graphical user interface (GUI) for comprehensive, flexible network management.

CiscoView provides dynamic status, statistics, and comprehensive configuration information for Cisco switches, routers, NASs, concentrators, and adapters. It displays a graphical view of Cisco devices, provides configuring and monitoring functions, and offers basic troubleshooting.

- **Modem Management**—Cisco offers two types of modems, basic and managed. Managed modems offer superior reporting and statistics in the CiscoView application, including troubleshooting and monitoring modem connections on individual modems or groups of modems while calls are in progress.

You can manage modems using the same tools used to manage the rest of the network. In addition, managed modems provide an out-of-band management feature that allows you to reduce problem detection and resolution time from a remote site.

Through out-of-band management, you can view real-time information (for current or previous calls) such as modem modulation scheme, modem protocol, modem EIA/TIA-232 signal states, modem transmit and receive states, and analog signal-to-noise ratio.

## MGCP on Cisco IOS Software

The Media Gateway Control Protocol (MGCP) runs on Cisco IOS software and the Cisco BTS 10200 Softswitch. The Cisco BTS 10200 Softswitch uses MGCP to control media gateways from external call control elements. A media gateway is a network element that provides conversion between audio signals carried on telephone circuits and data packets carried over the Internet or other packet network.

MGCP provides a call control architecture where the call control intelligence is outside the gates and handled by external call control elements. The MGCP commands supported include:

- **Create Connection**—Used by the Cisco BTS 10200 Softswitch to allocate and connect the bearer channels.
- **Modify Connection**—Used by the Cisco BTS 10200 Softswitch to change the parameters associated to a previously established connection.
- **Notification Request**—Used by the Cisco BTS 10200 Softswitch to instruct a gateway to watch for specific events, such as hook actions or DTMF tones on a specified end point.
- **Notify**—Used by the gateway to inform the Cisco BTS 10200 Softswitch when the requested events occur.
- **Audit Endpoint**—Used by the Cisco BTS 10200 Softswitch to audit the status of an endpoint.
- **Audit Connection**—Used by the Cisco BTS 10200 Softswitch to audit the status of a connection.
- **Restart in Progress**—Used by the gateway to notify the Cisco BTS 10200 Softswitch that the gateway or a group of endpoints managed by the gateway are being taken out of service or are being put back in service.

## DHCP on Cisco IOS Software

The Dynamic Host Configuration Protocol (DHCP) runs on Cisco IOS software. The Cisco IAD2421 serves as a DHCP server to retrieve IP addresses. This allows subscribers to connect their PCs to the Cisco IAD2421 without the need for any IP address management, minimizing operational overhead and costs associated with device configuration. For information on DHCP, see the DHCP information in the *Cisco IOS Configuration Fundamentals Configuration Guide* for your Cisco IOS software release.

## Cisco MGX8850

Two different configurations of this platform are supported. The configurations are as follows:

- MGX8850/PXM1/RPM-PR/VISM-PR/SRM
- MGX8850/PXM45/RPM-XF/VISM-PR/SRM-E

The first configuration—MGX8850/PXM1/RPM-PR/VISM-PR/SRM—includes the following:

- 19-inch rack mount. Redundant PXM1 (1.2.01)
- 24 I/O+4 SRM slot, PXM1, PXM-UI,
- MGX-VISM-8T1 (2.2.0)
- VISM-VOIP-G711
- MGX-SRM-3T3/C
- MGX-BNC-3T3-M - backcard

- 512 Meg SRAM
- MGX-RJ45-FE - FE card for RPM
- RPM 1-TO-N redundancy

The second configuration—MGX8850/PXM45/RPM-XF/VISM-PR/SRM-E—includes the following:

- 19-inch rack mount. Redundant PXM1 (1.2.01)
- 24 I/O+4 SRM slot, PXM1, PXM-UI,
- MGX-VISM-8T1 (2.2.0)
- VISM-VOIP-G711
- MGX-SRM-3T3/C
- MGX-BNC-3T3-M - backcard
- 512 Meg SRAM
- MGX-RJ45-FE - FE card for RPM
- RPM 1-TO-N redundancy

## MGX 8850 Diagnostics

The purpose of system diagnostics is to ensure the integrity of each and every control/data path and every hardware component involved in providing a path within the MGX8850 shelf. If enabled, periodic diagnostic tests are performed to detect faults in the system. Once detected, the MGX8850 shelf manager is informed and takes appropriate action. The MGX8850 system diagnostics design strategy is to develop a software module embedded in the PXM45 software running on the active PXM45 card.

Each service module (SM), as well as PXM45 itself, will provide local diagnostics functions specific for its card. These local diagnostics should provide a complete set of tests of each hardware component and data paths. The MGX8850 system diagnostics does not need to know what diagnostics functionalities are provided by these local diagnostics; it acts as a diagnostics controller which schedules and coordinates these local diagnostics and provides the result to the MGX8850 shelf manager.

The MGX8850 software (PXM45 and SM's) provides 4 types of diagnostics. Each diagnostic is performed in different situations or card states. A diagnostics procedure may be duplicated or repeated when necessary to ensure high quality service and to meet the RAS requirement. These diagnostics are as followed:

- Boot diagnostics performs a set of destructive tests (disrupts user traffic) on the hardware components that are required to bring up the card.
- Off-line diagnostics performs destructive tests on the standby card only. The off-line tests are comparable to the tests in Manufacturing diagnostics.
- On-line diagnostics monitor various components without disrupting user traffic (non-destructive tests). These diagnostics include the fully meshed connection test.
- Manufacturing diagnostics tests all hardware components.

# Command Line Interface

The PXM45 system diagnostics CLI provides the ability to configure diagnostics, to initiate the On-line or Off-line diagnostics, and to display diagnostics status. The commands are described in the following paragraphs:



## Note

---

All parameters are required unless specifically labeled (optional).

---

### cnfdiag

This command configures diagnostics. When this command is entered without any parameters, it will display the current configuration and status.

```
cnfdiag <slot> <onEnb> <offEnb> [<offCover> <offStart> <offDow>]
```

#### Parameters:

- *slot*—Specifies physical slot number. The value is from 1 to MAX\_SLOTS.
- *onEnb*—Indicates whether to enable or disable **online** diagnostics on this slot.
- *offEnb*—Indicates whether to enable or disable **offline** diagnostics on this slot.
- *offCover*—(optional) Specifies how much test coverage the **offline** diagnostics should perform. The coverage is defined as *light*, *medium*, and *full*. The *light* tests are less than 5 minutes, the *medium* tests are less than 30 minutes, and *full* is unlimited. Since the tests are card, please refer to diagnostics functional specification on each card for the type of tests are being performed for each coverage.
- *offStart*—(optional) Specifies the start time of the **offline** diagnostics. This option has a format --HH:MM, e.g. 03:45 or 22:15.
- *offDow*—(optional) Specifies the start day of week for the **offline** diagnostics. This option has a format --SMTWTFS, e.g. monday and wednesday -M-W----.

### abortofflinediag

This command aborts running offline diagnostics

```
abortofflinediag <slot>
```

#### Parameters

*slot*—Specifies the physical slot number. The value is from 1 to MAX\_SLOTS.

### clrdiagerr

This command clears diagnostics errors.

```
clrdiagerr <slot>
```

#### Parameters

*slot*—Specifies the physical slot number. The value is from 1 to MAX\_SLOTS.



**dspdiagcnf** This command displays the diagnostics configuration.

**Parameters**

None

**dspdiagstatus** This command displays the diagnostics status.

**Parameters**

None

**dspdiagerr** This command displays the diagnostics error.

**Parameters**

None.

## Diagnostic Figures

The following figures show the diagnostics configuration, status, and error screens. The configuration screen, [Figure 9-1](#), consists of the slot number, card type, on-line diagnostics configuration, and off-line diagnostics configuration. The status screen, [Figure 9-2](#), displays the cards that are currently running diagnostics. The error screen, [Figure 9-3](#), displays any errors that the diagnostics encounter.

**Figure 9-1 Diagnostics Configuration Screen**

```
POPEYE2> dspdiagcnf
```

Slot	Online Enable	----- Offline -----	Enable	Coverage	StartTime	SMTWTFSS
1	enable	enable	light	03:00	-M-W-F-	
2	enable	enable	light	03:00	-M-W-F-	
3	enable	enable	light	03:00	-M-W-F-	
4	disable	enable	full	03:00	-M-W-F-	
5	enable	enable	light	03:00	-M-W-F-	
6	enable	enable	light	03:00	-M-W-F-	
7	disable	disable	full	01:00	-----S	
8	enable	enable	full	01:00	-----S	
9	enable	disable	light	03:00	-M-W-F-	
10	enable	enable	medium	03:00	-M-W-F-	
11	enable	disable	full	22:00	-----S	
12	disable	enable	full	22:00	-----S	
13	enable	enable	medium	03:00	-M-W-F-	
14	enable	enable	medium	03:00	-M-W-F-	

104857

Figure 9-2 Diagnostics Status Screen

```
POPEYE2> dspdiagstatus
```

Slot	State
1	Ready
2	Ready
3	Online
4	Ready
5	Ready
6	Offline
7	Ready
8	Offline
9	Ready
10	Ready
11	Ready
12	Idle
13	Ready
14	Idle

104558

Figure 9-3 Diagnostics Error Screen

```
POPEYE2> dspdiagerr
```

Slot	Date	Time	Message
1	24-Aug	13:35	SAR send failed
2	--	--	
3	--	--	
4	--	--	
5	--	--	
6	18-Aug	03:24	HUMVEE IRQ test failed
7	--	--	
8	--	--	
9	--	--	
10	--	--	
11	--	--	
12	--	--	
13	--	--	
14	--	--	

104559

## Shellcon commands

There are no shell commands for the diagnostic modules since most of the code is run from the CLI.

## Diagnostic Troubleshooting

The following sections describe different diagnostic troubleshooting scenarios for the Cisco MGX 8850.

### Are “OnLine” Diagnostics Running

To determine if the “online” diagnostics are running, complete the following steps:

- 
- Step 1** Ensure that the diagnostics are enabled on the slot. This can be done by using the **dspdiagcnf** command.
  - Step 2** Make sure the second column “Online Enable” has been enabled for the slot in question. The **cnfdiag** command can be used to enable/disable per slot.
  - Step 3** The online diagnostics task runs on the node at regular intervals ( 30 sec). In order to verify if the online diagnostic task is running use the **dspdiagstat <slot>** to capture the number of attempts/failures on that specific slot. If all the numbers do not changes then the online diag is not running.
- 

### Are “Offline” Diagnostics Running

To determine if the “offline” diagnostics are running, complete the following steps:

- 
- Step 1** Ensure that the diagnostics were enabled on the slot. This can be done using the **dspdiagcnf** command. Make sure the column “Offline Enable” has been enabled for the slot in Question. Also you need to make sure the day of the week and the start time for the tstst are configured correctly by the user. The **cnfdiag** command can be used to enable/disable per slot.
  - Step 2** The “online” diagnostics task runs only on the standby card. When the “offline” diagnostics are triggered the card is reset and comes up in the diagnostics mode. Once the dianotics are completed it will be reset again returning to normal mode of operation (standby state).
  - Step 3** While the “offline” diagnostics are running, the command **dspdiagstatus** can be used to verify the status of the diagnostics running on the node. For each card on which the offline diagnostic is running “Offline” will be shown under the column heading “State.”
- 

### Non-Fatal Major Error Reported When “offline”/ “online” Diagnostics are Running

If non-fatal major errors are reported while the “offline”/ “online” diagnostics are running, complete the following steps:

- 
- Step 1** When diagnostics tests detect an error, a log is generated and the test is repeated four more times. If the error is persistent then it is reported as a non-fatal major error to the Shelf Manager.
  - Step 2** The **dspdiagerr** command can be used to determine the cause of the error on the node.
-

## “Offline” Diagnostics Task is Taking Too Long to Complete or is Hung

The offline diagnostics task is designed with different levels of coverage. The table below shows the types of coverages and the expected time for completion.

**Table 9-1** Offline Diagnosis Types of Coverage

Type of Coverage	Completion Time
Light	5 minutes
Medium	30 minutes
Full	2 hours +

It is possible that a hardware failure could cause an exception on the diagnostic tasks. The offline diagnostics test will attempt to recover from any test failure. In all other cases the **abortofflinediag** command can be used to reset the standby card where the offline diagnostics are running.

## Troubleshooting Alarms

The MGX 8850 switch displays alarm information on the PXM45, AXSM, and RPM cards, and it stores information on these cards inside the switch. This chapter describes how to interpret the alarm LEDs on the switch and how to obtain alarm reports through the CLI.

## Viewing and Responding to Alarms

The PXM45, AXSM, and RPM cards have LEDs for viewing alarm status and switches for responding to alarms. The following sections describe these controls.

### PXM45 Card Controls

Table 9-2 describes the LEDs and switches available on the front of the PXM45 card. Figure 9-4 shows these controls.



#### Note

Although there are LEDs for critical, major, and minor alarms on the PXM45, only one of these LEDs is set to on when multiple alarms are active. The switch always displays the status of the most severe alarm. Critical alarms are the most severe, and minor alarms are the least severe. For example if there were 2 major alarms and 10 minor alarms, the switch would set the major alarm LED to on.

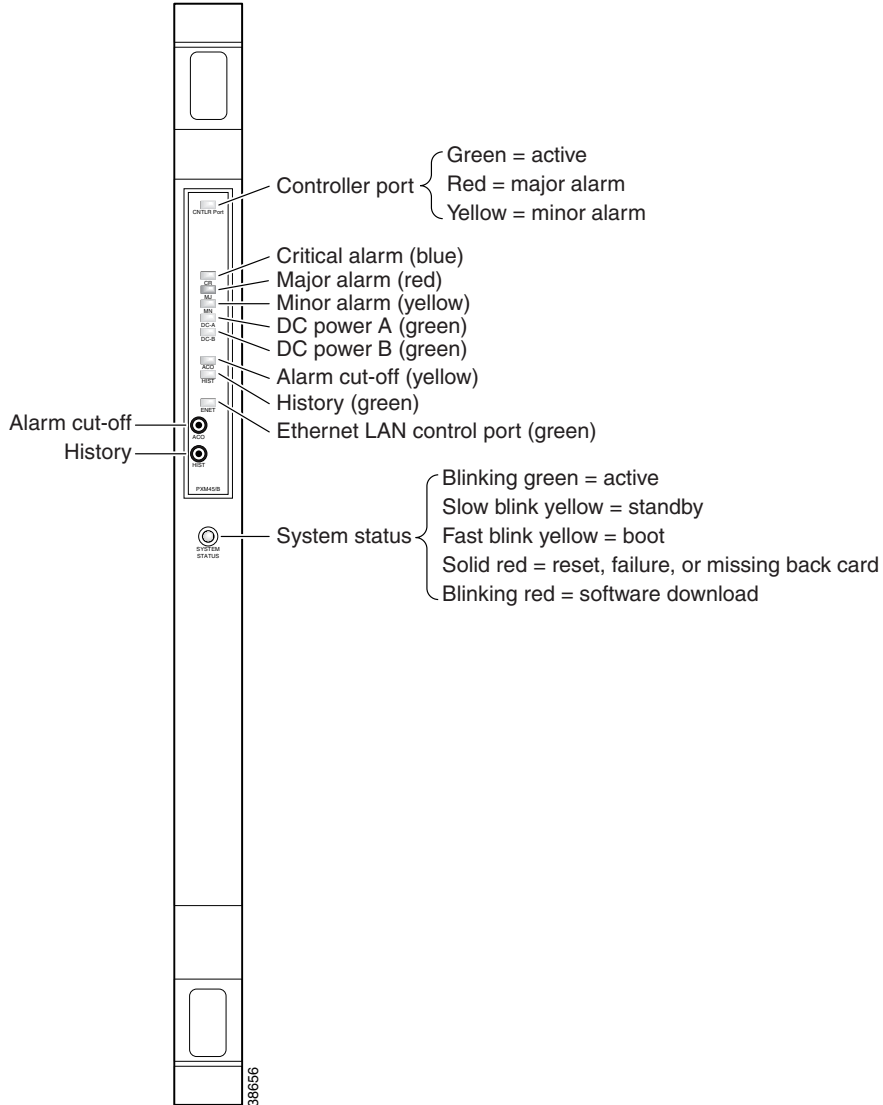
**Table 9-2** LED Indicators for PXM45

LED Label	Color	Meaning
CNTRLR Port (Controller Port)	Green	The Controller port is active.
	Red	Major alarm on the controller port.
	Yellow	Minor alarm on the controller port.
	None	No light indicates the port has not been activated (upped).

**Table 9-2 LED Indicators for PXM45 (continued)**

LED Label	Color	Meaning
System Status	Green	Blinking green indicates that the card is in the active state.
	Yellow	Slow blink yellow indicates that the card is in the standby state.
		Fast blink yellow indicates that the card is in the boot state.
	Red	Solid red indicates that the card is in the Reset state, the card has failed, or a back card is missing.
Blinking red indicates that the card is downloading new software.		
CR (Critical alarm)	Blue	Blue indicates a Critical Network alarm in the node.
MJ (Major alarm)	Red	Red indicates a Major Network alarm in the node.
MN (Minor alarm)	Yellow	Yellow indicates a Minor Network alarm in the node.
HIST (History)	Green	Green indicates that a network alarm occurred, but has been cleared.
ACO (Alarm cut-off)	Yellow	Yellow indicates that the ACO switch was pushed to clear the audible alarm indicator, but the alarm condition still exists.
DC-A	Green	Green indicates that the power supplies in tray "A" are functioning.
	None	No light indicates that power supply tray "A" is empty (no power modules).
DC-B	Green	Green indicates that the power supplies in tray "B" are functioning.
	None	No light indicates that power supply tray "B" is empty (no power modules).
ENET (Ethernet)	Green	Blinking green indicates that there is activity on the LAN Control Port.

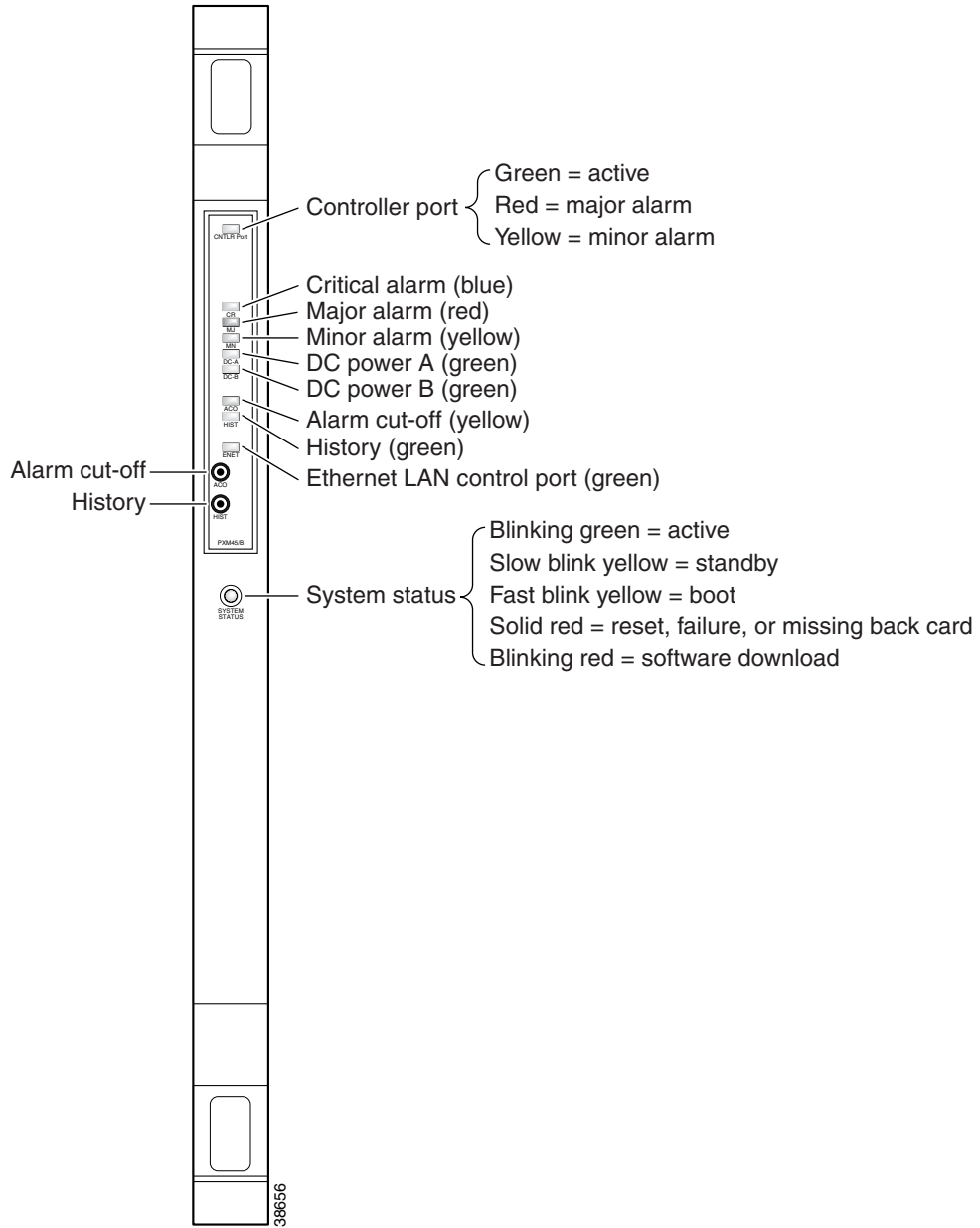
Figure 9-4 PXM45 Front Card Controls



# AXSM Card Controls

Figure 9-5 shows the LEDs available on the front of the AXSM card. Table 9-3 describes these LEDs.

Figure 9-5 AXSM Card Controls (MGX-AXSM-16-T3E3)



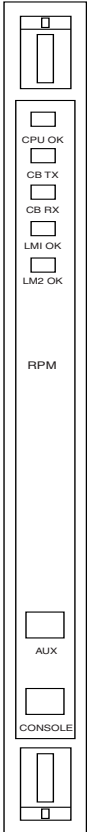
**Table 9-3 LED Indicators for AXSM Card**

LED	Color	Description
Active	Green	Card is active.
Standby	Yellow	Card is in standby mode.
Fail	Red	Failure detected on card.
Line	Green	The line is active and there are no alarms.
	Red	The line is active, but a local alarm has been detected.
	Yellow	The line is active, and a remote alarm has been detected.

## RPM-PR Card Controls

Table 9-4 shows the LEDs available on the front of the RPM-PR card and describes these LEDs.

**Table 9-4 LED Indicators for RPM-PR Card**

RPM-PR Card	LED	Color	Description
	CPU OK	Green	CPU is running.
		Yellow	
		Off	CPU is not running.
CB TX	On		Transmitting cells on cellbus.
	Off		Not transmitting cells on cellbus.
CB RX	On		Receiving cells from cellbus.
	Off		Not receiving cells from cellbus.
LM1	On		Port adapter installed and enabled in bay 1.
	Off		No port adapter installed in bay 1.
LM2	On		Port adapter installed and enabled in bay 2.
	Off		No port adapter installed in bay 2.



## Displaying Alarm Reports in the CLI

This section provides summary information about alarms on a shelf. The alarm manager also sets the alarm LEDs on the PXM card and sends a ShelfIntegratedAlarm Trap. You can use a CLI session to view the status of switch alarms. A set of CLI commands is provided for debugging hardware problems.

Alarms are reported in the following categories:

- [Node alarms](#)
- [Card alarms](#)
- [Clock alarms](#)
- [Environment alarms](#)
- [Slot alarms](#)
- [Switching alarms](#)
- [Xbar alarms](#)

This section describes how to display the different types of alarm reports.

**Note**

---

The procedures in the following sections can be completed by users at all access levels.

---

### Displaying Node Alarms

The alarm summary provides a mechanism for quickly determining the status of the node, and determining the area of the problem. The alarm command hierarchy uses ***dspndstatus*** or ***dapndalms*** as the initial command to determine the shelf status. The next level of indentation shows the alarm type, followed by the commands to get additional information for that alarm type.

- ***dspndstatus***—Shows the most severe alarm on the node
- ***dspndalms***—Shows a summary of all of the alarms in the following categories:

**Environment**

- ***dspenvalms*** - shows environment data for power supply, fan unit, DC Level, temperature.

**Clocking**

- ***dspclkalms*** - shows clock manager summary

**Switching**

- ***dspswalms*** - displays switching alarms

**dspndalms**

A node alarm report displays a summary report of all alarms on the node. To display node alarms, enter the following command:

```
pop20two.7.PXM.a > dspndalms
```

The following is an example of the node alarm report.

```
pop20one.7.PXM.a > dspndalms
Node Alarm Summary
```

Alarm Type	Critical	Major	Minor
-----	-----	-----	-----
Clock Alarms	0	0	0
Switching Alarms	0	0	0
Environment Alarms	0	0	0
Card Alarms	0	0	0

Typically, you would start investigating alarms by displaying the node alarms. Once you have identified the area that is producing the alarms, you would enter additional commands to display detailed information on those alarms. The following sections describe how to display these detailed reports.

## Displaying Card Alarms

A card alarm report can display the alarm status of all the cards within the node or the alarm status of a single card.

The following card alarm commands are available:

- **dspcdstatus** – Provides the most severe of the alarms under **dspcdalms**.
- **dspcdalms** – Provides an overview of all of the slots.
- **dspcdalms <slot>** provides more detail about that slot.

**dspcdalms**

To display card alarms, enter the following command:

```
pop20two.7.PXM.a > dspcdalms [slot]
```

Replace *slot* with the number of the card for which you want to display alarms. If you omit the slot number, the switch displays the alarms for all cards in the node as shown in the following example:

```
pop20one.7.PXM.a > dspcdalms
Card Alarm Summary
```

Slot	Critical	Major	Minor
----	-----	-----	-----
1	0	0	0
2	0	0	0
3	0	0	0
4	0	0	0
5	0	0	0
6	0	0	0
7	0	0	0
8	0	0	0
9	0	0	0
10	0	0	0
11	0	0	0
12	0	0	0
13	0	0	0
14	0	0	0

Use **dspcdalms <slot>** to see more detail.

The next example shows a card alarm report for an AXSM card in slot 1:

```
pop20one.7.PXM.a > dspcdalms 1
```

```
Card Alarm Summary
Alarm Type                Critical      Major      Minor
-----
Hardware Alarm            0            0            0
Card State Alarm         0            0            0
Disk Alarm                0            0            0
Line Alarm                0            0            0
Port Alarm                0            0            0
Feeder Alarm              0            0            0
Channel Alarm             0            0            0
```

## Displaying Clock Alarms

The MGX 8850 switch monitors the quality of its clock sources. If the timing for a clock source strays beyond the tolerance thresholds, an alarm is reported. To view the clock alarms, enter the following command:

```
pop20two.7.PXM.a > dspclkalarms
```

The following is an example clock alarm report:

```
pop20two.7.PXM.a > dspclkalarms
pop20two                System Rev: 02.00   Sep. 02, 2000 23:39:22 GMT
MGX8850                 Shelf Alarm: NONE
Clock Manager Alarm Summary
-----
Critical      Major      Minor
000           000       000
```

## Displaying Environment Alarms

An environmental alarm report displays the alarm status and operating statistics for the switch power supplies and cooling fans. To display the environmental alarm report, enter the following command:

```
pop20two.7.PXM.a > dspenvalms
```

The following is an example environmental alarm report:

```
pop20two.7.PXM.a > dspenvalms
pop20two                System Rev: 02.00   Sep. 02, 2000 23:40:57 GMT
MGX8850                 Shelf Alarm: NONE
ENVIRONMENTAL ALARM STATE INFO ^Notification Disabled
  Alarm Type      Unit  Threshold      DataType  Value      State
-----
Temperature                <= 50          Celsius   29        Normal

Power Supply             A1  none           None      none      Missing
Power Supply             A2  none           None      none      Missing
Power Supply             A3  none           None      none      Missing
DC Voltage               A   42 to 54       VoltsDC   0         Normal

Power Supply             B1  none           None      none      Missing
Power Supply             B2  none           None      none      Missing
Power Supply             B3  none           None      none      Missing
DC Voltage               B   42 to 54       VoltsDC   0         Normal

Top Fan Tray             1   >= 2000        RPM       3642     Normal
```

```

Top Fan Tray      2  >= 2000      RPM      3618      Normal
Top Fan Tray      3  >= 2000      RPM      3714      Normal
Top Fan Tray      4  >= 2000      RPM      3642      Normal
Top Fan Tray      5  >= 2000      RPM      3474      Normal
Top Fan Tray      6  >= 2000      RPM      3654      Normal
Top Fan Tray      7  >= 2000      RPM      3576      Normal
Top Fan Tray      8  >= 2000      RPM      3468      Normal
Top Fan Tray      9  >= 2000      RPM      3492      Normal

Bottom Fan Tray   1  >= 2000      RPM       0      Missing
Bottom Fan Tray   2  >= 2000      RPM       0      Missing
Bottom Fan Tray   3  >= 2000      RPM       0      Missing
Bottom Fan Tray   4  >= 2000      RPM       0      Missing
Bottom Fan Tray   5  >= 2000      RPM       0      Missing
Bottom Fan Tray   6  >= 2000      RPM       0      Missing
Bottom Fan Tray   7  >= 2000      RPM       0      Missing
Bottom Fan Tray   8  >= 2000      RPM       0      Missing
Bottom Fan Tray   9  >= 2000      RPM       0      Missing

+5V Input         4.850^ to 5.150^ VoltsDC  5.036    Informational
+3.3V Input       3.200^ to 3.400^ VoltsDC  3.298    Informational
+2.5V Input       2.425^ to 2.575^ VoltsDC  2.479    Informational
Calibration VDC   0x7e^ to 0x82^   Other    0x80     Informational

```

## Displaying Switching Alarms

Switching alarms identify problems with the switching components within the MGX 8850 switch. To display a report of all switching alarms, enter the following command:

```
pop20two.7.PXM.a > dspswalms
```

The following is a sample report showing no switching alarms.

```

pop20two.7.PXM.a > dspswalms
Node Switching Alarm Summary

Card Crossbar           Critical 0 Major 0 Minor 0
Crossbar Fabric         Critical 0 Major 0 Minor 0
Humvee Alarm            Critical 0 Major 0 Minor 0

```

## Displaying Crossbar Alarms

To display a report for xbar alarms, enter the following command:

```
pop20two.7.PXM.a > dspxbaralm
```

The following is a sample xbar alarm report.

```

pop20two.7.PXM.a > dspxbaralm
pop20two                               System Rev: 02.00   Sep. 02, 2000 23:47:19 GMT
MGX8850                                  Shelf Alarm: NONE

  Slot  Plane  Severity
  ----  -
    7    0     Minor
    7    1     Minor
    7    2     Minor
    8    0     None
    8    1     None
    8    2     None

```

When the MGX 8850 reports xbar alarms, you can use the following troubleshooting commands to collect more information:

- **dspxbar**
- **dspxbaralms**
- **dspxbarerrcnt**
- **dspxbarerrthresh**
- **dspxbarmgmt**
- **dspxbarstatus**

For more information on these commands, refer to the *MGX 8850 Command Reference*.

## PXM45x Alarm Issues

### Crossbar Alarm Commands

- **dspxbarerrthresh** – Display the threshold for the different alarms.
- **dspxbarmgmt** - Display loadsharing, auto shutdown configuration.

### Hardware Alarm Commands

- **dspcd** <slot #> on PXM shows alarm cause

### Card State Alarm Commands

- **dspcds** on PXM shows front and back card states
- **dspcd** <slot #>

### Disk Alarm Commands

- **dspcd** on active or stdby PXM

### Line Alarm Commands

- **dspalms** display additional detail on line alarms
- **dsplns** display includes line alarm status
- **dspalm** –sonet bay.ln displays alarms on a line

### Port Alarm Commands

- **dspnports** will **show** IF/Admin/ILMI state
- **cc** <slot #> (next command runs on axsm)
- **dspports** display admin/oper state

### Feeder Alarm Commands

- **cc** <slot #> (next command runs on axsm)
- **dspfdrs** display LMI Admin/UP.LMI alarms

- `dspfdr` IF #
- `dsplmistat` IF # to display LMI alarms

### Channel Alarm Commands

- `dspconinfo`
- `dspcons` –state fail - on PXM will **show** conditioned SPVCs
- `cc <slot#>` - The following commands are executed on the axsm
- `dspcons` – filt option – displays more information for port / channel alarms.  
(ing (1) | egr (2) | condn (3) | iffail (4) | mis (6) abit (7) | any (8) | none (9))
- `dspcon` IF # vpi vci – to get more information

The following basic types of alarms are raised for the crossbar switching fabric related issues

### Xbar Core Alarm

The xbar core alarms is raised when the errors detected on the crossbar links on the switch fabric card cross the alarm thresholds. The thresholds are user configurable for three severities which are Minor, Major and Critical for set and clear of the alarm. The threshold values for the alarm raising and the action taken for the errors seen are the same. The alarm is cleared when the errors go below the clear threshold values.

Some of the errors occur on a per plane basis rather than on a per link basis. These plane based alarms are raised when plane based errors on a xbar plane are detected. They are of three types SFrame Tick, SFrame Lock and ACP illegal target error. The SFrame Tick and SFrame lock error are critical errors and cause the whole plane to be unusable. The whole plane i.e. all the links on that plane will be shut down. So all slots are affected due to the plane based errors.

### Xbar Port Alarm:

The xbar port alarms is raised when the errors detected on the Xbar port e.g., Humvee transceiver port on AXSM, on the service modules cross the alarm thresholds. The thresholds use default values for the Minor, Major and Critical for set and clear of the alarm. The threshold values for the alarm raising and the action taken for the errors seen are the same. The alarm is not cleared when the errors go below the clear threshold values though for the xbar port alarms.

### Xbar Slot Bandwidth Alarm

The Xbar slot bandwidth alarm is raised on a per slot basis. The xbar slot bandwidth alarm is raised based on the number of crossbar links which are available for a particular service module. The three parameters which are used for raising the alarm are Maximum, Required, Available number of crossbar links. The alarms have only two severities Major and Critical. A Major alarm is set when the available number of links is less than the Max number of links and Critical alarm is raised when the operational number of links fall below the required number of links to support the bandwidth of the service module.

### Crossbar Core Alarms

If crossbar core alarms are present, then complete the following steps:

- 
- Step 1** Use `dspdevalms XBARCORE -pslot *` to display the core alarms for all slots. If specific slots are reporting errors then proceed to <Blue>“Step 2 Slot Centric De-bugging”. Otherwise if all service modules are reporting errors then proceed to <Blue>“Step 3 Plane centric de-bugging”.

- Step 2** Slot Centric De-bugging
- a. Use **dspdevalms** XBARCORE -pslot <pslot> to display the core alarm for the specific slot.
  - b. Use **dspdeverrr** XBARCORE -pslot <pslot> and **dspdeverrrhist** XBARCORE -pslot <pslot> to display the current and cumulative error counters for the different error types. The different error types that were in alarm in **a.** will have corresponding error counters.
- Step 3** Plane centric de-bugging
- a. Identify the particular crossbar plane that is reporting alarms against all service modules using **dspxbarplanealms**.
  - b. For the above switch card and plane, use **dspdevalm** XBARCORE -xslot <xbar\_slot> -pl <plane\_no> to display the alarms reported for different error types.
  - c. Use **dspdeverrr** XBARCORE -xslot <xbar\_slot> -pl <plane\_no> and **dspdeverrrhist** XBARCORE -xslot <xbar\_slot> -pl <plane\_no> to display the current and cumulative error counters for the different error types.
- 

### Crossbar Port Alarms

If crossbar port alarms are present, complete the following steps:

- Step 1** Use **dspswalms** to verify if all SM slots are reporting crossbar port alarms or only if specific slots are reporting port alarms. If all slots are reporting port alarms proceed to [Step 2](#), else proceed to [Step 3](#).
  - Step 2** If all slots are reporting crossbar port alarms, use **dsplog** -mod HMM\_ and **dsplog** -mod SHM\_ to identify the switching plane against which all the slots are reporting errors. The particular switching plane may be faulty.
  - Step 3** If a specific slot is reporting errors then **cc** to the slot and check if the humvee's on the slot are reporting any errors. Use **shellconn** command hvTestGetErrorCounters 1 (reads the accumulated error counter values) and hvTestGetErrorCounters 0 (reads the current error counters).
- 

### Crossbar Bandwidth Alarms

If crossbar bandwidth alarms are present, complete the following steps:

- Step 1** Use **dspxbarslotbwalms** to identify the slots reporting bandwidth alarms.
  - Step 2** Use **dspxbarslotbwalms** <pslot> to get detailed information for the slots reporting bandwidth alarms in [Step 1](#).
  - Step 3** Use **dspxbar** <plane\_no> to verify that the planes whose availability is reported UP but operational state is reported DOWN have been shut down. Use **dsplog** -mod HMM\_ and **dsplog** -mod SHM\_ to identify the reason for shut down.
-

## Displaying Log File Information

Log files record switch events such as operator login and command entry. To view the contents of the current log, enter the following command:

```
pop20two.7.PXM.a > dsplog [-sl <slot>] [-mod CLI]
```

To limit the log display to the events for a single slot, use the **-sl** option and replace *slot* with the appropriate slot number.

To limit the log display to CLI events, use the **-mod** option with the **CLI** keyword.

To display a list of archived log files, enter the following command:

```
pop20two.7.PXM.a > dsplogs
```

The log files are stored in the C:/LOG directory.

## Troubleshooting the Gateways

This section describes procedures for troubleshooting the Cisco Media Gateways. It also lists the actions you can take if you encounter situations not listed in this section.

### D-Channel

D-channels are 1xDS0 64K HDLC channels which carry the ISDN PRI Q.931 signalling messages over the PRI. The LAPD Q.921 protocol on top of HDLC channel ensures reliable and sequential delivery of these messages over the HDLC channel. These D-channels should be configured on the MGX8260 as well as the soft-switch (call-agent).

There are about 15 to 20 parameters associated with Q.921 which are user-configurable. These parameters are divided into two parts — the DLSAP parameters and MACSAP parameters. Most of these parameters are used as defaults and only a few parameters are modified. Therefore, you do not need to specify each one of these parameters every time a D-channel needs to be added. You can configure DLSAP and MACSAP templates and specify these templates while adding D-channels.

### DLSAP template/profile

This configuration is persistent and is associated with an SCC (this means the DLSAP profiles are not cleared when any service-card configuration is cleared). The DLSAP profiles are cleared only with either “clrndcnf” “clrcdnf” on SCC slot. These profiles are restored on the SCC on “resetnd”.

The **adddsp** command adds a DLSAP profile. This command could fail for the following reasons:

1. If the DLSAP profile is already added.
2. If the DLSAP index is out of range.
3. If one of the parameters being configured is out of range/illegal.

The **lsdsp** command displays a DLSAP profile. This command could fail for the following reasons:

1. If the DLSAP index specified in the command is NOT added.
2. If the DLSAP index is out of range.



The **lsdlsps** command displays all DLSAP profiles. This command should never fail. However, it will not display anything if there are no DLSAP profiles added.

The **deldlsps** command deletes the DLSAP profile. This command could fail for the following reasons:

1. If the DLSAP index specified in the command is NOT added.
2. If the DLSAP index is out of range.

## MACSAP template/profile

This configuration is persistent and is associated with an SCC (i.e., the MACSAP profiles are NOT cleared when any service-card configuration is cleared). The MACSAP profiles are cleared only with either “clrndcnf” “clrcdnf” on SCC slot. These profiles are restored on the SCC on “resetnd”.

The **addmacsaprof** command adds a MACSAP profile. This command could fail if:

1. MACSAP profile is already added.
2. MACSAP index is out of range.
3. One of the parameters being configured is out of range or illegal.

The **ismacsaprof** command displays a MACSAP profile. This command could fail if:

1. MACSAP index is NOT added.
2. MACSAP index is out of range.

The **ismacsaprofs** command displays all MACSAP profiles. This command should never fail. However, it will not display anything if there are no MACSAP profiles added.

The **delmacsaprof** command deletes the MACSAP profile. This command could fail if:

1. MACSAP index specified in the command is not added.
2. MACSAP index is out of range.

## addchan Command Fails

The **addchan** command adds a D-channel. This command could fail for the following reasons:

1. If the card specified by slot in the command is not ACTIVE. Verify by “lscds” command.
2. If the DS1 line specified by slot.line in the command is not added. Verify with **lsds1ln** command.
3. If either the DLSAP profile or MACSAP profile specified in the command is not added. Verify with **lsdlsps** and **ismacsaprof** command.
4. If any of the parameters specified are illegal.

## Isdchan Command Fails

The **isdchan** command displays all the D-channels on the currently active cards.

This command could fail for the following reasons:

1. If the specified D-channel is not added.
2. If the specified parameters are out of range/illegal.
3. If the logical slot specified in the command is not ACTIVE.

## deldchan Command Fails

The **deldchan** command deletes the specified D-channel. This command could fail if:

1. Specified D-channel is not added.
2. Specified parameters are out of range/illegal.
3. Logical slot specified in the command is not ACTIVE.

## D-Channel Is Down

The **ldlsapstatus** command displays the DLSAP status. If the status displays **dataXfer**, the D-channel is up and is ready to send and receive Q.931 PRI messages. Any other state indicates the D-channel is down. The reasons the D-channel could be down include:

1. The soft switch has not “ESTABLISH”ed the D-channel.

The D-channels on MGX8260 are controlled by the soft switch. Once the D-channels are added, the soft-switch needs to send a backhaul ESTABLISH\_REQ channel message on each D-channel configured on the MGX before using it for transferring Q.931 PRI signalling messages. Until MGX8260 receives a backhaul ESTABLISH\_REQ message, the D-channel MAC layer is shut to prevent peer from setting up the D-channel. Once soft-switch attempts to setup D-channel, the MAC is opened to send and receive SABME and UA messages.

2. The remote side is not up.

When soft switch issues an ESTABLISH\_REQ messages on a D-channel which is not in “dataXfer” state,

LAPD sends out a Q.921 SABME message on D-channel. To setup the D-channel to “dataXfer” state, the remote side should respond back with a Q.921 UA message on the same channel. The initiating end retries by sending SABME few more times (default of 3) periodically (default is every second) and if it does not get a response, LAPD sends backhaul RELEASE\_IND message to soft-switch indicating that LAPD can not setup the D-channel.

3. TEI mismatch.

If LAPD is receiving ESTABLISH\_REQ messages and the remote side is also up, one possible reason why the remote side is not responding to SABMEs is that the remote side is getting SABMEs on the wrong SAPI/TEI. The MGX8260 always uses SAPI 0. The TEI is user-configurable and should match on both ends. It is the last parameter dlsapNumTEI in the DLSAP profile configuration on the MGX8260.

4. User-Network mismatch.

Another possible reason for failing to establish a D-channel is when both the sides are either configured as User or both sides are configured as Network. Each message carries a C/R (command/response) field. User and Network devices use this field differently, so if the remote side is a Network device and it receives messages from a Network device, it drops all messages. Similarly, if the remote side is a User device and it receives messages from a User device, it drops all messages.

To fix this, change one of the end-points. The User/Network configuration is part of the MACSAP profile on MGX8260.

# Data Path Troubleshooting

Data path debugging and troubleshooting is required when any of the following cases occur:

- No Voice
- BERT Test Fails
- Tone Detection Fails

## There Is No Voice

### Fault Isolation

1. Make sure that T1/E1 lines and channel bank are configured correctly.
2. End point on NSC: determine the type of call:  
`dspvoiceparm <slot>, <port>` (on NSC, display voice params)
3. Port State=CHANNEL\_CONNECTED  
`-- connType=T1_VOIP, Primary Entry=1`  
`-- chanIdx 0 dse 0, dsp 0, chan 0`  
`-- Channel State=CHAN_ONLINE`  
`rtpPort 402 ecn 500 oldParm 0`  
`encType=GrpG711 silenceTmr 20 CNG 0 pktLoading a`  
`echoCan 4 dtmf 0 mf 0 fax 0 rxGain 0 txGain 0`

The results show that the call is a VoIP call (connType=T1\_VOIP), codec is G.711, VAD/CNG is off (CNG 0) and echoCan is On (echoCan 4). The DSP resource used is: dseNum=0 (dse 0) dspNum=0 (dsp 0) chanNum=0 (chan 0).

### Solution

- 
- Step 1** If it is a VoIP call, make sure that the DSP is alive  
`lsdspd` (on SCC, list DSP status)
- Step 2** Find out whether packets drop  
`dspvoicestat <slot>, <port>` (on NSC, display voice status)
- ```
pduIn      = 7687
pduDone    = 7695
ingrPacketCnt = 7687
ingrPacketDrpCnt = 32
...
egrPacketCnt = 7695
egrPacketDrpCnt = 1
```

**Step 3** Enter this command a few times. The PacketCnt should increase and the PacketDrpCnt should stay the same in normal case (for both ingress and egress).

**Step 4** If various PacketDrpCnt increase, check the ethernet port configuration on SCC:

```
lsethlns (on SCC, list ether lines)
```

```
Line      IP Address      Subnet Mask      Status      Gateway Addr
=====
9.1      192.168.4.123  255.255.255.0   Active      192.168.4.124
```

```
lsethln 9.1 (on SCC, list ether line 9.1)
```

```
Ether Line      : 9.1
MAC Address     : 10.20.30.40.50.60
IP Address      : 192.168.4.123
...
Duplex Mode     : full
```

**Step 5** If the configuration is correct, check on the statistics of the IP packets:

```
dspbimif 0 (on SCC, display BIM info on ether line 9.1)
received packets13456876
received packets with errors4508
.....
received crc errors          4508
.....
sent packets18790870
```

**Step 6** If the errors increase (enter this command a few times), check on the configuration of the BIM card, ethernet cable, etc.

If there are no errors in the BIM card, the problems may reside on TCG/DSE/DSP.

**Step 7** Provide the following information:

```
dspvoiceparm <slot>, <port>
dspvoicestat <slot>, <port> (enter this command a few times)
dspDcd <slot>, <port> (enter this command a few times)
c6Dump <dseNum>, <dspNum>
dspDspRsc <NSC slot>
lsevt 0 <NSC slot>
```

**Step 8** If the connType from dspvoiceparm is not T1\_VOIP (e.g. T1\_EC\_T1, etc), then the call is a TDM call. Since no DSE and C6 DSP are involved in TDM calls, the problem is likely on some of the devices along the data path. See the debugging guides for those devices for details. Be prepared to provide the following information when reporting the problem:

- dspvoiceparm <slot >, <port>
- dspDspRscAll <NSC slot>

- lsevt 0 <NSC slot>

### When the end point is on BSC:

**Step 1** Find out the DSP channel on which NSC is assigned to provide the service for this connection:

```
dspDspRscAll <NSC Slot>    (on SCC)
```

```
dspDspRscAll 0
```

```
DspChan 0: SRC SLOT 12 PORT 0 --> VIA SLOT 0 ECN (257, 11) --> DST ...
```

```
DspChan 1: SRC SLOT 12 PORT 1 --> VIA SLOT 0 ECN (769, 11) --> DST ...
```

The result shows that the DSP channel number 0 on the NSC slot 0 is used to service port 0 on the BSC slot 12 via ECN number 257. In order to use the dspvoiceparm(stat) commands, record the ECN number for the BSC port.

**Step 2** Use dspDspRscAll commands for all NSCs on the chassis until the specific BSC port is found. If the BSC port is not found, there is no DSP service required for the call. It will be a TDM call without echo cancellation.

The dspvoiceparm on BSC lists the parameters of the call on that port.

No dspvoicestat on BSC card.

```
dspvoiceparm <BSC slot> <port >    (on BSC, display voice parm)
```

```
Port State CHAN_BSC_CONNECTED, primaryDs0 1
```

**Step 3** If DSP service is required for the call, you must go to the NSC card to debug. Use dspvoiceparm and dspvoicestat the same way as the end point on NSC except that use '16' as the <slot> number and ECN number as the <port>.

```
dspvoiceparm 16, 257    (on NSC, display voice parms)
```

```
dspvoicestat 16, 257    (on NSC, display voice status)
```

If the connType from dspvoiceparm (on NSC) is VIA\_VOIP, it is a VoIP call. Follow the procedure for T1\_VOIP connections to debug.

### If the End point is on BSC (TDM):

**Step 1** If the connType from dspvoiceparm is not VIA\_VOIP (e.g VIA\_EC\_VIA, etc), it is a TDM call. Since no DSE and C6 DSP are involved in TDM calls, the problem is likely on the devices along the data path (cell drops?, etc). See the debugging guides for those devices for details. However, provide the following information when reporting the problem:

- dspvoiceparm <BSC slot> <port>
- dspvoiceparm <NSC slot> <port>
- dspDspRscAll <NSC slot>
- lsevt 0 <BSC slot>
- lsevt 0 <NSC slot>

## Fax/Modem Fails

Before starting your Fax/Modem, make sure that the connection is setup correctly (if possible, test the connection by talking on the phone).

If connected to channel bank, make sure that the channel bank is configured properly with the DS1 lines (robbitedBit, source of the clock).

If any switchover occurs while Fax/Modem is in progress, the Fax/Modem calls will be dropped. This is an expected result.

Provide the following information if your Fax/Modem fails:

- Take TCG trace on NSC
- Take DSE trace on NSC
- Enter the command dspvoiceparm (before fax/modem starts and afterwards)
- Enter the command dspvoicestat (a few times before and after fax/modem starts)
- Enter the command c6Dump

## COT/Testline Fails

If SCC switchover occurs, the tests will be terminated. This is an expected result.

If the switchover fails, it is likely that either the parameters are not sent down correctly from the call control or the DSP does not work correctly.

Provide the following information when reporting the problem:

- Take TCG trace on NSC
- Take DSE trace on NSC

## Tone Detection/Play Fails

The tone detection/play is enabled when the call is VoIP and the codec is G.726 or G.729. Otherwise, the tones are sent/received just like voice. Use the c6Dumpcommand to see whether the feature is enabled:

```
c6Dump <dse> <dsp>
chan  codec  vad/cng  dtmf    mf  ...
0      G.726    0        1      1  0
```

If 'dtmf' is set 1, the tone detection/play is enabled. (The dseNum, dspNum, chanNum can be retrieved from dspvoiceparm).

If detection/play is NOT enabled, the tones are treated like voice. This problem is not specific to the tones.

If it is enabled, the problems can be that the DSP does not detect the tone correctly or the DSE does not send/receive the NTE packets correctly. Provide the following information when reporting problems:

- Take DSE trace on NSC
- dspvoiceparm
- dspvoicestat
- c6Dump

## Line Interface and Switching Path Troubleshooting

Line interface and switching path troubleshooting is necessary when problems occur with any of the following:

- DS1 line interface
- E1 line interface
- DS3 line interface
- OC3 line interface
- ATM switching path components

Most line interface symptoms are caused by improper hardware configuration, such as cabling.

Other problems may be caused by the following:

- Software configuration, such as clocking, line type, encoding, and framing mismatch
- System configuration, such as DMC M13 mapping
- Genuine hardware failures which do occur (although rarely), such as broken optical cable, connectors

### E1 Line Interface Debug Methodology

- Always capture the output of `lsevt`, `lstraps`, and E1 CLI and engineering debug commands
- Always issue `lsds1ln` to verify configuration and check alarm status and alarm cause. Verify that the E1 line has not been mistakenly put in loopback state.
- Always issue `lsds1curst` and `lsds1totst` to inspect performance statistics; perform `lsds1curst` multiple times to detect trends
- RED - LOS - check cables; in case of BSC/DMC 1:1 redundancy also check the corresponding DS3 Y-cables
- RED - LOF – confirm near end and far end have the same line type (DS1 vs. E1) and framing type (ESF, D4, E1-CRC-MF etc.)
- YELLOW – the remote end is in RED alarm

If performance statistics show recurring control slip seconds (in output of `lsds1curst` or `lsds1totst`), verify that the various nodes in the network are configured to have the SAME reference clock source. For multi-chassis and PRI type of applications, the various nodes in the system must have the same reference clock to synchronize clock sources.

If BOTH local and remote end DS1 lines are in RED, isolate fault by first putting remote end in LINE loopback (either by performing line loopback on remote node directly or by sending loopback code from local end using `chds1ln`). Then initiate BERT test (using `onbertds1`) from local end to verify local side. Remember to UNDO loopback on remote end.

#### Special case 1: No voice when the MGX8260 is connected to E1 channel bank

Make sure the E1 line robbed bit signaling is turned on and the correct robbed bit pattern (0101) is selected.

#### Special case 2: DMC M13 mapped NSC DS1 lines in RED alarm

Use `lsm13s` to verify M13 mappings; use `lsds3ln` to verify the mapped DMC DS3 line state

**Special case 3: DS1 line disappears/comes up with wrong configuration after BSC/NSC switch over/back**

Check event log for DS1 and DBM related error events; issue the following DBM debug command on SCC:

```
dbmdisptab (63+slot #), 0, 1
```

**Example:**

For service card in slot 2 (1-based):

```
MMS.9.ACTIVE-> dbmdisptab 65, 0, 1
DB(65) Table(0) :          tName:          DS1CFG          tFileName:
C:/CONFIG/DB/c_1_Hd/DS1CFG          tCbFn:          DS1Callback          tInitFn
tEntryInfoFn          dslLineTblEntryInfoFn          tUpgradeFn          c_1_Hd_DS1CFG_upgrade
tDowngradeFn          c_1_Hd_DS1CFG_downgrade          tVersion          DB.01.00
tCbFnId:          0          tCbFnAddr:          0          tMaxEntries:          16
tCurrentEntries:          1          tTotalEntrySize:          44          tUsrSpecEntrySize:40
tNextEntry:          1          tTableStartAddr:          0          tPad:          4
tValid:          1          tCkSum:          0
HD DB(65) Table(0) :Entry (0) :00000000 00000002 00000002 00000001 00000001
00000001 00000000 00000002 00000008 0000007f          00000000value = 0 = 0x0
```

**Special case 4: DS1 line in alarm state but call control (e.g., MPC) did not release call on DS1**

- Verify trap event in lstraps output
- Capture output of MPC engineering debug command mpcDispSts

Try to reconcile trap recorded in lstraps output vs MPC's view of traps received

## Call Control

The Media Gateway Control Protocol (MGCP) defines the interaction between a Soft Switch (Call Agent) and the Media Gateway (MGX8260). Note that all active calls are preserved across SCC, BSC, or NSC switchover. However, transient calls are dropped.

## Debugging Commands

There are several engineering debug commands that can be executed to determine various conditions/status of calls/lines/trunks. These commands are listed in [Table 9-5](#):

**Table 9-5** *Debug Commands*

| Command               | Description                                                                                                                                                     |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>ibpmuxPrtDChan</b> | Displays the status of all the active cards which have D-channels and the status of all the D-channels on them.                                                 |
| <b>ibpmuxPrtOn 4</b>  | Displays all the backhaul messages received/transmitted by IBPMUX module on the SCC from/to the soft switch, as well as from/to LAPDs on service cards.         |
| <b>ibpmuxPrtOff</b>   | Turns off the display of backhaul messages received/transmitted by IBPMUX module on the SCC from/to the soft switch, as well as from/to LAPDs on service cards. |



Table 9-5 Debug Commands (continued)

| Command                                                   | Description                                                                                                                                                                                                                                   |
|-----------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>prrOn 28</b>                                           | Displays all the backhaul messages received or transmitted by the service card to IBPMUX module on the SCC. It also displays all the LAPD messages received/transmitted on all the D-channels.                                                |
| <b>prrOff</b>                                             | Turns off the display of backhaul messages received or transmitted by the service card to IBPMUX module on the SCC, as well as all the LAPD messages received/transmitted on all the D-channels.                                              |
| <b>pccDispCalls</b>                                       | Displays all calls and corresponding call information present in the system                                                                                                                                                                   |
| <b>pccTrunksPrint</b>                                     | Displays the ether trunks present in the system and the number of calls each one has on it.                                                                                                                                                   |
| <b>pccdbmDispCb</b>                                       | Displays information on the PCCDBM task                                                                                                                                                                                                       |
| <b>pccDispNumActCalls</b>                                 | Displays the number of all the active calls in the system.                                                                                                                                                                                    |
| <b>pccdbmDispActCon</b>                                   | Displays all active calls in the system that are stored by the PCCDBM task.                                                                                                                                                                   |
| <b>pccdbmDispUsedMncobj</b>                               | Displays the Ram DB call objects used in the system. RAM DB is kept in PCCDBM task.                                                                                                                                                           |
| <b>pccdbmDispFreeMncobj</b>                               | Displays the Ram DB call objects free in the system. RAM DB is kept in PCCDBM task.                                                                                                                                                           |
| <b>PrcPrintCotObj</b>                                     | Displays all call object relating to the following operations :<br>Announcement, Transponder and LB COT, Milliwat Test                                                                                                                        |
| <b>PrcPrintLines</b> ( <i>module number-zero based</i> ): | Display Line Status for each module. This information includes information about the admin status and the physical status of the line                                                                                                         |
| <b>PrcPrintDiskDb</b>                                     | Displays the contents of PRC module hard disk DB. This includes information on the echo cancellation option for all DS1 lines, admin status for all lines and modules and some other miscellaneous information about resource control module. |
| <b>mscpPrtSts</b>                                         | Print Statistics for IPDC.                                                                                                                                                                                                                    |
| <b>mscpClrSts</b>                                         | Clear Statistics for IPDC.                                                                                                                                                                                                                    |

## Turning on Trace Debugging



### Warning

**System performance is severely affected if trace debugging is turned on. It is strongly recommended that the craftperson and/or system engineer (SE) do not enable trace debugging on a live customer system or during stress and/or performance testing on the MGX8850.**

No debug information will print on the screen until the command **tyredir 1** is entered. This command redirects console information to the current terminal in use. Also, it is usually prudent to change the idle time to some amount of time longer than is necessary for the current test to run. Use the command **chidletm #** (where # is the amount of time in minutes to wait before timing out the active session). System security maybe jeopardized if the timeout value is changed to a large number such that it takes

a long time to automatically logout an idle telnet session and the telnet session is left unattended for unauthorized personnel to access the system. It is therefore recommended that the timeout value be restored to its original value.

The **mscpPrtOn** command turns debugging on for Protocol layer messages prints. It takes a single parameter value (2,3 or 4) which scales the amount of debug info to print. The number 2 will display the least amount of debug and the number 4 will display the most. Use the following command to receive the minimum debug information:

```
mscpPrtOn 2
```

Use the following command to receive the maximum debug information:

```
mscpPrtOn 4
```

The debug trace command **prtOn** takes a single parameter that specifies which software element to trace.

Trace debugging can be turned off by entering the command **mscpPrtOff** and **prtOff**. Printing to the terminal can be prevented by entering **ttyredir 0**. However, Cisco strongly recommends that the **mscpPrtOff/PrtOff** commands be used to turn off trace debugging because, once the trace debugging is turned on and even though the trace output is not directed to the terminal, system performance is still drastically slowed down .

## Media Gateway Errors

Use the **lsndinf** command to verify that the MGX8850 is set up in MGCP protocol. If not, then use the **chprotocol** command to change it to MGCP. MGCP is a standard protocol defined by the Internet Engineering Task Force (IETF). MGCP supports TDM, VoIP, and VoATM. Note that VoIP and VoATM are mutually exclusive.

Once the MGX8850 is running in MGCP protocol mode, the MGCP specific parameters need to be configured. Configuring these parameters makes it possible for the MGX8850 to communicate with its corresponding Call Agent.

Before making any changes to the MGCP protocol parameters, it is best to see how the switch is already configured. Use the commands **lsmgcp** and **msmgcpdef** to display the current MGCP parameter values.

## System Redundancy

SCC, NSC, and BSC are three types of cards that support redundancy. SCC and BSC support 1:1 redundancy and NSC supports n:1 redundancy.

### SCC Redundancy

SCC redundancy need not be configured. Each MGX8260 can have upto 2 SCCs, on only slots 9 and 10. When both SCCs are present, one goes to Active state while the other goes to Standby state, based on several criteria.

The Active SCC provides all the system functionality until there is a failure or a reset or if that card is removed from the MGX8260. When that happens, if there is a Standby SCC, the Standby SCC becomes active and provides the system functionality. Active calls are not dropped, however they might experience a loss of voice for a fraction of a second. Some of the new calls may get dropped during this switchover. The newly-active SCC becomes available within a few seconds.

Typically, both SCCs run the same software image. However, it is possible for SCCs not to run the same software image when there is only 1 SCC in the node and you tftp a different image to the SCC, and then insert another SCC which has an old image. In this case, the active SCC will check the image file checksum and transfer the image file from Active to Standby if they are different.

You must reset the Standby SCC after the file transfer. To check whether the Active and Standby are running different images, use “lscds” command and verify the software version.

Each SCC has a hard-disk on board. This hard-disk houses the persistent database (called HD-DB) in a set of files. The non-persistent database (also called RAM-DB) is stored in RAM files and are not restored if the node is reset/rebooted. Persistent database includes fast-ethernet lines configured on SCC, the number and type of service cards present in the node, the service-card redundancy configuration, the DS1 to DMC-DS3 mappings. The SCC hard disk also houses all the service card HD-DBs because service cards do not carry hard disks. Besides, if the configuration is stored on SCC, then it is easy to replace a faulty service-card with a new service-card.

## Standby SCC Stays in Mismatch State

This occurs when the Standby SCC configuration does not match the Active SCC configuration. Both SCCs should have identical configuration, such as BIM-type, BC-type, DMC, etc. This problem can be caused by any of the following:

1. If your previous Standby SCC had a 4-FE BIM and you replaced it with OC3 BIM.
2. If you replaced your 4-FE Standby SCC backcard with OC3 SCC backcard.
3. If you have a DMC with the Active SCC and you do not have a DMC with the Standby SCC. If you do not have a DMC with the Active SCC, you must unplug the DMC that is with the Standby SCC.

## Standby SCC Goes to FAIL State

This problem can be caused by a variety of reasons, such as when DB Sync to standby SCC fails, DMC initialization on Standby SCC fails, DBM update to standby SCC fails, etc. This should be a rare occurrence and should be logged with the following information:

1. Output on Active SCC of “lscd” command for Standby SCC
2. Output on Active SCC of “lscds” command
3. Output on Active and Standby SCC of “lsevt” command
4. Screen dump of Active and Standby SCCs at the time of failure if available
5. Version of both SCCs

# Troubleshooting VISM Cards

Use the following troubleshooting tools and techniques to assist you in maintaining your VISM card:

- [“VISM Card LEDs” section on page 9-32](#)
- [“VISM and PXM Display, Log, and Diagnostic Loopback Path CLI Commands” section on page 9-34](#)
- [“VISM Alarms” section on page 9-36](#)
- [“UNIX Snoop Trace Tool” section on page 9-36](#)
- [“Symptoms and Solutions” section on page 9-37](#)

## VISM Card LEDs

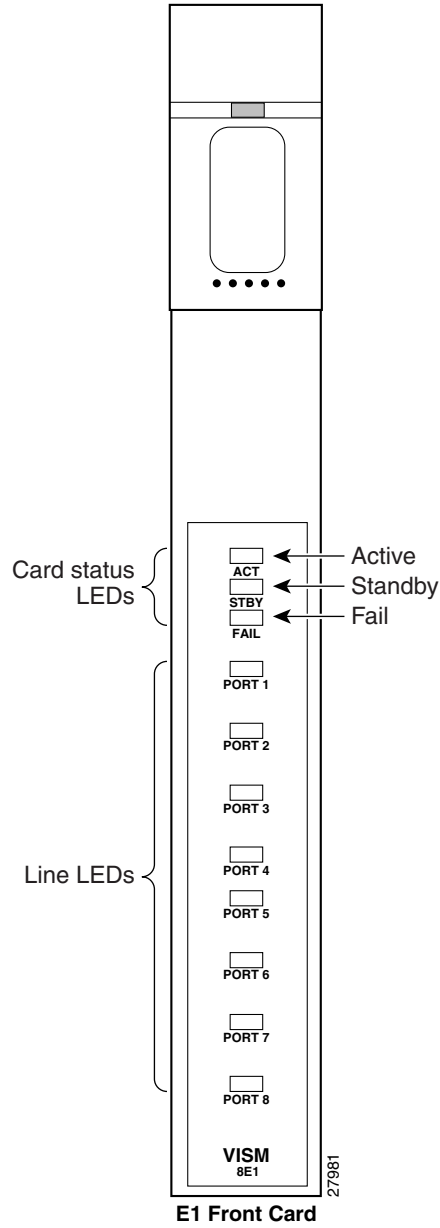
The VISM card uses the following three card status LEDs (see [Figure 9-6](#)) to indicate certain states:

- ACT—Green indicates the active state.
- STBY—Orange, or blinking orange, indicates one of the following:
  - VISM is in the standby state.
  - VISM is in the mismatch state.
  - VISM card DSPs are currently involved in the VISM card bootup.
- FAIL—Red indicates the failure state, or certain stages of the bootup process.

The VISM card uses eight line status LEDs (see [Figure 9-6](#)) to indicate the following states of the eight T1 or E1 ports on the VISM back card:

- Green—A line has been added and there is no alarm on that line.
- Orange—A line has been added and there is a yellow alarm condition on the line.
- Red—A line has been added and there is one of the following conditions on the line:
  - Loss of signal (LOS) (red alarm condition)
  - Loss of frame (LOF)
  - Alarm indication signal (AIS)

Figure 9-6 VISM Front Card LEDs



## VISM and PXM Display, Log, and Diagnostic Loopback Path CLI Commands

You can use the following commands to troubleshoot your VISM card:

- The VISM **dspcd** command
- The PXM **dsplog** command
- PXM diagnostic loopback commands



### Note

Refer to the Cisco MGX 8000 Series platform command reference guides for more information on PXM commands.

### VISM Display Card CLI Command

Use the VISM **dspcd** command to display the following types of information about your current VISM card:

- State of the VISM card
- Type of VISM card
- Version number and part numbers
- Daughter card version numbers and part numbers

The following example shows the results of a typical **dspcd** command:

```
NODENAME.1.3.VISM8.a > dspcd
ModuleSlotNumber:      17
  FunctionModuleState:  Active
  FunctionModuleType:   VISM-8T1
  FunctionModuleSerialNum: SAK0331006P
  FunctionModuleHWRev:   0.0
  FunctionModuleFWRev:   2.0.0_11Nov01_2
  FunctionModuleResetReason: ?
  LineModuleType:       LM-RJ48-8T1
  LineModuleState:      Present
  mibVersionNumber:     21
  configChangeTypeBitMap: CardCnfChng, LineCnfChng
  pcb part no - (800 level): 800-04399-01
  pcb part no - (73 level):  73-03618-01
  Fab Part no - (28 level):  28-02791-01
  PCB Revision:         08

Daughter Card Information:
  Daughter Card Serial Number: SAK0331003P
  pcb part no - (73 level):    73-03722-01
  Fab Part no - (28 level):    28-02905-01
  PCB Revision:               04
```

## PXM Display Log CLI Command

Use the PXM **dsplog** command to display useful information for troubleshooting your VISM card. The log is maintained by the PXM. A VISM entry is displayed in the log in the following format:

- Date and time of the log
- Slot number of the VISM card from which a message is logged
- The process on the VISM card that logged that message
- Severity of the message:
  - 1 = Fatal error which causes the card to reboot
  - 6 = All other errors
- A log message description

The following example shows the results of a typical **dsplog** command:

```
09/09/2001-02:09:01 03 cam VISM-6-9157
VISM got time from PXM
```

## PXM Diagnostic Loopback Path CLI Commands

The VISM-8T1 and VISM-8E1 cards provide the capability for creating loopback paths for diagnostic purposes. Use the VISM and PXM diagnostic loopback CLI commands to troubleshoot your VISM cards. The following loopback configurations are possible:

- Local line loopback. Use the PXM **addlnloop** command to enable local line loopback on a line-by-line basis. Use the PXM **dellnloop** command to disable local line loopback.
- Remote line loopback. The PXM **cnfbert** command is a T1/E1 diagnostic test package which includes some loopback tests.

Use the BERT and loopback functions to test the integrity of T1 and E1 lines. You can use the the PXM **cnfbert** command on the PXM to perform the following actions:

- Run BERT on a per-line basis on the VISM card.
- Put a VISM line on a TDM side loopback.
- Put a VISM line on a network side loopback.
- Cause the VISM to put test equipment residing on the far side into loopback.
- OAM loopback through the CPU toward the network (per VC). This loopback is enabled automatically; no PXM or VISM CLI commands are required.
- DS0 loopback, at the compression DSP toward the TDM side. Use the PXM **addendptloop** command to enable DS0 loopback on a DS0-by-DS0 basis. Use the PXM **delendptloop** command to disable DS0 loopbacks.
- VC remote loopback. Use the PXM **addconloop** command to enable VC remote loopbacks. Use the PXM **delconloop** command to disable remote loopbacks.

## PXM1E and PXM 45 Display CLI Commands

Refer to the *Cisco MGX 8850 Installation and Configuration Guide* and the *Cisco MGX 8000 Series Switch Command Reference* for information on the following PXM1, PXM1E, and PXM45 card display commands.

## VISM Alarms

Table 9-6 describes VISM T1 and E1 card alarms.

**Table 9-6 VISM T1 and E1 Card Alarms**

| Error                                 | Alarm Type       | Down stream (ATM side) | Up Stream (TDM side) | Comments                                        |
|---------------------------------------|------------------|------------------------|----------------------|-------------------------------------------------|
| Link Failure—receive LOS <sup>1</sup> | LOS <sup>1</sup> | AIS <sup>2</sup>       | RAI <sup>3</sup>     | RAI <sup>3</sup> returned on the transmit line. |
| Receive RAI <sup>3</sup>              | Yellow           | RAI <sup>3</sup>       | None                 | —                                               |
| Receive LOF <sup>4</sup>              | —                | AIS <sup>2</sup>       | RAI <sup>3</sup>     | RAI <sup>3</sup> returned on the transmit line. |
| Receive AIS <sup>2</sup>              | AIS <sup>2</sup> | AIS <sup>2</sup>       | RAI <sup>3</sup>     | RAI <sup>3</sup> returned on the transmit line. |

1. LOS = Loss of service.
2. AIS = Alarm indication signal.
3. RAI = Remote alarm indicator.
4. LOF = Loss of frame.

Refer to T1.403 for DS1 and G.704 for E1 definitions of alarm states. Alarms are propagated to the remote end over the ATM network in accordance with ATM specifications.

## UNIX Snoop Trace Tool

Use the UNIX snoop trace tool to assist in diagnosing a problem. The **snoop** command can determine if there is any activity between the VISM and the call agent. The following example shows the command and a typical resulting terminal display:

```
snoop -x 42 -ta <ip address of CA> port <udp port of CA>
E.g snoop -x 42 -ta vismvsc1 port 2427
```



## Symptoms and Solutions

This section includes possible solutions to the following possible symptoms:

- “VISM Card Did Not Become Active” section on page 9-37
- “T1/E1 Configuration Mismatch” section on page 9-37
- “DSP Download Failure” section on page 9-39
- “VISM Front Card/Back Card Mismatch” section on page 9-39
- “Cannot Use the cc Command to Access a VISM Card” section on page 9-40
- “VISM Card Resets Intermittently” section on page 9-40
- “VISM Card Does Not Accept a Firmware Download” section on page 9-40
- “Echo Is Heard on a Voice Call” section on page 9-41
- “VISM Card LEDs Are Not Lighted” section on page 9-41

### VISM Card Did Not Become Active

Investigate the following possible causes for a VISM card that does not become active:

- An E1 card is inserted in a slot where a T1 card was present, or a T1 card is inserted in a slot where an E1 card was present, resulting in configuration mismatch.
- The minimum number (five) of DSPs failed to download.
- A front card type does not match the back card type—if the front card is T1 and the back card is E1, or the front card is E1 and the back card is T1.
- The VISM card MIB image version does not match the PXM disk MIB image version.

### T1/E1 Configuration Mismatch

Use the PXM `dspecds` command to identify a T1/E1 configuration mismatch, as follows:

```

NODENAME.1.7.PXM.a > dspecds
Slot  CardState  CardType  CardAlarm  Redundancy
-----
1.1   Empty
1.2   Empty
1.3   Empty
1.4   Empty
1.5   Mismatch    VISM-8E1  Clear
1.6   Empty
1.7   Active      PXM1-OC3  Clear
1.8   Empty
1.9   Empty
1.10  Empty
1.11  Empty
1.12  Empty
1.13  Empty
1.14  Empty
1.15  Empty
1.16  Empty
1.17  Empty
1.18  Empty
1.19  Empty

```

Use the PXM **dspsmcnf** command to identify a T1/E1 configuration mismatch, as follows:

```
NODENAME.1.7.PXM.a > dspsmcnf
slot      Card      Rate      Channel      MIB      Feature
No.      Type      Control   ized        IMA      MULTRKS   Version  Bits
-----
1        <-----> No configuration file exist for this slot <-----
2        <-----> No configuration file exist for this slot <-----
3        VISM-8T1   Off       Off         Off      Off       20      0x0
4        <-----> No configuration file exist for this slot <-----
5        VISM-8T1   Off       Off         Off      Off       20      0x0
6        <-----> No configuration file exist for this slot <-----
9        <-----> No configuration file exist for this slot <-----
10       <-----> No configuration file exist for this slot <-----
11       <-----> No configuration file exist for this slot <-----
12       <-----> No configuration file exist for this slot <-----
13       <-----> No configuration file exist for this slot <-----
14       <-----> No configuration file exist for this slot <-----
17       <-----> No configuration file exist for this slot <-----
18       <-----> No configuration file exist for this slot <-----
19       <-----> No configuration file exist for this slot <-----
20       <-----> No configuration file exist for this slot <-----
21       <-----> No configuration file exist for this slot <-----
22       <-----> No configuration file exist for this slot <-----
25       <-----> No configuration file exist for this slot <-----
26       <-----> No configuration file exist for this slot <-----
27       <-----> No configuration file exist for this slot <-----
28       <-----> No configuration file exist for this slot <-----
29       <-----> No configuration file exist for this slot <-----
30       <-----> No configuration file exist for this slot <-----
```

Use the PXM **dsplog** command to show a card mismatch log entry, logged by VISM card on slot 5, as follows:

```
09/09/2001-00:01:47 05 dspllog VISM-6-9025
VISM going to standby : Config. Mismatch between PXM and VISM
```

Use the VISM **dspecd** command to display the following information:

```
NODENAME.1.5.VISM8.s > dspecd
ModuleSlotNumber:      5
FunctionModuleState:   Mismatch
FunctionModuleType:    VISM-8E1
FunctionModuleSerialNum: CAB12345678
FunctionModuleHWRev:   0.13
FunctionModuleFWRev:   2.2.10g.pm
FunctionModuleResetReason: WatchDog timeout reset
LineModuleType:        Missing
LineModuleState:       Not Present
mibVersionNumber:      20
configChangeTypeBitMap: CardCnfChng, LineCnfChng
cardIntegratedAlarm:   Clear
pcb part no - (800 level): 800-03530-01
pcb part no - (73 level): 73-03021-01
Fab Part no - (28 level): 28-02492-01
PCB Revision:          01
Daughter Card Information:
Daughter Card Serial Number: CAB12345678
pcb part no - (73 level): 73-03022-01
Fab Part no - (28 level): 28-02493-01
PCB Revision:          01 value = 34 = 0x22 = ''
```

## DSP Download Failure

Use the PXM **dsplog** command to determine if the minimum number (five) of the DSPs failed to download. The terminal displays results similar to the following:

```
NODENAME.1.7.PXM.a > dsplog
01/01/2001-00:02:10 05 tDspmD1 VISM-6-9193
DSPM task errors : 6 DSPs failed to download
```

If the number of DSPs (six in the above case) is greater than five, the card will fail to be in the active state. If this condition happens repeatedly, replace the card.

Use the following PXM **dspecds** command, and the results, to determine the current state of VISM DSPs:

```
NODENAME.1.7.PXM.a > dspecds
Slot CardState CardType CardAlarm Redundancy
---- -
1.1 Empty Clear
1.2 Empty Clear
1.3 Empty Clear
1.4 Empty Clear
1.5 Failed VISM-8E1 Clear
1.6 Empty Clear
1.7 Active PXM1-OC3 Clear
1.8 Empty Clear
1.9 Empty Clear
1.10 Empty Clear
1.11 Empty Clear
1.12 Empty Clear
1.13 Empty Clear
1.14 Empty Clear
1.15 Empty Clear
1.16 Empty Clear
1.17 Empty Clear
1.18 Empty Clear
1.19 Empty Clear
```

## VISM Front Card/Back Card Mismatch

Use the following PXM **dsplog** command to investigate a possible VISM front card/back card mismatch:

```
NODENAME.1.7.PXM.a > dsplog
01/01/2001-00:02:24 05 cmm VISM-6-9025
VISM going to standby : Config. Mismatch between ASC and VISMV
01/01/2001-00:02:24 05 cmm VISM-6-9023
Mismatch Backcard
01/01/2001-00:02:24 05 cmm VISM-6-9023
Mismatch Backcard
```

In a mismatch condition, use the PXM **dspecds** command to display the following type of information:

```
NODENAME.1.7.PXM.a > dspecds
Slot CardState CardType CardAlarm Redundancy
---- -
1.1 Empty Clear
1.2 Empty Clear
1.3 Empty Clear
1.4 Empty Clear
1.5 Mismatch VISM-8E1 Clear
1.6 Empty Clear
1.7 Active PXM1-OC3 Clear
1.8 Empty Clear
```

```

1.9 Empty Clear
1.10 Empty Clear
1.11 Empty Clear
1.12 Empty Clear
1.13 Empty Clear
1.14 Empty Clear
1.15 Empty Clear
1.16 Empty Clear
1.17 Empty Clear
1.18 Empty Clear
1.19 Empty Clear

```

Use the VISM **dspecd** command to display the following types of information:

```

NODENAME.1.5.VISM8.s > dspecd
ModuleSlotNumber: 5
FunctionModuleState: Mismatch
FunctionModuleType: VISM-8E1
FunctionModuleSerialNum: CAB0246014P
FunctionModuleHWRev: 0.0
FunctionModuleFWRev: 2.2.10g.pm
FunctionModuleResetReason: Reset by ASC from Cell Bus
LineModuleType: LM-RJ48-8T1
LineModuleState: Invalid
mibVersionNumber: 20
configChangeTypeBitMap: CardCnfChng, LineCnfChng
cardIntegratedAlarm: Clear
pcb part no - (800 level): 800-04399-01
pcb part no - (73 level): 73-03618-01
Fab Part no - (28 level): 28-02791-01
PCB Revision: 05
Daughter Card Information:
Daughter Card Serial Number: CAB024601FF
pcb part no - (73 level): 73-03722-01
Fab Part no - (28 level): 28-02905-01
PCB Revision: 02 value = 34 = 0x22 = ''

```

## Cannot Use the cc Command to Access a VISM Card

Use the PXM **dspecds** command to verify if the VISM card is in the active or standby state. If the VISM card is not in the active or standby state, you cannot use the **cc** command to access the card.

## VISM Card Resets Intermittently

Investigate the following possibilities to determine why the VISM card is resetting intermittently:

- Bad hardware device on the card. Replace any corrupt hardware.
- Daughter card is not attached correctly to the VISM card. As a result, the VISM card is not able to maintain its abilities. Ensure that the daughter card is making electrical contact to the motherboard, and is mechanically secure.

## VISM Card Does Not Accept a Firmware Download

There must be a VISM card in the slot to which firmware is being downloaded. Ensure that the VISM card is seated in the slot, and that it is making electrical contacts to the backplane. The card must be in either the active or boot state. Confirm this is the case and try again.

## Echo Is Heard on a Voice Call

Ensure that the call has the ECAN feature enabled. If the echo delay is longer than the provision tail length, ECAN does not work. Use the VISM **cnfecantail** command to configure a larger value for the tail length.

## VISM Card LEDs Are Not Lighted

The VISM card may not be inserted completely in the slot. Ensure that the VISM card is seated in the slot correctly, with top and bottom half portions of the VISM card making electrical contact with the backplane.

## Firmware Does Not See the Card Insert Bit Status As Set

This symptom can also indicate a bad VISM card or bad MGX slot.

# Physical Indicators

## VISM Card LED Indications

The VISM card has three card status LEDs and 8 line status LEDs, organized as follows:

### VISM Front Card LEDs

*Table 9-7 VISM Card Front LEDs*

| LED COLOR | INDICATION                                                                                                                                                                   |
|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Green     | Active state.                                                                                                                                                                |
| Orange    | Standby state or when the VISM card DSPs are getting downloaded as part of the card booting up.<br>A standby LED will be blinking orange when the card is in the boot state. |
| Red       | Fail state. Red LED will be lit when the card is in the FAIL state.                                                                                                          |

## Line LEDs

VISM has eight line LEDs which indicate the following:

**Table 9-8 VISM Card Line LEDs**

| LED COLOR | INDICATION                                                                               |
|-----------|------------------------------------------------------------------------------------------|
| Green     | The line has been added and there is no alarm on that line.                              |
| Orange    | The line has been added and there is a YELLOW alarm condition on the line.               |
| Red       | The line has been added and there is a LOS condition (RED alarm condition) on the line.. |

## Port LED indications

### DSPM task errors: DSPs failed to download

Card serial port access  
 Common HW failures  
 Card did not become active

#### Possible Causes

Three possible causes exist.

1. An E1 card is inserted in a slot where a T1 card WAS present (or vice-versa), resulting in a configuration mismatch.
2. When at least the minimum number of DSPs failed to download - currently the threshold is fixed at 5.
3. When the backcard type does not match the front card type - if the front card is of type T1 (E!) and the backcard type is E1 (T1).

### VISM Going to Standby : Configuration Mismatch Between ASC and VISMV

When a minimum number of DSPs failed to download, the "dsplog" on the PXM shows the following:

```
01/01/1970-00:02:10 05 tDspmDI VISM-6-9193
```

```
DSPM task errors : 6 DSPs failed to download
```

If the number of DSPs (6 in the above case) is greater than 5, then, the card will fail to come up ACTIVE.

### Backcard Type Does Not Match the Front Card Type

The following message displays: VISM going to standby : Config. Mismatch between ASC and VISMV.

```
FunctionModuleState: Mismatch
```

```
FunctionModuleResetReason: Reset by ASC from Cell Bus
```

## Card Does Not Respond to Ping from Router

### Symptom

Cannot 'CC' to VISM card.

### Action

Check whether the card is in the ACTIVE/STANDBY state, using the "dspcds" CLI on PXM. If the VISM card is not in the ACTIVE/STANDBY state, "cc" to that slot is not possible.

## CiscoView Does Not Show VISM Card Configuration

### Symptoms

Card constantly reboots -- becomes Active and then resets again.

Card resets occasionally.

### Possible Causes

There are many reasons the above two could happen.

(a) Bad part (like older version of Nile4)

(b) Daughter card is not attached correctly to the VISM card, as a result, VISM card is not able to come up.

### Action

Make sure that daughter card has electrical contact to the mother board, and is mechanically held tight.

## dspcds on the PXM Shows VISM card as failed

### Symptoms

Cannot reset VISM card from PXM

Cannot download FW to VISM

### Action

For downloading a slot-specific image, there should be a VISM card on the slot to which firmware is being downloaded in the ACTIVE state or in the BOOT state. Confirm this and try again.

Also, make sure that VISM card is properly seated in the slot, and has electrical contacts to the backplane.

## Cannot Make a Call from the Cisco BTS 10200

### Action

Verify that the VISM IP address is configured on the Cisco BTS 10200.

Verify that the lines between the Cisco BTS 10200 and the VISM are in service.

Verify that you can ping the VISM from the Cisco BTS 10200. If this fails, determine whether the routing tables on the Cisco BTS 10200 have been configured correctly.

Verify that there is an entry for destination 10.0.0.0.

Verify that the Cisco BTS 10200 IP address has been added to the VISM's list. Execute the CLI command 'dspdns' to determine if the Cisco BTS 10200 IP address is configured. If not, add the Cisco BTS 10200 IP address.

## Calls Are Getting Rejected from VISM

There could be several reasons why calls could get rejected. Following are some of the most common ones.

Verify state of the gateway. Execute the CLI command 'dspgwstate'. If this indicates that the Gateway has been commanded out of service or that the gw is in alarm state, execute the CLI 'cnfgwis' to bring the Gateway into service.

Verify that the lines are added and in service. Verify that the appropriate lines have been enabled on the VISM and that they are not in alarm. This is indicated by green LEDs on the front panel corresponding to each of the lines. This can also be determined by using the CLI dsplns. If there is no problem here, verify that the lines are in service. To determine the state of the line, do 'dsplnstate <line number>'. If the display indicates that the line has been configured OOS, execute the 'cnflnis <line number>' to bring the line in service.

Verify that the endpoints have been added. This can be done by executing the CLI command dspendpts. Use addendpt or addendpts to add the endpoints, if they have not already been added.

Verify that the VISM's domain name configured on the VISM card matches whatever is configured on the Cisco BTS 10200. Do 'dspvismdn' to display the domain name configured for the VISM. To configure the VISM domain name, use the command - 'cnfvismdn'.

Calls (CRCX msgs from the CA) can also get rejected if a connection already exists on the endpoint on the VISM. In this case, the Cisco BTS 10200 is not synchronous with the VISM. The VISM will have to be reset.

Messages sent from the Cisco BTS 10200/CA will be rejected by the VISM, if the Cisco BTS 10200 is sending on a port that is not configured on the VISM for that CA. Messages sent from the VISM will also be sent only to the port configured for that CA.

A snoop trace will be helpful in determining the cause of failure between the VISM and Cisco BTS 10200 and could help trace the problem. This can be started using the command - snoop -x 42 -ta <ip address of CA> port <udp port of CA>.

## Echo Can Be Heard on the Voice Call

### Action

Make sure that the echo cancellation is turned on. Under ShellConn, do a dspm\_disp\_table to find out whether a call has echo cancellation. The display from dspm\_disp\_table tells you which echo cancellation DSP is used. Read from the display to find the tail length to which the echo cancellation is provisioned. If the echo delay is longer than the provisioned tail length, the echo cancellation will not work. Provision the tail length (cnfecantail) to a bigger value.



## Voice Is Distorted

Find out the compression DSP that the call is on. Use the shellConn command **dspm\_get\_err** to display error statistics on the DSP. If the error count is non-zero, and keeps increasing as this command is entered again, then this is a source of the problem.

## VISM Card Has All Leds Turned Off After Insertion In A Chasis Cause

The VISM card is not inserted completely in the slot. Firmware does not see the Card Insert Bit status as set.

### Action

Make sure that the VISM card is properly seated in the slot, with the top and bottom half portions of the VISM card making electrical contact with back plane.

## VISM Logs

VISM logs describe the following:

- Date & time of the log
- Slot number of the VISM card from which a message is logged
- Process on the VISM card that logged the message
- Severity of the message — if it is a fatal error causing card reboot, severity is 1. For all other messages, severity is 6.
- Message number, found in `/include/vism_error.h`
- Single line description — the log message.

## VISM to RPM Connection Problems

### Debugging/Correlating SGCP Messages Between Call Agent and VISM Gateway

Three levels of counters are available to determine whether any SGCP messages are lost between the Call agent and VISM. At the lowest level `dmciPrintShmem` can be used to display the DMCI blocks transferred between the host and the DM processors.

`dmciPrintMsgCnt` can be used to display the counters corresponding to specific message types. This command is extremely useful to make sure that for every SGCP message received from the Call agent, a response is sent.





# Troubleshooting the Cisco BTS 10200 Softswitch

---

This chapter describes various troubleshooting techniques for the Cisco BTS 10200 Softswitch. It includes the following sections:

- [Architecture, page 10-1](#)
- [Components, page 10-5](#)
- [Troubleshooting, page 10-10](#)
- [Cisco BTS 10200 Failure, page 10-17](#)
- [Operating System Failure, page 10-17](#)

## Architecture

This section briefly describes the Cisco BTS 10200 Softswitch architecture from an external components perspective. It describes the following types of components:

- [Call Agent, page 10-2](#)
- [Terminations, page 10-2](#)
- [Interfaces, page 10-3](#)

The Cisco BTS 10200 Softswitch connects to a variety of media gateways (MGWs) using the Media Gateway Control Protocol (MGCP), and supports MGCP 0.1. The Call Agent (CA) provides signaling and call processing for the Cisco BTS 10200 Softswitch.

Media gateways provide bearer paths between voice and packet networks, as well as connection control, endpoint control, auditing and status functions. These gateways are equipped with voice coders that convert voice into packets, and voice decoders that convert packets into voice. Connections are grouped in calls, which means that a call can have one or more connections. One or more Call Agents set up connections and calls.

The SuperPoP/Regional Office hosts all the servers needed to provide solution services. The media gateways are also typically located here where the PSTN trunks terminate.

## Call Agent

Call processing is performed with MGCP 1.0/NCS call control signaling with the Cisco BTS10200 call agent deployed in an active/stand mode. Feature servers, which provide the logic for enhanced services, are part of this complex. An EMS system which manages the call agent and the feature servers and provides subscriber/network provisioning functions is also part of the call agent infrastructure residing in the SuperPOP. The call agent runs on a Continuous Computing platform or Sun hardware and SS7/ISUP trunks terminate on this platform. The Cisco BTS 10200 Softswitch converts between SS7 signaling and Media Gateway Control Protocol for call setup and tear down. Release 3.5.3 of the Cisco BTS 10200 call agent is used in the BLISS solution Release 1.5 architecture.

At a high level, the Cisco BTS10200 call agent provides the following capabilities:

- Call signaling capabilities including SS7 (ISUP), MTP-3, and TCAP. Support for MGCP call control with the TGWs and NCS signaling on the MTA side.
- SS7/ISUP interactions with the PSTN SS7 network which includes support for SCP database dip applications like 800 number and LNP services.
- Universal Signaling interworking functions between protocols associated with each leg of the call.
- Address resolution and Call Routing
- CDR generation. Support of Event Messaging.
- Resource management and connection control
- Service Access Function to access services executing on the external server platforms, such as feature servers, SCPs, and so on.
- Management interfaces (using SNMP and/or CORBA and/or CLIs)
- Gate management function and DQOS support

The call agent supports deployment of feature servers on separate platforms. The call routing intelligence resides on the call agent and feature logic resides on the feature server. The Feature Control Protocol (FCP) is used to communicate with the feature servers. Either SIP or SIP-T can be used for inter-call agent communication. SIP is also used to communicate with the messaging platform. Support for the PacketCable CMS-CMS standard, [PKT-SP-CMSS-I04-040730 Call Management Server Signaling Specification](#), is also provided on the Cisco BTS 10200 Softswitch.

## Terminations

A termination refers to the physical link between the Cisco BTS 10200 Softswitch and a media gateway (MGW). The types of gateway terminations are listed in [Table 10-1](#).

**Table 10-1 Gateway Terminations**

| Gateway             | Type of Signaling                             | Type of Termination | Assignment                                       |
|---------------------|-----------------------------------------------|---------------------|--------------------------------------------------|
| Trunk gateway (CAS) | Channel associated signaling (CAS) using MGCP | CAS trunk           | Each CAS trunk is assigned to a CAS trunk group  |
| Trunk gateway (CCS) | Common channel signaling (CCS) using SS7      | SS7 trunk           | Each SS7 trunk is assigned to an SS7 trunk group |

## Interfaces

In the Cisco BLISS for Cable solution, an interface is any device that the solution components use to accomplish internetworking. The relevant interfaces in the solution are the following:

- **Trunking Gateway Interface**—Trunking gateways (TGW) are high-density PSTN to packet network gateways. These gateways typically support thousands of DS0 circuits and provide the bearer paths between PSTN circuit-switched facilities and packet-switched networks.

Two types of links are required for a TGW to connect with a peer PSTN switch:

- SS7 access link via the STP and the call agent
- Bearer circuits through the TGW

The Cisco BTS 10200 Softswitch supports these links by sending the proper SS7 messages to the STP, as well as providing bearer channel control through MGCP between the CA and the TGW.

- **Integrated Access Devices (IAD) Interface**—An IAD supports voice, data and video signal transport over a single circuit. The IAD distributes these signals to telephones (voice) and LANs (data and video).
- **Announcement Server Interface**—An announcement server is a media server that stores network-based announcements, and plays them to a caller upon a request from the CA. The announcement server interfaces with the Cisco BTS 10200 Softswitch using MGCP protocol.
- **Record Keeping Server Interface**—A record keeping server is
- **CALEA Server Interface**—to be determined
- **Feature Control Protocol Interface**—Cisco developed the Feature Control Protocol (FCP) as a Multipurpose Internet Mail Extension (MIME) application on top of the Session Initiation Protocol (SIP). FCP uses SIP for transport, and is the external protocol between the feature server and the call agent. It carries call state control and status information that is needed for external feature control, and provides an interface for both external and internal feature servers.

External feature servers are not supported in this release of the Cisco Broadband Local Integrated Services Solution.

- **Operations Support System Interfaces**—The Cisco BTS 10200 Softswitch OSS interface consists of the following parts:
  - Command Line Interface (CLI) over Telnet
  - Common Object Request Broker Architecture (CORBA)
  - SNMP traps, status, control and measurement
  - Billing interface (FTP)
  - Bulk provisioning (FTP)
- **Element Management System Interfaces**—The Element Management System (EMS) provides a flexible mechanism to transport information over any protocol to any external device. The EMS interface design takes into account that each carrier has its own unique set of Operations Support Systems (OSS). The EMS provides a decoupling layer between the external protocols used within the service provider's network and the internal protocols of the FS and CA. The Cisco BTS 10200 Softswitch system does not need to interpret the specific data formats used by the carrier's other network elements.

Local operators use a workstation or PC with a command line interface (CLI) to communicate with the EMS. Sessions can be either interactive or batch mode:

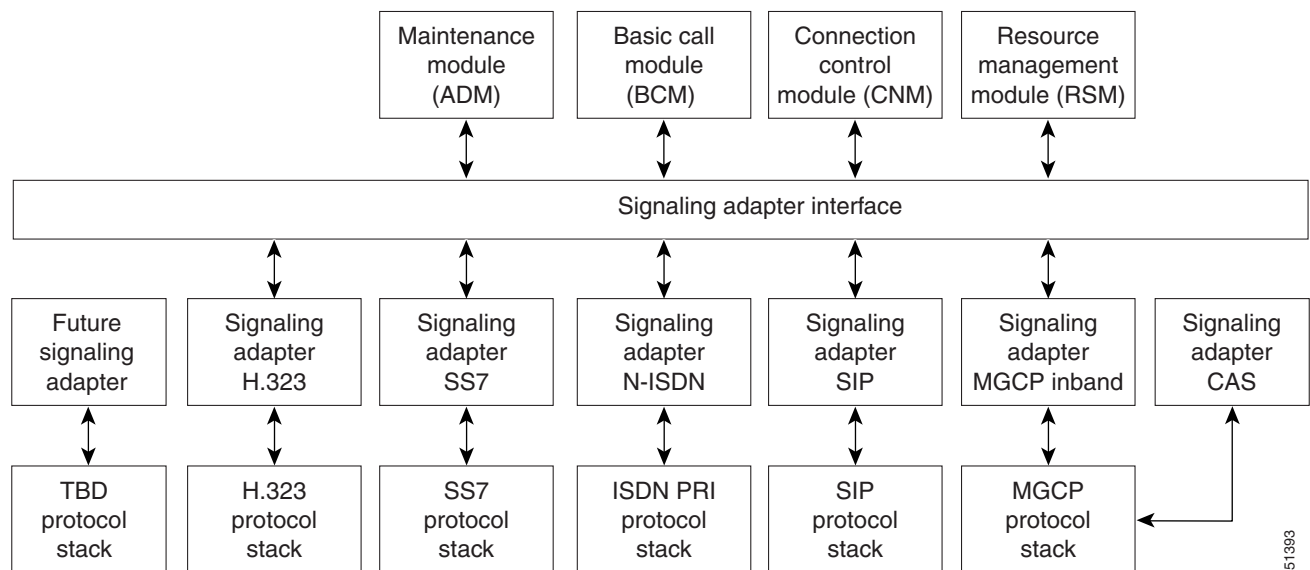
- Interactive—using Telnet
- Batch mode—using File Transfer Protocol (FTP)

- **Media Gateways Interface to the PSTN**—The Cisco BTS 10200 Softswitch provides both originating and terminating two-wire and four-wire continuity check (COT), a necessary feature within the PSTN for automatic monitoring of circuit quality. An IOS image that supports the control protocol is required for use in conjunction with the call agent software.
- **Signaling Interfaces**—The CA also provides monitoring and control of external NEs. It connects to multiple networks—using several types of signaling systems—via the Signaling Adapter Interfaces (SAI) as illustrated in Figure 10-1. The SAI converts incoming and outgoing signaling to and from the standard internal format of the CA. This interface allows the CA to connect to multiple networks and exchange signaling messages to set up, tear down and transfer calls.

The types of external signaling supported are:

- SS7
- SIP
- MGCP
- CAS
- ISDN

Figure 10-1 Signaling Adapter Architecture



The signaling adapters provide:

- uniform primitives (indications) for all interactions between different signaling protocols and the CA modules
- uniform data structures containing common information elements from different signaling protocols
- call control primitives for exchanging call signaling messages between the CA and the signaling network
- maintenance primitives for signaling link hardware maintenance and signaling protocol provisioning

# Components

This section describes the Cisco BTS 10200 Softswitch components:

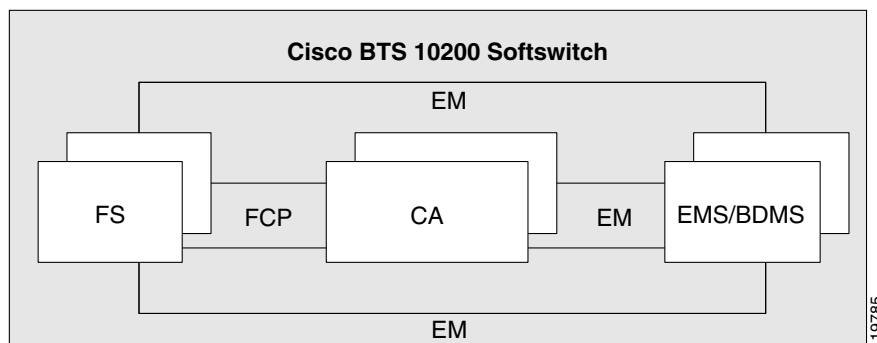
- [Rack Configuration, page 10-6](#)
- [Feature Server Architecture, page 10-8](#)
- [EMS Architecture, page 10-8](#)
- [Continuous Computing AXi, page 10-9](#)
- [Reference Documentation, page 10-9](#)

The Cisco Broadband Local Integrated Services Solution uses the Cisco BTS 10200 Softswitch, [Figure 10-2](#), as a call agent (CA). Call agent hosts used in this version of the solution are Continuous Computing Based Systems and a Sun A1000 disk array. Each call agent host supports a minimum of 49K DS0 channels with a throughput of 100 DS0 calls (POTS) per second (setup and tear-down), with an average hold time of three minutes. It provides at least 99.999 percent availability.

The call agent application is active on only one call agent host platform at a time, and switches to the standby call agent host platform under failure conditions. The result is that call agent host failure and switchover events are invisible at the signaling point.

The call agent includes a scalable, open host that provides SS7 interfaces, alarms, and a reliable IP link between the call agent and media gateways. The following sections provide detailed call agent specifications for the Continuous Computing-based systems and Sun disk array.

**Figure 10-2 Cisco BTS 10200 Softswitch Components**



EM – Element management link

FCP – Feature control protocol

CA – Call agent

EMS/BDMS – Element management system/bulk data management system

The functions of these call agent components are identified in [Table 10-2](#).

**Table 10-2 Cisco BTS 10200 Softswitch Features and Call Types**

| Feature | Support for...                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| EMS     | Mediation device between an NMS <sup>1</sup> and one or more CAs. It also supports OAMP <sup>2</sup> functions, which include the following element management areas: <ul style="list-style-type: none"> <li>• Billing management</li> <li>• Traffic management</li> <li>• Fault management</li> <li>• Event management</li> <li>• Configuration management (status and control)</li> <li>• Security management</li> </ul> |
| CA      | Serves as a CMS <sup>3</sup> and MGC <sup>4</sup> . Handles the establishment, processing, and tear-down of telephony calls.                                                                                                                                                                                                                                                                                               |
| FS      | Provides POTS <sup>5</sup> , Centrex, Tandem, and AIN <sup>6</sup> network services to the calls controlled by the CAs and provides processing for service features such as call forwarding, call waiting, and local number portability.                                                                                                                                                                                   |

1. NMS = network management station.
2. OAMP = operation, administration, maintenance, and provisioning.
3. CMS = call management system.
4. MGC = media gateway controller.
5. POTS = plain old telephone service.
6. AIN = advanced intelligent network.

## Rack Configuration

The Cisco BTS 10200 Softswitch components include:

- CA, FS—Two application servers, each with four CPUs
- EMS—Two administration processors
- Disk Array—A redundant array of inexpensive disks (RAID) storage system with replicated 100 GB disk space. The disk array maintains a minimum of 48 hours of data in the areas of billing, traffic measurements, alarms, events, security logs, and activity logs.
- Two switch routers
- Cabinet, 92 inches (2340 mm) high x 24 inches (600 mm) wide x 36 inches (900 mm) deep, with 84 inches (2135 mm) minimum available vertical rack space (Zone 4 seismic-rated cabinet optional)

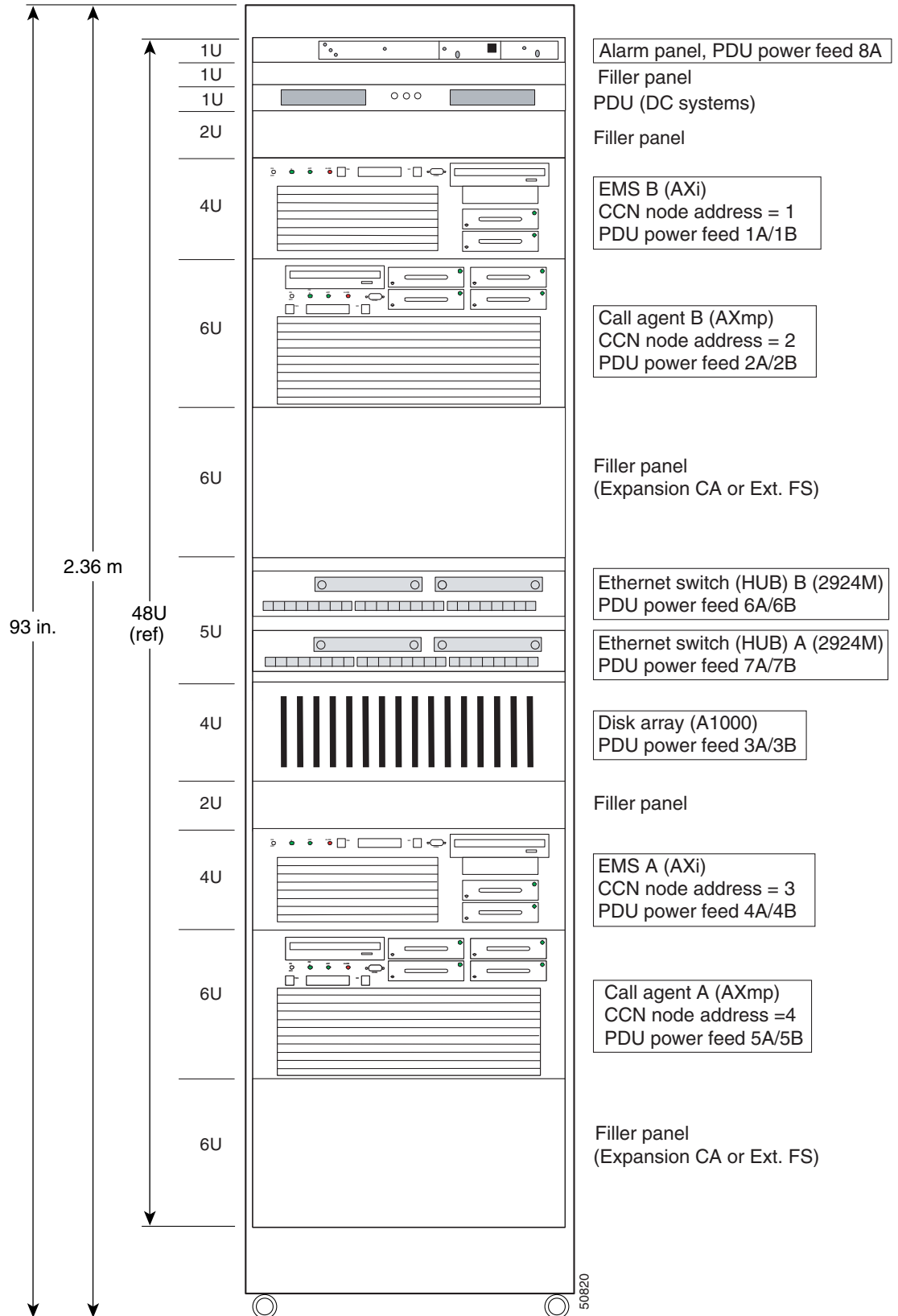
The complete Cisco BTS 10200 Softswitch system weighs approximately 800 lb (363 kg), including the cabinet and all equipment as shown in [Figure 10-3](#).

Each CA, FS application server has the following connectors:

- Two V.35 or two T1 connectors for SS7 connectivity
- Two Quad Ethernet connectors for links to two switch routers



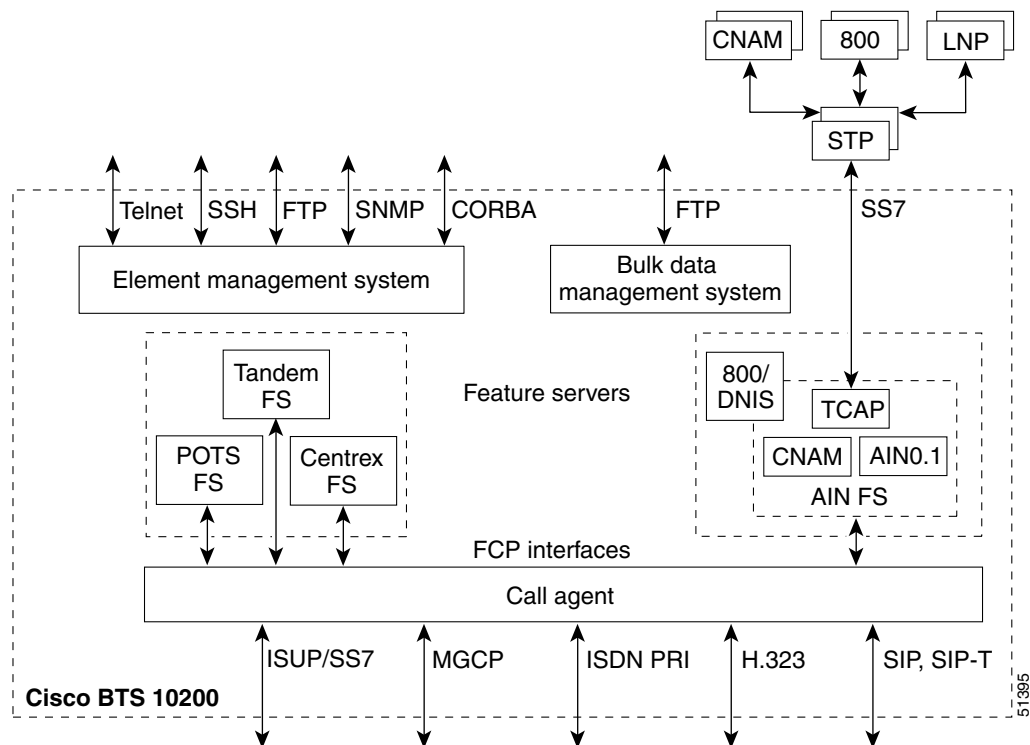
Figure 10-3 Typical Cisco BTS 10200 Softswitch Rack Configuration



## Feature Server Architecture

The purpose of the FS is to provide access to features through a well-defined interface. The Cisco BTS 10200 Softswitch architecture separates FS (which provides feature control) from CA (which provides call control) with a clear interface, Feature Control Protocol (FCP), defined between them. The independent architecture (FS separate from the CA) provides support for POTS, Centrex, AIN, 800 service, and other enhanced services from multiple FS. These FSs can be located internally, on the same machine as the CA, as shown in Figure 10-4. CA-to-FS communication is through FCP. Alternatively, the FS (for POTS, Centrex, and Tandem) can be located externally, on a separate machine from the CA. In this case, the CA communicates with both the internal and external FS through FCP.

Figure 10-4 Architecture with Internal Feature Servers



## EMS Architecture

The management functions of the EMS are partitioned along the guidelines described by the Telecommunications Management Network (TMN) standards. This facilitates future migration to these standards with minimal impact to the existing architecture. These areas include:

- Billing management
- Traffic management
- Fault management
- Event management
- Queuing and audit management
- Configuration management (status and control)
- Security management

## Cisco BTS 10200 Softswitch Controller Hosts

Each telephony controller host supports a minimum of 49K DS0 channels with a throughput of 100 DS0 calls (POTS) per second (setup and tear-down), with an average hold time of three minutes. It provides at least 99.9994 percent availability.

The call-processing application is active on only one telephony controller host platform at a time, and switches to the standby telephony controller host platform under failure conditions. The result is that telephony controller host failure and switchover events are invisible to the signaling point.

The telephony controller includes a scalable, open host that provides SS7 interfaces, alarms, and a reliable IP link between the telephony controller and media gateways.

## Continuous Computing AXmp

The Continuous Computing AXmp provides full functional redundancy and is designed to recover from any hardware failure within one second, with no data loss. In addition, the Continuous Computing AXmp meets and exceeds Network Equipment Building System (NEBS) Level 3 standards.

### Cards, Modules, and Connections

- Each Continuous Computing Server includes Fast Ethernet 100BASE-T network interface cards (NICs).
- Each Ethernet NIC is connected by 100BASE-T to an Ethernet switch, such as the Catalyst 6509.

## Continuous Computing AXi

The AXi is a general purpose Sun Ultra SPARC server. The AXi is rack-mountable and is NEBS and ETSI compliant.

## Reference Documentation

For each component of the call agent, refer to the documentation provided with the particular component. For information about the call agent, see the following publications:

- *Cisco BTS 10200 Softswitch (Continuous Computing-Based Systems) Cable Installation*
- *Cisco BTS 10200 Softswitch Command-Line Interface (CLI) Reference Guide*
- *Cisco BTS 10200 Softswitch Operations, Maintenance, and Troubleshooting (OMT) Guide*
- *Cisco BTS 10200 Softswitch Application Installation (Duplex Systems)*
- *Cisco BTS 10200 Softswitch System Description*

These publications are available online on the [Cisco website](#) or on the Cisco Documentation CD-ROM that shipped with your system.

# Troubleshooting

This section presents procedures for troubleshooting the Cisco BTS 10200 Softswitch. It includes the following subsections:

- [Verify Running Processes, page 10-10](#)
- [Verify Current Status, page 10-10](#)

## Verify Running Processes

Perform the following steps to open Unix shells on the primary and secondary EMS platforms and on the primary and secondary CA/FS platforms. These four shells can be used to determine the status of the primary and secondary CA/FS and EMS/BDMS.

You will need the network names and/or addresses of the systems, as well as the root password. These can be provided to you by the system administrator.

To determine the processes running on the Cisco BTS 10200 Sofswitch, complete the following steps:

- 
- Step 1** Ensure that your workstation has connectivity via TCP/IP to communicate with the primary EMS unit.
- Step 2** Open four separate Unix shells or XTerm windows. Each window will be dedicated to one of the four units: primary EMS/BDMS, secondary EMS/BDMS, primary CA/FS, and secondary CA/FS.
- Step 3** Enter `ssh` and the IP address or domain name of the applicable unit at the prompt in each of the four shells. This will be the unit to which this shell is dedicated.
- ```
ssh -l <CLI user name> <ip address>
```
- Each unit in the system responds with its login prompt.
- Step 4** Enter the user name `root` at the login prompt in each of the four shells.
- ```
root
```
- Step 5** Enter the root password for the applicable unit at the password prompt in each of the four shells. Each unit in the system responds with a command prompt.
- Step 6** Enter the UNIX command `ps -aef` at each command prompt to show all processes on each component.
- All processes should be in the "running" state. A list of all the BTS 10200 process is contained in the `platform.cfg` file located at `/opt/OptiCall/CA $nnn$ /bin/platform.cfg` (where "CA  $nnn$ " is your Call Agent).
- 

## Verify Current Status

The Cisco BTS 10200 Softswitch can employ any (or all) of the following signaling protocols:

- SS7—ISUP and TCAP
- SIP—SIP and SIP-T
- MGCP—gateway control
- CAS—DTMF/MF, PBX, 911, PSAP, OSPS
- ISDN—PRI, NI2, and other variants

The call processing logic in the Cisco BTS 10200 Softswitch is based on the IN Capability Set 2 (CS2) half call model. The interface between the basic call module (BCM), which provides the core call processing logic, and the signaling interface adapters (SIA) is protocol independent.

To verify the current status of the Cisco BTS 10200 Softswitch you can enter commands using the command line interface (CLI). Logging into a CLI session is a Secure Shell (SSH) function, not a UNIX function. You must use SSH to connect to the EMS using your user name and password, which invokes a CLI shell. After you log in only the CLI command prompt appears on the screen. To enter commands using the CLI, enter the command with all its required parameters (tokens) and any optional parameters you wish.

To log in from the client-side, perform the following steps:

---

**Step 1** Enter `ssh -l username IPaddress`

On the first SSH login from the client-side, expect a message similar to this:

```
The authenticity of host [hostname] can't be established.
Key fingerprint is 1024 5f:a0:0b:65:d3:82:df:ab:42:62:6d:98:9c:fe:e9:52.
Are you sure you want to continue connecting (yes/no)?
```

**Step 2** Enter “y” or “yes.”

The password prompt appears. From this point on, all communications are encrypted. Subsequent SSH logins will prompt only for a password.

---

## Verify Alarm Status

To verify the current alarm status of the Cisco BTS 10200 Softswitch, perform the following steps:

---

**Step 1** Start a CLI session by using a valid login id.

**Step 2** Enter the command `CLI> rtrv-arms::CONT`

This command retrieves the alarm status of the system. Look for alarms with "FAIL", "UNAVAIL" and "OOS" descriptions.

For example, "`nlink525a:npath525,LID=0:OOS`" is a major alarm stating that an NAS IP path has failed.

Look for a recommended action under the alarms section of the Cisco BTS 10200 Operations Guide.

---

## Verify Media Gateways

This section describes diagnostic tests that can be performed on media gateways. Media gateways must be in the MAINT state for testing.

To verify the current status of the media gateways, perform the following steps:

---

**Step 1** Use the following `control` command to force a media gateway into the MAINT state for testing:

```
control mgw id=c2421.65; mode=forced; target-state=maint;
```

- Step 2** To display the media gateway test menu and perform specific tests, enter the command `diag mgw`. You should receive a response similar to the following example:

```
Reply: Diagnostic MGW Menu
(1) MGW Network Connectivity Test
(2) MGW MGCP Connectivity Test
(3) ALL
```

Test 1 verifies that there is a path to the device by pinging it, test 2 verifies that the device has MGCP connectivity, and test 3 performs both tests 1 and 2.

- Step 3** To perform test 1 on media gateway **ubr-03** enter the command `diag mgw id=ubr-03; test=1;` You should receive a response similar to the following example:

```
MEDIA GATEWAY LINE DIAGNOSTIC TEST EXECUTED -> diag mgw
ID -> ubr-03
TEST-TYPE -> ADM-MGW-NETW-CONNECTIVITY-TEST
TEST-DURATION -> 0
RESULT -> TEST-SUCCESS
REASON -> PASSED
Reply: Diagnostic command executed.
```

- Step 4** To perform test 2 on media gateway **ubr-03** enter the command `diag mgw id=ubr-03; test=2;` You should receive a response similar to the following example:

```
MEDIA GATEWAY LINE DIAGNOSTIC TEST EXECUTED -> diag mgw
ID -> ubr-03
TEST-TYPE -> ADM-MGW-MGCP-CONNECTIVITY-TEST
TEST-DURATION -> 0
RESULT -> TEST-SUCCESS
REASON -> PASSED
Reply: Diagnostic command executed.
```

- Step 5** To perform both test 1 and test 2 on media gateway **ubr-03** enter the command `diag mgw id=ubr-03; test=3;`

You should receive a response similar to the following example:

```
MEDIA GATEWAY LINE DIAGNOSTIC TEST EXECUTED -> diag mgw
ID -> ubr-03
TEST-TYPE -> ADM-MGW-NETW-CONNECTIVITY-TEST
TEST-DURATION -> 11
RESULT -> TEST-SUCCESS
REASON -> PASSED
MEDIA GATEWAY LINE DIAGNOSTIC TEST EXECUTED -> diag mgw
ID -> ubr-03
TEST-TYPE -> ADM-MGW-MGCP-CONNECTIVITY-TEST
TEST-DURATION -> 0
RESULT -> TEST-SUCCESS
REASON -> PASSED
Reply: Diagnostic command executed.
```

## Verify Trunk Terminations

This section describes diagnostic tests that can be performed on trunk terminations. All trunk groups and trunk terminations must be in the MAINT state for testing.

To verify the current status of Cisco BTS 10200 Softswitch trunks and trunk groups, perform the appropriate procedure(s) in the following sections.

## SS7-controlled Trunk Groups

When an SS7-controlled trunk group's administrative state is set to out-of-service (OOS), the trunk group cannot be used for outgoing calls; however, incoming calls on that trunk group are still honored.

- Trunk states are not changed.
- The operational state of that trunk group is not changed or affected.

If incoming and outgoing calls need to be blocked, then all trunks in that trunk group should be set OOS.

When the trunk group admin state is set to in service (INS), both incoming and outgoing calls can be made and no trunk states are changed or affected.



### Note

Set COT, CVM, and CQM on the terminating gateway or switch to perform these tests. Otherwise, the test (or tests) will fail.

To verify that all SS7 signaling links are in service, perform the following steps:

- Step 1** Use the following **control** command to force an SS7-controlled trunk termination into the MAINT state for testing:

```
control ss7-trunk-termination tgn-id=103; cic=13; mode=forced;
target-state=maint;
```

- Step 2** Enter the command **CLI> diag ss7-trunk-termination**.

The following menu should be displayed:

```
Reply: Diagnostic SS7 Trunk Group Menu.
(1) SS7 MGCP Connectivity Test
(2) SS7 Termination Connection Test
(3) SS7 COT Test
(4) SS7 CQM Test
(5) SS7 CVT Test
(6) ALL
```

- Test 1 tests if MGCP has access to the SS7 trunk termination.
- Test 2 tests if there is a path to the device (ping).
- Test 3 tests the integrity of the SS7 Bearer Path.
- Test 4 queries the SS7 circuit (or group of circuits) status. A range of CICs can be specified (to a maximum of twenty four). Both remote and local trunk states are displayed in the results.
- Test 5 tests to ensure that each end of the circuit has sufficient and consistent information for using the circuit in call connections. CLLI names are included.
- Test 6 performs tests 1 through 5.

- Step 3** Select the test(s) you wish to run, the signaling trunk group id, the cic, and enter a command similar to the following:

```
diag ss7-trunk-termination tgn-id=103; cic=13; test=1;
```

You should receive a response similar to the following:

```
TRUNK DIAGNOSTIC TEST EXECUTED -> diag trunk
TG-NUM -> 103
CIC -> 13
TEST-TYPE -> ADM-MGW-MGCP-CONNECTIVITY-TEST
```

```
TEST-DURATION -> 0
RESULT -> TEST-SUCCESS
REASON -> PASSED: Reason: AUEP-NACK received with RespCode = 510
Reply: Diagnostic command executed.
```

- Step 4** Run any additional tests that might be needed to determine that all SS7 signaling links are reachable and in service.
- 

## ISDN-controlled Trunk Groups

When an ISDN-controlled trunk group's administrative state is set to out-of-service (OOS), D channels corresponding to the trunk group are disconnected.

- Operational state of all trunks in the trunk group are set to locally blocked, which overwrites any other states of trunks in that trunk group prior to the trunk group going out-of-service
- The trunk group cannot be used for outgoing calls and incoming calls cannot be received because the D channel is down.

When an ISDN-controlled trunk group is set to in-service (INS), all trunks in the trunk group are brought in-service and both incoming and outgoing calls are allowed.

The original state of some of the trunks prior to the trunk group going out-of-service might not be recovered when the trunk group goes back in-service and might have to be restored manually.

To verify that all ISDN-controlled trunk terminations are in service, perform the following steps:

---

- Step 1** Use the following **control** command to force an ISDN-controlled trunk termination into the MAINT state for testing:

```
control isdn-trunk-termination tgn-id=17; cic=1; mode=forced;
target-state=maint;
```

- Step 2** Enter the command **CLI> diag isdn-trunk-termination**.

The following menu should be displayed:

```
Reply: Diagnostic ISDN Trunk Group Menu.
(1) ISDN MGCP Connectivity Test
(2) ISDN Termination Connection Test
(3) ALL
```

Test 1 tests MGCP access to the ISDN-controlled trunk termination, test 2 determines if there is a path to the device by pinging it, and test 3 performs both tests 1 and 2.

- Step 3** To perform test 1 on ISDN trunk group 17, enter the following command:

```
diag isdn-trunk-termination test=1; tgn-id=17; cic=1;
```

You should receive a response similar to the following example:

```
TRUNK DIAGNOSTIC TEST EXECUTED -> diag trunk
TG-NUM -> 17
CIC -> 1
TEST-TYPE -> ADM-MGW-MGCP-CONNECTIVITY-TEST
TEST-DURATION -> 0
RESULT -> TEST-SUCCESS
REASON -> PASSED: Reason: AUEP-NACK received with RespCode = 510
Reply: Diagnostic command executed.
```

- Step 4** To perform test 2 on ISDN trunk group 17, enter the following command:

```
diag isdn-trunk-termination test=2; tgn-id=17; cic=1;
```



You should receive a response similar to the following example:

```
TRUNK DIAGNOSTIC TEST EXECUTED -> diag trunk
TG-NUM -> 17
CIC -> 1
TEST-TYPE -> ADM-TERM-CONNECTION-TEST
TEST-DURATION -> 0
RESULT -> TEST-SUCCESS
REASON -> PASSED: Reason: AUEP-NACK received with RespCode = 510
Reply: Diagnostic command executed.
```

**Step 5** To perform both test 1 and test 2 on ISDN trunk group 17, enter the following command:

```
diag isdn-trunk-termination test=3; tgn-id=17; cic=1;
```

You should receive a response similar to the following example:

```
TRUNK DIAGNOSTIC TEST EXECUTED -> diag trunk
TG-NUM -> 17
CIC -> 1
TEST-TYPE -> ADM-MGW-MGCP-CONNECTIVITY-TEST
TEST-DURATION -> 0
RESULT -> TEST-SUCCESS
REASON -> PASSED: Reason: AUEP-NACK received with RespCode = 510
TG-NUM -> 17
CIC -> 1
TEST-TYPE -> ADM-TERM-CONNECTION-TEST
TEST-DURATION -> 0
RESULT -> TEST-SUCCESS
REASON -> PASSED: Reason: AUEP-NACK received with RespCode = 510
Reply: Diagnostic command executed.
```

**Step 6** Run any additional tests that might be needed to determine that all ISDN-controlled trunk terminations and trunk groups are in service.

## CAS-controlled Trunk Groups

When a CAS-controlled trunk group's administrative state is set to out-of-service (OOS), the trunk group cannot be used for outgoing calls; however, incoming calls on that trunk group are honored.

- Trunk states are not changed and the operational state of the trunk group is not changed or affected.
- If both incoming and outgoing calls are to be blocked, all trunks in a trunk group should be set OOS.

When a CAS-controlled trunk group's administrative state is set to in-service (INS), both incoming and outgoing calls can be made and no trunk states are changed or affected.

To verify that all CAS-controlled trunk terminations are in service, perform the following steps:

**Step 1** Use the following **control** command to force a CAS-controlled trunk termination into the MAINT state for testing:

```
control cas-trunk-termination tgn-id=64; cic=1; mode=forced;
target-state=maint;
```

**Step 2** Enter the command **CLI> diag cas-trunk-termination**.

The following menu should be displayed:

```
Reply: Diagnostic CAS Trunk Group Menu.
(1) CAS MGCP Connectivity Test
(2) CAS Termination Connection Test
(3) ALL
```

Test 1 tests MGCP access to the CAS-controlled trunk termination, test 2 determines if there is a path to the device by pinging it, and test 3 performs both tests 1 and 2.

**Step 3** To perform test 1 on CAS trunk group 64, enter the following command:

```
diag cas-trunk-termination test=1; tgn-id=64; cic=1;
```

You should receive a response similar to the following:

```
Reply: Diagnostic CAS Trunk Group Menu.
(1) CAS MGCP Connectivity Test
(2) CAS Termination Connection Test
(3) ALL
```

Test 1 tests MGCP access to the CAS-controlled trunk termination, test 2 determines if there is a path to the device by pinging it, and test 3 performs both tests 1 and 2.

**Step 4** To perform test 1 on CAS trunk group 64, enter the following command:

```
diag cas-trunk-termination test=1; tgn-id=64; cic=1;
```

You should receive a response similar to the following example:

```
TRUNK DIAGNOSTIC TEST EXECUTED -> diag trunk
TG-NUM -> 64
CIC -> 1
TEST-TYPE -> ADM-MGW-MGCP-CONNECTIVITY-TEST
TEST-DURATION -> 0
RESULT -> TEST-SUCCESS
REASON -> PASSED: Reason: AUPE-NACK received with RespCode = 510
Reply: Diagnostic command executed.
```

**Step 5** To perform test 2 on CAS trunk group 64, enter the following command:

```
diag cas-trunk-termination test=2; tgn-id=64; cic=1;
```

You should receive a response similar to the following example:

```
TRUNK DIAGNOSTIC TEST EXECUTED -> diag trunk
TG-NUM -> 64
CIC -> 1
TEST-TYPE -> ADM-TERM-CONNECTION-TEST
TEST-DURATION -> 32
RESULT -> TEST-SUCCESS
REASON -> PASS successfully.
Reply: Diagnostic command executed.
```

**Step 6** To perform test 3 on CAS trunk group 64, enter the following command:

```
diag cas-trunk-termination test=3; tgn-id=64; cic=1;
```

You should receive a response similar to the following example:

```
TRUNK DIAGNOSTIC TEST EXECUTED -> diag trunk
TG-NUM -> 64
CIC -> 1
TEST-TYPE -> ADM-MGW-MGCP-CONNECTIVITY-TEST
TEST-DURATION -> 11
RESULT -> TEST-SUCCESS
REASON -> PASSED: Reason: AUPE-NACK received with RespCode = 510

TRUNK DIAGNOSTIC TEST EXECUTED -> diag trunk
TG-NUM -> 64
CIC -> 1
TEST-TYPE -> ADM-TERM-CONNECTION-TEST
TEST-DURATION -> 32
RESULT -> TEST-SUCCESS
REASON -> PASS successfully.
Reply: Diagnostic command executed.
```

### SIP-controlled Trunk Groups

When a SIP-controlled trunk group's administrative state is set to out-of-service (OOS), the trunk group cannot be used for outgoing calls and incoming calls on that trunk group are rejected.

SIP-controlled trunk groups do not have physical resources; therefore, no mechanism can be used to indicate to the remote switch the non-availability of the trunk group. The operational state of the trunk group is set to "not used."

When a SIP-controlled trunk group's administrative state is set to in-service (INS), all trunks in the trunk group are brought in-service and both incoming and outgoing calls are allowed.

### H323-controlled Trunk Groups

When an H323-controlled trunk group's administrative state is set to out-of-service (OOS), the trunk group cannot be used for outgoing calls; however, incoming calls on that trunk group are still allowed.

H323-controlled trunk groups do not have physical resources; therefore, the media gateway's administrative state is not affected when the trunk group is set to OOS.

H323-controlled trunk groups contain media gateway ids. When a media gateway is set to OOS no incoming or outgoing calls are allowed through that gateway id because H3A unregisters that gateway id with the gatekeeper.

When an H323-controlled trunk group's administrative state is set to in-service (INS), both incoming and outgoing calls are allowed, if the media gateways corresponding to that trunk group are in-service.

## Cisco BTS 10200 Failure

The Cisco BTS 10200 hosts run in active-standby mode. The call-processing application is active on only one Cisco BTS 10200 platform at a time, and the application switches to the standby platform when a critical alarm occurs. The result is that Cisco BTS 10200 failure and switchover events are invisible to the signaling network.

Cisco BTS 10200 alarms are configured as minor, major, or critical. Critical alarms are generated whenever any significant failure occurs. Any critical alarm causes a switchover to occur. For example, if the call engine or EMS should fail, there is a disconnection from the process manager (procM) and a switchover to the standby system.

## Operating System Failure

An operating system (OS) or hardware failure in the active Cisco BTS 10200 can also cause a switchover to the standby Cisco BTS10200. The standby Cisco BTS 10200 detects the failure of the active Cisco BTS 10200 and instructs the system to initiate a switchover. The standby Cisco BTS 10200 then takes over all call-processing functions. The switchover is transparent to all the gateways.





## Element Management and MIBs

---

This chapter provides an overview of the performance monitoring features and useful SNMP MIB files related to the Cisco uBR7246vxr, Cisco GSR10012, and MTAs.

### Cisco uBR7246vxr MIBs

This section includes descriptions of the following useful SNMP MIBs for the uBR7246VXR:

- CISCO-CABLE-SPECTRUM-MIB.my
- CISCO-DOCS-EXT-MIB.my
- DOCS-CABLE-DEVICE-MIB.my
- DOCS-IF-MIB.my

Information on these and other SNMP MIBs is available at the following URL at Cisco Connection Online (CCO): <http://www.cisco.com/public/mibs/>

### CISCO-CABLE-SPECTRUM-MIB.my

This is the MIB Module for Cable Spectrum Management for MCNS compliant cable modem termination systems (CMTS).

Spectrum management is a software/hardware feature provided in the CMTS so that the CMTS may sense both downstream and upstream plant impairments, report them to a management entity, and automatically mitigate them where possible.

The CMTS directly senses upstream transmission errors. It may also indirectly monitor the condition of the plant by keeping a record of modem state changes. It is desirable to perform these functions without reducing throughput or latency and without creating additional packet overhead on the RF plant.

The purpose of cable Spectrum Management is to prevent long term service interruptions caused by upstream noise events in the cable plant. It is also used for fault management and trouble shooting the cable network. When modems are detected to go on-line and off-line by flap detectors, the cable operators can look at the flap list and spectrum tables to determine the possible causes.

### Flap List Group

CMTS maintains a list of polled MTAs. When a polled MTA triggers a flap detector the modem is considered intermittent and is added into the Flap List (ccsFlapObjects).

There are 3 flap detectors defined. The flap count (ccsFlapTotal) is increased when any one of the flap detectors is triggered.

(1) Registration Flap: A CM may fail the registration process due to not being able to get an IP address. When that happens the CMTS will receive the Initial Maintenance packet from the CM sooner than expected and the CM is considered a flapping modem. In addition to the flap count ccsFlapInsertionFails will be increased; thus these two counters may tend to track each other for unauthorized modems. Another causes of registration flap may be downstream loss of sync or upstream ranging failure.

(2) Station Maintenance Flap: When the CMTS receives a Miss followed by a Hit then the modem will be added into the Flap List and the flap count will be increased. If ratio of Miss/Hit is high, then an upstream impairment is indicated.

(3) Power Adjustment Flap: When the CM upstream transmit power is adjusted and the adjustment is greater than the threshold (ccsPowerAdjustThreshold), the modem is added into the Flap List. In addition to the flap count ccsFlapPowerAdjustCnt will be increased. Excessive power adjustment is an indication of poor or failing plant components. It may also indicate the exposure of plant components to the forces of wind, moisture, or temperature.

**Table 11-1 CISCO-CABLE-SPECTRUM-MIB.my Objects**

| Object                 | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ccsFlapListMaxSize     | The maximum number of modems that a flap list can support. This number controls the size of the flap list. For every MAC domain or downstream, the maximum number of MTAs that can be supported is 8191. The user may want to increase or decrease the Flap List size according to the number of downstreams and the number of modem line cards in the CMTS.<br><br>When the number of modems exceeds the max flap list size, the additional modems are ignored. The flap detector is an information filter to avoid inundating a management agent with data which is less meaningful as a function of size. |
| ccsFlapListCurrentSize | The current number of modems in the flap list. Its value will be less than or equal to ccsFlapListMaxSize.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| ccsFlapAging           | The flap entry aging threshold. Periodically, the aging process scans through the flap list and removes the MTAs that have not flapped for that many minutes.                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| ccsFlapInsertionTime   | The insertion-time is an empirically derived, worst-case number of seconds which the requires to complete registration. The time taken by MTAs to complete their registration is measured by the cable operators and this information helps to determine the insertion time. If the MTA has not completed the registration stage within this insertion-time setting, the MTA will be inserted into the flap-list.                                                                                                                                                                                            |
| ccsFlapTable           | This table keeps the records of modem state changes. It can be used to identify the problematic MTAs. An entry can be deleted from the table but can not be added to the table.                                                                                                                                                                                                                                                                                                                                                                                                                              |
| ccsFlapEntry           | List of attributes for an entry in the ccsFlapTable. An entry in this table exists for each MTA that triggered one of our flap detectors.                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| ccsFlapMacAddr         | MAC address of the MTA's Cable interface. Identifies a flap-list entry for a flapping MTA.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

Table 11-1 CISCO-CABLE-SPECTRUM-MIB.my Objects (continued)

| Object                   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ccsFlapUpstreamIfIndex   | The ifIndex of the Cable upstream interface whose ifType is docsCableUpstream(129). The CMTS detects a flapping MTA from its Cable upstream interface.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| ccsFlapDownstreamIfIndex | The ifIndex of the Cable downstream interface whose ifType is docsCableDownstream(128).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| ccsFlapInsertionFails    | <p>The number of times a MTA registered more frequently than expected. Excessive registration is defined as the presence of a time span between two successive registration cycles which is less than a threshold span (ccsFlapInsertionTime).</p> <p>A MTA may fail the ranging or registration process due to not being able to get an IP address. When the MTA can not finish registration within the insertion time, it retries the process and sends the Initial Maintenance packet again. CMTS will receive the Initial Maintenance packet from the MTA sooner than expected and the MTA is considered a flapping modem.</p> <p>This count may indicate:</p> <ul style="list-style-type: none"> <li>• Intermittent downstream sync loss, or</li> <li>• DHCP or modem registration problems.</li> </ul> <p>The Flap Count (ccsFlapTotal) will be increased when this counter is increased.</p> <p>Discontinuities in the value of this counter can occur if this entry is removed from the table and then re-added, and are indicated by a change in the value of ccsFlapCreateTime.</p> |
| ccsFlapHits              | <p>The number of times the CMTS receives the Ranging request from the MTA.</p> <p>The CMTS issues a Station Maintenance transmit opportunity at a typical rate of once every 10 seconds and waits for a Ranging request from the MTA. If the CMTS receives a Ranging request then the Hit count will be increased by 1.</p> <p>If the FlapTotal count is high, both Hits and Misses counts are high, and other counters are relatively low then the flapping is probably caused by the modem going up and down. The Hits and Misses counts are keep-alive polling statistics. The Hits count should be much greater than the Misses count.</p> <p>Discontinuities in the value of this counter can occur if this entry is removed from the table and then re-added, and are indicated by a change in the value of ccsFlapCreateTime.</p>                                                                                                                                                                                                                                                      |

Table 11-1 CISCO-CABLE-SPECTRUM-MIB.my Objects (continued)

| Object           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ccsFlapMisses    | <p>The number of times the CMTS misses the Ranging request from the MTA.</p> <p>The CMTS issues a Station Maintenance packet every 10 seconds and waits for a Ranging request from the MTA. If the CMTS misses a Ranging request within 25 msec then the Misses count are increased.</p> <p>If ccsFlapTotal is high, Hits and Misses are high but ccsFlapPowerAdjustments and ccsFlapInsertionFails are low then the flapping is probably caused by the modem going up and down.</p> <p>Miss counts can indicate:</p> <ul style="list-style-type: none"> <li>• Intermittent upstream,</li> <li>• Laser clipping, or</li> <li>• Noise bursts.</li> </ul> <p>Laser clipping can happen if the signal power is too high when the upstream electrical signal is converted to an optical signal. When it happens the more input produces less output, until finally there is no more increase in output. This phenomena is called laser clipping.</p> <p>Discontinuities in the value of this counter can occur if this entry is removed from the table and then re-added, and are indicated by a change in the value of ccsFlapCreateTime.</p> |
| ccsFlapCrcErrors | <p>The number of times the CMTS upstream receiver flagged a packet with a CRC error.</p> <p>If ccsFlapCrcErrors is high, it indicates the cable upstream may have high noise level. The modem may not be flapping yet but it may be a potential problem.</p> <p>This count can indicate:</p> <ul style="list-style-type: none"> <li>• Intermittent upstream,</li> <li>• Laser clipping, or</li> <li>• Noise bursts.</li> </ul> <p>Laser clipping can happen if the signal power is too high when the upstream electrical signal is converted to an optical signal. When it happens the more input produces less output, until finally there is no more increase in output. This phenomena is called laser clipping.</p> <p>Discontinuities in the value of this counter can occur if this entry is removed from the table and then re-added, and are indicated by a change in the value of ccsFlapCreateTime.</p>                                                                                                                                                                                                                          |



Table 11-1 CISCO-CABLE-SPECTRUM-MIB.my Objects (continued)

| Object                  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ccsFlapPowerAdjustments | <p>The number of times the MTA upstream transmit power is adjusted during station maintenance. When the adjustment is greater than the power adjustment threshold the counter will be increased. The power adjustment threshold is chosen in an implementation- dependant manner.</p> <p>The Flap Count (ccsFlapTotal) will be increased when this counter is increased.</p> <p>If ccsFlapTotal is high, ccsFlapPowerAdjustments is high but the Hits and Misses are low and ccsFlapInsertionFails are low then the flapping is probably caused by an improper transmit power level setting at the modem end.</p> <p>This count can indicate:</p> <ul style="list-style-type: none"> <li>• Amplifier degradation,</li> <li>• Poor connections, or</li> <li>• Wind, moisture, or temperature sensitivity.</li> </ul> <p>Discontinuities in the value of this counter can occur if this entry is removed from the table and then re-added, and are indicated by a change in the value of ccsFlapCreateTime.</p> |
| ccsFlapTotal            | <p>Whenever the MTA passes flap detection, then the flap counter is increased.</p> <p>There are 3 flap detectors defined:</p> <p>(1) When ccsFlapInsertionFails is increased the Flap count will be increased.</p> <p>(2) When the CMTS receives a Miss followed by a Hit then the Flap count will be increased.</p> <p>(3) When ccsFlapPowerAdjustments is increased the Flap count will be increased.</p> <p>Discontinuities in the value of this counter can occur if this entry is removed from the table and then re-added, and are indicated by a change in the value of ccsFlapCreateTime.</p>                                                                                                                                                                                                                                                                                                                                                                                                         |
| ccsFlapLastFlapTime     | The flap time is set whenever the MTA triggers a flap detector.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

Table 11-1 CISCO-CABLE-SPECTRUM-MIB.my Objects (continued)

| Object            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ccsFlapCreateTime | The time that this entry was added to the table. If an entry is removed and then later re-added, there may be a discontinuity in the counters associated with this entry. This timestamp can be used to detect those discontinuities.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| ccsFlapRowStatus  | <p>Controls and reflects the status of rows in this table.</p> <p>When a MTA triggers a flap detector, if an entry does not already exist for this MTA, and ccsFlapListCurrentSize is less than ccsFlapListMaxSize, then an entry will be created in this table. Its instance of this object will be set to active(1). All flapping modems have the status of active(1).</p> <p>Active entries are removed from the table after they have not triggered any additional flap detectors for the period of time defined in csmFlapAging. Alternatively, setting this instance to destroy(6) will remove the entry immediately.</p> <p>To prevent an entry from being aged out, the entry should be set to notInService(2). The entry will remain in the table until this instance is set to active by CMTS (and ages out) or destroy. Upon the next trigger of a flap detector, the entry is reset to active. An entry in the notInService state can only be set, by the user, to destroy. A user is not allowed to change a notInService entry to active.</p> <p>createAndGo(4) and createAndWait(5) are not supported.</p> |

## CISCO-DOCS-EXT-MIB.my

This is the MIB module for the Cisco specific extension objects of Data Over Cable Service, Radio Frequency interface. There is a standard MIB for Data-Over-Cable Service Interface Specifications (DOCSIS) and in Cisco, it is called DOCS-IF-MIB. Besides the objects in DOCS-IF-MIB, this MIB module contains the extension objects to manage the MTA Termination Systems (CMTS).

This MIB module includes objects for the scheduler that supports Quality of Service (QoS) of MCNS/DOCSIS compliant Radio Frequency (RF) interfaces in cable modem termination systems (CMTS). The purpose is to let users configure attributes of the schedulers in order to ensure the Quality of Service and fairness for modem requests according to users' business needs. This MIB also provides the following:

- objects for various states of the schedulers, allowing you to monitor the schedulers' current status.
- connection status objects for MTAs and Customer Premise Equipment (CPE), to allow you to easily get the connection status and manage access group information about MTAs and CPE.
- objects for upstream configuration for automated spectrum management in order to mitigate upstream impairment.
- objects to keep count of the total # of modems, # of registered and # of active modems on the MAC interface as well as each upstream.

## Scheduler QoS Control Group

To ensure Quality of Service and fairness, the scheduler needs to control the traffic. This group includes attributes that user can configure how the scheduler controls the traffic and attributes showing the current status of the scheduler admission and rate control.

For each Service ID, there is one Quality of Service profile associated with it. The QoS profile limits the request (upstream)/packet (downstream) size for the Service ID and also defines the minimum guaranteed upstream bandwidth. Each modem's request associated with a Service ID needs to follow the Quality of Service profile constraints.

- Quality of Service control upstream table (cdxQosCtrlUp)

Because upstream's bandwidth(BW) is limited, the upstream scheduler needs to control the registration according to the upstream's bandwidth (BW) capacity for new MTA asking to be supported in this upstream. This table contains the configurable objects that can enable or disable the controlling process of the scheduler and the state objects that shows the current status of the scheduler.

- Rate Limiting table (cdxQosIfRateLimit)

After a MTA is registered, upstream and downstream schedulers will control the bandwidth request/packet size to ensure the Quality of Service and fairness by a rate limiting algorithm. This table contains attributes related to the rate limiting algorithms.

- Cmts Service Extension Table (cdxIfCmtsService)

This table extends the information about a Service ID in docsIfCmtsServiceTable.

For each Service ID, there is one Quality of Service profile associated with it and the profile limits the request/packet size for the Service ID. This table shows downstream traffic statistics and the various counts that the Service ID exceeds the limit in its Quality of Service profile.

## Scheduler QoS Queue Group

To ensure Quality of Service and fairness, the scheduler maintains a set of queues for different services and puts MTA requests/packets for that Sid in different queue according to the Quality of Service profile of the Sid. Each queue has a name and order within the queue set. The scheduler will serve the requests/packets in higher order queue before serving the requests/packets in lower order queue.

- Scheduler bandwidth request queues table (cdxBWQueue)

This table displays the attributes for these queues in a cable interface scheduler that supports Quality of Service.

## CMTS MTAs Customer Premises Equipment (CPE) Group

This group contains tables in CMTS for information about MTAs (cable modems) and Customer Premises Equipment (CPE) that connects to the MTA.

- Cable modem (CM) or Customer Premises Equipments (CPE) Table (cdxCmCpe)

This table contains information about MTAs.

- CMTS CM status extension table (cdxCmtsCmStatus)

This table extends the MTA status information in docsIfCmtsCmStatusTable.

- CMTS MAC extension Table (cdxCmtsCm)

This table extends the attributes for CMTS MAC interface. It includes attributes of the MTA notification enabling/disabling and the interval of MTA notification sent by the CMTS for a MTA that the Mac interface supports.

- CMTS cable modem channel override operation table (cdxCmtsCmChOver)

This table may be used to perform downstream/upstream load balancing or failure recovery. A CMTS operator can instruct a MTA to move to a new downstream or upstream channel or both.

There can be more than one entry for a MTA, so there is a time stamp for each entry to show the time when this operation is initiated.

Prior to creating an entry you should first generate a pseudo-random serial number to be used as the index to this sparse table; then create the associated instance of the row status object. Also—either in the same or in successive PDUs—create the associated instance of the command and parameter objects; and modify the default values for any of the parameter objects if the defaults are not appropriate.

Once the appropriate instances of all the command objects have been created, either by an explicit SNMP set request or by default, the row status should be set to active to initiate the operation.

Once an operation has been activated, it cannot be stopped. That is, it will run until either the CMTS has generated downstream frequency and/or upstream channel override fields in the RNG-RSP message sent to a MTA or time out. In either case, the operation is completed.

Once the operation is completed, the real result of the operation to the MTA cannot be known from this table. The result of the MTA's downstream frequency and the upstream channel id can be checked from other MIB tables. For example, use docsIfCmtsServiceTable from DOCS-IF-MIB to check whether the MTA's downstream frequency and upstream channel id are changed. Please note that even if the CMTS has generated downstream frequency and/or upstream channel override fields in the RNG-RSP message sent to a MTAs, if the MTA cannot lock the instructed downstream frequency or no upstream channel id could be used, it may reconnect back to the original downstream frequency and upstream channel id.

Once the operation completes, the management station should retrieve the values of the cdxCmtsCmChOverState objects of interest, and should then delete the entry. In order to prevent old entries from clogging the table, entries will be aged out, but an entry will never be deleted within 15 minutes of completing.

- CMTS cable modem table (cdxCmtsCm)

This table contains attributes or configurable parameters -- for MTAs from a CMTS.

A CMTS operator can use this table to report a MTA's attributes or configure a MTA by a MTA's MAC address.

## CMTS Upstream Group

Upstream impairment mitigation techniques are crucial to enhancing the communications reliability of two-way HFC cable plants. The hardware and software based capabilities built in to the CMTS assist in automatic noise mitigation.

This group contains tables in CMTS for configuring the upstream channel attributes for automated Spectrum Management.

In addition the group also has the count of MTAs on this upstream. Separate counts are used to represent the number of active, registered and total number MTAs on this upstream.

- CMTS Upstream Channel Table (cdxIfUpChannel)

This table contains the additional upstream channel attributes. The additional configurable objects for automated Spectrum Management are the modulation profile and channel width needed for the frequency hop algorithm used for noise mitigation.

Another upstream channel attribute is the number of MTAs. There are three objects to represent each of the following counts:

- Total: # of modems that were seen on this upstream since boot.
- Active: # of modems that are active (not online or reset).
- Registered: # of modems that are registered and online.

## Cisco DOCS Extension MIB Notifications

Table 11-2 CISCO-DOCS-EXT-MIB.my Objects

| Object                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| cdxQosCtrlUpAdmissionCtrl    | <p>The admission control status for minimum guaranteed upstream bandwidth scheduling service requests for this upstream.</p> <p>When this object is set to 'true', if there is a new modem with minimum guaranteed upstream bandwidth scheduling service in its QoS class requesting to be supported in this upstream, the upstream scheduler will check the virtual reserved bandwidth remaining capacity before giving admission to this new modem. If there is not enough reserved upstream bandwidth to serve the modem's minimum guaranteed bandwidth, the registration request will be rejected.</p> <p>This object is set to 'false' to disable admission control. That is, there will be no checking for bandwidth capacity and the upstream interface scheduler just admits modem registration requests.</p> <p>This object is not meant for Unsolicited Grant Service (UGS) scheduling service as admission control is a requirement in this case.</p> |
| cdxQosCtrlUpMaxRsvdBWPercent | <p>The percentage of upstream maximum reserved bandwidth to the raw bandwidth if the admission control is enabled on this upstream.</p> <p>For example, if the upstream interface has raw bandwidth 1,600,000 bits/second and cdxQosCtrlUpMaxRsvdBWPercent is 200 percent, then this upstream scheduler will set the maximum of virtual reserved bandwidth capacity to 3,200,000 bits/second (1,600,000 * 2) to serve MTAs with minimum guaranteed upstream bandwidth.</p> <p>The default value is 100 percent (that is, maximum reserved bandwidth is the raw bandwidth.) Whenever the admission control is changed (on to off, off to on), this value will be reset to the default value 100.</p> <p>If the admission control is disabled, the value will be reset to 100 (the default value).</p>                                                                                                                                                             |
| cdxQosCtrlUpAdmissionRejects | <p>The count of MTA registration requests rejected on this upstream interface due to insufficient reserved bandwidth for serving the MTAs with Unsolicited Grant Service (UGS) scheduling service when UGS is supported and for serving the MTAs with minimum guaranteed bandwidth in its Quality of Service class when admission control is enabled on this upstream interface.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

Table 11-2 CISCO-DOCS-EXT-MIB.my Objects (continued)

| Object                   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| cdxQosCtrlUpReservedBW   | The current total reserved bandwidth in bits per second of this upstream interface. It is the sum of all MTAs' minimum guaranteed bandwidth in bits per second currently supported on this upstream.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| cdxQosCtrlUpMaxVirtualBW | The maximum virtual bandwidth capacity of this upstream interface if the admission control is enabled. It is the raw bandwidth in bits per second times the percentage. If the admission control is disabled, then this object will contain the value zero.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| cdxQosIfRateLimitAlgm    | <p>To ensure fairness, the CMTS will throttle the rate for bandwidth request (upstream)/packet sent (downstream) at which CMTS issues grants (upstream) or allow packet to be send (downstream) such that the flow never gets more than its provisioned peak rate in bps.</p> <p>There are two directions for every Service Id (Sid) traffic: downstream and upstream. Each direction is called a service flow here and assigned one token bucket with chosen algorithm.</p> <p>The rate limiting algorithm are:</p> <p>noRateLimit(1): The rate limiting is disabled. No rate limiting.</p> <p>oneSecBurst(2): Bursty 1 second token bucket algorithm.</p> <p>carLike(3): Average token usage (CAR-like) algorithm.</p> <p>wtExPacketDiscard(4): Weighted excess packet discard algorithm.</p> <p>shaping(5): token bucket algorithm with shaping.</p> <p>Upstream supports the following:</p> <ul style="list-style-type: none"> <li>• No rate limiting (1)</li> <li>• Bursty 1 second token bucket algorithm(2)</li> <li>• Average token usage (CAR-like) algorithm(3)</li> <li>• Token bucket algorithm with shaping(5)-default for upstream.</li> </ul> <p>Downstream supports the following:</p> <ul style="list-style-type: none"> <li>• No rate limiting (1)</li> <li>• Bursty 1 second token bucket algorithm(2)-default for downstream</li> <li>• Average token usage (CAR-like) algorithm(3)</li> <li>• Weighted excess packet discard algorithm(4)</li> </ul> |

Table 11-2 CISCO-DOCS-EXT-MIB.my Objects (continued)

| Object                 | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| cdxQosIfRateLimitExpWt | <p>Weight for exponential moving average of loss rate for weighted excess packet discard algorithm to maintain. The higher value of the weight makes the algorithm more sensitive to the recent bandwidth usage by the Sid.</p> <p>The default value is 1 and whenever the rate limiting algorithm is changed to weighted excess packet discard algorithm, this value will be reset to the default 1.</p> <p>If the rate limiting algorithm is not weighted excess packet discard algorithm, the value is always the default value 1.</p> |



Table 11-2 CISCO-DOCS-EXT-MIB.my Objects (continued)

| Object                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| cdxQosIfRateLimitShpMaxDelay | <p>The maximum shaping delay in milliseconds. That is, the maximum amount time of buffering the CMTS will allow for any rate exceeded flow. If the max buffering delay is large, the grants/packets of the flow will be buffered for a longer period of time even though the flow is rate exceeded. This means fewer chances of drops for such rate exceeded flow. However, too large a max shaping delay can result in quick drainage of packet buffers at the CMTS, since several packets will be in the shaping (delay) queue waiting for their proper transmission time. Also note that delaying a flows packets (especially TCP flows) for extended periods of time is useless, since the higher protocol layers may assume a packet loss after a certain amount of time.</p> <p>The maximum shaping delay is only applied to rate limit algorithm: Token bucket algorithm with shaping. If the rate limit algorithm is not Token bucket algorithm with shaping, the value is always na(1) which is not applicable.</p> <p>If the token count is less than the size of request/packet, CMTS computes the shaping delay time after which the deficit number of tokens would be available. If the shaping delay time is greater than the maximum shaping delay, the request/packet will be dropped.</p> <p>The enumerations for maximum shaping delay are:</p> <ul style="list-style-type: none"> <li>• na(1): maximum shaping delay is not applied to the current rate limit algorithm</li> <li>• msec128(2): maximum shaping delay is 128 milliseconds</li> <li>• msec256(3): maximum shaping delay is 256 milliseconds</li> <li>• msec512(4): maximum shaping delay is 512 milliseconds</li> <li>• msec1024(5): maximum shaping delay is 1024 milliseconds</li> </ul> <p>The downstream maximum shaping delay is configurable and the default value is msec128(2). Whenever the downstream rate limit algorithm is changed to Token bucket algorithm with shaping from other rate limit algorithm, the value will be reset to the default value.</p> <p>The upstream maximum shaping delay is not configurable and it is read-only value.</p> |

Table 11-2 CISCO-DOCS-EXT-MIB.my Objects (continued)

| Object                          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| cdxQosIfRateLimitShpGranularity | <p>The width in milliseconds of each element in shaping delay queue, that is, the shaping granularity.</p> <p>The shaping granularity is only applied to rate limit algorithm: Token bucket algorithm with shaping. It controls how accurately the algorithm quantizes the shaping delay for a rate exceeded flow. If granularity is large, several shaping delay values will all be quantized to the same element in the queue resulting in less accurate rate shaping for the flows in bits/sec. On the other hand, choosing too small granularity causes more memory to be used for the shaper block, and also can cost a bit more in runtime overhead.</p> <p>If the rate limit algorithm is not Token bucket algorithm with shaping, the value is always na(1) which is not applicable.</p> <p>The enumerations for shaping granularity are:</p> <ul style="list-style-type: none"> <li>• na(1): shaping granularity is not applied to the current rate limit algorithm</li> <li>• msec1(2): shaping granularity in 1 milliseconds</li> <li>• msec2(3): shaping granularity in 2 milliseconds</li> <li>• msec4(4): shaping granularity in 4 milliseconds</li> <li>• msec8(5): shaping granularity in 8 milliseconds</li> <li>• msec16(6): shaping granularity in 16 milliseconds</li> </ul> <p>The downstream shaping granularity is configurable and the default value is msec4(4). Whenever the downstream rate limit algorithm is changed to Token bucket algorithm with shaping from other rate limit algorithm, the value will be reset to the default value.</p> <p>The upstream shaping granularity is not configurable and it is read-only value.</p> |
| cdxIfCmtsServiceOutOctets       | The cumulative number of Packet Data octets sent for this Service ID.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| cdxIfCmtsServiceOutPackets      | The cumulative number of Packet data packets sent for this Service ID.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

Table 11-2 CISCO-DOCS-EXT-MIB.my Objects (continued)

| Object                         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| cdxQosMaxUpBWExcessRequests    | <p>The number of upstream bandwidth requests which exceeds the maximum upstream bandwidth allowed for a service defined in the Quality of Service profile associated with this Sid. The request which exceeds the maximum upstream bandwidth allowed will be rejected by the upstream's rate limiting process using one of the rate limiting algorithm.</p> <p>Note that the value of this counter cannot be directly used to know the number of upstream packets that got dropped at the MTA. A single upstream packet drop of a modem can result in up to 16 increments in this counter, since the modem keeps retrying and keeps getting bandwidth request drops at CMTS if it has consumed its peak rate.</p> |
| cdxQosMaxDownBWExcessPackets   | <p>The number of downstream bandwidth packets which exceeds the maximum downstream bandwidth allowed for a service defined in the Quality of Service profile associated with this Sid. The packet which exceeds the maximum downstream bandwidth allowed will be dropped by the downstream's rate limiting process using one of the rate limiting algorithm.</p>                                                                                                                                                                                                                                                                                                                                                  |
| cdxBWQueueNameCode             | <p>The name code for the queue.</p> <ul style="list-style-type: none"> <li>• cirQ: Committed Information Rate (CIR) type of service</li> <li>• tbeQ: Tiered Best Effort (TBE) type of service</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| cdxBWQueueOrder                | <p>The relative order of this queue to the other queues within the cable interface. The smaller number has higher order. That is, 0 is the highest order and 10 is the lowest order. The scheduler will serve the requests in higher order queue up to the number of requests defined in cdxBWQueueNumServedBeforeYield before serving requests in the next higher order queue.</p> <p>If there are n queues on this interface, the queue order will be 0 to n-1 and maximum number of requests defined as cdxBWQueueNumServedBeforeYield in order 0 queue will be served before the requests in order 1 queue to be served.</p>                                                                                  |
| cdxBWQueueNumServedBeforeYield | <p>The maximum number of requests/packets the scheduler can serve before yielding to another queue. The value 0 means all requests must be served before yielding to another queue.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| cdxBWQueueType                 | <p>The queuing type which decides the position of a request/packet within the queue.</p> <p>unknown (1): queue type unknown.</p> <p>other (2): not fifo, and not priority.</p> <p>fifo (3): first in first out.</p> <p>priority (4): each bandwidth request has a priority and the position of the request within the queue depends on its priority.</p>                                                                                                                                                                                                                                                                                                                                                          |

**Table 11-2 CISCO-DOCS-EXT-MIB.my Objects (continued)**

| Object                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| cdxBWQueueMaxDepth    | The maximum number of requests/packets which the queue can support.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| cdxBWQueueDepth       | The current number of requests/packets in the queue.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| cdxBWQueueDiscards    | The number of requests/packets discarded because of queue overflow (queue depth > queue maximum depth).                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| cdxCmCpeMacAddress    | The Mac address to identify a MTA or a Customer Premises Equipment.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| cdxCmCpeType          | Indicate this entry is for MTA or Customer Premises Equipment. The enumerations are: <ul style="list-style-type: none"> <li>• cm(1): MTA (cable modem)</li> <li>• cpe(2): Customer Premises Equipment</li> </ul>                                                                                                                                                                                                                                                                                                                                                    |
| cdxCmCpeIpAddress     | IP address of the MTA .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| cdxCmCpeCmtsServiceId | The MTA's primary Service ID if the type is cm. The primary Service ID for the CM which the CPE connects if the type is cpe.                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| cdxCmCpeCmStatusIndex | Pointer to an entry in docsIfCmtsCmStatusTable identifying status of the CM (which the CPE connects to).                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| cdxCmCpeAccessGroup   | ASCII text to identify the Access Group for a CM or CPE. Access Group is to filter the upstream traffic for that CM or CPE.                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| cdxCmCpeResetNow      | Setting this object to true(1) causes the device to reset. Reading this object always returns false(2).<br><br>For cdxCmCpeType value cm(1), CMTS removes the CM from the Station Maintenance List and would cause the CM to reset its interface.<br><br>For cdxCmCpeType value cpe(2), CMTS removes the CPE's MAC address from the internal address table. It then rediscovers and associates the CPE with the correct CM during the next DHCP lease cycle. By resetting the CPE, the user can replace an existing CPE or change its network interface card (NIC). |

Table 11-2 CISCO-DOCS-EXT-MIB.my Objects (continued)

| Object               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| cdxCmtsCmStatusValue | <p>Current MTA connectivity state. The object extends states in docsIfCmtsCmStatusValue in more details.</p> <p>The enumerations are:</p> <p>offline(1): modem considered offline.</p> <p>others(2): states is in docsIfCmtsCmStatusValue.</p> <p>initRangingRcvd(3): modem sent initial ranging.</p> <p>initDhcpReqRcvd(4): dhcp request received.</p> <p>onlineNetAccessDisabled(5): modem registered, but network access for the CM is disabled.</p> <p>onlineKekAssigned(6): modem registered, BPI enabled and KEK assigned.</p> <p>onlineTekAssigned(7): modem registered, BPI enabled and TEK assigned.</p> <p>rejectBadMic(8): modem did attempt to register but registration was refused due to bad mic.</p> <p>rejectBadCos(9): modem did attempt to register but registration was refused due to bad COS.</p> <p>kekRejected(10): KEK modem key assignment rejected.</p> <p>tekRejected(11): TEK modem key assignment rejected.</p> <p>online(12): modem registered, enabled for data.</p> <p>initTftpPacketRcvd(13): tftp packet received and option file tranfer started.</p> <p>initTodRquestRcvd(14): Time of the Day (TOD) request received.</p> <p>The ranging, rangingAborted, rangingComplete, and ipComplete states in docsIfCmtsCmStatusValue is others in this object since this object is extension of docsIfCmtsCmStatusValue.</p> <p>The registrationComplete state in docsIfCmtsCmStatusValue could be online, onlineNetAccessDisabled, onlineKekAssigned, or onlineTekAssigned in this object.</p> <p>The accessDenied state in docsIfCmtsCmStatusValue could be rejectBadMic, rejectBadCos in this object for the possible reasons of MTA registration abort.</p> <p>The CMTS only reports states it is able to detect.</p> |

Table 11-2 CISCO-DOCS-EXT-MIB.my Objects (continued)

| Object                                                            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| cdxIfCmtsCmStatusOnlineTimes                                      | <p>The number of times that the modem changes the connectivity state from 'offline' to 'online' over the time period from the modem's first ranging message received by CMTS until now.</p> <p>The modem is considered as 'online' when the value for cdxCmtsCmStatusValue is any of these values:</p> <ul style="list-style-type: none"> <li>• online(5)</li> <li>• onlineNetAccessDisabled(6)</li> <li>• onlineKekAssigned(7)</li> <li>• onlineTekAssigned(8)</li> </ul> <p>The modem is considered as 'offline' for other values for cdxCmtsCmStatusValue.</p>                                                                                      |
| cdxIfCmtsCmStatusPercentOnline                                    | <p>The percentage of time that the modem stays 'online' over the time period from the modem's first ranging message received by CMTS until now.</p> <p>The value for this object is 100 times bigger than the real percentage value. For example, 32.15% will be value 3215.</p> <p>The modem is considered as 'online' when the value for cdxCmtsCmStatusValue is any of these values:</p> <ul style="list-style-type: none"> <li>• online(5)</li> <li>• onlineNetAccessDisabled(6)</li> <li>• onlineKekAssigned(7)</li> <li>• onlineTekAssigned(8)</li> </ul> <p>The modem is considered as 'offline' for other values for cdxCmtsCmStatusValue.</p> |
| cdxIfCmtsCmStatusMinOnlineTime<br>cdxIfCmtsCmStatusMinOfflineTime | <p>The minimum period of time the modem stayed 'online' ['offline'] over the time period from the modem's first ranging message received by CMTS until now.</p> <p>The modem is considered as 'online' when the value for cdxCmtsCmStatusValue is any of these values:</p> <ul style="list-style-type: none"> <li>• online(5)</li> <li>• onlineNetAccessDisabled(6)</li> <li>• onlineKekAssigned(7)</li> <li>• onlineTekAssigned(8)</li> </ul> <p>The modem is considered as 'offline' for other values for cdxCmtsCmStatusValue.</p>                                                                                                                  |

Table 11-2 CISCO-DOCS-EXT-MIB.my Objects (continued)

| Object                                                        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| cdxCmtsCmStatusAvgOnlineTime<br>cdxCmtsCmStatusAvgOfflineTime | <p>The average period of time the modem stayed 'online' ['offline'] over the time period from the modem's first ranging message received by CMTS until now.</p> <p>The modem is considered as 'online' when the value for cdxCmtsCmStatusValue is any of these values:</p> <ul style="list-style-type: none"> <li>• online(5)</li> <li>• onlineNetAccessDisabled(6)</li> <li>• onlineKekAssigned(7)</li> <li>• onlineTekAssigned(8)</li> </ul> <p>The modem is considered as 'offline' for other values for cdxCmtsCmStatusValue.</p> |
| cdxCmtsCmStatusMaxOnlineTime<br>cdxCmtsCmStatusMaxOfflineTime | <p>The maximum period of time the modem stayed 'online' ['offline'] over the time period from the modem's first ranging message received by CMTS until now.</p> <p>The modem is considered as 'online' when the value for cdxCmtsCmStatusValue is any of these values:</p> <ul style="list-style-type: none"> <li>• online(5)</li> <li>• onlineNetAccessDisabled(6)</li> <li>• onlineKekAssigned(7)</li> <li>• onlineTekAssigned(8)</li> </ul> <p>The modem is considered as 'offline' for other values for cdxCmtsCmStatusValue.</p> |
| cdxCmtsCmStatusDynSidCount                                    | The number of active dynamic SIDs on this modem.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| cdxCmtsCmOnOffTrapEnable                                      | An indication of whether the cdxCmtsCmOnOffNotification is enabled. The default value is false(2).                                                                                                                                                                                                                                                                                                                                                                                                                                    |

Table 11-2 CISCO-DOCS-EXT-MIB.my Objects (continued)

| Object                     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| cdxCmtsCmOnOffTrapInterval | <p>The interval for cdxCmtsCmOnOffNotification sent by CMTS for one online/offline state change if cdxCmtsCmOnOffTrapEnable is true.</p> <p>If there are more than one state changes to online/offline for a MTA during this interval, only one cdxCmtsCmOnOffNotification is sent by CMTS for the first state change to online and one cdxCmtsCmOnOffNotification for the first state changing to offline if cdxCmtsCmOnOffTrapEnable is true.</p> <p>This is to avoid too many notifications sent for a MTA online/offline state changes during a short period of time.</p> <p>If the value is 0, then cdxCmtsCmOnOffNotification will be sent for every state changes to online/offline for a MTA if cdxCmtsCmOnOffTrapEnable is true.</p> <p>If cdxCmtsCmOnOffTrapEnable value changes from true to false or from false to true, this value will remain no change as before.</p> <p>The default value is 600 seconds.</p> |
| cdxCmtsCmDefaultMaxCpes    | <p>The default maximum number of permitted CPEs per modem in this cable interface. A modem can override this value by setting the object cdxCmtsCmMaxCpeNumber in the cdxCmtsCmTable.</p> <p>The value 0 means no maximum limit.</p> <p>Setting the value will not affect the already connected CPEs to the modems in this cable interface.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| cdxCmtsCmTotal             | The total count of MTAs on this cable mac interface since boot.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| cdxCmtsCmActive            | The count of MTAs that are active. Active MTAs are recognized by the cdxCmtsCmStatusValue other than offline(1).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| cdxCmtsCmRegistered        | <p>The count of MTAs that are registered and online on this cable mac interface. Registered MTAs are those with one of the following values:</p> <p>registrationComplete(6) of docsIfCmtsCmStatusValue OR either of online(12), kekRejected(10), onlineKekAssigned(6), tekRejected(11), onlineTekAssigned(7) of cdxCmtsCmStatusValue</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |



Table 11-2 CISCO-DOCS-EXT-MIB.my Objects (continued)

| Object                           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| cdxCmtsCmChOverTimeExpiration    | <p>The time period to expire a CMTS channel override operation. Within the time period, if the CMTS cannot send out a RNG-RSP message with channel override fields to a MTA specified in the operation, the CMTS will abort the operation. The possible reason is that the MTA does not repeat the initial ranging.</p> <p>The change to this object will not affect the already active operations in this cdxCmtsCmChOverTable.</p> <p>Once the operation completes, the management station should retrieve the values of the cdxCmtsCmChOverState object of interest, and should then delete the entry from cdxCmtsCmChOverTable. In order to prevent old entries from clogging the table, entries will be aged out, but an entry will never be deleted within 15 minutes of completing.</p> |
| cdxCmtsCmChOverSerialNumber      | Object which specifies a unique entry in the table. A management station wishing to initiate a channel override operation should use a pseudo-random value for this object when creating or modifying an instance of a cdxCmtsCmChOverEntry.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| cdxCmtsCmChOverMacAddress        | <p>The mac address of the MTA that the CMTS instructs to move to a new downstream and/or upstream channel.</p> <p>This column must be set to a valid Mac address currently in the CMTS in order for this entry's row status to be set to active successfully.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| cdxCmtsCmChOverDownFrequency     | The new downstream frequency which the MTA is instructed to move to. The value 0 is to ask the CMTS not to override the downstream frequency.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| cdxCmtsCmChOverUpChannelId       | The new channel Id which the MTA is instructed to move to. The value -1 is to ask the CMTS not to override the upstream channel Id.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| cdxCmtsCmChOverTrapOn Completion | Specifies whether or not a cdxCmtsCmChOverNotification should be issued on completion of the operation. If such a notification is desired, it is the responsibility of the management entity to ensure that the SNMP administrative model is configured in such a way as to allow the notification to be delivered.                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| cdxCmtsCmChOverOpInitiatedTime   | The value of sysUpTime at which the operation was initiated. Since it is possible to have more than one entry in this table for a MTA, this object can help to distinguish the entries for the same MTA.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

Table 11-2 CISCO-DOCS-EXT-MIB.my Objects (continued)

| Object                   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| cdxCmtsCmChOverState     | <p>The status of the specified channel override operation.</p> <p>The enumerations are:</p> <ul style="list-style-type: none"> <li>• messageSent(1): the CMTS has sent a RNG-RSP message with channel override to the MTA.</li> <li>• commandNotActive(2): the command is not in active mode due to this entry's row status is not in active yet.</li> <li>• noOpNeed(3): The downstream frequency and the upstream channel Id in this entry are the same as original ones when this entry's row status is set to active, so CMTS does not need to do any operation.</li> <li>• modemNotFound(4): The modem is not found in the CMTS at the time when the command becomes active.</li> <li>• waitToSendMessage(5): specified the operation is active and CMTS is waiting to send a RNG-RSP message with channel override to the MTA.</li> <li>• timeOut(6): specified the operation is timed out. That is, the CMTS cannot send a RNG-RSP message with channel override to the MTA within the time specified in the object of cdxCmtsCmChOverTimeExpiration. The possible reason is that the MTA does not repeat the initial ranging.</li> </ul> <p>The possible state change diagram is as below:<br/> [commandNotActive -&gt;] waitToSendMessage -&gt; messageSent or timeOut.<br/> [commandNotActive -&gt;] noOpNeeded or modemNotFound.</p> |
| cdxCmtsCmChOverRowStatus | <p>The status of this table entry.</p> <p>This value for cdxCmtsCmChOverMacAddress must be valid Mac address currently in the CMTS in order for the row status to be set to active successfully.</p> <p>Once the row status becomes active and state becomes waitToSendMessage, the entry cannot not be changed except to delete the entry by setting the row status to destroy(6) and since the operation cannot be stopped, the destroy(6) will just cause the SNMP agent to hide the entry from application and the SNMP agent will delete the entry right after the operation is completed.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

Table 11-2 CISCO-DOCS-EXT-MIB.my Objects (continued)

| Object                          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| cdxCmtsCmMaxCpeNumber           | <p>The maximum number of permitted CPEs connecting to the modem.</p> <p>The value -1 means to use the default value of maximum hosts per modem in the CMTS cable interface which the modem connects to and the value is defined in cdxCmtsCmDefaultMaxCpes in the cdxCmtsMacExtTable.</p> <p>The value 0 means no maximum limit.</p> <p>Setting the value will not affect the already connected CPEs to the modem.</p>                                                                                                                                                                                                                 |
| cdxCmtsCmCurrCpeNumber          | The current number of CPEs connecting to the modem. The value 0 means no hosts connecting to the modem.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| cdxIfUpChannelWidth             | <p>The lower bound for the bandwidth of this upstream channel. The bandwidth specified by docsIfUpChannelWidth is used as the upper bound of the upstream channel. The two objects, docsIfUpChannelWidth and cdxIfUpChannelWidth, in conjunction, define the upstream channel width range to be used for the automated spectrum management.</p> <p>This object returns 0 if the channel width is undefined or unknown.</p>                                                                                                                                                                                                             |
| cdxIfUpChannelModulationProfile | <p>The secondary modulation profile for the upstream channel. This should be a QPSK modulation profile if the primary profile is QAM-16. The CMTS will switch from primary profile (QAM16) to secondary profile (QPSK) depending on the noise level of a particular spectrum band.</p> <p>This is an entry identical to the docsIfModIndex in the docsIfCmtsModulationTable that describes this channel. This channel is further instantiated there by a grouping of interval usage codes which together fully describe the channel modulation. This object returns 0 if the docsIfCmtsModulationTable does not exist or is empty.</p> |
| cdxIfUpChannelCmTotal           | The total count of MTAs on this upstream channel since boot.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| cdxIfUpChannelCmActive          | The count of MTAs that are active. Active MTAs are recognized by the cdxCmtsCmStatusValue other than offline(1).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| cdxIfUpChannelCmRegistered      | The count of MTAs that are registered and online on this upstream. Registered MTAs are those with one of the following values: registrationComplete(6) of docsIfCmtsCmStatusValue OR online(12), kekRejected(10), onlineKekAssigned(6), tekRejected(11), onlineTekAssigned(7) of cdxCmtsCmStatusValue.                                                                                                                                                                                                                                                                                                                                 |

Table 11-2 CISCO-DOCS-EXT-MIB.my Objects (continued)

| Object                      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| cdxCmtsCmOnOffNotification  | This notification indicates that the MTA is coming online and going offline. A notification is sent from the CMTS for a MTA status changing to online or offline within the interval specified in <code>cdxCmtsCmOnOffTrapInterval</code> .                                                                                                                                                                                                                                                                                                                                                                                          |
| cdxCmtsCmChOverNotification | This notification is sent at the completion of a CMTS channel override operation if <code>cdxCmtsCmChOverTrapOnCompletion</code> is true in the original entry.<br><br>Once a channel override operation has been activated, it cannot be stopped. That is, it will run until either the CMTS has generated downstream frequency and/or upstream channel override fields in the RNG-RSP message sent to a MTA or <code>cdxCmtsCmChOverTimeExpiration</code> time expired. In either case, the operation is completed. State in the <code>cdxCmtsCmChOverState</code> object will tell in which condition the operation is completed. |

## DOCS-CABLE-DEVICE-MIB.my

This is the MIB Module for MCNS-compliant MTAs and cable-modem termination systems.

- The Access table (`docsDevNmAccessTable`) provides one level of security for access to the device by network management stations. The table controls access to SNMP objects by network management stations. If the table is empty, access to SNMP objects is unrestricted. This table exists only on SNMPv1 or v2c agents and does not exist on SNMPv3 agents (see the conformance section for details). Specifically, for v3 agents, the appropriate MIBs and security models apply in lieu of this table.

Entries in the table are ordered by `docsDevNmAccessIndex`. The first matching entry (e.g. matching IP address and community string) is used to derive access.

Note that access is also constrained by the community strings and any vendor-specific security.

- The Server Access group (`docsDevServer`) describes server access and parameters used for initial provisioning and bootstrapping.
- The Event Reporting group (`docsDevEv`) controls the reporting of the various classes of events.

This group includes:

- the Control table in which a combination of logging and reporting mechanisms may be chosen for each event priority. The mapping of event types to priorities is vendor-dependent. Vendors may also choose to allow the user to control that mapping through proprietary means.
- the Events table (`DocsDevEvent`), which contains a log of network and device events that may be of interest in fault isolation and troubleshooting.

Multiple sequential identical events are represented by incrementing `docsDevEvCounts` and setting `docsDevEvLastTime` to the current time rather than creating multiple rows.

Entries are created with the first occurrence of an event. `docsDevEvControl` can be used to clear the table. Individual events can not be deleted.

- Link Level Control Filtering group (docsDevFilterLLC)

LLC (Link Level Control) filters can be defined on an inclusive or exclusive basis: CMs can be configured to forward only packets matching a set of layer three protocols, or to drop packets matching a set of layer three protocols. Typical use of these filters is to filter out possibly harmful protocols.

- Link Level Control Filter table contains a list of filters to apply to (bridged) LLC traffic. The filters in this table are applied to incoming traffic on the appropriate interface(s) prior to any further processing (e.g. before handing the packet off for level 3 processing, or for bridging). The specific action taken when no filter is matched is controlled by docsDevFilterLLCUnmatchedAction.
- Filter IP table (docsDevFilterIp) contains an ordered list of filters or classifiers to apply to IP traffic. Filter application is ordered by the filter index, rather than by a best match algorithm (Note that this implies that the filter table may have gaps in the index values). Packets which match no filters will have policy 0 in the docsDevFilterPolicyTable applied to them if it exists. Otherwise, Packets which match no filters are discarded or forwarded according to the setting of docsDevFilterIpDefault.

Any IP packet can theoretically match multiple rows of this table. When considering a packet, the table is scanned in row index order (e.g. filter 10 is checked before filter 20). If the packet matches that filter (which means that it matches ALL criteria for that row), actions appropriate to docsDevFilterIpControl and docsDevFilterPolicyId are taken. If the packet was discarded processing is complete. If docsDevFilterIpContinue is set to true, the filter comparison continues with the next row in the table looking for additional matches.

If the packet matches no filter in the table, the packet is accepted or dropped for further processing based on the setting of docsDevFilterIpDefault. If the packet is accepted, the actions specified by policy group 0 (e.g. the rows in docsDevFilterPolicyTable which have a value of 0 for docsDevFilterPolicyId) are taken if that policy group exists.

Logically, this table is consulted twice during the processing of any IP packet - once upon its acceptance from the L2 entity, and once upon its transmission to the L2 entity. In actuality, for MTAs, IP filtering is generally the only IP processing done for transit traffic. This means that inbound and outbound filtering can generally be done at the same time with one pass through the filter table.

Entries in this table describe a filter to apply to IP traffic received on a specified interface. All identity objects in this table (e.g. source and destination address/mask, protocol, source/dest port, TOS/mask, interface and direction) must match their respective fields in the packet for any given filter to match. To create an entry in this table, docsDevFilterIpIfIndex must be specified.

- The Filter Polity Table maps between a policy group ID and a set of policies to be applied. All rows with the same docsDevFilterPolicyId are part of the same policy group and are applied in the order in which they are in this table.

docsDevFilterPolicyTable exists to allow multiple policy actions to be applied to any given classified packet. The policy actions are applied in index order For example:

| Index | ID | Type  | Action |
|-------|----|-------|--------|
| 1     | 1  | TOS   | 1      |
| 9     | 5  | TOS   | 1      |
| 12    | 1  | IPSEC | 3      |

This says that a packet which matches a filter with policy id 1, first has TOS policy 1 applied (which might set the TOS bits to enable a higher priority), and next has the IPSEC policy 3 applied (which may result in the packet being dumped into a secure VPN to a remote encryptor).

Policy ID 0 is reserved for default actions and is applied only to packets which match no filters in docsDevIpFilterTable.

- The TOS Policy Action table is used to describe Type of Service (TOS) bits processing.

This table is an adjunct to the docsDevFilterIpTable, and the docsDevFilterPolicy table. Entries in the latter table can point to specific rows in this (and other) tables and cause specific actions to be taken. This table permits the manipulation of the value of the Type of Service bits in the IP header of the matched packet as follows:

Set the tosBits of the packet to (tosBits & docsDevFilterTosAndMask) | docsDevFilterTosOrMask

This construct allows you to do a clear and set of all the TOS bits in a flexible manner.

- CPE IP Management and anti spoofing group (docsDevCpe). (Only implemented on MTAs.)

**Table 11-3 DOCS-CABLE-DEVICE-MIB.my Objects**

| Object                   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| docsDevRole              | Defines the current role of this device. cm (1) is a MTA, cmtsActive(2) is a CMTS which is controlling the system of MTAs, and cmtsBackup(3) is a CMTS which is currently connected, but not controlling the system (not currently used).<br><br>In general, if this device is a 'cm', its role will not change during operation or between reboots. If the device is a 'cmts' it may change between cmtsActive and cmtsBackup and back again during normal operation. Note: At this time, the DOCSIS standards do not support the concept of a backup CMTS, cmtsBackup is included for completeness. |
| docsDevDateTime          | The date and time, with optional time zone information.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| docsDevResetNow          | Setting this object to true(1) causes the device to reset. Reading this object always returns false(2).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| docsDevSerialNumber      | The manufacturer's serial number for this device.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| docsDevSTPControl        | This object controls operation of the spanning tree protocol (as distinguished from transparent bridging). If set to stEnabled(1) then the spanning tree protocol is enabled, subject to bridging constraints. If noStFilterBpdu(2), then spanning tree is not active, and Bridge PDUs received are discarded. If noStPassBpdu(3) then spanning tree is not active and Bridge PDUs are transparently forwarded. Note that a device need not implement all of these options, but that noStFilterBpdu(2) is required.                                                                                   |
| Entries in Access table: |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| docsDevNmAccessIndex     | Index used to order the application of access entries.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| docsDevNmAccessIp        | The IP address (or subnet) of the network management station. The address 255.255.255.255 is defined to mean any NMS. If traps are enabled for this entry, then the value must be the address of a specific device.                                                                                                                                                                                                                                                                                                                                                                                   |

**Table 11-3 DOCS-CABLE-DEVICE-MIB.my Objects (continued)**

| <b>Object</b>                                                                                                                 | <b>Description</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| docsDevNmAccessIpMask                                                                                                         | The IP subnet mask of the network management stations. If traps are enabled for this entry, then the value must be 255.255.255.255.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| docsDevNmAccessCommunity                                                                                                      | The community string to be matched for access by this entry. If set to a zero length string then any community string will match. When read, this object SHOULD return a zero length string.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| docsDevNmAccessControl                                                                                                        | Specifies the type of access allowed to this NMS. Setting this object to none(1) causes the table entry to be destroyed. Read(2) allows access by 'get' and 'get-next' PDUs. ReadWrite(3) allows access by 'set' as well. RoWithtraps(4), rwWithTraps(5), and trapsOnly(6) control distribution of Trap PDUs transmitted by this device.                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| docsDevNmAccessInterfaces                                                                                                     | <p>Specifies the set of interfaces from which requests from this NMS will be accepted.</p> <p>Each octet within the value of this object specifies a set of eight interfaces, with the first octet specifying ports 1 through 8, the second octet specifying interfaces 9 through 16, etc. Within each octet, the most significant bit represents the lowest numbered interface, and the least significant bit represents the highest numbered interface. Thus, each interface is represented by a single bit within the value of this object. If that bit has a value of '1' then that interface is included in the set.</p> <p>Note that entries in this table apply only to link-layer interfaces (e.g., Ethernet and CATV MAC). Upstream and downstream channel interfaces must not be specified.</p> |
| docsDevNmAccessStatus                                                                                                         | Controls and reflects the status of rows in this table. Rows in this table may be created by either the create-and-go or create-and-wait paradigms. There is no restriction on changing values in a row of this table while the row is active.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Procedures for using the following group are described in section 3.2.1 of the DOCSIS Radio Frequency Interface Specification |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| docsDevSwServer                                                                                                               | The address of the TFTP server used for software upgrades. If the TFTP server is unknown, return 0.0.0.0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| docsDevSwFilename                                                                                                             | The file name of the software image to be loaded into this device. Unless set via SNMP, this is the file name specified by the provisioning server that corresponds to the software version that is desired for this device. If unknown, the string '(unknown)' is returned.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

Table 11-3 DOCS-CABLE-DEVICE-MIB.my Objects (continued)

| Object                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| docsDevSwAdminStatus         | <p>If set to upgradeFromMgt(1), the device will initiate a TFTP software image download using docsDevSwFilename. After successfully receiving an image, the device will set its state to ignoreProvisioningUpgrade(3) and reboot. If the download process is interrupted by a reset or power failure, the device will load the previous image and, after re-initialization, continue to attempt loading the image specified in docsDevSwFilename.</p> <p>If set to allowProvisioningUpgrade(2), the device will use the software version information supplied by the provisioning server when next rebooting (this does not cause a reboot).</p> <p>When set to ignoreProvisioningUpgrade(3), the device will disregard software image upgrade information from the provisioning server.</p> <p>Note that reading this object can return upgradeFromMgt(1). This indicates that a software download is currently in progress, and that the device will reboot after successfully receiving an image.</p> <p>At initial startup, this object has the default value of allowProvisioningUpgrade(2).</p> |
| docsDevSwOperStatus          | <p>InProgress(1) indicates that a TFTP download is underway, either as a result of a version mismatch at provisioning or as a result of a upgradeFromMgt request. CompleteFromProvisioning(2) indicates that the last software upgrade was a result of version mismatch at provisioning. CompleteFromMgt(3) indicates that the last software upgrade was a result of setting docsDevSwAdminStatus to upgradeFromMgt. Failed(4) indicates that the last attempted download failed, ordinarily due to TFTP timeout.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| docsDevSwCurrentVers         | <p>The software version currently operating in this device. This object should be in the syntax used by the individual vendor to identify software versions. Any CM MUST return a string descriptive of the current software load. For a CMTS, this object SHOULD contain either a human readable representation of the vendor specific designation of the software for the chassis, or of the software for the control processor. If neither of these is applicable, this MUST contain an empty string.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Server Access group objects: |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |



**Table 11-3 DOCS-CABLE-DEVICE-MIB.my Objects (continued)**

| <b>Object</b>            | <b>Description</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| docsDevServerBootState   | <p>If operational(1), the device has completed loading and processing of configuration parameters and the CMTS has completed the Registration exchange.</p> <p>If disabled(2) then the device was administratively disabled, possibly by being refused network access in the configuration file.</p> <p>If waitingForDhcpOffer(3) then a DHCP Discover has been transmitted and no offer has yet been received.</p> <p>If waitingForDhcpResponse(4) then a DHCP Request has been transmitted and no response has yet been received.</p> <p>If waitingForTimeServer(5) then a Time Request has been transmitted and no response has yet been received.</p> <p>If waitingForTftp(6) then a request to the TFTP parameter server has been made and no response received.</p> <p>If refusedByCmts(7) then the Registration Request/Response exchange with the CMTS failed.</p> <p>If forwardingDenied(8) then the registration process completed, but the network access option in the received configuration file prohibits forwarding.</p> |
| docsDevServerDhcp        | The IP address of the DHCP server that assigned an IP address to this device. Returns 0.0.0.0 if DHCP was not used for IP address assignment.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| docsDevServerTime        | The IP address of the Time server (RFC-868). Returns 0.0.0.0 if the time server IP address is unknown.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| docsDevServerTftp        | The IP address of the TFTP server responsible for downloading provisioning and configuration parameters to this device. Returns 0.0.0.0 if the TFTP server address is unknown.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| docsDevServerConfigFile  | The name of the device configuration file read from the TFTP server. Returns an empty string if the configuration file name is unknown.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Event reporting objects: |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| docsDevEvControl         | <p>Setting this object to resetLog(1) empties the event log. All data is deleted.</p> <p>Setting it to useDefaultReporting(2) returns all event priorities to their factory-default reporting. Reading this object always returns useDefaultReporting(2).</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| docsDevEvSyslog          | The IP address of the Syslog server. If 0.0.0.0, syslog transmission is inhibited.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |

Table 11-3 DOCS-CABLE-DEVICE-MIB.my Objects (continued)

| Object                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| docsDevEvThrottleAdminStatus | <p>Controls the transmission of traps and syslog messages with respect to the trap pacing threshold.</p> <p>unconstrained(1) causes traps and syslog messages to be transmitted without regard to the threshold settings.</p> <p>maintainBelowThreshold(2) causes trap transmission and syslog messages to be suppressed if the number of traps would otherwise exceed the threshold.</p> <p>stopAtThreshold(3) causes trap transmission to cease at the threshold, and not resume until directed to do so.</p> <p>inhibited(4) causes all trap transmission and syslog messages to be suppressed.</p> <p>A single event is always treated as a single event for threshold counting. That is, an event causing both a trap and a syslog message is still treated as a single event.</p> <p>Writing to this object resets the thresholding state.</p> <p>At initial startup, this object has a default value of unconstrained(1).</p> |
| docsDevEvThrottleInhibited   | <p>If true(1), trap and syslog transmission is currently inhibited due to thresholds and/or the current setting of docsDevEvThrottleAdminStatus. In addition, this is set to true(1) if transmission is inhibited due to no syslog (docsDevEvSyslog) or trap (docsDevNmAccessEntry) destinations having been set.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| docsDevEvThrottleThreshold   | <p>Number of trap/syslog events per docsDevEvThrottleInterval to be transmitted before throttling.</p> <p>A single event is always treated as a single event for threshold counting. That is, an event causing both a trap and a syslog message is still treated as a single event.</p> <p>At initial startup, this object returns 0.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| docsDevEvThrottleInterval    | <p>The interval over which the trap threshold applies. At initial startup, this object has a value of 1.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

Table 11-3 DOCS-CABLE-DEVICE-MIB.my Objects (continued)

| Object             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| docsDevEvPriority  | <p>The priority level that is controlled by this entry.</p> <p>emergency(1)<br/> alert(2)<br/> critical(3)<br/> error(4)<br/> warning(5)<br/> notice(6)<br/> information(7)<br/> debug(8)</p> <p>These are ordered from most (emergency) to least (debug) critical. Each event with a CM or CMTS has a particular priority level associated with it (as defined by the vendor). During normal operation no event more critical than notice(6) should be generated. Events between warning and emergency should be generated at appropriate levels of problems (e.g. emergency when the box is about to crash).</p> |
| docsDevEvReporting | <p>Defines the action to be taken on occurrence of this event class. Implementations may not necessarily support all options for all event classes, but at minimum must allow traps and syslogging to be disabled. If the local(0) bit is set, then log to the internal log, if the traps(1) bit is set, then generate a trap, if the syslog(2) bit is set, then send a syslog message (assuming the syslog address is set).</p>                                                                                                                                                                                   |
| docsDevEvIndex     | <p>Provides relative ordering of the objects in the event log. This object will always increase except when (a) the log is reset via docsDevEvControl, (b) the device reboots and does not implement non-volatile storage for this log, or (c) it reaches the value <math>2^{31}</math>. The next entry for all the above cases is 1.</p>                                                                                                                                                                                                                                                                          |
| docsDevEvFirstTime | <p>The time that this entry was created.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| docsDevEvLastTime  | <p>If multiple events are reported via the same entry, the time that the last event for this entry occurred, otherwise this should have the same value as docsDevEvFirstTime.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| docsDevEvCounts    | <p>The number of consecutive event instances reported by this entry. This starts at 1 with the creation of this row and increments by 1 for each subsequent duplicate event.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| docsDevEvLevel     | <p>The priority level of this event as defined by the vendor.</p> <p>emergency(1)<br/> alert(2)<br/> critical(3)<br/> error(4)<br/> warning(5)<br/> notice(6)<br/> information(7)<br/> debug(8)</p> <p>These are ordered from most serious (emergency) to least serious (debug).</p>                                                                                                                                                                                                                                                                                                                               |

Table 11-3 DOCS-CABLE-DEVICE-MIB.my Objects (continued)

| Object                                                                                                                                                                                               | Description                                                                                                                                                                                                                                                                                                                                                                 |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Vendors will provide their own enumerations for the following objects. The interpretation of the enumeration is unambiguous for a particular value of the vendor's enterprise number in sysObjectID. |                                                                                                                                                                                                                                                                                                                                                                             |
| docsDevEvId                                                                                                                                                                                          | For this product, uniquely identifies the type of event that is reported by this entry.                                                                                                                                                                                                                                                                                     |
| docsDevEvText                                                                                                                                                                                        | Provides a human-readable description of the event, including all relevant context (interface numbers, etc.).                                                                                                                                                                                                                                                               |
| Link Level Control Filtering objects:                                                                                                                                                                |                                                                                                                                                                                                                                                                                                                                                                             |
| docsDevFilterLLCUnmatchedAction                                                                                                                                                                      | If set to discard(1), any L2 packet which does not match at least one filter in the docsDevFilterLLCTable will be discarded. If set to accept(2), any L2 packet which does not match at least one filter in the docsDevFilterLLCTable will be accepted for further processing (e.g., bridging). At initial system startup, this object returns accept(2).                   |
| docsDevFilterLLCIndex                                                                                                                                                                                | Index used for the identification of filters (note that LLC filter order is irrelevant).                                                                                                                                                                                                                                                                                    |
| docsDevFilterLLCStatus                                                                                                                                                                               | Controls and reflects the status of rows in this table. There is no restriction on changing any of the associated columns for this row while this object is set to active.                                                                                                                                                                                                  |
| docsDevFilterLLCIfIndex                                                                                                                                                                              | The entry interface to which this filter applies. The value corresponds to ifIndex for either a CATV MAC or another network interface. If the value is zero, the filter applies to all interfaces. In cable modems, the default value is the customer side interface. In CMTSs, this object has to be specified to create a row in this table.                              |
| docsDevFilterLLCProtocolType                                                                                                                                                                         | The format of the value in docsDevFilterLLCProtocol: either a two-byte Ethernet Ethertype, or a one-byte 802.2 SAP value. EtherType(1) also applies to SNAP-encapsulated frames.                                                                                                                                                                                            |
| docsDevFilterLLCProtocol                                                                                                                                                                             | The layer three protocol for which this filter applies. The protocol value format depends on docsDevFilterLLCProtocolType. Note that for SNAP frames, etherType filtering is performed rather than DSAP=0xAA.                                                                                                                                                               |
| docsDevFilterLLCMatches                                                                                                                                                                              | Counts the number of times this filter was matched.                                                                                                                                                                                                                                                                                                                         |
| Filter IP objects:                                                                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                             |
| docsDevFilterIpDefault                                                                                                                                                                               | The default behavior for (bridged) packets that do not match IP filters is defined by docsDevFilterIpDefault. If set to discard(1), all packets not matching an IP filter will be discarded. If set to accept(2), all packets not matching an IP filter will be accepted for further processing (e.g., bridging). At initial system startup, this object returns accept(2). |
| docsDevFilterIpIndex                                                                                                                                                                                 | Index used to order the application of filters. The filter with the lowest index is always applied first.                                                                                                                                                                                                                                                                   |

Table 11-3 DOCS-CABLE-DEVICE-MIB.my Objects (continued)

| Object                   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| docsDevFilterIpStatus    | Controls and reflects the status of rows in this table. Specifying only this object (with the appropriate index) on a CM is sufficient to create a filter row which matches all inbound packets on the ethernet interface, and results in the packets being discarded. docsDevFilterIpIfIndex (at least) must be specified on a CMTS to create a row. Creation of the rows may be done via either create-and-wait or create-and-go, but the filter is not applied until this object is set to (or changes to) active. There is no restriction in changing any object in a row while this object is set to active. |
| docsDevFilterIpControl   | If set to discard(1), all packets matching this filter will be discarded and scanning of the remainder of the filter list will be aborted. If set to accept(2), all packets matching this filter will be accepted for further processing (e.g., bridging). If docsDevFilterIpContinue is set to true, see if there are other matches, otherwise done. If set to policy (3), execute the policy entries matched by docsDevIpFilterPolicyId in docsDevIpFilterPolicyTable.<br><br>If docsDevFilterIpContinue is set to true, continue scanning the table for other matches, otherwise done.                         |
| docsDevFilterIpIfIndex   | The entry interface to which this filter applies. The value corresponds to ifIndex for either a CATV MAC or another network interface. If the value is zero, the filter applies to all interfaces. Default value in cable modems is the index of the customer-side (e.g. ethernet) interface. In CMTSs, this object MUST be specified to create a row in this table.                                                                                                                                                                                                                                              |
| docsDevFilterIpDirection | Determines whether the filter is applied to inbound(1) traffic—default, outbound(2) traffic, or traffic in both(3) directions.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| docsDevFilterIpBroadcast | If set to true(1), the filter only applies to multicast and broadcast traffic. If set to false(2), the filter applies to all traffic. Default: false.                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| docsDevFilterIpSaddr     | The source IP address, or portion thereof, that is to be matched for this filter. The source address is first masked (and'ed) against docsDevFilterIpSmask before being compared to this value. A value of 0 for this object and 0 for the mask matches all IP addresses.                                                                                                                                                                                                                                                                                                                                         |
| docsDevFilterIpSmask     | A bit mask that is to be applied to the source address prior to matching. This mask is not necessarily the same as a subnet mask, but 1's bits must be left-most and contiguous.                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| docsDevFilterIpDaddr     | The destination IP address, or portion thereof, that is to be matched for this filter. The destination address is first masked (and'ed) against docsDevFilterIpDmask before being compared to this value. A value of 0 for this object and 0 for the mask matches all IP addresses.                                                                                                                                                                                                                                                                                                                               |

**Table 11-3 DOCS-CABLE-DEVICE-MIB.my Objects (continued)**

| <b>Object</b>                 | <b>Description</b>                                                                                                                                                                                                                                                                                                                                                                        |
|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| docsDevFilterIpDmask          | A bit mask that is to be applied to the destination address prior to matching. This mask is not necessarily the same as a subnet mask, but 1's bits must be left-most and contiguous.                                                                                                                                                                                                     |
| docsDevFilterIpProtocol       | The IP protocol value that is to be matched. For example: icmp is 1, tcp is 6, udp is 17. A value of 256 matches ANY protocol.                                                                                                                                                                                                                                                            |
| docsDevFilterIpSourcePortLow  | If docsDevFilterIpProtocol is udp or tcp, this is the inclusive lower bound of the transport-layer source port range that is to be matched, otherwise it is ignored during matching.                                                                                                                                                                                                      |
| docsDevFilterIpSourcePortHigh | If docsDevFilterIpProtocol is udp or tcp, this is the inclusive upper bound of the transport-layer source port range that is to be matched, otherwise it is ignored during matching.                                                                                                                                                                                                      |
| docsDevFilterIpDestPortLow    | If docsDevFilterIpProtocol is udp or tcp, this is the inclusive lower bound of the transport-layer destination port range that is to be matched, otherwise it is ignored during matching.                                                                                                                                                                                                 |
| docsDevFilterIpDestPortHigh   | If docsDevFilterIpProtocol is udp or tcp, this is the inclusive upper bound of the transport-layer destination port range that is to be matched, otherwise it is ignored during matching.                                                                                                                                                                                                 |
| docsDevFilterIpMatches        | Counts the number of times this filter was matched. This object is initialized to 0 at boot, or at row creation, and is reset only upon reboot.                                                                                                                                                                                                                                           |
| docsDevFilterIpTos            | This is the value to be matched to the packet's TOS (Type of Service) value (after the TOS value is and'd with docsDevFilterIpTosMask). A value for this object of 0 and a mask of 0 matches all TOS values.                                                                                                                                                                              |
| docsDevFilterIpTosMask        | The mask to be applied to the packet's TOS value before matching.                                                                                                                                                                                                                                                                                                                         |
| docsDevFilterIpContinue       | If this value is set to true, and docsDevFilterIpControl is anything but discard (1), continue scanning and applying policies. Default: false.                                                                                                                                                                                                                                            |
| docsDevFilterIpPolicyId       | This object points to an entry in docsDevFilterPolicyTable. If docsDevFilterIpControl is set to policy (3), execute all matching policies in docsDevFilterPolicyTable. If no matching policy exists, treat as if docsDevFilterIpControl were set to accept (1). If this object is set to the value of 0, there is no matching policy, and docsDevFilterPolicyTable MUST NOT be consulted. |
| Filter Policy objects:        |                                                                                                                                                                                                                                                                                                                                                                                           |
| docsDevFilterPolicyIndex      | Index value for the Filter Policy table.                                                                                                                                                                                                                                                                                                                                                  |
| docsDevFilterPolicyId         | Policy ID for this entry. A policy ID can apply to multiple rows of this table, all relevant policies are executed. Policy 0 (if populated) is applied to all packets which do not match any of the filters. N.B. If docsDevFilterIpPolicyId is set to 0, it DOES NOT match policy 0 of this table.                                                                                       |
| docsDevFilterPolicyStatus     | Object used to create an entry in this table.                                                                                                                                                                                                                                                                                                                                             |

**Table 11-3 DOCS-CABLE-DEVICE-MIB.my Objects (continued)**

| Object                           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| docsDevFilterPolicyPtr           | This object points to a row in an applicable filter policy table. Currently, the only standard policy table is docsDevFilterTosTable. Per the textual convention, this object points to the first accessible object in the row. E.g. to point to a row in docsDevFilterTosTable with an index of 21, the value of this object would be the object identifier docsDevTosStatus.21. Vendors must adhere to the same convention when adding vendor specific policy table extensions. The default upon row creation is a null pointer which results in no policy action being taken. |
| TOS Policy Action table objects: |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| docsDevFilterTosIndex            | The unique index for this row. There are no ordering requirements for this table and any valid index may be specified.                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| docsDevFilterTosStatus           | The object used to create and delete entries in this table. A row created by specifying just this object results in a row which specifies no change to the TOS bits. A row may be created using either the create-and-go or create-and-wait paradigms. There is no restriction on the ability to change values in this row while the row is active.                                                                                                                                                                                                                              |
| docsDevFilterTosAndMask          | This value is bitwise and'd with the matched packet's TOS bits.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| docsDevFilterTosOrMask           | After bitwise and'ing with the above bits, the packet's TOS bits are bitwise or'd with these bits.                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

## DOCS-IF-MIB.my

This is the MIB Module for MCNS/DOCSIS compliant Radio Frequency (RF) interfaces in MTAs and CMTSs.

This MIB is composed of the following groups and tables:

- Base Group
  - The Downstream Channel table (docsIfDownstreamChannel) describes the attributes of downstream channels (frequency bands). This table is implemented on both the MTA and the CMTS.
  - The Upstream Channel table (docsIfUpstreamChannel) describes the attributes of attached upstream channels (frequency bands). This table is implemented on both the CM and the CMTS. For the CM, only attached channels appear in the table, and the table is read-only.
  - The Qos Profile table (docsIfQosProf) describes the attributes for each class of service. The entries in this table are referenced from the docsIfServiceEntries. They exist as a separate table in order to reduce redundant information in docsIfServiceTable. This table is implemented at both the CM and the CMTS. The CM need only maintain entries for the classes of service referenced by its docsIfServiceTable.

If implemented as read-create in the CMTS, creation of entries in this table is controlled by the value of docsIfCmtsQosProfilePermissions.

If implemented as read-only, entries are created based on information in REG-REQ MAC messages received from MTAs (CMTS implementation), or based on information extracted from the TFTP option file (cable modem implementation). In the CMTS, read-only entries are removed if no longer referenced by docsIfCmtsServiceTable.

An entry in this table must not be removed while it is referenced by an entry in docsIfCmServiceTable (MTA) or docsIfCmtsServiceTable (CMTS).

An entry in this table should not be changeable while it is referenced by an entry in docsIfCmtsServiceTable.

If this table is created automatically, there should only be a single entry for each Class of Service. Multiple entries with the same Class of Service parameters are not recommended.

- The Signal Quality table (docsIfSigQ) at the CM describes the PHY signal quality of downstream channels; at the CMTS, describes the PHY signal quality of upstream channels. At the CMTS, this table may exclude contention intervals.
- Cable Modem Group
  - The CM MAC table (docsIfCm) describes the attributes of each CM MAC interface, extending the information available from ifEntry.
  - The CM Status table (docsIfCmStatus) maintains a number of status objects and counters for MTAs. This table is implemented only at the CM.
  - The cable modem Service table (docsIfCmService) describes the attributes of each upstream service queue on an MTA.
- CMTS Group
  - The CMTS MAC table (docsIfCmts) describes the attributes of each CMTS MAC interface, extending the information available from ifEntry. Mandatory for all CMTS devices.
  - The CMTS Status table (docsIfCmtsStatus) maintains a number of status objects and counters.
  - The CM Status (within CMTS) table (docsIfCmtsCmStatus) maintains status information for each MTA connected to this CMTS. This table is implemented only at the CMTS. It contains per CM status information available in the CMTS.
  - The CMTS Service table (docsIfCmtsService) describes the attributes of upstream service queues in a CMTS. Entries in this table exist for each ifEntry with an ifType of docsCableMaclayer(127), and for each service queue (Service ID) within this MAC layer. Entries in this table are created with the creation of individual Service IDs by the MAC layer and removed when a Service ID is removed.
  - The CMTS Modulation table (docsIfCmtsMod) describes a modulation profile associated with one or more upstream channels. Entries in this table can be re-used by one or more upstream channels. An upstream channel will have a modulation profile for each value of docsIfModIntervalUsageCode.



Table 11-4 DOCS-IF-MIB.mib Objects

| Object                      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| docsIfDownChannelId         | The CMTS identification of the downstream channel within this particular MAC interface. If the interface is down, the object returns the most current value. If the downstream channel ID is unknown, this object returns a value of 0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| docsIfDownChannelFrequency  | The center of the downstream frequency associated with this channel. This object will return the current tuner frequency. If a CMTS provides IF output, this object will return 0, unless this CMTS is in control of the final downstream RF frequency. See the associated compliance object for a description of valid frequencies that may be written to this object.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| docsIfDownChannelWidth      | The bandwidth of this downstream channel. Most implementations are expected to support a channel width of 6 MHz (North America) and/or 8 MHz (Europe). See the associated compliance object for a description of the valid channel widths for this object.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| docsIfDownChannelModulation | The modulation type associated with this downstream channel. If the interface is down, this object either returns the configured value (CMTS), the most current value (CM), or the value of unknown(1). See the associated conformance object for write conditions and limitations. See DOCSIS Radio Frequency Interface Specification, Section 3.6.2. for specifics on the modulation profiles implied by qam64 and qam256.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| docsIfDownChannelInterleave | <p>The Forward Error Correction (FEC) interleaving used for this downstream channel.</p> <p>Values are defined as follows (latency in milliseconds):</p> <p>taps8Increment16(3): protection 5.9/4.1 usec, latency.22/.15ms</p> <p>taps16Increment8(4): protection 12/8.2 usec, latency.48/.33 ms</p> <p>taps32Increment4(5): protection 24/16 usec, latency.98/.68 ms</p> <p>taps64Increment2(6): protection 47/33 usec, latency 2/1.4 ms</p> <p>taps128Increment1(7): protection 95/66 usec, latency 4/2.8 ms</p> <p>If the interface is down, this object either returns the configured value (CMTS), the most current value (CM), or the value of unknown(1).</p> <p>The value of other(2) is returned if the interleave is known but not defined in the above list.</p> <p>See DOCSIS Radio Frequency Interface Specification, Section 4.3.2. for the FEC configuration described by the setting of this object.</p> |

Table 11-4 DOCS-IF-MIB.my Objects (continued)

| Object                              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| docsIfDownChannelPower              | At the CMTS, the operational transmit power. At the CM, the received power level. May be set to zero at the CM if power level measurement is not supported.<br><br>If the interface is down, this object either returns the configured value (CMTS), the most current value (CM) or the value of 0. See DOCSIS Radio Frequency Interface Specification, Table 4-12 and Table 4-13. for recommended and required power levels.                       |
| docsIfUpChannelId                   | The CMTS identification of the upstream channel.                                                                                                                                                                                                                                                                                                                                                                                                    |
| docsIfUpChannelFrequency            | The center of the frequency band associated with this upstream channel. This object returns 0 if the frequency is undefined or unknown. Minimum permitted upstream frequency is 5,000,000 Hz for current technology. See the associated conformance object for write conditions and limitations.                                                                                                                                                    |
| docsIfUpChannelWidth                | The bandwidth of this upstream channel. This object returns 0 if the channel width is undefined or unknown. Minimum permitted channel width is 200,000 Hz currently. See the associated conformance object for write conditions and limitations.                                                                                                                                                                                                    |
| docsIfUpChannelModulation Profile   | An entry identical to the docsIfModIndex in the docsIfCmtsModulationTable that describes this channel.<br><br>This channel is further instantiated there by a grouping of interval usage codes which together fully describe the channel modulation. This object returns 0 if the docsIfCmtsModulationTable entry does not exist or docsIfCmtsModulationTable is empty. See the associated conformance object for write conditions and limitations. |
| docsIfUpChannelSlotSize             | The number of 6.25 microsecond ticks in each upstream mini-slot. Returns zero if the value is undefined or unknown. See the associated conformance object for write conditions and limitations.                                                                                                                                                                                                                                                     |
| docsIfUpChannelTxTimingOffset       | A measure of the current round trip time at the CM, or the maximum round trip time seen by the CMTS. Used for timing of CM upstream transmissions to ensure synchronized arrivals at the CMTS. Units are in terms of (6.25 microseconds/64).                                                                                                                                                                                                        |
| docsIfUpChannelRangingBackoff Start | The initial random backoff window to use when retrying Ranging Requests. Expressed as a power of 2. A value of 16 at the CMTS indicates that a proprietary adaptive retry mechanism is to be used. See the associated conformance object for write conditions and limitations.                                                                                                                                                                      |
| docsIfUpChannelRangingBackoff End   | The final random backoff window to use when retrying Ranging Requests. Expressed as a power of 2. A value of 16 at the CMTS indicates that a proprietary adaptive retry mechanism is to be used. See the associated conformance object for write conditions and limitations.                                                                                                                                                                        |

Table 11-4 DOCS-IF-MIB.my Objects (continued)

| Object                         | Description                                                                                                                                                                                                                                                                 |
|--------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| docsIfUpChannelTxBackoffStart  | The initial random backoff window to use when retrying transmissions. Expressed as a power of 2. A value of 16 at the CMTS indicates that a proprietary adaptive retry mechanism is to be used. See the associated conformance object for write conditions and limitations. |
| docsIfUpChannelTxBackoffEnd    | The final random backoff window to use when retrying transmissions. Expressed as a power of 2. A value of 16 at the CMTS indicates that a proprietary adaptive retry mechanism is to be used. See the associated conformance object for write conditions and limitations.   |
| docsIfQosProfPriority          | A relative priority assigned to this service when allocating bandwidth. Zero indicates lowest priority; and seven indicates highest priority. Interpretation of priority is device-specific. MUST NOT be changed while this row is active.                                  |
| docsIfQosProfMaxUpBandwidth    | The maximum upstream bandwidth, in bits per second, allowed for a service with this service class. Zero if there is no restriction of upstream bandwidth. MUST NOT be changed while this row is active.                                                                     |
| docsIfQosProfGuarUpBandwidth   | Minimum guaranteed upstream bandwidth, in bits per second, allowed for a service with this service class. MUST NOT be changed while this row is active.                                                                                                                     |
| docsIfQosProfMaxDown Bandwidth | The maximum downstream bandwidth, in bits per second, allowed for a service with this service class. Zero if there is no restriction of downstream bandwidth. MUST NOT be changed while this row is active.                                                                 |
| docsIfQosProfMaxTxBurst        | The maximum number of mini-slots that may be requested for a single upstream transmission. A value of zero means there is no limit. MUST NOT be changed while this row is active.                                                                                           |
| docsIfQosProfBaselinePrivacy   | Indicates whether Baseline Privacy is enabled for this service class. MUST NOT be changed while this row is active.                                                                                                                                                         |
| docsIfQosProfStatus            | This object is used to create or delete rows in this table. This object MUST NOT be changed from active while the row is referenced by any entry in either docsIfCmServiceTable (on the CM), or the docsIfCmtsServiceTable (on the CMTS).                                   |
| docsIfSigQIncludesContention   | Value is true(1) if this CMTS includes contention intervals in the counters in this table. Always false(2) for CMs.                                                                                                                                                         |
| docsIfSigQUnerrored            | Codewords received on this channel without error. This includes all codewords, whether or not they were part of frames destined for this device.                                                                                                                            |
| docsIfSigQCorrecteds           | Codewords received on this channel with correctable errors. This includes all codewords, whether or not they were part of frames destined for this device.                                                                                                                  |
| docsIfSigQUncorrectables       | Codewords received on this channel with uncorrectable errors. This includes all codewords, whether or not they were part of frames destined for this device.                                                                                                                |

Table 11-4 DOCS-IF-MIB.my Objects (continued)

| Object                     | Description                                                                                                                                                                                                                                                                                                                                                             |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| docsIfSigQSignalNoise      | Signal/Noise ratio as perceived for this channel. At the CM, describes the Signal/Noise of the downstream channel. At the CMTS, describes the average Signal/Noise of the upstream channel.                                                                                                                                                                             |
| docsIfSigQMicroreflections | Total microreflections including in-channel response as perceived on this interface, measured in dBc below the signal level. This object is not assumed to return an absolutely accurate value, but should give a rough indication of microreflections received on this interface. It is up to the implementor to provide information as accurate as possible.          |
| docsIfSigQEqualizationData | At the CM, returns the equalization data for the downstream channel. At the CMTS, returns the average equalization data for the upstream channel. Returns an empty string if the value is unknown or if there is no equalization data available or defined.                                                                                                             |
| docsIfCmCmtsAddress        | Identifies the CMTS that is believed to control this MAC domain. At the CM, this will be the source address from SYNC, MAP, and other MAC-layer messages. If the CMTS is unknown, returns 00-00-00-00-00-00.                                                                                                                                                            |
| docsIfCmCapabilities       | Identifies the capabilities of the MAC implementation at this interface. Note that packet transmission is always supported. Therefore, there is no specific bit required to explicitly indicate this capability.                                                                                                                                                        |
| docsIfCmRangingTimeout     | Waiting time for a Ranging Response packet.                                                                                                                                                                                                                                                                                                                             |
| docsIfCmStatusValue        | Current MTA connectivity state, as specified in the RF Interface Specification.<br>other(1)<br>notReady(2)<br>notSynchronized(3)<br>phySynchronized(4)<br>usParametersAcquired(5)<br>rangingComplete(6)<br>ipComplete(7)<br>todEstablished(8)<br>securityEstablished(9)<br>paramTransferComplete(10)<br>registrationComplete(11)<br>operational(12)<br>accessDenied(13) |
| docsIfCmStatusCode         | Status code for this MTA as defined in the RF Interface Specification. The status code consists of a single character indicating error groups, followed by a two- or three-digit number indicating the status condition.                                                                                                                                                |
| docsIfCmStatusTxPower      | The operational transmit power for the attached upstream channel.                                                                                                                                                                                                                                                                                                       |
| docsIfCmStatusResets       | Number of times the CM reset or initialized this interface.                                                                                                                                                                                                                                                                                                             |

**Table 11-4 DOCS-IF-MIB.my Objects (continued)**

| <b>Object</b>                | <b>Description</b>                                                                                                                                                                                                                                                                                                         |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| docsIfCmStatusLostSyncs      | Number of times the CM lost synchronization with the downstream channel.                                                                                                                                                                                                                                                   |
| docsIfCmStatusInvalidMaps    | Number of times the CM received invalid MAP messages.                                                                                                                                                                                                                                                                      |
| docsIfCmStatusInvalidUcds    | Number of times the CM received invalid UCD messages.                                                                                                                                                                                                                                                                      |
| docsIfCmStatusT1Timeouts     | Number of times counter T1 expired in the CM.                                                                                                                                                                                                                                                                              |
| docsIfCmStatusT2Timeouts     | Number of times counter T2 expired in the CM.                                                                                                                                                                                                                                                                              |
| docsIfCmStatusT3Timeouts     | Number of times counter T3 expired in the CM.                                                                                                                                                                                                                                                                              |
| docsIfCmStatusT4Timeouts     | Number of times counter T4 expired in the CM.                                                                                                                                                                                                                                                                              |
| docsIfCmStatusRangingAborted | Number of times the ranging process was aborted by the CMTS.                                                                                                                                                                                                                                                               |
| docsIfCmServiceId            | Identifies a service queue for upstream bandwidth. The attributes of this service queue are shared between the CM and the CMTS. The CMTS allocates upstream bandwidth to this service queue based on requests from the CM and on the class of service associated with this queue.                                          |
| docsIfCmServiceQosProfile    | The index in docsIfQosProfileTable describing the quality of service attributes associated with this particular service. If no associated entry in docsIfQosProfileTable exists, this object returns a value of zero.                                                                                                      |
| docsIfCmServiceTxSlotsImmed  | The number of upstream mini-slots which have been used to transmit data PDUs in immediate (contention) mode. This includes only those PDUs which are presumed to have arrived at the headend (i.e., those which were explicitly acknowledged.) It does not include retransmission attempts or mini-slots used by Requests. |
| docsIfCmServiceTxSlotsDed    | The number of upstream mini-slots which have been used to transmit data PDUs in dedicated mode (i.e., as a result of a unicast Data Grant).                                                                                                                                                                                |
| docsIfCmServiceTxRetries     | The number of attempts to transmit data PDUs containing requests for acknowledgment which did not result in acknowledgment.                                                                                                                                                                                                |
| docsIfCmServiceTxExceededs   | The number of data PDUs transmission failures due to excessive retries without acknowledgment.                                                                                                                                                                                                                             |
| docsIfCmServiceRqRetries     | The number of attempts to transmit bandwidth requests which did not result in acknowledgment.                                                                                                                                                                                                                              |
| docsIfCmServiceRqExceededs   | The number of requests for bandwidth which failed due to excessive retries without acknowledgment.                                                                                                                                                                                                                         |
| docsIfCmtsCapabilities       | Identifies the capabilities of the CMTS MAC implementation at this interface. Note that packet transmission is always supported. Therefore, there is no specific bit required to explicitly indicate this capability.                                                                                                      |
| docsIfCmtsSyncInterval       | The interval between CMTS transmission of successive SYNC messages at this interface.                                                                                                                                                                                                                                      |

**Table 11-4 DOCS-IF-MIB.my Objects (continued)**

| <b>Object</b>                         | <b>Description</b>                                                                                                                                                                                                                                                                                                       |
|---------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| docsIfCmtsUcdInterval                 | The interval between CMTS transmission of successive Upstream Channel Descriptor messages for each upstream channel at this interface.                                                                                                                                                                                   |
| docsIfCmtsMaxServiceIds               | The maximum number of service IDs that may be simultaneously active.                                                                                                                                                                                                                                                     |
| docsIfCmtsInvitedRanging Attempts     | The maximum number of attempts to make on invitations for ranging requests. A value of zero means the system should attempt to range forever.                                                                                                                                                                            |
| docsIfCmtsInsertInterval              | The amount of time to elapse between each broadcast station maintenance grant. Broadcast station maintenance grants are used to allow new MTAs to join the network. Zero indicates that a vendor-specific algorithm is used instead of a fixed time. Maximum amount of time permitted by the specification is 2 seconds. |
| docsIfCmtsStatusInvalidRange Reqs     | This object counts invalid RNG-REQ messages received on this interface.                                                                                                                                                                                                                                                  |
| docsIfCmtsStatusRanging Aborted       | This object counts ranging attempts that were explicitly aborted by the CMTS.                                                                                                                                                                                                                                            |
| docsIfCmtsStatusInvalidRegReqs        | This object counts invalid REG-REQ messages received on this interface.                                                                                                                                                                                                                                                  |
| docsIfCmtsStatusFailedRegReqs         | This object counts failed registration attempts, i.e., authentication failures and class of service failures, on this interface.                                                                                                                                                                                         |
| docsIfCmtsStatusInvalidData Reqs      | This object counts invalid data request messages received on this interface.                                                                                                                                                                                                                                             |
| docsIfCmtsStatusT5Timeouts            | This object counts the number of times counter T5 expired on this interface.                                                                                                                                                                                                                                             |
| docsIfCmtsCmStatusMacAddress          | MAC address of this MTA. If the MTA has multiple MAC addresses, this is the MAC address associated with the Cable interface.                                                                                                                                                                                             |
| docsIfCmtsCmStatusIpAddress           | IP address of this MTA. If the MTA has no IP address assigned, or the IP address is unknown, this object returns a value of 0.0.0.0. If the MTA has multiple IP addresses, this object returns the IP address associated with the Cable interface.                                                                       |
| docsIfCmtsCmStatusDown ChannelIfIndex | IfIndex of the downstream channel this CM is connected to. If the downstream channel is unknown, this object returns a value of zero.                                                                                                                                                                                    |
| docsIfCmtsCmStatusUpChannel IfIndex   | IfIndex of the upstream channel this CM is connected to. If the upstream channel is unknown, this object returns a value of zero.                                                                                                                                                                                        |
| docsIfCmtsCmStatusRxPower             | The receive power as perceived for upstream data from this MTA. If the receive power is unknown, this object returns a value of zero.                                                                                                                                                                                    |

Table 11-4 DOCS-IF-MIB.my Objects (continued)

| Object                             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| docsIfCmtsCmStatusTimingOffset     | A measure of the current round trip time for this CM. Used for timing of CM upstream transmissions to ensure synchronized arrivals at the CMTS. Units are in terms of (6.25 microseconds/64). Returns zero if the value is unknown.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| docsIfCmtsCmStatusEqualizationData | Equalization data for this CM. Returns an empty string if the value is unknown or if there is no equalization data available or defined.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| docsIfCmtsCmStatusValue            | Current MTA connectivity state, as specified in the RF Interface Specification. Returned status information is the CM status as assumed by the CMTS, and indicates the following events:<br><br>other(1)—any state other than below.<br><br>ranging(2)—the CMTS has received an Initial Ranging Request message from the CM, and the ranging process is not yet complete.<br><br>rangingAborted(3)—the CMTS has sent a Ranging Abort message to the CM.<br><br>rangingComplete(4)—the CMTS has sent a Ranging Complete message to the CM.<br><br>ipComplete(5)—the CMTS has received a DHCP reply message and forwarded it to the CM.<br><br>registrationComplete(6)—the CMTS has sent a Registration Response message to the CM.<br><br>accessDenied(7)—the CMTS has sent a Registration Aborted message to the CM.<br><br>The CMTS only needs to report states it is able to detect. |
| docsIfCmtsCmStatusUnerrored        | Codewords received without error from this MTA.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| docsIfCmtsCmStatusCorrected        | Codewords received with correctable errors from this MTA.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| docsIfCmtsCmStatusUncorrectables   | Codewords received with uncorrectable errors from this MTA.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| docsIfCmtsCmStatusSignalNoise      | Signal/Noise ratio as perceived for upstream data from this MTA. If the Signal/Noise is unknown, this object returns a value of zero.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| docsIfCmtsCmStatusMicroreflections | Total microreflections including in-channel response as perceived on this interface, measured in dBc below the signal level. This object is not assumed to return an absolutely accurate value, but should give a rough indication of microreflections received on this interface. It is up to the implementor to provide information as accurate as possible.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| docsIfCmtsServiceCmStatus          | Pointer to an entry in docsIfCmtsCmStatusTable identifying the MTA using this Service Queue. If multiple MTAs are using this Service Queue, the value of this object is zero.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| docsIfCmtsServiceAdminStatus       | Allows a service class for a particular modem to be suppressed, (re-)enabled, or deleted altogether.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

Table 11-4 DOCS-IF-MIB.my Objects (continued)

| Object                              | Description                                                                                                                                                                                                                                          |
|-------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| docsIfCmtsServiceQosProfile         | The index in docsIfQosProfileTable describing the quality of service attributes associated with this particular service. If no associated docsIfQosProfileTable entry exists, this object returns a value of zero.                                   |
| docsIfCmtsServiceCreateTime         | The value of sysUpTime when this entry was created.                                                                                                                                                                                                  |
| docsIfCmtsServiceInOctets           | The cumulative number of Packet Data octets received on this Service ID. The count does not include the size of the Cable MAC header.                                                                                                                |
| docsIfCmtsServiceInPackets          | The cumulative number of Packet Data packets received on this Service ID.                                                                                                                                                                            |
| docsIfCmtsModControl                | The modulation type used on this channel. Returns other(1) if the modulation type is neither qpsk or qam16. See the reference for the modulation profiles implied by qpsk or qam16. See the conformance object for write conditions and limitations. |
| docsIfCmtsModPreambleLen            | The preamble length for this modulation profile in bits. Default value is the minimum needed by the implementation at the CMTS for the given modulation profile.                                                                                     |
| docsIfCmtsModDifferential Encoding  | Specifies whether or not differential encoding is used on this channel.                                                                                                                                                                              |
| docsIfCmtsModFECError Correction    | The number of correctable errored bytes (t) used in forward error correction code. The value of 0 indicates no correction is employed. The number of check bytes appended will be twice this value.                                                  |
| docsIfCmtsModFECCodeWord Length     | The number of data bytes (k) in the forward error correction codeword. This object is not used if docsIfCmtsModFECErrorCorrection is zero.                                                                                                           |
| docsIfCmtsModScramblerSeed          | The 15 bit seed value for the scrambler polynomial.                                                                                                                                                                                                  |
| docsIfCmtsModMaxBurstSize           | The maximum number of mini-slots that can be transmitted during this channel's burst time. Returns zero if the burst length is bounded by the allocation MAP rather than this profile. Default value is 0 except for shortData, where it is 8.       |
| docsIfCmtsModGuardTimeSize          | The number of symbol-times which must follow the end of this channel's burst. Default value is the minimum time needed by the implementation for this modulation profile.                                                                            |
| docsIfCmtsModLastCodeword Shortened | Indicates if the last FEC codeword is truncated.                                                                                                                                                                                                     |



**Table 11-4 DOCS-IF-MIB.my Objects (continued)**

| <b>Object</b>                    | <b>Description</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| docsIfCmtsModScrambler           | Indicates if the scrambler is employed.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| docsIfCmtsQosProfile Permissions | <p>This object specifies permitted methods of creating entries in docsIfQosProfileTable.</p> <p>CreateByManagement(0) is set if entries can be created using SNMP.</p> <p>UpdateByManagement(1) is set if updating entries using SNMP is permitted.</p> <p>CreateByModems(2) is set if entries can be created based on information in REG-REQ MAC messages received from MTAs.</p> <p>Information in this object is only applicable if docsIfQosProfileTable is implemented as read-create. Otherwise, this object is implemented as read-only and returns CreateByModems(2). Either CreateByManagement(0) or CreateByModems(1) must be set when writing to this object.</p> |

