Cisco cBR Series Converged Broadband Routers Troubleshooting and Network Management Configuration Guide for Cisco IOS XE Fuji 16.7.x

First Published: 2017-11-23

Americas 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: 408 527-0883

© 2017 Cisco Systems, Inc. All rights reserved.

CONTENTS

CHAPTER 1

Call Home 1

- Hardware Compatibility Matrix for the Cisco cBR Series Routers 1
- Prerequisites for Call Home 2
- Restrictions for Call Home 3
- Information About Call Home 3
  - Benefits of Call Home 3
  - Obtaining Smart Call Home Services 4
    - Anonymous Reporting 4
    - Smart Licensing 5
- How to Configure Call Home 5
  - Configuring Smart Call Home (Single Command) 5
  - Configuring Call Home 6
    - Enabling and Disabling Call Home 7
    - Configuring Contact Information 7
    - Configuring Destination Profiles 9
    - Subscribing to Alert Groups 14
    - Configuring General email Options 18
    - Sending Call Home Messages Manually 24
- Configuring Diagnostic Signatures 29
  - Prerequisites for Diagnostic Signatures 29
  - Information About Diagnostic Signatures 29
    - Diagnostic Signature Overview 29
    - Diagnostic Signature Downloading 30
    - Diagnostic Signature Signing 30
    - Diagnostic Signature Workflow 31
    - Diagnostic Signature Events and Actions 31

How to Configure Diagnostic Signatures 33
Configuring the Service Call Home for Diagnostic Signatures 33
Configuring Diagnostic Signatures 35
Verifying the Call Home Configuration 36
Configuration Example for Call Home 41
Example: Call Home Configuration 41
Example: Configuring HTTP Transport for Call Home on the Cisco cBR Series Router 42
Example: Configuring Email Transport for Call Home on the Cisco cBR Series Router 44
Default Settings 46
Alert Groups Trigger Events and Commands 47
Message Contents 51
Sample syslog Alert Notification in XML Format 55
Additional References 64
Feature Information for Call Home 65

CHAPTER 2 **SNMP Support over VPNs—Context-Based Access Control 67**
Finding Feature Information 67
Hardware Compatibility Matrix for the Cisco cBR Series Routers 67
Restrictions for SNMP Support over VPNs—Context-Based Access Control 68
Information About SNMP Support over VPNs—Context-Based Access Control 68
SNMP Versions and Security 68
SNMPv1 or SNMPv2 Security 69
SNMPv3 Security 69
SNMP Notification Support over VPNs 70
VPN-Aware SNMP 70
VPN Route Distinguishers 70
SNMP Contexts 71
How to Configure SNMP Support over VPNs—Context-Based Access Control 71
Configuring an SNMP Context and Associating the SNMP Context with a VPN 71
Configuring SNMP Support and Associating an SNMP Context 73
Configuration Examples for SNMP Support over VPNs—Context-Based Access Control 75
Example: Configuring Context-Based Access Control 75
Additional References 76
Feature Information for SNMP Support over VPNs—Context-Based Access Control 78

CHAPTER 3 **SNMP Engine Enhancement** 79

Hardware Compatibility Matrix for the Cisco cBR Series Routers 79
Restrictions for SNMP Cache Engine Enhancement 80
Information About SNMP Cache Engine Enhancement 80
How to Configure SNMP Cache Engine Enhancement 81
Verifying the SNMP Cache Engine Status 82
Additional References 83
Feature Information for SNMP Cache Engine Enhancement 83

CHAPTER 4 **Onboard Failure Logging** 85

Finding Feature Information 85
Hardware Compatibility Matrix for the Cisco cBR Series Routers 85
Understanding OBFL 86
Configuring OBFL 87
Displaying OBFL Logging Information 87
Clearing OBFL Logging 87
Configuration and Verification Examples 88
Feature Information for Onboard Failure Logging 90

CHAPTER 5 **Control Point Discovery** 91

Hardware Compatibility Matrix for the Cisco cBR Series Routers 91
Prerequisites for Control Point Discovery 92
Restrictions for Control Point Discovery 92
Information About Control Point Discovery 93
Control Points 93
Network Layer Signaling (NLS) 93
NLS for CPD 93
Control Point Discovery 94
CPD Protocol Hierarchy 94
Control Relationship 94
How to Configure CPD 95
Enabling CPD Functionality 95
Examples for CPD Enable 96

Debugging CPD Functionality 96
Configuring Control Relationship Identifier 96
Examples 97
Enabling NLS Functionality 97
Examples 97
Debugging NLS Functionality 98
Configuring Authorization Group Identifier and Authentication Key 98
Examples 98
Configuring NLS Response Timeout 99
Examples 99
Additional References 99
Feature Information for Control Point Discovery 100

CHAPTER 6 IPDR Streaming Protocol 101
Restrictions for Configuring IPDR Streaming Protocol 101
Information About IPDR Streaming Protocol 102
Data Collection Methodologies 102
How to Configure IPDR Streaming Protocol 103
Configuring the IPDR Session 103
Configuring the IPDR Type 104
Configuring the IPDR Collector 104
Configuring the IPDR Associate 105
Configuring the IPDR Template 105
Configuring the IPDR Exporter 106
Configuration Examples for IPDR Streaming Protocol 107
Example: Configuring the IPDR Session 107
Example: Configuring the IPDR Type 107
Example: Configuring the IPDR Collector 108
Example: Configuring the IPDR Associate 108
Example: Configuring the IPDR Template 108
Example: Configuring the IPDR Exporter 108
Verifying IPDR Streaming Protocol 108
Verifying the IPDR Collector 109
Verifying IPDR exporter 109

Verifying IPDR session 109
Verifying IPDR Session Collector 110
Verifying IPDR Session Template 110
Additional References 110
Feature Information for IPDR Streaming Protocol 110

CHAPTER 7 **Usage-Based Billing (SAMIS) 113**
Hardware Compatibility Matrix for the Cisco cBR Series Routers 113
Prerequisites for Usage-Based Billing (SAMIS) 114
Restrictions for Usage-based Billing 115
Information About Usage-based Billing 116
Feature Overview 116
Usage-Based Billing and DOCSIS Support on the Cisco CMTS Routers 116
Standards 117
IPDR Service Definition Schemas 117
IPDR CM-STATUS-2008 118
DOCSIS SAMIS Service Definitions 118
DOCSIS Diagnostic Log Service Definitions 119
DOCSIS Spectrum Measurement Service Definition 119
DOCSIS CMTS CM Registration Status Service Definition 120
DOCSIS CMTS CM Upstream Status Service Definition 120
DOCSIS CMTS Topology Service Definition 120
DOCSIS CPE Service Definition 120
DOCSIS CMTS Utilization Statistics Service Definition 121
Modes of Operation 121
Billing Record Format 122
SNMP Support 125
Benefits 126
How to Configure the Usage-based Billing Feature 126
Enabling Usage-based Billing Feature File Mode Using CLI Commands 126
Enabling Usage-based Billing Feature File Mode Using SNMP Commands 128
Examples for Enabling Usage Billing using SNMP Mode 130
Enabling Usage-based Billing Feature Streaming Mode Using CLI Commands 131
Enabling Usage-based Billing Feature Streaming Mode Using SNMP Commands 132

Examples for SNMP Commands 136
Enabling and Configuring the Secure Copy Protocol (optional) 137
Configuring the Cisco CMTS for SSL Operation 139
Prerequisites for CA 139
Retrieving Records from a Cisco CMTS in File Mode 140
Using SCP 140
Using TFTP 141
Using SNMP 142
Using SNMP 146
Examples To Transfer Using SNMP 147
Disabling the Usage-based Billing Feature 148
Configuring Certified SSL Servers for Usage-Based Billing 149
Generating SSL Server Certification 150
Configuring and Testing the Cisco CMTS for Certified SSL Server Support 150
Monitoring the Usage-based Billing Feature 151
Configuration Examples for Usage-based Billing 153
File Mode Configuration (with Secure Copy) 153
Non-Secure Streaming Mode Configuration 153
Secure Streaming Mode Configuration 154

CHAPTER 8 **Frequency Allocation Information for the Cisco CMTS Routers** 155
Frequency Allocation for the Cisco CMTS Routers 155

CHAPTER 9 **Flap List Troubleshooting** 167
Finding Feature Information 167
Hardware Compatibility Matrix for the Cisco cBR Series Routers 167
Prerequisites for Flap List Troubleshooting 168
Restrictions for Flap List Troubleshooting 168
Information About Flap List Troubleshooting 169
Feature Overview 169
Information in the Flap List 169
Cisco Cable Manager and Cisco Broadband Troubleshooter 170
Benefits 171
How to Configure Flap List Troubleshooting 171

Configuring Flap List Operation Using the CLI (optional) 171
Clearing the Flap List and Counters Using the CLI (optional) 172
Enabling or Disabling Power Adjustment Using the CLI (optional) 173
Configuring Flap List Operation Using SNMP (optional) 175
Clearing the Flap List and Counters Using SNMP (optional) 176
How to Monitor and Troubleshoot Using Flap Lists 176
Displaying the Flap List Using the show cable flap-list Command 176
Displaying the Flap List Using the show cable modem flap Command 177
Displaying the Flap List Using SNMP 178
Displaying Flap-List Information for Specific Cable Modems 179
Example 179
Troubleshooting Suggestions 180
Troubleshooting Tips 180
Performing Amplitude Averaging 181
Using Other Related Commands 181
Configuration Examples for Flap List Troubleshooting 183
Additional References 183
Feature Information for Flap List Troubleshooting 184

CHAPTER 10 **Maximum CPE and Host Parameters** 185
Finding Feature Information 185
Hardware Compatibility Matrix for the Cisco cBR Series Routers 185
Information About the MAX CPE and Host Parameters 186
MAX CPE 187
MAX Host 188
Specifying an Unlimited Value for Max Host 188
MAX CPE IP 188
MAX CPE IPv6 189
Interoperation of the Maximum CPE Parameters 189
Benefits 190
How to Configure the MAX CPE and Host Parameters 190
Configuring the Maximum Number of CPE Devices on the Cisco CMTS 190
Configuration Examples 192
Additional References 193

Feature Information for Maximum CPE and Host Parameters 194

CHAPTER 11 SNMP Background Synchronization 195

Information About SNMP Background Synchronization 195

How to Configure SNMP Background Synchronization 196

Enabling SNMP Background Synchronization 196

Setting Data Interval 196

Verifying SNMP Background Synchronization 197

Configuring Example for SNMP Background Synchronization 203

Feature Information for SNMP Background Synchronization 203

CHAPTER 12 Online Offline Diagnostics 205

Overview of Online Offline Diagnostics 205

Benefits of Online Offline Diagnostics 205

Prerequisites for Online Offline Diagnostics 206

Restrictions for Online Offline Diagnostics 206

How to Configure Online Offline Diagnostics 206

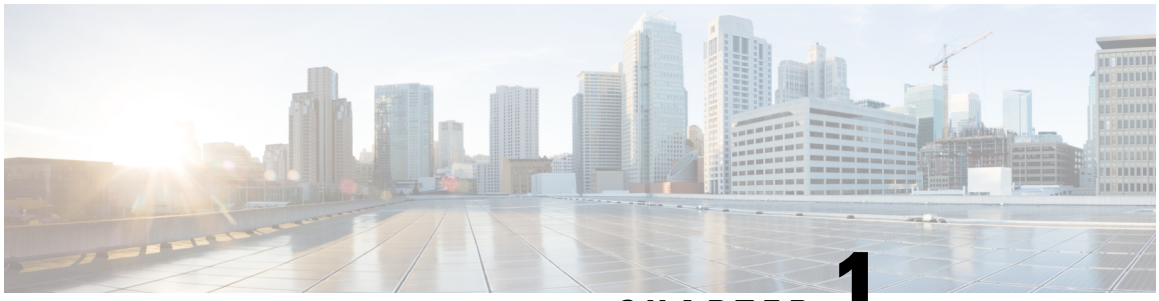
Configuring Field Diagnostic Test 206

Verifying the Testing Process 206

Removing the Field Diagnostic Image from a Line Card 207

Configuration Example for Online Offline Diagnostics 207

Feature Information for Online Offline Diagnostics 207



CHAPTER 1

Call Home

Call Home offers proactive diagnostics and real-time alerts on select Cisco devices, which provides higher network availability and increased operational efficiency. Smart Call Home is a secure connected service of Cisco SMARTnet for the Cisco cBR routers.

Finding Feature Information

Your software release may not support all the features that are documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. The Feature Information Table at the end of this document provides information about the documented features and lists the releases in which each feature is supported.

Contents

- Hardware Compatibility Matrix for the Cisco cBR Series Routers, on page 1
- Prerequisites for Call Home, on page 2
- Restrictions for Call Home, on page 3
- Information About Call Home, on page 3
- How to Configure Call Home, on page 5
- Configuring Diagnostic Signatures, on page 29
- Verifying the Call Home Configuration, on page 36
- Configuration Example for Call Home, on page 41
- Default Settings, on page 46
- Alert Groups Trigger Events and Commands, on page 47
- Message Contents, on page 51
- Additional References, on page 64
- Feature Information for Call Home, on page 65

Hardware Compatibility Matrix for the Cisco cBR Series Routers

Note The hardware components that are introduced in a given Cisco IOS-XE Release are supported in all subsequent releases unless otherwise specified.

Table 1: Hardware Compatibility Matrix for the Cisco cBR Series Routers

Cisco CMTS Platform	Processor Engine	Interface Cards
Cisco cBR-8 Converged Broadband Router	**Cisco IOS-XE Release 16.5.1 and Later Releases** Cisco cBR-8 Supervisor: • PID—CBR-SUP-250G • PID—CBR-CCAP-SUP-160G • PID—CBR-CCAP-SUP-60G • PID—CBR-SUP-8X10G-PIC	**Cisco IOS-XE Release 16.5.1 and Later Releases** Cisco cBR-8 CCAP Line Cards: • PID—CBR-LC-8D30-16U30 • PID—CBR-LC-8D31-16U30 • PID—CBR-RF-PIC • PID—CBR-RF-PROT-PIC • PID—CBR-CCAP-LC-40G • PID—CBR-CCAP-LC-40G-R Cisco cBR-8 Downstream PHY Modules: • PID—CBR-D30-DS-MOD • PID—CBR-D31-DS-MOD Cisco cBR-8 Upstream PHY Modules: • PID—CBR-D30-US-MOD • PID—CBR-D31-US-MOD

Prerequisites for Call Home

- Contact e-mail address (required for full registration with Smart Call Home, optional if Call Home is enabled in anonymous mode), phone number (optional), and street address information (optional) should be configured so that the receiver can determine the origin of messages received.

  Note Contact e-mail address is not required if you enable Smart Call Home by enabling smart licensing.

- At least one destination profile (predefined or user-defined) must be configured. The destination profile(s) configured depends on whether the receiving entity is a pager, e-mail, or automated service such as Cisco Smart Call Home.
  - If the destination profile uses e-mail message delivery, you must specify a Simple Mail Transfer Protocol (SMTP) server.
  - Configuring the trustpool certificate authority (CA) is not required for HTTPS server connection as the trustpool feature is enabled by default.

- The router must have IP connectivity to an e-mail server or the destination HTTP(S) server.
- To use Cisco Smart Call Home service, an active service contract covering the device is required to provide full Smart Call Home service.

Note An active service contract is only required for full Smart Call Home services like automatically raising a Cisco Technical Assistance Center (TAC) case.

Restrictions for Call Home

- If there is no IP connectivity or if the interface in the VRF to the profile destination is down, Smart Call Home messages cannot be sent.
- Smart Call Home operates with any SMTP server.
- You can configure up to five SMTP servers for Smart Call Home.

Information About Call Home

The Call Home feature provides email-based and web-based notification of critical system events. A versatile range of message formats are available for optimal compatibility with pager services, standard email, or XML-based automated parsing applications. Common uses of this feature may include direct paging of a network support engineer, email notification to a network operations center, XML delivery to a support website, and use of Cisco Smart Call Home services for direct case generation with the Cisco Systems Technical Assistance Center (TAC).

The Call Home feature can deliver alert messages containing information on configuration, environmental conditions, inventory, syslog, snapshot, and crash events.

The Call Home feature can deliver alerts to multiple recipients, referred to as *Call Home destination profiles* , each with configurable message formats and content categories. A predefined destination profile (CiscoTAC-1) is provided, and you also can define your own destination profiles. The CiscoTAC-1 profile is used to send alerts to the backend server of the Smart Call Home service, which can be used to create service requests to Cisco TAC, the service will depend on the Smart Call Home service support in place for your device and the severity of the alert.

Flexible message delivery and format options make it easy to integrate specific support requirements.

Benefits of Call Home

- Automatic execution and attachment of relevant CLI command output.
- Multiple message format options such as the following:
  - Short Text—Suitable for pagers or printed reports.
  - Full Text—Fully formatted message information suitable for human reading.

  - XML—Matching readable format using Extensible Markup Language (XML). The XML format enables communication with the Cisco TAC.

- Multiple concurrent message destinations.
- Multiple message categories including configuration, crash, diagnostic, environment, inventory, snapshot, and syslog.
- Filtering of messages based on severity and pattern matching.
- Scheduling of periodic message sending.

Obtaining Smart Call Home Services

If you have a service contract directly with Cisco, you can register for the Smart Call Home service. Smart Call Home analyzes Smart Call Home messages and provides background information and recommendations. For critical issues, Automatic Service Requests are generated with the Cisco TAC.

Smart Call Home offers the following features:

- Continuous device health monitoring and real-time alerts.
- Analysis of Smart Call Home messages and, if needed, Automatic Service Request generation routed to the correct TAC team, including detailed diagnostic information to speed problem resolution.
- Secure message transport directly from your device or through an HTTP proxy server or a downloadable Transport Gateway (TG). You can use a TG aggregation point to support multiple devices or in cases where security dictates that your devices may not be connected directly to the Internet.
- Web-based access to Smart Call Home messages and recommendations, inventory, and configuration information for all Smart Call Home devices provides access to associated field notices, security advisories, and end-of-life information.

You need the following items to register for Smart Call Home:

- SMARTnet contract number for your router.
- Your e-mail address
- Your Cisco.com username

For information about how to configure Call Home to work with the Smart Call Home service, see the Smart Call Home.

Anonymous Reporting

Smart Call Home is a service capability included with many Cisco service contracts and is designed to assist customers resolve problems more quickly. In addition, the information gained from crash messages helps Cisco understand equipment and issues occurring in the field. If you decide not to use Smart Call Home, you can still enable Anonymous Reporting to allow Cisco to securely receive minimal error and health information from the device. If you enable Anonymous Reporting, your customer identity will remain anonymous, and no identifying information is sent.

Note When you enable Anonymous Reporting, you acknowledge your consent to transfer the specified data to Cisco or to vendors operating on behalf of Cisco (including countries outside the United States). Cisco maintains the privacy of all customers. For information about how Cisco treats personal information, see the Cisco Privacy Statement at Cisco Online Privacy Statement

When Call Home is configured in an anonymous way, only crash, inventory, and test messages are sent to Cisco. No identifying information is sent.

For more information about what is sent in these messages, see the Alert Group Trigger Events and Commands section.

Smart Licensing

Smart Licensing uses the Smart Call Home service.

The Smart Licensing service is an alternative licensing architecture to Cisco Software Licensing (CSL). Smart Licensing uses the Cisco Smart Software Manager as a backend tool for managing licenses. Smart Call Home must be configured before using the Smart Licensing. By default, Smart Licensing and Smart Call Home are enabled on the Cisco cBR routers.

For more information about Smart Licensing, see Cisco Smart Licensing on the Cisco cBR Router.

How to Configure Call Home

Configuring Smart Call Home (Single Command)

Smart Call Home is enabled by default on the router. The CiscoTAC-1 profile to send data to Cisco is also enabled by default.

You do not need to use the single command to enable Smart Call Home on the router unless you need to change to anonymous mode or add HTTP proxy using the single command.

To enable all Call Home basic configurations using a single command, perform the following steps:

SUMMARY STEPS

1. **configure terminal**
2. **call-home reporting** { **anonymous** | **contact-email-addr** *email-address* } [**http-proxy** { *ipv4-address* | *ipv6-address* | **name** } **port** *port number*]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device#`	Enters global configuration mode.

	Command or Action	Purpose
	`configure terminal`	
Step 2	**call-home reporting** { **anonymous** | **contact-email-addr** *email-address* } [**http-proxy** { *ipv4-address* | *ipv6-address* | **name** } **port** *port number*] **Example:** `Device(config)# call-home reporting contact-email-addr email@company.com`	Enables all Call Home basic configurations using a single command. • **anonymous** —Enables Call-Home TAC profile to only send crash, inventory, and test messages and send the messages in an anonymous way. • **contact-email-addr** —Enables Smart Call Home service full reporting capability and sends a full inventory message from Call-Home TAC profile to Smart Call Home server to start full registration process. • **http-proxy** { *ipv4-address* | *ipv6-address* | **name** —An ipv4 or ipv6 address or server name. Maximum length is 64. • **port** *port number* —Port number. Range is 1 to 65535. **Note** HTTP proxy option allows you to make use of your own proxy server to buffer and secure internet connections from your devices. **Note** After successfully enabling Call Home either in anonymous or full registration mode using the **call-home reporting** command, an inventory message is sent out. If Call Home is enabled in anonymous mode, an anonymous inventory message is sent out. If Call Home is enabled in full registration mode, a Full Inventory message for full registration mode is sent. For more information about what is sent in these messages, see Alert Groups Trigger Events and Commands, on page 47.

Configuring Call Home

For security reasons, we recommend that you use the HTTPS transport options, due to the additional payload encryption that HTTPS offers. The Transport Gateway software is downloadable from Cisco.com and is available if you require an aggregation point or a proxy for connection to the Internet.

The implementation on the router supports the trustpool feature (embedded CA certificates in IOS images). The trustpool feature simplifies configuration to enable Smart Call Home service on configured devices. It eliminates the requirement of manually configuring the trustpool and provides automatic update of the CA certificate should it change in the future.

Enabling and Disabling Call Home

To enable or disable the Call Home feature, complete the following steps:

SUMMARY STEPS

1. **configure terminal**
2. **service call-home**
3. **no service call-home**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router#` **`configure terminal`**	Enters global configuration mode.
Step 2	**service call-home** **Example:** `Router(config)#` **`service call-home`**	Enables the Call Home feature.
Step 3	**no service call-home** **Example:** `Router(config)#` **`no service call-home`**	Disables the Call Home feature.

Configuring Contact Information

Each router must include a contact e-mail address. You can optionally include a phone number, street address, contract ID, customer ID, and site ID.

To assign the contact information, complete the following steps:

SUMMARY STEPS

1. **configure terminal**
2. **call-home**
3. **contact-email-addr** *email-address*
4. **phone-number** + *phone-number*
5. **street-address** *street-address*
6. **customer-id** *text*
7. **site-id** *text*

8. **contract-id** *text*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router>` **`configure terminal`**	Enters global configuration mode.
Step 2	**call-home** **Example:** `Router(config)#` **`call-home`**	Enters call home configuration mode.
Step 3	**contact-email-addr** *email-address* **Example:** `Router(cfg-call-home)#` **`contact-email-addr username@example.com`**	Assigns the customer's e-mail address. Enter up to 200 characters in e-mail address format with no spaces.
Step 4	**phone-number** + *phone-number* **Example:** `Router(cfg-call-home)#` **`phone-number +1-222-333-4444`**	(Optional) Assigns the customer's phone number. **Note** The number must begin with a plus (**+)** prefix, and may contain only dashes (-) and numbers. Enter up to 16 characters. If you include spaces, you must enclose your entry within double quotation marks (" ").
Step 5	**street-address** *street-address* **Example:** `Router(cfg-call-home)#` **`street-address "1234 Any Street, Any city, Any state, 12345"`**	(Optional) Assigns the customer's street address where RMA equipment can be shipped. Enter up to 200 characters. If you include spaces, you must enclose your entry within double quotation marks (" ").
Step 6	**customer-id** *text* **Example:** `Router(cfg-call-home)#` **`customer-id Customer1234`**	(Optional) Identifies the customer ID. Enter up to 64 characters. If you include spaces, you must enclose your entry within double quotation marks (" ").

	Command or Action	Purpose
Step 7	**site-id** *text* **Example:** `Router(cfg-call-home)#` **`site-id Site1ManhattanNY`**	(Optional) Identifies the customer site ID. Enter up to 200 characters. If you include spaces, you must enclose your entry within double quotation marks (“ ”).
Step 8	**contract-id** *text* **Example:** `Router(cfg-call-home)#` **`contract-id Company1234`**	(Optional) Identifies the customer’s contract ID for the router. Enter up to 64 characters. If you include spaces, you must enclose your entry within double quotation marks (“ ”).

Configuring Destination Profiles

A destination profile contains the required delivery information for an alert notification. At least one destination profile is required. You can configure multiple destination profiles of one or more types.

You can create and define a new destination profile or copy and use the predefined destination profile. If you define a new destination profile, you must assign a profile name. You can control which profile to be used for Smart Licensing by enabling or disabling smart-licensing data of that profile. Only one active profile can have smart-license data enabled.

Note If you use the Smart Call Home service, the destination profile must use the XML message format.

A destination profile includes the following information:

- Profile name—String that uniquely identifies each user-defined destination profile. The profile name is limited to 31 characters and is not case-sensitive. You cannot use **all** as a profile name.
- Transport method—Transport mechanism, either email or HTTP (including HTTPS), for delivery of alerts.
  - For user-defined destination profiles, email is the default, and you can enable either or both transport mechanisms. If you disable both methods, email is enabled.
  - For the predefined CiscoTAC-1 profile, you can enable either transport mechanism, but not both.
- Destination address—The actual address related to the transport method by which the alert should be sent. You can change the destination of the CiscoTAC-1 profile.
- Message formatting—The message format used for sending the alert. The format options for a user-defined destination profile are long-text, short-text, or XML. The default is XML. For the predefined CiscoTAC-1 profile, only XML is allowed.
- Message size—The maximum destination message size. The valid range is 50 to 3,145,728 bytes. The default is 3,145,728 bytes.

- Reporting method—You can choose which data to report for a profile. You can enable reporting of Smart Call Home data or Smart Licensing data, or both. Only one active profile is allowed to report Smart Licensing data at a time.
- Anonymous reporting—You can choose for your customer identity to remain anonymous, and no identifying information is sent.
- Subscribing to interesting alert-groups—You can choose to subscribe to alert-groups highlighting your interests.
- Message severity level—The Call Home severity level that the alert must meet before a Call Home message is generated to all e-mail addresses in the destination profile. An alert is not generated if the Call Home severity level of the alert is lower than the message severity level set for the destination profile.

You can also configure a destination profile to allow periodic inventory update messages by using the inventory alert group.

A pre-defined destination profile CiscoTAC-1 is supported. It supports the XML message format. This profile is preconfigured with Cisco Smart Call Home server HTTPS URL, email address to reach the server, maximum message size, and message severity level for each alert group.

Important We recommend that you do not use the message severity level 0. If you use message severity level 0, all syslogs will trigger Call Home messages, which can cause CPU and memory issues.

This section contains the following:

Creating a New Destination Profile

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**call-home** **Example:** `Router(config)# call-home`	Enters Call Home configuration mode.
Step 4	**profile** *name* **Example:** `Router(cfg-call-home)# profile profile1`	Enters the Call Home destination profile configuration mode for the specified destination profile. If the specified destination profile does not exist, it is created.
Step 5	**destination transport-method** { **email** | **http** }	(Optional) Enables the message transport method.

	Command or Action	Purpose
	Example: `Router(cfg-call-home-profile)# destination transport-method email`	• **email** —Sets the e-mail message transport method. • **http** —Sets the HTTP message transport method. **Note** The **no** option disables the method.
Step 6	**destination address** { **email** *email-address* | **http** *url* } **Example:** `Router(cfg-call-home-profile)# destination address email myaddress@example.com`	Configures the destination e-mail address or URL to which Call Home messages are sent. **Note** When entering a destination URL, include either **http://** or **https://**, depending on whether the server is a secure server. If the destination is a secure server, you must also configure a trustpool CA.
Step 7	**destination preferred-msg-format** { **long-text** | **short-text** | **xml** } **Example:** `Router(cfg-call-home-profile)# destination preferred-msg-format xml`	(Optional) Configures a preferred message format. The default is XML. • **long-text** —Configures the long text message format. • **short-text** —Configures the short text message format. • **xml** —Configures the XML message format.
Step 8	**destination message-size** *bytes* **Example:** `Router(cfg-call-home-profile)# destination message-size 3,145,728`	(Optional) Configures a maximum destination message size for the destination profile.
Step 9	**active** **Example:** `Router(cfg-call-home-profile)# active`	Enables the destination profile. By default, the profile is enabled when it is created. If you activate a profile which enables smart-licensing data while smart-licensing data is already being reported in another active profile, you will receive an error message.
Step 10	**reporting** { **all** | **smart-call-home-data** | **smart-licensing-data** } **Example:** `Router(cfg-call-home-profile)# reporting smart-call-home-data`	Configures the type of data to report for a profile. You can select either to report Smart Call Home data or Smart Licensing data. Selecting the **all** option reports data for both types of data.
Step 11	**end** **Example:** `Router(cfg-call-home-profile)# end`	Returns to privileged EXEC mode.
Step 12	**show call-home profile** { *name* | **all** } **Example:** `Router# show call-home profile profile1`	Displays destination profile configuration for specified profile or all configured profiles.

	Command or Action	Purpose
Step 13	**show call-home smart-licensing** **Example:** `Router# show call-home smart-licensing`	Displays the current Call Home Smart Licensing settings for the configured destination profiles.
Step 14	**show call-home smart-licensing statistics** **Example:** `Router# show call-home smart-licensing statistics`	Displays the Call Home Smart Licensing statistics.

Copying a Destination Profile

You can create a new destination profile by copying an existing profile

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**call-home** **Example:** `Router(config)# call-home`	Enters Call Home configuration mode.
Step 4	**copy profile** *source-profile target-profile* **Example:** `Router(cfg-call-home)# copy profile profile1 profile2`	Creates a new destination profile with the same configuration settings as the existing destination profile. • *source-profile* —Name of the source destination profile. • *target-profile* —Name of the target or new destination profile.

Renaming a Destination Profile

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password, if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**call-home** **Example:** `Router(config)# call-home`	Enters Call Home configuration mode.
Step 4	**rename profile** *source-profile target-profile* **Example:** `Router(cfg-call-home)# rename profile profile1 profile2`	Renames the existing destination profile. • *source-profile* —Name of the source destination profile. • *target-profile* —Name of the target destination profile.

Setting Profiles to Anonymous Mode

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**call-home** **Example:** `Router(config)# call-home`	Enters Call Home configuration mode.
Step 4	**profile** *name* **Example:** `Router(cfg-call-home)# profile profile1`	Enters the Call Home destination profile configuration mode for the specified destination profile. If the specified destination profile does not exist, it is created.
Step 5	**anonymous-reporting-only** **Example:** `Router(cfg-call-home-profile)# anonymous-reporting-only`	Sets the profile to anonymous mode. **Note** By default, the profile sends a full report of all types of events subscribed in the profile. When **anonymous-reporting-only** is set, only crash, inventory, and test messages are sent.

Subscribing to Alert Groups

An alert group is a predefined subset of Call Home alerts that are supported. You can select one or more alert groups to be received by a destination profile.

- Configuration
- Crash
- Diagnostic
- Environment
- Inventory
- Snapshot
- Syslog

The triggering events for each alert group are listed in the Alert Groups Trigger Events and Commands, and the contents of the alert group messages are listed in the Message Contents.

You can select one or more alert groups to be received by a destination profile.

Note Call Home alerts are only sent to destination profiles that have subscribed to the alert group containing that Call Home alert. The alert group must be enabled. The Call Home event severity must be at or above the message severity set in the destination profile.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**call-home** **Example:** `Router(config)# call-home`	Enters Call Home configuration mode.
Step 4	**alert-group** { **all** | **configuration** | **crash** | **diagnostic** | **environment** | **inventory** | **snapshot** | **syslog** } **Example:** `Router(cfg-call-home)# alert-group all`	Enables the specified alert group. Use the keyword **all** to enable all alert groups. By default, all alert groups are enabled.

	Command or Action	Purpose
Step 5	**profile** *name* **Example:** `Router(cfg-call-home)# profile profile1`	Enters the Call Home destination profile configuration mode for the specified destination profile. If the specified destination profile does not exist, it is created.
Step 6	**subscribe-to-alert-group configuration** [**periodic** { **daily** *hh:mm* | **monthly** *date hh:mm* | **weekly** *day hh:mm* }] **Example:** `Router(cfg-call-home-profile)# subscribe-to-alert-group configuration periodic daily 12:00`	Subscribes this destination profile to the Configuration alert group. The Configuration alert group can be configured for periodic notification.
Step 7	**subscribe-to-alert-group crash** **Example:** `Router(cfg-call-home-profile)# subscribe-to-alert-group crash`	Subscribes to the Crash alert group in user profile. By default, Cisco TAC profile subscribes to the Crash alert group and cannot be unsubscribed.
Step 8	**subscribe-to-alert-group diagnostic** [**severity** { **catastrophic** | **disaster** | **fatal** | **critical** | **major** | **minor** | **warning** | **notification** | **normal** | **debugging** }] **Example:** `Router(cfg-call-home-profile)# subscribe-to-alert-group syslog severity major`	Subscribes this destination profile to the Diagnostic alert group. The Diagnostic alert group can be configured to filter messages based on severity.
Step 9	**subscribe-to-alert-group environment** [**severity** { **catastrophic** | **disaster** | **fatal** | **critical** | **major** | **minor** | **warning** | **notification** | **normal** | **debugging** }] **Example:** `Router(cfg-call-home-profile)# subscribe-to-alert-group environment severity major`	Subscribes this destination profile to the Environment alert group. The Environment alert group can be configured to filter messages based on severity.
Step 10	**subscribe-to-alert-group inventory** [**periodic** { **daily** *hh:mm* | **monthly** *date hh:mm* | **weekly** *day hh:mm* }] **Example:** `Router(cfg-call-home-profile)# subscribe-to-alert-group inventory periodic daily 12:00`	Subscribes this destination profile to the Inventory alert group. The Inventory alert group can be configured for periodic notification
Step 11	**subscribe-to-alert-group snapshot** [**periodic** { **daily** *hh:mm* | **monthly** *date hh:mm* | **weekly** *day hh:mm* | **hourly** *mm* | **interval** *mm* }] **Example:**	Subscribes this destination profile to the Snapshot alert group. The Snapshot alert group can be configured for periodic notification. By default, the Snapshot alert group has no command to run. You can add commands into the alert group. In doing

	Command or Action	Purpose
	`Router(cfg-call-home-profile)#` **`subscribe-to-alert-group snapshot periodic daily 12:00`**	so, the output of the commands added in the Snapshot alert group will be included in the snapshot message.
Step 12	**subscribe-to-alert-group syslog** [**severity** { **catastrophic** | **disaster** | **fatal** | **critical** | **major** | **minor** | **warning** | **notification** | **normal** | **debugging** }] [**pattern** *string*] **Example:** `Router(cfg-call-home-profile)#` **`subscribe-to-alert-group syslog severity major`**	Subscribes this destination profile to the Syslog alert group. The Syslog alert group can be configured to filter messages based on severity. You can specify a pattern to be matched in the syslog message. If the pattern contains spaces, you must enclose it in quotes (""). You can specify a text pattern to be matched within each syslog message. If you configure a pattern, a Syslog alert group message is sent only if it contains the specified pattern and meets the severity threshold. If the pattern contains spaces, you must enclose it in quotes (“”). You can specify up to five patterns for each destination profile.
Step 13	**subscribe-to-alert-group all** **Example:** `Router(cfg-call-home-profile)#` **`subscribe-to-alert-group all`**	(Optional) Subscribes to all available alert groups. **Important** Entering this command causes the generation of a large number of syslog messages. We recommend that you subscribe to alert groups individually, using appropriate severity levels and patterns when possible.

Periodic Notification

When you subscribe a destination profile to either the Configuration, Inventory, or Snapshot alert group, you can choose to receive the alert group messages asynchronously or periodically at a specified time. The following time intervals are available:

- Daily—Specify the time of day to send, using an hour:minute format *hh:mm*, with a 24-hour clock (for example, 14:30).
- Weekly—Specify the day of the week and time of day in the format day *hh:mm*, where the day of the week is spelled out (for example, monday).
- Monthly—Specify the numeric date, from 1 to 31, and the time of day, in the format date *hh:mm*.
- Interval—Specifies the interval at which the periodic message is sent, from 1 to 60 minutes.
- Hourly—Specifies the minute of the hour at which the periodic message is sent, from 0 to 59 minutes.

Note Hourly and by interval periodic notifications are available for the Snapshot alert group only.

Message Severity Threshold

Call Home allows you to filter messages based on severity. You can associate each predefined or user-defined destination profile with a Call Home threshold from 0 (least urgent) to 9 (most urgent). The default is 0 (all messages are sent).

When you subscribe a destination profile to the Environment or Syslog alert group, you can set a threshold for relay of alert group messages based on the message severity level. Any message with a value lower than the destination profile threshold is not sent to the destination.

When you subscribe to an alert group in a destination profile with a specified severity, you subscribe to getting messages triggered by the events that have same or higher severity in that alert group.

Note Subscribing to syslog message at low severity level is not recommended, as it would trigger too many syslog messages that might lower the system performance.

Note Call Home severity levels are not the same as system message logging severity levels.

Table 2: Severity and Syslog Level Mapping

Smart Call Home Level	Keyword	syslog Level	Description
9	**catastrophic**	—	Network-wide catastrophic failure.
8	**disaster**	—	Significant network impact.
7	**fatal**	Emergency (0)	System is unusable.
6	**critical**	Alert (1)	Critical conditions that indicate that immediate attention is needed.
5	**major**	Critical (2)	Major conditions.
4	**minor**	Error (3)	Minor conditions.
3	**warning**	Warning (4)	Warning conditions.
2	**notification**	Notice (5)	Basic notification and informational messages. Possibly independently insignificant.
1	**normal**	Information (6)	Normal event signifying return to normal state.
0	**debugging**	Debug (7)	Debugging messages.

Syslog Pattern Matching

When you subscribe a destination profile to the Syslog alert group, you can optionally specify a text pattern to be matched within each syslog message. If you configure a pattern, a Syslog alert group message will be sent only if it contains the specified pattern and meets the severity threshold. If the pattern contains spaces, you must enclose it in quotes (" ") when configuring it. You can specify up to five patterns for each destination profile.

Configuring Snapshot Command List

To configure the snapshot command list, perform the following steps:

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device#` **`configure terminal`**	Enters global configuration mode.
Step 2	**call-home** **Example:** `Device(config)#` **`call-home`**	Enters Call Home configuration mode.
Step 3	[**no** | **default**] **alert-group-config snapshot** **Example:** `Device(cfg-call-home)#` **`alert-group-config snapshot`**	Enters snapshot configuration mode. The **no** or **default** command will remove all snapshot command.
Step 4	[**no** | **default**] **add-command** *command string* **Example:** `Device(cfg-call-home-snapshot)#` **`add-command`** *`"show version"`*	Adds the command to the Snapshot alert group. The **no** or **default** command will remove the corresponding command. • *command string* —IOS command. Maximum length is 128.
Step 5	**end** **Example:** `Device(cfg-call-home-snapshot)#` **`exit`**	Exits and saves the configuration.

Configuring General email Options

Configuring the Mail Server

To use the e-mail message transport, you must configure at least one Simple Mail Transfer Protocol (SMTP) e-mail server address. You can specify up to four backup e-mail servers, for a maximum of five total mail-server definitions.

Consider the following guidelines when configuring the mail server:

- Backup e-mail servers can be defined by repeating the **mail-server** command using different priority numbers.
- The **mail-server priority** *number* parameter can be configured from 1 to 100. The server with the highest priority (lowest priority number) is tried first.

To configure general email options, perform the following steps:

SUMMARY STEPS

1. **configure terminal**
2. **call-home**
3. **mail-server** { *ipv4-address* | *name* } **priority** *number*
4. **sender from** *email-address*
5. **sender reply-to** *email-address*
6. **source-interface** *interface-name*
7. **source-ip-address** *ipv4/ipv6 address*
8. **vrf** *vrf-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device#` **`configure terminal`**	Enters global configuration mode.
Step 2	**call-home** **Example:** `Device(config)#` **`call-home`**	Enters call home configuration mode.
Step 3	**mail-server** { *ipv4-address* | *name* } **priority** *number* **Example:** `Device(cfg-call-home)#` **`mail-server stmp.example.com priority 1`**	Assigns an email server address and its relative priority among configured email servers. Provide either of these: • The email server's IP address or • The email server's fully qualified domain name (FQDN) of 64 characters or less. Assign a priority number between 1 (highest priority) and 100 (lowest priority).

	Command or Action	Purpose
Step 4	**sender from** *email-address* **Example:** `Device(cfg-call-home)#` **`sender from username@example.com`**	(Optional) Assigns the e-mail address that will appear in the from field in Call Home e-mail messages. If no address is specified, the contact e-mail address is used.
Step 5	**sender reply-to** *email-address* **Example:** `Device(cfg-call-home)#` **`sender reply-to username@example.com`**	(Optional) Assigns the e-mail address that will appear in the reply-to field in Call Home e-mail messages.
Step 6	**source-interface** *interface-name* **Example:** `Device(cfg-call-home)#` **`source-interface loopback1`**	Assigns the source interface name to send call-home messages. *interface-name* —Source interface name. Maximum length is 64. **Note** For HTTP messages, use the **ip http client source-interface** *interface-name* command in global configuration mode to configure the source interface name. This allows all HTTP clients on the device to use the same source interface.
Step 7	**source-ip-address** *ipv4/ipv6 address* **Example:** `Device(cfg-call-home)#` **`ip-address 209.165.200.226`**	Assigns source IP address to send call-home messages. • *ipv4/ipv6 address* —Source IP (ipv4 or ipv6) address. Maximum length is 64.
Step 8	**vrf** *vrf-name* **Example:** `Device(cfg-call-home)#` **`vrf`** *`vpn1`*	(Optional) Specifies the VRF instance to send call-home email messages. If no vrf is specified, the global routing table is used. **Note** For HTTP messages, if the source interface is associated with a VRF, use the **ip http client source-interface** *interface-name* command in global configuration mode to specify the VRF instance that will be used for all HTTP clients on the device.

Specifying Rate Limit for Sending Call Home Messages

To specify the rate limit for sending Call Home messages, perform the following steps:

SUMMARY STEPS

1. **configure terminal**
2. **call-home**
3. **rate-limit** *number*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device#` **`configure terminal`**	Enters global configuration mode.
Step 2	**call-home** **Example:** `Device(config)#` **`call-home`**	Enters call home configuration mode.
Step 3	**rate-limit** *number* **Example:** `Device(cfg-call-home)#` **`rate-limit 40`**	Specifies a limit on the number of messages sent per minute. • *number* —Range 1 to 60. The default is 20.

Specifying HTTP Proxy Server

To specify an HTTP proxy server for sending Call Home HTTP(S) messages to a destination, perform the following steps:

SUMMARY STEPS

1. **configure terminal**
2. **call-home**
3. **http-proxy** {*ipv4-address* | *ipv6-address name*} *name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device#` **`configure terminal`**	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**call-home** **Example:** `Device(config)# call-home`	Enters call home configuration mode.
Step 3	**http-proxy** {*ipv4-address* | *ipv6-address name*} *name* **Example:** `Device(config)# http-proxy 10.1.1.1 port 1`	Specifies the proxy server for the HTTP request.

Enabling AAA Authorization to Run IOS Commands for Call Home Messages

To enable AAA authorization to run IOS commands that enable the collection of output for a Call Home message, perform the following steps:

SUMMARY STEPS

1. **configure terminal**
2. **call-home**
3. **aaa-authorization**
4. **aaa-authorization** [**username** *username*]

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	Example:
	`Device#`
	`configure terminal`
		Enters global configuration mode.

Step 2	**call-home**
	Example:
	`Device(config)#`
	`call-home`
		Enters call home configuration mode.

Step 3	**aaa-authorization**
	Example:
	`Device(cfg-call-home)#`
	`aaa-authorization`
		Enables AAA authorization.
		Note By default, AAA authorization is disabled for Call Home.

Step 4	**aaa-authorization** [**username** *username*]	Specifies the username for authorization.

	Command or Action	Purpose
	Example: `Device(cfg-call-home)#` **`aaa-authorization username`** *`username`*	• **username** *user* —Default username is callhome. Maximum length is 64.

Configuring Syslog Throttling

To enable or disable Call Home syslog message throttling and avoid sending repetitive Call Home syslog messages, perform the following steps:

SUMMARY STEPS

1. **configure terminal**
2. **call-home**
3. [**no**] **syslog-throttling**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device#` **`configure terminal`**	Enters global configuration mode.
Step 2	**call-home** **Example:** `Device(config)#` **`call-home`**	Enters call home configuration mode.
Step 3	[**no**] **syslog-throttling** **Example:** `Device(cfg-call-home)#` **`syslog-throttling`**	Enables or disables Call Home syslog message throttling and avoids sending repetitive Call Home syslog messages. By default, syslog message throttling is enabled.

Configuring Call Home Data Privacy

The **data-privacy** command scrubs data, such as passwords and IP addresses, from running configuration files to protect the privacy of customers. Enabling the **data-privacy** command can affect CPU utilization when scrubbing a large amount of data. Currently, **show** command output is not being scrubbed except for configuration messages in the **show running-config** all and show startup-config data.

SUMMARY STEPS

1. **configure terminal**
2. **call-home**
3. **data-privacy** { **level** {**normal** | **high** } | **hostname** }

DETAILED STEPS

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device#` **`configure terminal`**	Enters global configuration mode.
Step 2	**call-home** **Example:** `Device(config)#` **`call-home`**	Enters call home configuration mode.
Step 3	**data-privacy** { **level** {**normal**	**high** }	**hostname** } **Example:** `Device(cfg-call-home)#` **`data-privacy level high`**	Scrubs data from running configuration file to protect the privacy of the user. The default data-privacy level is normal. **Note** Enabling the data-privacy command can affect CPU utilization when scrubbing a large amount of data. • **normal** —Scrubs sensitive data such as passwords. • **high** —Scrubs all normal-level commands plus the IP domain name and IP address commands. • **hostname** —Scrubs all high-level commands plus the hostname command. **Note** Scrubbing the hostname from configuration messages can cause Smart Call Home processing failure on some platforms.

Sending Call Home Messages Manually

Sending a Call Home Test Message Manually

You can use the **call-home test** command to send a user-defined Call Home test message.

SUMMARY STEPS

1. **call-home test** [**“** *test-message* **”**] **profile** *name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**call-home test** [**“** *test-message* **”**] **profile** *name* **Example:** `Router#` **`call-home test profile profile1`**	Sends a test message to the specified destination profile. The user-defined test message text is optional, but must be enclosed in quotes (“ ”) if it contains spaces. If no user-defined message is configured, a default message is sent.

Sending Call Home Alert Group Messages Manually

Before you begin

- Only the snapshot, crash, configuration, and inventory alert groups can be sent manually. Syslog alert groups cannot be sent manually.
- When you manually trigger a snapshot, configuration, or inventory alert group message and you specify a destination profile name, a message is sent to the destination profile regardless of the profile's active status, subscription status, or severity setting.
- When you manually trigger a snapshot, configuration, or inventory alert group message and do not specify a destination profile name, a message is sent to all active profiles that have either a normal or periodic subscription to the specified alert group.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router>` **`enable`**	Enables privileged EXEC mode. • Enter your password, if prompted.
Step 2	**call-home send alert-group snapshot** [**profile** *name*] **Example:** `Router#` **`call-home send alert-group snapshot profile profile1`**	Sends a snapshot alert group message to one destination profile if specified, or to all subscribed destination profiles.
Step 3	**call-home send alert-group crash** [**profile** *name*] **Example:** `Router#` **`call-home send alert-group configuration profile profile1`**	Sends a crash alert group message to one destination profile if specified, or to all subscribed destination profiles.
Step 4	**call-home send alert-group configuration** [**profile** *name*] **Example:** `Router#` **`call-home send alert-group configuration profile profile1`**	Sends a configuration alert group message to one destination profile if specified, or to all subscribed destination profiles.

	Command or Action	Purpose
Step 5	**call-home send alert-group inventory** [**profile** *name*] **Example:** `Router# call-home send alert-group inventory`	Sends an inventory alert group message to one destination profile if specified, or to all subscribed destination profiles.

Submitting Call Home Analysis and Report Requests

You can use the **call-home request** command to submit information about your system to Cisco Systems to receive helpful analysis and report information specific to your system. You can request a variety of reports, including security alerts, known bugs, best practices, and command references.

Note the following guidelines when manually sending Call Home analysis and report requests:

- If a **profile** *name* is specified, the request is sent to the profile. If no profile is specified, the request is sent to the Cisco TAC profile. The recipient profile does not need to be enabled for the call-home request. The profile should specify the e-mail address where the transport gateway is configured so that the request message can be forwarded to the Cisco TAC and the user can receive the reply from the Smart Call Home service.
- The **ccoid** *user-id* is the registered identifier of the Smart Call Home user. If the *user-id* is specified, the response is sent to the e-mail address of the registered user. If no *user-id* is specified, the response is sent to the contact e-mail address of the device.
- Based on the keyword specifying the type of report requested, the following information is returned:
  - **config-sanity** —Information on best practices as related to the current running configuration.
  - **bugs-list** —Known bugs in the running version and in the currently applied features.
  - **command-reference** —Reference links to all commands in the running configuration.
  - **product-advisory** —Product Security Incident Response Team (PSIRT) notices, End of Life (EOL) or End of Sales (EOS) notices, or field notices (FN) that may affect devices in your network.

To submit a request for analysis and report information from the Cisco Output Interpreter tool, complete the following steps:

SUMMARY STEPS

1. **call-home request output-analysis** **“** *show-command* **”**
2. **call-home request** { **config-sanity** | **bugs-list** | **command-reference** | **product-advisory** }

DETAILED STEPS

	Command or Action	Purpose

Step 1	**call-home request output-analysis** **“** *show-command* **”**
	Example:
	`[`
	`profile`
		Sends the output of the specified **show** command for analysis. The **show** command must be contained in quotes (“”).

	Command or Action	Purpose
	name] [**ccoid** *user-id*] **Example:** Device# **call-home request output-analysis "show diag" profile TG**	
Step 2	**call-home request** { **config-sanity** | **bugs-list** | **command-reference** | **product-advisory** } **Example:** [**profile** *name*] [**ccoid** *user-id*] **Example:** Device# **call-home request config-sanity profile TG**	Sends the output of a predetermined set of commands, such as the **show running-config all** and **show version** commands, for analysis. In addition, the **call home request product-advisory** subcommand includes all inventory alert group commands. The keyword specified after the **call-home request** command specifies the type of report requested.

Manually Sending Command Output Message for One Command or a Command List

You can use the **call-home send** command to execute a CLI command and e-mail the command output to Cisco or to an e-mail address that you specify.

Note the following guidelines when sending the output of a command:

- The specified IOS command or list of IOS commands can be any run command, including commands for all modules. The command must be contained in quotes ("").
- If the email option is selected using the "email" keyword and an email address is specified, the command output is sent to that address. If neither the email nor the HTTP option is specified, the output is sent in long-text format with the specified service request number to the Cisco TAC (attach@cisco.com).
- If neither the "email" nor the "http" keyword is specified, the service request number is required for both long-text and XML message formats and is provided in the subject line of the email.

- If the HTTP option is specified without a profile name or destination URL, the CiscoTac-1 profile destination HTTP or HTTPS URL is used as the destination. The destination email address can be specified so that Smart Call Home can forward the message to the email address. The user must specify either the destination email address or an SR number but they can also specify both.
- If a profile is specified and the profile has callhome@cisco.com as one of its email destination, you must use XML as the message format. If you use long-text format, an error message is displayed.

To execute a command and send the command output, complete the following step:

Procedure

	Command or Action	Purpose
Step 1	Use one of the following commands: • **call-home send** {*cli command* | *cli list*} [**email** [**profile** *profile-name* | *email*] [**msg-format** {**long-text** | **xml**}]] [**tac-sevice-request** *SR#*] • **call-home send** {*cli command* | *cli list*} [**http** [**profile** *profile-name* | *URL-dest*] [**destination-email-address** *email*]] [**tac-sevice-request** *SR#*] **Example:** `Router# call-home send "show version;show running-config show inventory" email support@example.com msg-format xml`	Executes the CLI or CLI list and sends output via email or HTTP. • {*cli command* | *cli list*}—Specifies the IOS command or list of IOS commands (separated by ';'). It can be any run command, including commands for all modules. The commands must be contained in quotes (""). • **email** [**profile** *profile-name* | *email*] [**msg-format** {**long-text** | **xml**}]—If the email option is selected and a profile name is specified, the command output will be sent to the email address configured in the profile. If an email address is specified, the command output will be sent to the specified email address. The message is in long-text or XML format with the service request number in the subject. The profile name or email address, the service request number, or both must be specified. The service request number is required if the profile name or email address is not specified (default is attach@cisco.com for long-text format and callhome@cisco.com for XML format). • **http** [**profile** *profile-name* | *URL-dest*] [**destination-email-address** *email*] —If the http option is selected without a profile name or destination URL, the command output will be sent to Smart Call Home backend server (URL specified in TAC profile) in XML format. If a profile name or destination URL is specified, the command output will be sent to the destination URLs configured in the profile (profile-name case) or the destination URL specified in the command. **destination-email-address** *email* can be specified so that the backend server can forward the message to the email address. The email address, the service request number, or both must be specified.

	Command or Action	Purpose
		• **tac-service-request** *SR#*—Specifies the service request number. The service request number is required if the email address is not specified.

Configuring Diagnostic Signatures

The Diagnostic Signatures feature downloads digitally signed signatures to devices. Diagnostic Signatures (DS) files are formatted files that collate knowledge of diagnostic events and provide methods to troubleshoot them without a need to upgrade the Cisco software. The aim of DS is to deliver flexible intelligence that can detect and collect troubleshooting information that can be used to resolve known problems in customer networks.

Prerequisites for Diagnostic Signatures

Before you download and configure diagnostic signatures (DSes) on a device, you must ensure that the following conditions are met:

- You must assign a DS to the device. Refer to the "Diagnostic Signature Downloading" section for more information on how to assign DSes to devices.
- HTTP/Secure HTTP (HTTPS) transport is required for downloading DS files. You must install the certification authority (CA) certificate to enable the authentication of the destination HTTPS server.

Note If you configure the trustpool feature, the CA certificate is not required.

Information About Diagnostic Signatures

Diagnostic Signature Overview

Diagnostic signatures (DS) for the Call Home system provides a flexible framework that allows the defining of new events and corresponding CLIs that can analyze these events without upgrading the Cisco software.

DSs provide the ability to define more types of events and trigger types than the standard Call Home feature supports. The DS subsystem downloads and processes files on a device as well as handles callbacks for diagnostic signature events.

The Diagnostic Signature feature downloads digitally signed signatures that are in the form of files to devices. DS files are formatted files that collate the knowledge of diagnostic events and provide methods to troubleshoot these events.

DS files contain XML data to specify the event description, and these files include CLI commands or scripts to perform required actions. These files are digitally signed by Cisco or a third party to certify their integrity, reliability, and security.

The structure of a DS file can be one of the following formats

- Metadata-based simple signature that specifies the event type and contains other information that can be used to match the event and perform actions such as collecting information by using the CLI. The signature can also change configurations on the device as a workaround for certain bugs.
- Embedded Event Manager (EEM) Tool Command Language (Tcl) script-based signature that specifies new events in the event register line and additional action in the Tcl script.
- Combination of both the formats above.

The following basic information is contained in a DS file:

- ID (unique number)—unique key that represents a DS file that can be used to search a DS.
- Name (ShortDescription)—unique description of the DS file that can be used in lists for selection.
- Description—long description about the signature.
- Revision—version number, which increments when the DS content is updated.
- Event & Action—defines the event to be detected and the action to be performed after the event happens.

Diagnostic Signature Downloading

To download the diagnostic signature (DS) file, you require the secure HTTP (HTTPS) protocol. If you have already configured an email transport method to download files on your device, you must change your assigned profile transport method to HTTPS to download and use DS.

Cisco software uses a PKI Trustpool Management feature, which is enabled by default on devices, to create a scheme to provision, store, and manage a pool of certificates from known certification authorities (CAs). The trustpool feature installs the CA certificate automatically. The CA certificate is required for the authentication of the destination HTTPS servers.

There are two types of DS update requests to download DS files: regular and forced-download.

Regular download requests DS files that were recently updated. You can trigger a regular download request either by using a periodic configuration or by initiating an on-demand CLI. The regular download update happens only when the version of the requested DS is different from the version of the DS on the device. Periodic download is only started after there is any DS assigned to the device from DS web portal. After the assignment happens, the response to the periodic inventory message from the same device will include a field to notify device to start its periodic DS download/update. In a DS update request message, the status and revision number of the DS is included such that only a DS with the latest revision number is downloaded.

Forced-download downloads a specific DS or a set of DSes. You can trigger the forced-download update request only by initiating an on-demand CLI. In a force-download update request, the latest version of the DS file is downloaded irrespective of the current DS file version on the device.

The DS file is digitally signed, and signature verification is performed on every downloaded DS file to make sure it is from a trusted source.

Diagnostic Signature Signing

The diagnostic signature (DS) files are digitally signed before they are made available for downloading. The following methods are used for digitally signing DS files:

- Signing algorithm (Rivest Shamir and Adleman [RSA] 2048 bits)
- Request keypairs to Abraxas system, which is the digital signing client

- DS signed via secure socket layer (SSL) through a code signing client, where the signature is embedded using XML tags
- Public keys are embedded in the DS subsystem (Cisco signed, partner signed, third-party signed) in the Cisco software. The digitally signed DS file contains the product name such as Diagnostic_Signatures (Cisco signed), Diagnostic_Signatures_Partner, Diagnostic_Signatures_3rd_Party. The product names are only used to sign the DS files.

The digital signing client can be found at https://abraxas.cisco.com/SignEngine/submit.jsp

These conditions that must be met to verify the digital signature in a DS file:

- Code sign component support must be available in Cisco software.
- Various public keys that verify the different kinds of diagnostic signatures must be included in platforms where DS is supported.
- After parsing and retrieving the DS, the DS must execute the verification application program interface (API) to verify that the DS is valid.

Diagnostic Signature Workflow

The diagnostic signature feature is enabled by default in Cisco software. The following is the workflow for creating diagnostic signatures:

1. Find the DSs you want to download and assign them to the device. This step is mandatory for regular periodic download, but not required for forced download.
2. The device downloads all assigned DS(es) or a specific DS by regular periodic download or by on-demand forced download.
3. The device verifies the digital signature of every single DS. If verification passes, the device stores the DS file into a non-removable disk, such as bootflash or hard disk, so that DS files can be read after the device is reloaded. On the routers, the DS file is stored in the bootflash:/call home directory.
4. The device continues sending periodic regular DS download requests to get the latest revision of DS and replace the older one in device.
5. The device monitors the event and executes the actions defined in the DS when the event happens.

Diagnostic Signature Events and Actions

The events and actions sections are the key areas used in diagnostic signatures. The event section defines all event attributes that are used for event detection. The action section lists all actions which should be performed after the event happens, such as collecting **show** command outputs and sending them to Smart Call Home to parse.

Diagnostic Signature Event Detection

Event detection in a DS is defined in two ways: single event detection and multiple event detection.

Single Event Detection

In single event detection, only one event detector is defined within a DS. The event specification format is one of the following two types:

- DS event specification type: syslog, periodic, configuration, Online Insertion Removal (OIR) immediate, and callhome are the supported event types, where “immediate” indicates that this type of DS does not detect any events, its actions are performed once it is downloaded, and the call-home type modifies the current CLI commands defined for existing alert-group.
- The Embedded Event Manager (EEM) specification type: supports any new EEM event detector without having to modify the Cisco software.

  Other than using EEM to detect events, a DS is triggered when a Tool Command Language (Tcl) script is used to specify event detection types.

Multiple Event Detection

Multiple event detection involves defining two or more event detectors, two ore more corresponding tracked object states, and a time period for the events to occur. The specification format for multiple event detection can include complex event correlation for tracked event detectors. For example, three event detectors (syslog, OIR, and IPSLA) are defined during the creation of a DS file. The correlation that is specified for these event detectors is that the DS will execute its action if both syslog and OIR events are triggered simultaneously, or if IPSLA is triggered alone.

Diagnostic Signature Actions

The diagnostic signature (DS) file consists of various actions that must be initiated when an evnt occurs. The action type indicates the kind of action that will be initiated in response to a certain event.

Variables are elements within a DS file that are used to customize the files.

DS actions are categorized into the following five types:

- call-home
- command
- emailto
- script
- message

DS action types call-home and emailto collect event data and send a message to call-home servers or to the defined email addresses. The message uses "diagnostic-signature" as its message type and DS ID as the message sub-type.

The commands defined for the DS action type initiate CLI commands that can change configuration of the device, collect show command outputs, or run any EXEC command on the device. The DS action type script executes Tcl scripts.

DS action type message defines action to generate message to notify or remind user certain important information. The message could be broadcasted to all TTY lines or generated as a syslog entry.

Action Types

DS actions are categorized into the following four types:

- Call-home
- Command
- Emailto
- Script

DS action types call-home and emailto collect event data and send a message to call-home servers or to the defined email addresses. The message includes the following elements:

- Message type—diagnostic-signature
- Message subtype—ds-id
- Message description—event-id : ds name

The commands defined for the DS action type initiates CLI commands that can change configuration of the device. The DS action type script executes Tcl scripts.

Diagnostic Signature Variables

Variables are referenced within a DS and are used to customize the DS file. All DS variable names have the prefix ds_ to separate them from other variables. The following are the supported DS variable types:

- System variable: variables assigned automatically by the device without any configuration changes. The Diagnostic Signatures feature supports two system variables: ds_hostname and ds_signature_id.
- Environment variable: values assigned manually by using the **environment** *variable-name variable-value* command in call-home diagnostic-signature configuration mode. Use the **show call-home diagnostic-signature** command to display the name and value of all DS environment variables. If the DS file contains unresolved environment variables, this DS will stay in pending status until the variable gets resolved.
- Prompt variable: values assigned manually by using the **call-home diagnostic-signature install** *ds-id* command in privileged EXEC mode. If you do not set this value, the status of the DS indicates pending.
- Regular expression variable: values assigned from a regular expression pattern match with predefined CLI command outputs. The value is assigned during the DS run.
- Syslog event variable: values assigned during a syslog event detection in the DS file. This variable is valid only for syslog event detection.

How to Configure Diagnostic Signatures

Configuring the Service Call Home for Diagnostic Signatures

Configure the Service Call Home feature to set attributes such as the contact email address where notifications related with diagnostic signatures (DS) are sent and destination HTTP/secure HTTP (HTTPS) URL to download the DS files from.

You can also create a new user profile, configure correct attributes and assign it as the DS profile. For periodic downloads, the request is sent out just following full inventory message. By changing the inventory periodic configuration, the DS periodic download also gets rescheduled.

Note The predefined CiscoTAC-1 profile is enabled as a DS profile by default and Cisco recommends using it. If used, you only need to change the destination transport-method to the **http** setting.

Before you begin

Before you download and configure diagnostic signatures (DSs) on a device, you must ensure that the following conditions are met:

- You must assign one or more DSs to the device.
- HTTP/Secure HTTP (HTTPS) transport is required for downloading DS files. You must install the certification authority (CA) certificate to enable the authentication of the destination HTTPS server.

Note If you configure the trustpool feature, the CA certificate is not required.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**service call-home** **Example:** `Router(config)# service call-home`	Enables Call Home service on a device.
Step 4	**call-home** **Example:** `Router(config)# call-home`	Enters Call Home configuration mode.
Step 5	**contact-email-addr** *email-address* **Example:** `Router(cfg-call-home)# contact-email-addr username@example.com`	Assigns customer's e-mail address. You can enter a maximum of 200 characters in e-mail address format with no spaces. **Note** You can use any valid e-mail address. You cannot use spaces.
Step 6	**mail-server** { *ipv4-address* | *name* } **priority** *number* **Example:** `Router(cfg-call-home)# mail-server 10.1.1.1 priority 4`	(Optional) Configures a Simple Mail Transfer Protocol (SMTP) email server address for Call Home. This command is only used when sending email is part of the actions defined in any DS.
Step 7	**profile** *name* **Example:** `Router(cfg-call-home)# profile profile1`	Enters the Call Home destination profile configuration mode for the specified destination profile. If the specified destination profile does not exist, it is created.
Step 8	**destination transport-method** { **email** | **http** }	(Optional) Enables the message transport method.

	Command or Action	Purpose
	Example: `Router(cfg-call-home-profile)# destination transport-method email`	• **email** —Sets the e-mail message transport method. • **http** —Sets the HTTP message transport method. **Note** To configure diagnostic signatures, you must use the **http** option.
Step 9	**destination address** { **email** *email-address* | **http** *url* } **Example:** `Router(cfg-call-home-profile)# destination address http https://tools.cisco.com/its/service/oddce/services/DDCEService`	Configures the destination e-mail address or URL to which Call Home messages are sent. **Note** To configure diagnostic signatures, you must use the **http** option.
Step 10	**subscribe-to-alert-group inventory** [**periodic** { **daily** *hh:mm* | **monthly** *date hh:mm* | **weekly** *day hh:mm* }] **Example:** `Router(cfg-call-home-profile)# subscribe-to-alert-group inventory periodic daily 12:00`	Subscribes this destination profile to the Inventory alert group. The Inventory alert group can be configured for periodic notification **Note** This command is used only for the periodic downloading of DS files.

What to do next

Set the profile configured in the previous procedure as the DS profile and configure other DS parameters.

Configuring Diagnostic Signatures

Before you begin

Configure the Service Call Home feature to set attributes for the Call Home profile. You can either use the default CiscoTAC-1 profile or use the newly-created user profile.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**call-home** **Example:** `Router(config)# call-home`	Enters Call Home configuration mode.

	Command or Action	Purpose
Step 4	**diagnostic-signature** **Example:** `Router(cfg-call-home)# diagnostic-signature`	Enters call-home diagnostic signature mode.
Step 5	**profile** *ds-profile-name* **Example:** `Router(cfg-call-home-diag-sign)# profile user1`	Specifies the destination profile on a device that DS uses.
Step 6	**environment** *ds_env-var-name ds-env-var-value* **Example:** `Router(cfg-call-home-diag-sign)# environment ds_env1 envarval`	Sets the environment variable value for DS on a device.
Step 7	**end** **Example:** `Router(cfg-call-home-diag-sign)# end`	Exits call-home diagnostic signature mode and returns to privileged EXEC mode.
Step 8	**call-home diagnostic-signature** { { **deinstall** | **download** } { *ds-id* | **all** } | **install** *ds-id* } **Example:** `Router# call-home diagnostic-signature download 6030`	Downloads, installs, and uninstalls diagnostic signature files on a device.
Step 9	**show call-home diagnostic-signature** [*ds-id* [**actions** | **events** | **prerequisite** | **prompt** | **variables**] | **failure** | **statistics** [download]] **Example:** `Router# show call-home diagnostic-signature actions`	Displays the call-home diagnostic signature information.

Verifying the Call Home Configuration

- **show call-home** —Displays the Call Home configuration summary.

  Following is a sample output of the command:

```
Router# show call-home

Current call home settings:
    call home feature : enable
    call home message's from address: Not yet set up
    call home message's reply-to address: Not yet set up

    vrf for call-home messages: Not yet set up

    contact person's email address: sch-smart-licensing@cisco.com (default)

    contact person's phone number: Not yet set up
    street address: Not yet set up
```

```
    customer ID: Not yet set up
    contract ID: Not yet set up
    site ID: Not yet set up

    source ip address: Not yet set up
    source interface: TenGigabitEthernet4/1/1
    Mail-server[1]: Address: 173.36.13.143 Priority: 60
    http proxy: Not yet set up

    Diagnostic signature: enabled
    Profile: CiscoTAC-1 (status: ACTIVE)

    Smart licensing messages: enabled
    Profile: CiscoTAC-1 (status: ACTIVE)

    aaa-authorization: disable
    aaa-authorization username: callhome (default)
    data-privacy: normal
    syslog throttling: enable

    Rate-limit: 20 message(s) per minute

    Snapshot command[0]: show cable modem summary totalb
    Snapshot command[1]: show cable modem summary total

Available alert groups:
    Keyword                  State   Description
    ------------------------ ------- --------------------------------
    configuration            Enable  configuration info
    crash                    Enable  crash and traceback info
    diagnostic               Enable  diagnostic info
    environment              Enable  environmental info
    inventory                Enable  inventory info
    snapshot                 Enable  snapshot info
    syslog                   Enable  syslog info

Profiles:
    Profile Name: CiscoTAC-1
    Profile Name: test
```

- **show call-home detail**—Displays the Call Home configuration in detail.

  Following is a sample output of the command:

```
Router# show call-home detail

Current call home settings:
    call home feature : enable
    call home message's from address: Not yet set up
    call home message's reply-to address: Not yet set up

    vrf for call-home messages: Not yet set up

    contact person's email address: sch-smart-licensing@cisco.com (default)

    contact person's phone number: Not yet set up
    street address: Not yet set up
    customer ID: Not yet set up
    contract ID: Not yet set up
    site ID: Not yet set up

    source ip address: Not yet set up
    source interface: TenGigabitEthernet4/1/1
    Mail-server[1]: Address: 173.36.13.143 Priority: 60
```

```
    http proxy: Not yet set up

    Diagnostic signature: enabled
    Profile: CiscoTAC-1 (status: ACTIVE)

    Smart licensing messages: enabled
    Profile: CiscoTAC-1 (status: ACTIVE)

    aaa-authorization: disable
    aaa-authorization username: callhome (default)
    data-privacy: normal
    syslog throttling: enable

    Rate-limit: 20 message(s) per minute

    Snapshot command[0]: show cable modem summary totalb
    Snapshot command[1]: show cable modem summary total

Available alert groups:
    Keyword                  State   Description
    ------------------------ ------- --------------------------------
    configuration            Enable  configuration info
    crash                    Enable  crash and traceback info
    diagnostic               Enable  diagnostic info
    environment              Enable  environmental info
    inventory                Enable  inventory info
    snapshot                 Enable  snapshot info
    syslog                   Enable  syslog info

Profiles:

Profile Name: CiscoTAC-1
    Profile status: ACTIVE
    Profile mode: Anonymous Reporting Only
    Reporting Data: Smart Call Home, Smart Licensing
    Preferred Message Format: xml
    Message Size Limit: 3145728 Bytes
    Transport Method: http
    Email address(es): callhome@cisco.com
    HTTP  address(es): https://tools.cisco.com/its/service/oddce/services/DDCEService

    Periodic configuration info message is scheduled every 17 day of the month at 09:39


    Periodic inventory info message is scheduled every 17 day of the month at 09:24

    Alert-group              Severity
    ------------------------ ------------
    crash                    debug
    diagnostic               minor
    environment              minor
    inventory                normal

    Syslog-Pattern           Severity
    ------------------------ ------------
    .*                       major
```

- **show call-home alert-group** —Displays the available alert groups and their status.

  Following is a sample output of the command:

```
Router# show call-home alert-group

Available alert groups:
```

```
Keyword                  State   Description
------------------------ ------- ------------------------------
configuration            Enable  configuration info
crash                    Enable  crash and traceback info
diagnostic               Enable  diagnostic info
environment              Enable  environmental info
inventory                Enable  inventory info
snapshot                 Enable  snapshot info
syslog                   Enable  syslog info
```

- **show call-home mail-server status**—Checks and displays the availability of the configured email servers.

  Following is a sample output of the command:

```
Router# show call-home mail-server status

    Mail-server[1]: Address: 173.36.13.143 Priority: 60
```

- **show call-home profile** {**all** | *name*} —Displays the configuration of the specified destination profile. Use the keyword **all** to display the configuration of all destination profiles.

  Following is a sample output of the command:

```
Router# show call-home profile CiscoTac-1

Profile Name: CiscoTAC-1
    Profile status: ACTIVE
    Profile mode: Full Reporting
    Reporting Data: Smart Call Home, Smart Licensing
    Preferred Message Format: xml
    Message Size Limit: 3145728 Bytes
    Transport Method: email
    Email address(es): callhome@cisco.com
    HTTP  address(es): http://10.22.183.117:8080/ddce/services/DDCEService

    Periodic configuration info message is scheduled every 17 day of the month at 09:39


    Periodic inventory info message is scheduled every 17 day of the month at 09:24

    Alert-group              Severity
    -----------------------  ------------
    crash                    debug
    diagnostic               minor
    environment              minor
    inventory                normal

    Syslog-Pattern           Severity
    -----------------------  ------------
    .*                       major
```

- **show call-home statistics** [**detail** | **profile** *profile-name*]—Displays the statistics of Call Home events.

  Following is a sample output of the command:

```
Router# show call-home statistics

Message Types    Total                Email                HTTP
-------------   -------------------- -------------------- ------------------
Total Success   4                    3                    1
```

```
    Config      1                   1                   0
    Crash       0                   0                   0
    Diagnostic  0                   0                   0
    Environment 0                   0                   0
    Inventory   1                   0                   1
    Snapshot    0                   0                   0
    SysLog      2                   2                   0
    Test        0                   0                   0
    Request     0                   0                   0
    Send-CLI    0                   0                   0
    SCH         0                   0                   0

Total In-Queue  0                   0                   0
    Config      0                   0                   0
    Crash       0                   0                   0
    Diagnostic  0                   0                   0
    Environment 0                   0                   0
    Inventory   0                   0                   0
    Snapshot    0                   0                   0
    SysLog      0                   0                   0
    Test        0                   0                   0
    Request     0                   0                   0
    Send-CLI    0                   0                   0
    SCH         0                   0                   0

Total Failed    0                   0                   0
    Config      0                   0                   0
    Crash       0                   0                   0
    Diagnostic  0                   0                   0
    Environment 0                   0                   0
    Inventory   0                   0                   0
    Snapshot    0                   0                   0
    SysLog      0                   0                   0
    Test        0                   0                   0
    Request     0                   0                   0
    Send-CLI    0                   0                   0
    SCH         0                   0                   0

Total Ratelimit
      -dropped  0                   0                   0
    Config      0                   0                   0
    Crash       0                   0                   0
    Diagnostic  0                   0                   0
    Environment 0                   0                   0
    Inventory   0                   0                   0
    Snapshot    0                   0                   0
    SysLog      0                   0                   0
    Test        0                   0                   0
    Request     0                   0                   0
    Send-CLI    0                   0                   0
    SCH         0                   0                   0

Last call-home message sent time: 2015-03-06 18:21:49 GMT+00:00
```

- **show call-home diagnostic-signature**—Displays the configuration of diagnostic signature information.

  Following is a sample output of the command:

```
Router# show call-home diagnostic-signature

Current diagnostic-signature settings:
 Diagnostic-signature: enabled
 Profile: CiscoTAC-1 (status: ACTIVE)
 Environment variable:
```

```
            Not yet set up

Downloaded DSes:
                                                                Last Update
DS ID    DS Name                          Revision Status     (GMT-05:00)
-------- ------------------------------- -------- ---------- -------------------
```

- **show call-home version**—Displays the Call Home version information.

  Following is a sample output of the command:

```
Router# show call-home version

Call-Home Version 3.0
Component Version:
 call-home: (rel4)1.0.15
 eem-call-home: (rel2)1.0.5
```

Configuration Example for Call Home

Example: Call Home Configuration

Following is a configuration example for configuring the HTTPS transport :

```
ip host tools.cisco.com 72.163.4.38
vrf definition smart-vrf
 !
 address-family ipv4
 exit-address-family
 !
 address-family ipv6
 exit-address-family
!
interface TenGigabitEthernet4/1/1
 vrf forwarding smart-vrf
 ip address 172.22.11.25 255.255.255.128
 no ip proxy-arp
!
ip route vrf smart-vrf 72.163.4.38 255.255.255.255 172.22.11.1
!
ip http client source-interface TenGigabitEthernet4/1/1
!
```

Following is a configuration example for configuring email options:

```
call-home
 mail-server 173.36.13.143 priority 60
 source-interface TenGigabitEthernet4/1/1
 vrf smart-vrf
 alert-group-config snapshot
  add-command "show cable modem summary total"
 profile "test"
  active
  destination transport-method email
```

```
  destination address email call-home@cisco.com
  subscribe-to-alert-group configuration
  subscribe-to-alert-group crash
  subscribe-to-alert-group diagnostic severity debug
  subscribe-to-alert-group environment severity debug
  subscribe-to-alert-group inventory
  subscribe-to-alert-group syslog severity major pattern .*
  subscribe-to-alert-group syslog severity notification pattern "^.+UPDOWN.+changed state
to (down|up)$"
  subscribe-to-alert-group snapshot periodic daily 12:00
!
ip route vrf smart-vrf 173.36.13.143 255.255.255.255 172.22.11.1
!
```

Example: Configuring HTTP Transport for Call Home on the Cisco cBR Series Router

Step 1 Back up the current running configuration file.

Step 2 Verify the built-in router certificates.

Example:

```
Router# show crypto pki trustpool | include Class 3 Public

    ou=Class 3 Public Primary Certification Authority
    ou=Class 3 Public Primary Certification Authority
```

Step 3 (Optional) Configure VRF.

Example:

```
Router(config)# vrf def smart-vrf
Router(config-vrf)# address-family ipv4
Router(config-vrf-af)# exit-address-family
Router(config-vrf)# address-family ipv6
Router(config-vrf-af)# exit-address-family
```

Step 4 Set up the network interface.

Example:

```
Router(config)# interface TenGigabitEthernet4/1/1
Router(config)# vrf forward smart-vrf
Router(config-if)# ip address 172.22.11.25 255.255.255.128
Router(config-if)# no ip proxy-arp
Router(config-if)# no shut
```

Note If IPv6 is enabled, you must configure IPv6 address.

Step 5 Set up the Cisco portal.

Example:

```
Router(config)# ip host tools.cisco.com 72.163.4.38
Router(config)# ip route vrf smart-vrf 72.163.4.38 255.255.255.255 172.22.11.1
```

Step 6 Verify the data path.

Example:

```
!Verify the connectivity to TenGigabitEthernet4/1/1 interface
Router# ping vrf smart-vrf 172.22.11.25

!Verify the connectivity to TenGigabitEthernet4//1/1 gateway
Router# ping vrf smart-vrf 172.22.11.1

!Verify the connectivity to tools.cisco.com
Router# ping vrf smart-vrf 72.163.4.38
```

Step 7 Configure the HTTP client interface.

Example:

```
Router(config)# ip http client source-interface TenGigabitEthernet4/1/1
```

Step 8 Send the Call Home alert group message manually and verify the configuration.

Example:

```
Router# call-home send alert inventory profile CiscoTAC-1

Sending inventory info call-home message ...
Please wait. This may take some time ...

Router# show call-home statistics | include Total
Message Types    Total               Email               HTTP
Total Success   0                   0                   0
Total In-Queue  1                   0                   1
Total Failed    0                   0                   0
Total Ratelimit

Router# show call-home statistics | include Total
Message Types    Total               Email               HTTP
Total Success   1                   0                   1
Total In-Queue  0                   0                   0
Total Failed    0                   0                   0
Total Ratelimit
```

Step 9 Display the Call Home configuration.

Example:

```
Router# show call-home profile CiscoTAC-1

Profile Name: CiscoTAC-1
    Profile status: ACTIVE
    Profile mode: Full Reporting
    Reporting Data: Smart Call Home, Smart Licensing
    Preferred Message Format: xml
    Message Size Limit: 3145728 Bytes
    Transport Method: http
    Email address(es): callhome@cisco.com
    HTTP  address(es): https://tools.cisco.com/its/service/oddce/services/DDCEService

    Periodic configuration info message is scheduled every 15 day of the month at 15:37

    Periodic inventory info message is scheduled every 15 day of the month at 15:22
Alert-group               Severity
    ------------------------  ------------
    crash                     debug
```

```
diagnostic                minor
environment               minor
inventory                 normal

Syslog-Pattern            Severity
------------------------  ------------
.*                        major
```

Example: Configuring Email Transport for Call Home on the Cisco cBR Series Router

Step 1 Back up the current running configuration file.

Step 2 (Optional) Configure VRF.

Example:

```
Router(config)# vrf def smart-vrf
Router(config-vrf)# address-family ipv4
Router(config-vrf-af)# exit-address-family
Router(config-vrf)# address-family ipv6
Router(config-vrf-af)# exit-address-family
```

Step 3 Set up the network interface.

Example:

```
Router(config)# interface TenGigabitEthernet4/1/1
Router(config)# vrf forward smart-vrf
Router(config-if)# ip address 172.22.11.25 255.255.255.128
Router(config-if)# no ip proxy-arp
Router(config-if)# no shut
```

Note If IPv6 is enabled, you must configure IPv6 address.

Step 4 Verify the data path.

Example:

```
!Verify the connectivity to TenGigabitEthernet4/1/1 interface
Router# ping vrf smart-vrf 172.22.11.25

!Verify the connectivity to TenGigabitEthernet4//1/1 gateway
Router# ping vrf smart-vrf 172.22.11.1

!Verify the connectivity to tools.cisco.com
Router# ping vrf smart-vrf 72.163.4.38
```

Step 5 (Optional) Configure Call Home.

Example:

```
Router(config)# call-home
```

```
!Configure the TenGigabitEthernet 4/1/1
Router(cfg-call-home)# source-ip-address 172.22.11.25
```

Step 6 Configure the mail server and verify the configuration.

Example:

```
Router(config)# call-home
Router(cfg-call-home)# mail-server 173.36.13.143 priority 60
Router(cfg-call-home)# vrf smart-vrf
Router(cfg-call-home)# exit
Router(config)# ip route vrf smart-vrf 173.36.13.143 255.255.255.255 172.22.11.1
Router(config)# end

Router# ping vrf smart-vrf 173.36.13.143
…

Router# show call-home mail status

Please wait. Checking for mail server status ...

Mail-server[1]: Address: 173.36.13.143 Priority: 60 [Available]
```

Note The VRF configuration is optional.

Step 7 Create a new destination profile and subscribe to alert group.

Example:

```
Router(config)# call-home
Router(cfg-call-home)# alert-group-config snapshot
Router(cfg-call-home-snapshot)# add-command "show cable modem summary total”
Router(cfg-call-home-snapshot)# exit
Router(cfg-call-home)# profile test
Router(cfg-call-home-profile)# active
Router(cfg-call-home-profile)# destination transport-method email
Router(cfg-call-home-profile)# destination address email xyz@company.com
Router(cfg-call-home-profile)# subscribe syslog severity notification pattern "^.+UPDOWN.+changed
state to (down|up)$”
Router(cfg-call-home-profile)# subscribe-to-alert-group snapshot periodic daily 12:00
Router(cfg-call-home-profile)# end
```

Step 8 Send the Call Home alert group message manually and verify the configuration.

Example:

```
Router# call-home send alert-group inventory profile test
Sending inventory info call-home message ...
Please wait. This may take some time ...

Router# show call-home statistics | include Total
Message Types    Total               Email               HTTP
Total Success   1                   0                   1
Total In-Queue  2                   2                   0
Total Failed    0                   0                   0
Total Ratelimit

Router# show call-home statistics | include Total
Message Types    Total               Email               HTTP
Total Success   3                   2                   1
Total In-Queue  0                   0                   0
Total Failed    0                   0                   0
```

```
Total Ratelimit
```

Step 9 Display the Call Home configuration.

Example:

```
Router# show call-home profile test

Profile Name: test
    Profile status: ACTIVE
    Profile mode: Full Reporting
    Reporting Data: Smart Call Home
    Preferred Message Format: xml
    Message Size Limit: 3145728 Bytes
    Transport Method: email
    Email address(es): abcd@company.com
    HTTP  address(es): Not yet set up

    Periodic snapshot info message is scheduled daily at 12:00

    Alert-group               Severity
    ------------------------  ------------
    configuration             normal
    crash                     debug
    diagnostic                debug
    environment               debug
    inventory                 normal
Syslog-Pattern            Severity
    ------------------------  ------------
    ^.+UPDOWN.+changed state
     to (down|up)$            notification
```

Default Settings

Table 3: Default Call Home Parameters

Parameters	Default
Call Home feature status	Enabled
User-defined profile status	Active
Predefined CiscoTAC-1 profile status	Active
Transport method	HTTP
Message format type	XML
Alert group status	Enabled
Call Home message severity threshold	Debug
Message rate limit for messages per minute	20

Parameters	Default
AAA authorization	Disabled
Call Home syslog message throttling	Enabled
Data privacy level	Normal

Alert Groups Trigger Events and Commands

The table below lists the supported alert groups and the default command output included in Call Home messages generated for the alert group.

Table 4: Call Home Alert Groups, Events, and Actions

Alert Group	Call Home Trigger Event	Syslog Event	Severity	Description and Executed Commands
Configuration	—	—	**normal** **periodic**	Periodic events related to configuration sent monthly. Commands executed: • **show platform** • **show version** • **show inventory** • **show running-config all** • **show startup-config**

Alert Group	Call Home Trigger Event	Syslog Event	Severity	Description and Executed Commands
Crash	—	—	**debug**	Events generated by a crash on the router, such as Supervisor or line card crash. Commands executed: Crash traceback • **show version** • **show logging** • **show region** • **show stack** Crash system • **show version** • **show inventory** • **show logging** • **show region** • **show stack** • **more crashinfo-file** Crash module • **show version** • **show inventory** • **show platform** • **show logging** • **show region** • **show stack** • **more crashinfo-file**

Alert Group	Call Home Trigger Event	Syslog Event	Severity	Description and Executed Commands
Diagnostic	—	—	**minor**	Events generated by diagnostics. Commands executed: • **show platform** • **show version** • **show diagnostic event slot detail** • **show inventory** • **show buffers** • **show logging** • **show diagnostic events slot all**
Environmental	FAN_FAILURE	CBR_PEM-6-FANOK CBR_PEM-3-FANFAIL	**minor**	Events related to power, fan, and environment sensing elements, such as temperature alarms. Commands executed: • **show platform** • **show environment** • **show inventory** • **show logging**
	TEMPERATURE_ALARM	ENVIRONMENTAL-1-ALERT		
	POWER_SUPPLY_FAILURE	CBR_PEM-6-PEMOK CBR_PEM-3-PEMFAIL		

Alert Group	Call Home Trigger Event	Syslog Event	Severity	Description and Executed Commands
Inventory	OIR_REMOVE OIR_INSERTION	—	**normal**	Inventory status that is provided whenever a unit is cold booted, or when FRUs are inserted or removed. This alert is considered a non-critical event, and the information is used for status and entitlement. Command executed: • **show platform** • **show version** • **show inventory oid** • **show diag all eeprom detail** • **show interfaces** • **show file systems** • **show bootflash: all** • **show data-corruption** • **show memory statistics** • **show process memory** • **show process cpu** • **show process cpu history** • **show license udi** • **show license detail** • **show buffers** • **show platform software proc slot monitor cycle**
Snapshot	—	—	**normal**	User-generated CLI commands.
Syslog	—	—	**major**	Events generated by Syslog messages. Commands executed: • **show inventory** • **show logging**

Alert Group	Call Home Trigger Event	Syslog Event	Severity	Description and Executed Commands
Test	—	—	**normal**	User-generated test message sent to the destination profile. Commands executed: • **show inventory** • **show platform** • **show version**

Message Contents

Smart Call Home supports the following message formats:

- Short Text Message Format
- Common Fields for Full Text and XML Messages
- Fields Specific to Alert Group Messages for Full Text and XML Messages
- Inserted Fields for a Reactive and Proactive Event Message
- Inserted Fields for an Inventory Event Message
- Inserted Fields for a User-Generated Test Message

The table below describes the short text formatting option for all message types.

Table 5: Short Text Message Format

Data Item	Description
Device identification	Configured device name
Date/time stamp	Time stamp of the triggering event
Error isolation message	Plain English description of triggering event
Alarm urgency level	Error level such as that applied to system message

The table below describes the first set of common event message fields for full text or XML messages.

Table 6: Common Fields for Full Text and XML Messages

Data Item (Plain Text and XML)	Description (Plain Text and XML)	Call-Home Message Tag (XML Only)
Time stamp	Date and time stamp of event in ISO time notation: *YYYY-MM-DD HH:MM:SS GMT+HH:MM.*	CallHome/EventTime
Message name	Name of message.	For short text message only
Message type	Name of message type, specifically "Call Home".	CallHome/Event/Type
Message subtype	Specific type of message: full, delta, test	CallHome/Event/SubType
Message group	Name of alert group, specifically "reactive". Optional, because default is "reactive". .	For long-text message only
Severity level	Severity level of message	Body/Block/Severity
Source ID	Product type for routing through the workflow engine. This is typically the product family name.	For long-text message only
Device ID	Unique device identifier (UDI) for the end device that generated the message. This field should be empty if the message is nonspecific to a device. The format is *type@Sid@serial*. • *type* is the product model number from the backplane IDPROM. • @ is a separator character. • *Sid* is C, identifying the serial ID as a chassis serial number· • *serial* is the number identified by the Sid field. An example is WS-C6509@C@12345678	CallHome/CustomerData/ContractData/DeviceId
Customer ID	Optional user-configurable field used for contract information or other ID by any support service.	CallHome/CustomerData/ContractData/CustomerId
Contract ID	Optional user-configurable field used for contract information or other ID by any support service.	CallHome/CustomerData/ContractData/ContractId

Data Item (Plain Text and XML)	Description (Plain Text and XML)	Call-Home Message Tag (XML Only)
Site ID	Optional user-configurable field used for Cisco-supplied site ID or other data meaningful to alternate support service.	CallHome/CustomerData/ContractData/SiteId
Server ID	If the message is generated from the device, this is the unique device identifier (UDI) of the device. The format is *type@Sid@serial*. • *type* is the product model number from the backplane IDPROM. • @ is a separator character. • *Sid* is C, identifying the serial ID as a chassis serial number. • *serial* is the number identified by the Sid field. An example is WS-C6509@C@12345678.	For long text message only
Message description	Short text that describes the error.	CallHome/MessageDescription
Device name	Node that experienced the event (hostname of the device).	CallHome/CustomerData/SystemInfo/NameName
Contact name	Name of person to contact for issues associated with the node that experienced the event.	CallHome/CustomerData/SystemInfo/Contact
Contact e-mail	E-mail address of person identified as the contact for this unit.	CallHome/CustomerData/SystemInfo/ContactEmail
Contact phone number	Phone number of the person identified as the contact for this unit.	CallHome/CustomerData/SystemInfo/ContactPhoneNumber
Street address	Optional field that contains the street address for RMA part shipments associated with this unit.	CallHome/CustomerData/SystemInfo/StreetAddress
Model name	Model name of the device (the specific model as part of a product family name).	CallHome/Device/Cisco_Chassis/Model
Serial number	Chassis serial number of the unit.	CallHome/Device/Cisco_Chassis/SerialNumber
Chassis part number	Top assembly number of the chassis.	/aml/body/chassis/partNo
System object ID	System Object ID that uniquely identifies the system.	CallHome/Device/Cisco_Chassis/ AdditionalInformation/AD@name=“sysObjectID”
System description	System description for the managed element.	CallHome/Device/Cisco_Chassis/ AdditionalInformation/AD@name=“sysDescr”

The table below describes the fields specific to alert group messages for full text and XML. These fields may be repeated if multiple commands are executed for an alert group.

Table 7: Fields Specific to Alert Group Messages for Full Text and XML Messages

Data Item (Plain Text and XML)	Description (Plain Text and XML)	XML Tag (XML Only)
Command output name	Exact name of the issued command.	/aml/attachments/attachment/name
Attachment type	Specific command output.	/aml/attachments/attachment/type
MIME type	Either plain text or encoding type.	/aml/attachments/attachment/mime
Command output text	Output of command automatically executed.	/mml/attachments/attachment/atdata

The table below describes the reactive and proactive event message format for full text or XML messages.

Table 8: Inserted Fields for a Reactive and Proactive Event Message

Data Item (Plain Text and XML)	Description (Plain Text and XML)	XML Tag (XML Only)
Chassis hardware version	Hardware version of chassis.	/aml/body/chassis/hwVersion
Supervisor module software version	Top-level software version.	/aml/body/chassis/swVersion
Affected FRU name	Name of the affected FRU that is generating the event message.	/aml/body/fru/name
Affected FRU serial number	Serial number of the affected FRU.	/aml/body/fru/serialNo
Affected FRU part number	Part number of the affected FRU.	/aml/body/fru/partNo
FRU slot	Slot number of the FRU that is generating the event message.	/aml/body/fru/slot
FRU hardware version	Hardware version of the affected FRU.	/aml/body/fru/hwVersion
FRU software version	Software version(s) that is running on the affected FRU.	/aml/body/fru/swVersion

The table below describes the inventory event message format for full text or XML messages.

Table 9: Inserted Fields for an Inventory Event Message

Data Item (Plain Text and XML)	Description (Plain Text and XML)	XML Tag (XML Only)
Chassis hardware version	Hardware version of the chassis.	/aml/body/chassis/hwVersion
Supervisor module software version	Top-level software version.	/aml/body/chassis/swVersion
FRU name	Name of the affected FRU that is generating the event message.	/aml/body/fru/name
FRU s/n	Serial number of the FRU.	/aml/body/fru/serialNo
FRU part number	Part number of the FRU.	/aml/body/fru/partNo
FRU slot	Slot number of the FRU.	/aml/body/fru/slot

Data Item (Plain Text and XML)	Description (Plain Text and XML)	XML Tag (XML Only)
FRU hardware version	Hardware version of the FRU.	/aml/body/fru/hwVersion
FRU software version	Software version(s) that is running on the FRU.	/aml/body/fru/swVersion

The table below describes the user-generated test message format for full text or XML.

Table 10: Inserted Fields for a User-Generated Test Message

Data Item (Plain Text and XML)	Description (Plain Text and XML)	XML Tag (XML Only)
Process ID	Unique process ID.	/aml/body/process/id
Process state	State of process (for example, running or halted).	/aml/body/process/processState
Process exception	Exception or reason code.	/aml/body/process/exception

Sample syslog Alert Notification in XML Format

```
<?xml version="1.0" encoding="UTF-8"?>
<soap-env:Envelope
xmlns:soap-env="http://www.w3.org/2003/05/soap-envelope">
<soap-env:Header>
<aml-session:Session
xmlns:aml-session="http://www.cisco.com/2004/01/aml-session"
soap-env:mustUnderstand="true"
soap-env:role="http://www.w3.org/2003/05/soap-envelope/role/next">
<aml-session:To>http://tools.cisco.com/neddce/services/DDCEService</aml
-session:To>
<aml-session:Path>
<aml-session:Via>http://www.cisco.com/appliance/uri</aml-session:Via>
</aml-session:Path>
<aml-session:From>http://www.cisco.com/appliance/uri</aml-session:From>
<aml-session:MessageId>MA:FXS1739Q0NR:548F4417</aml-session:MessageId>
</aml-session:Session>
</soap-env:Header>
<soap-env:Body>
<aml-block:Block
xmlns:aml-block="http://www.cisco.com/2004/01/aml-block">
<aml-block:Header>
<aml-block:Type>http://www.cisco.com/2005/05/callhome/syslog</aml-block
:Type>
<aml-block:CreationDate>2014-12-16 04:27:03
GMT+08:00</aml-block:CreationDate>
<aml-block:Builder>
<aml-block:Name>CBR8</aml-block:Name>
<aml-block:Version>2.0</aml-block:Version>
</aml-block:Builder>
<aml-block:BlockGroup>
<aml-block:GroupId>GB:FXS1739Q0NR:548F4417</aml-block:GroupId>
<aml-block:Number>0</aml-block:Number>
<aml-block:IsLast>true</aml-block:IsLast>
<aml-block:IsPrimary>true</aml-block:IsPrimary>
<aml-block:WaitForPrimary>false</aml-block:WaitForPrimary>
</aml-block:BlockGroup>
<aml-block:Severity>6</aml-block:Severity>
</aml-block:Header>
<aml-block:Content>
```

```
<ch:CallHome xmlns:ch="http://www.cisco.com/2005/05/callhome"
version="1.0">
<ch:EventTime>2014-12-16 04:26:59 GMT+08:00</ch:EventTime>
<ch:MessageDescription>Dec 16 04:26:59.885 CST: %ENVIRONMENTAL-1-ALERT:
Temp: INLET, Location: 6, State: Critical, Reading: 53
Celsius</ch:MessageDescription> <ch:Event> <ch:Type>syslog</ch:Type>
<ch:SubType></ch:SubType> <ch:Brand>Cisco Systems</ch:Brand>
<ch:Series>CBR8 Series Routers</ch:Series> </ch:Event>
<ch:CustomerData> <ch:UserData> <ch:Email>xxxx@company.com</ch:Email>
</ch:UserData>
<ch:ContractData>
<ch:CustomerId></ch:CustomerId>
<ch:SiteId></ch:SiteId>
<ch:ContractId></ch:ContractId>
<ch:DeviceId>CBR-8-CCAP-CHASS@C@FXS1739Q0NR</ch:DeviceId>
</ch:ContractData>
<ch:SystemInfo>
<ch:Name>sig-cbr</ch:Name>
<ch:Contact></ch:Contact>
<ch:ContactEmail>xxxx@company.com</ch:ContactEmail>
<ch:ContactPhoneNumber></ch:ContactPhoneNumber>
<ch:StreetAddress></ch:StreetAddress>
</ch:SystemInfo>
<ch:CCOID></ch:CCOID>
</ch:CustomerData>
<ch:Device>
<rme:Chassis xmlns:rme="http://www.cisco.com/rme/4.0">
<rme:Model>CBR-8-CCAP-CHASS</rme:Model>
<rme:HardwareVersion>0.1</rme:HardwareVersion>
<rme:SerialNumber>FXS1739Q0NR</rme:SerialNumber>
<rme:AdditionalInformation>
<rme:AD name="PartNumber" value="000-00000-00" /> <rme:AD
name="SoftwareVersion" value="15.5(20141214:005145) " /> <rme:AD
name="SystemObjectId" value="1.3.6.1.4.1.9.1.2141" /> <rme:AD
name="SystemDescription" value="Cisco IOS Software, IOS-XE Software
(X86_64_LINUX_IOSD-ADVENTERPRISEK9-M), Experimental Version
15.5(20141214:005145) [ece5_throttle_ios-ram-ece5-bk 105] Copyright (c)
1986-2014 by Cisco Systems, Inc.
Compiled Sun 14-Dec-14 00:20 by ram" /> <rme:AD name="ServiceNumber"
value="" /> <rme:AD name="ForwardAddress" value="" />
</rme:AdditionalInformation> </rme:Chassis> </ch:Device> </ch:CallHome>
</aml-block:Content> <aml-block:Attachments> <aml-block:Attachment
type="inline"> <aml-block:Name>show inventory</aml-block:Name>
<aml-block:Data encoding="plain"> <![CDATA[show inventory Load for five
secs: 2%/0%; one minute: 2%; five minutes: 2% Time source is NTP,
04:27:02.278 CST Tue Dec 16 2014
NAME: "Chassis", DESCR: "Cisco cBR-8 CCAP Chassis"
PID: CBR-8-CCAP-CHASS  , VID: V01, SN: FXS1739Q0NR

NAME: "sup 0", DESCR: "Cisco cBR CCAP Supervisor Card"
PID: CBR-CCAP-SUP-160G , VID: V01, SN: CAT1736E05L

NAME: "harddisk 4/1", DESCR: "Hard Disk"
PID: UGB88RTB100HE3-BCU-DID, VID:    , SN: 11000072780

NAME: "sup-pic 4/1", DESCR: "Cisco cBR CCAP Supervisor Card PIC"
PID: CBR-SUPPIC-8X10G  , VID: V01, SN: CAT1735E004

NAME: "SFP+ module 4/1/0", DESCR: "iNSI xcvr"
PID: SFP+ 10GBASE-SR   , VID: A   , SN: FNS1727294V

NAME: "SFP+ module 4/1/1", DESCR: "iNSI xcvr"
PID: SFP+ 10GBASE-SR   , VID: A   , SN: FNS172727WZ
```

```
NAME: "SFP+ module 4/1/4", DESCR: "iNSI xcvr"
PID: 10GE ZR           , VID:     , SN: AGM120525EW

NAME: "sup 1", DESCR: "Cisco cBR CCAP Supervisor Card"
PID: CBR-CCAP-SUP-160G , VID: V01, SN: CAT1736E05L

NAME: "clc 6", DESCR: "Cisco cBR CCAP Line Card"
PID: CBR-CCAP-LC-40G   , VID: V01, SN: CAT1736E0EN

NAME: "Cable PHY Module", DESCR: "CLC Downstream PHY Module 6/0"
PID: cBR-8-GEMINI      , VID: V01 , SN: CSJ13152101

NAME: "Cable PHY Module", DESCR: "CLC Upstream PHY Module 6/2"
PID: cBR-8-LEOBEN      , VID: V01 , SN: TST98765432

NAME: "Power Supply Module 0", DESCR: "Cisco cBR CCAP AC Power Supply"
PID: PWR-3KW-AC-V2     , VID: V02, SN: DTM173702KQ

NAME: "Power Supply Module 2", DESCR: "Cisco cBR CCAP AC Power Supply"
PID: PWR-3KW-AC-V2     , VID: V02, SN: DTM173702GD


sig-cbr#]]></aml-block:Data>
</aml-block:Attachment>
<aml-block:Attachment type="inline">
<aml-block:Name>show logging</aml-block:Name> <aml-block:Data
encoding="plain"> <![CDATA[show logging Load for five secs: 2%/0%; one
minute: 2%; five minutes: 2% Time source is NTP, 04:27:02.886 CST Tue
Dec 16 2014

Syslog logging: enabled (0 messages dropped, 51 messages rate-limited,
0 flushes, 0 overruns, xml disabled, filtering disabled)

No Active Message Discriminator.



No Inactive Message Discriminator.


    Console logging: level debugging, 213 messages logged, xml disabled,
                     filtering disabled
    Monitor logging: level debugging, 0 messages logged, xml disabled,
                     filtering disabled
    Buffer logging:  level debugging, 262 messages logged, xml disabled,
                    filtering disabled
    Exception Logging: size (4096 bytes)
    Count and timestamp logging messages: disabled
    Persistent logging: disabled

No active filter modules.

    Trap logging: level informational, 209 message lines logged
        Logging Source-Interface:       VRF Name:

Log Buffer (1000000 bytes):

*Dec 15 20:20:16.188: Rommon debug: debugFlagsStr[7], flags[0x7] *Dec
15 20:20:16.188: TRACE - Debug flag set 0x7 *Dec 15 20:20:16.188: TRACE
- Register NV N:systemInitByEvent V:True with no CallBack *Dec 15
20:20:16.188: TRACE - Register NV N:routingReadyByEvent V:True with no
CallBack *Dec 15 20:20:16.188: TRACE - Smart agent init started.
Version=1.2.0_dev/22
*Dec 15 20:20:16.188: ERROR - PD init failed: The requested operation
```

```
is not supported *Dec 15 20:20:16.188: ERROR - Pre Role Init Failed:
The requested operation is not supported *Dec 15 20:20:16.188: TRACE -
Smart agent init Done. status 10, state 4294967295, init 0 enable 0
Current Role Invalid *Dec 15 20:20:16.188: TRACE - Shutdown Started
*Dec 15 20:20:16.188: DEBUG - Scheduler shutdown start *Dec 15
20:20:16.188: ERROR - Failed to set shutdown watched boolean (code
Invalid argument (22)). Going the hard way!!!
*Dec 15 20:20:16.188: DEBUG - Destroying XOS stuff to exit dispatch
loop *Dec 15 20:20:16.188: DEBUG - XDM dispatch loop about to exit *Dec
15 20:20:16.188: DEBUG - Scheduler shutdown end *Dec 15 20:20:16.188:
ERROR - SmartAgent not initialized.
*Dec 15 20:20:16.188: ERROR - Smart Agent not a RF client *Dec 15
20:20:16.188: ERROR - Smart Agent not a CF client *Dec 15 20:20:16.188:
TRACE - Setting Ha Mgmt Init FALSE *Dec 15 20:20:16.188: TRACE -
Shutting down Any Role *Dec 15 20:20:17.432: (DBMS RPHA) Client
initialization; status=success *Dec 15 20:20:17.432: CABLE Parser
Trace:  cable_parser_init:82 *Dec 15 20:20:17.774: ****
mcprp_ubr_punt_init: Initialized*****
-->RF_STATUS_SEND_RF_STATE received-->RF_PROG_INITIALIZATION received
*Dec 15 20:20:20.790: CWAN OIR debugging enabled (ROMMON variable
DEBUG_CWAN_OIR set)-->RF_PROG_ACTIVE_FAST
received-->RF_PROG_ACTIVE_DRAIN
received-->RF_PROG_ACTIVE_PRECONFIG
received-->received-->RF_PROG_ACTIVE_POSTCONFIG
received-->RF_PROG_ACTIVE received
*Dec 15 20:20:20.841: **** IPC port 0x1000E created!
*Dec 15 20:20:20.841:  **** CIPC RP Server created UBRCCE_CIPC_14/0 !
*Dec 15 20:20:28.294: %SPANTREE-5-EXTENDED_SYSID: Extended SysId
enabled for type vlan *Dec 15 20:20:31.944: %VOICE_HA-7-STATUS: CUBE
HA-supported platform detected.
*Dec 15 20:20:33.391:  instant_msg_handle_proc_sup started!!
*Dec 15 20:20:33.391:  queue_msg_handle_proc_sup started!!
*Dec 15 20:20:35.603: %IOSXE_MGMTVRF-6-CREATE_SUCCESS_INFO: Management
vrf Mgmt-intf created with ID 1, ipv4 table-id 0x1, ipv6 table-id
0x1E000001
*Dec 15 20:20:34.513: %IOSXE-6-PLATFORM: CLC4: cpp_cp: Process
CPP_PFILTER_EA_EVENT__API_CALL__REGISTER
*Dec 15 20:20:03.806: %HW_PFU-3-PFU_IDPROM_CORRUPT: R0/0: cmand:  The
PEM/FM idprom could be read, but is corrupt in slot P11 The system will
run without environmental monitoring for this component *Dec 15
20:20:09.012: %SYSTEM-3-SYSTEM_SHELL_LOG: R0/0:  2014/12/15
20:20:08 : <anon>
*Dec 15 20:20:13.919: %IOSXE-4-PLATFORM: R0/0: kernel: astro: FD open
*Dec 15 20:20:13.919: %IOSXE-4-PLATFORM: R0/0: kernel: astro: astro:
mmio_start=d0000000 mmio_len=2000000
*Dec 15 20:20:13.919: %IOSXE-4-PLATFORM: R0/0: kernel: astro: Done
astro Memory map base_ptr ffffc90016600000, astro_reg_ptr ffffc90016600000...
*Dec 15 20:20:16.259: %IOSXE-4-PLATFORM: R0/0: kernel: astro: FD open
*Dec 15 20:20:16.553: %CPPHA-7-START: F0: cpp_ha:  CPP 0 preparing
ucode *Dec 15 20:20:17.220: %CPPHA-7-START: F0: cpp_ha:  CPP 0 startup
init *Dec 15 20:20:18.549: %PMAN-3-PROC_EMPTY_EXEC_FILE: F0: pvp.sh:
Empty executable used for process iosdb *Dec 15 20:20:20.003:
%PMAN-3-PROC_EMPTY_EXEC_FILE: CLC4: pvp.sh:  Empty executable used for
process iosdb *Dec 15 20:20:20.783: %PMAN-3-PROC_EMPTY_EXEC_FILE: CLC4:
pvp.sh:  Empty executable used for process iosdb *Dec 15 20:20:24.061:
%HW_PFU-3-PFU_IDPROM_CORRUPT: R0/0: cmand:  The PEM/FM idprom could be
read, but is corrupt in slot P11 The system will run without
environmental monitoring for this component *Dec 15 20:20:31.722:
%CPPHA-7-START: F0: cpp_ha:  CPP 0 running init *Dec 15 20:20:32.070:
%CPPHA-7-READY: F0: cpp_ha:  CPP 0 loading and initialization complete
*Dec 15 20:20:36.528 UTC: TRACE - Platform EventCB invoked. EventType:
8 *Dec 15 20:20:36.528 UTC: DEBUG - Hostname changed. Old:sig-cbr
New:sig-cbr *Dec 15 20:20:36.528 UTC: %CNS IQ:0.1 ID:0
Changed:[sig-cbr] *Dec 15 20:20:36.528 UTC: %CNS IQ:0.2 ID:1
```

```
Changed:[sig-cbr] *Dec 15 20:20:36.528 UTC: %CNS IQ:0.3 ID:2
Changed:[sig-cbr] *Dec 15 20:20:36.594 UTC: %SYS-5-LOG_CONFIG_CHANGE:
Buffer logging: level debugging, xml disabled, filtering disabled, size
(1000000) *Dec 16 04:20:36.597 CST: %SYS-6-CLOCKUPDATE: System clock
has been updated from 20:20:36 UTC Mon Dec 15 2014 to 04:20:36 CST Tue
Dec 16 2014, configured from console by console.
*Dec 16 04:20:36.607 CST: spa_type 2946 ports 8 *Dec 16 04:20:36.622
CST: spa_type 2946 ports 8 *Dec 16 04:20:37.350 CST:
cmts_set_int_us_qos_flags: move US-QOS flags 0 to CDMAN *Dec 16
04:20:37.350 CST: cmts_set_int_us_default_weights: move US-QOS weights
to CDMAN *Dec 16 04:20:36.625 CST: %IOSXE-4-PLATFORM: R0/0: kernel:
astro: FD open *Dec 16 04:20:43.221 CST: %LINEPROTO-5-UPDOWN: Line
protocol on Interface Video6/0/0, changed state to up *Dec 16
04:20:43.223 CST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Video6/0/1, changed state to up *Dec 16 04:20:43.502 CST: % Redundancy
mode change to SSO

*Dec 16 04:20:43.502 CST: %VOICE_HA-7-STATUS: NONE->SSO; SSO mode will
not take effect until after a platform
reload.-->RF_STATUS_REDUNDANCY_MODE_CHANGE received *Dec 16
04:20:44.220 CST: %SYS-5-CONFIG_I: Configured from memory by console
*Dec 16 04:20:44.228 CST: %IOSXE_OIR-6-INSCARD: Card (rp) inserted in
slot R1 *Dec 16 04:20:44.229 CST: %IOSXE_OIR-6-INSCARD: Card (fp)
inserted in slot F0 *Dec 16 04:20:44.229 CST: %IOSXE_OIR-6-ONLINECARD:
Card (fp) online in slot F0 *Dec 16 04:20:44.263 CST:
%IOSXE_OIR-6-INSCARD: Card (fp) inserted in slot F1 *Dec 16
04:20:44.263 CST: %IOSXE_OIR-6-INSCARD: Card (cc) inserted in slot 4
*Dec 16 04:20:44.263 CST: %IOSXE_OIR-6-ONLINECARD: Card (cc) online in
slot 4 *Dec 16 04:20:44.264 CST: %IOSXE_OIR-6-INSCARD: Card (cc)
inserted in slot 5 *Dec 16 04:20:44.264 CST: %IOSXE_OIR-6-INSCARD: Card
(cc) inserted in slot 6 *Dec 16 04:20:44.330 CST: %IOSXE_OIR-6-INSSPA:
SPA inserted in subslot 4/1 *Dec 16 04:20:44.751 CST: %SYS-5-RESTART:
System restarted -- Cisco IOS Software, IOS-XE Software
(X86_64_LINUX_IOSD-ADVENTERPRISEK9-M), Experimental Version
15.5(20141214:005145) [ece5_throttle_ios-ram-ece5-bk 105] Copyright (c)
1986-2014 by Cisco Systems, Inc.
Compiled Sun 14-Dec-14 00:20 by ram
*Dec 16 04:20:44.775 CST: %XML-SRVC: Security Enforcement XML
Service(111) OK. PID=574
*Dec 16 04:20:44.775 CST: %SSH-5-ENABLED: SSH 1.99 has been enabled
*Dec 16 04:20:45.453 CST: %LINK-3-UPDOWN: Interface GigabitEthernet0,
changed state to up *Dec 16 04:20:45.543 CST: %LINK-5-CHANGED:
Interface TenGigabitEthernet4/1/2, changed state to administratively
down *Dec 16 04:20:45.546 CST: %LINK-5-CHANGED: Interface
TenGigabitEthernet4/1/3, changed state to administratively down *Dec 16
04:20:45.548 CST: %LINK-5-CHANGED: Interface TenGigabitEthernet4/1/4,
changed state to administratively down *Dec 16 04:20:45.551 CST:
%LINK-5-CHANGED: Interface TenGigabitEthernet4/1/5, changed state to
administratively down *Dec 16 04:20:45.571 CST: %LINK-5-CHANGED:
Interface TenGigabitEthernet4/1/6, changed state to administratively
down *Dec 16 04:20:45.574 CST: %LINK-5-CHANGED: Interface
TenGigabitEthernet4/1/7, changed state to administratively down *Dec 16
04:20:45.576 CST: %LINK-5-CHANGED: Interface TenGigabitEthernet5/1/0,
changed state to administratively down *Dec 16 04:20:45.578 CST:
%LINK-5-CHANGED: Interface TenGigabitEthernet5/1/1, changed state to
administratively down *Dec 16 04:20:45.580 CST: %LINK-5-CHANGED:
Interface TenGigabitEthernet5/1/2, changed state to administratively
down *Dec 16 04:20:45.582 CST: %LINK-5-CHANGED: Interface
TenGigabitEthernet5/1/3, changed state to administratively down *Dec 16
04:20:45.584 CST: %LINK-5-CHANGED: Interface TenGigabitEthernet5/1/4,
changed state to administratively down *Dec 16 04:20:45.586 CST:
%LINK-5-CHANGED: Interface TenGigabitEthernet5/1/5, changed state to
administratively down *Dec 16 04:20:45.588 CST: %LINK-5-CHANGED:
Interface TenGigabitEthernet5/1/6, changed state to administratively
```

```
down *Dec 16 04:20:45.590 CST: %LINK-5-CHANGED: Interface
TenGigabitEthernet5/1/7, changed state to administratively down *Dec 16
04:20:45.596 CST: %LINK-3-UPDOWN: Interface Integrated-Cable6/0/0:0,
changed state to down *Dec 16 04:20:45.602 CST: %LINK-3-UPDOWN:
Interface Integrated-Cable6/0/0:1, changed state to down *Dec 16
04:20:45.603 CST: %LINK-3-UPDOWN: Interface Integrated-Cable6/0/0:2,
changed state to down *Dec 16 04:20:45.604 CST: %LINK-3-UPDOWN:
Interface Integrated-Cable6/0/0:3, changed state to down *Dec 16
04:20:45.606 CST: %LINK-3-UPDOWN: Interface Integrated-Cable6/0/0:4,
changed state to down *Dec 16 04:20:45.607 CST: %LINK-3-UPDOWN:
Interface Integrated-Cable6/0/0:5, changed state to down *Dec 16
04:20:45.608 CST: %LINK-3-UPDOWN: Interface Integrated-Cable6/0/0:6,
changed state to down *Dec 16 04:20:45.610 CST: %LINK-3-UPDOWN:
Interface Integrated-Cable6/0/0:7, changed state to down *Dec 16
04:20:45.648 CST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Bundle1, changed state to up *Dec 16 04:20:45.649 CST: %LINK-3-UPDOWN:
Interface Bundle1, changed state to up *Dec 16 04:20:45.649 CST:
%LINK-3-UPDOWN: Interface Cable6/0/0, changed state to down *Dec 16
04:20:45.649 CST: %SNMP-5-LINK_DOWN: LinkDown:Interface
Cable6/0/0 changed state to down
*Dec 16 04:20:45.666 CST: %LINK-3-UPDOWN: Interface
Wideband-Cable6/0/0:0, changed state to down *Dec 16 04:20:45.666 CST:
%LINK-3-UPDOWN: Interface Wideband-Cable6/0/0:1, changed state to down
*Dec 16 04:20:45.681 CST: %LINK-3-UPDOWN: Interface
Wideband-Cable6/0/0:2, changed state to down *Dec 16 04:20:45.681 CST:
%LINK-3-UPDOWN: Interface Wideband-Cable6/0/0:3, changed state to down
*Dec 16 04:20:45.681 CST: %LINK-3-UPDOWN: Interface
Wideband-Cable6/0/0:4, changed state to down *Dec 16 04:20:45.681 CST:
%LINK-3-UPDOWN: Interface Wideband-Cable6/0/0:5, changed state to down
*Dec 16 04:20:45.682 CST: %LINK-3-UPDOWN: Interface
Wideband-Cable6/0/0:6, changed state to down *Dec 16 04:20:45.682 CST:
%LINK-3-UPDOWN: Interface Wideband-Cable6/0/0:7, changed state to down
*Dec 16 04:20:45.685 CST: %LINK-3-UPDOWN: Interface
Integrated-Cable6/0/1:0, changed state to down *Dec 16 04:20:45.694
CST: %LINK-3-UPDOWN: Interface Integrated-Cable6/0/1:1, changed state
to down *Dec 16 04:20:45.694 CST: %LINK-3-UPDOWN: Interface Cable6/0/1,
changed state to down *Dec 16 04:20:45.694 CST: %SNMP-5-LINK_DOWN:
LinkDown:Interface
Cable6/0/1 changed state to down
*Dec 16 04:20:45.699 CST: %LINK-3-UPDOWN: Interface
Wideband-Cable6/0/1:0, changed state to down *Dec 16 04:20:45.703 CST:
%LINK-3-UPDOWN: Interface Wideband-Cable6/0/1:1, changed state to down
*Dec 16 04:20:45.706 CST: %LINK-3-UPDOWN: Interface
Integrated-Cable6/0/1:2, changed state to down *Dec 16 04:20:45.707
CST: %LINK-3-UPDOWN: Interface Integrated-Cable6/0/1:3, changed state
to down *Dec 16 04:20:45.709 CST: %LINK-3-UPDOWN: Interface
Wideband-Cable6/0/2:0, changed state to down *Dec 16 04:20:46.469 CST:
%SNMP-5-COLDSTART: SNMP agent on host sig-cbr is undergoing a cold
start *Dec 16 04:20:46.472 CST: %LINEPROTO-5-UPDOWN: Line protocol on
Interface GigabitEthernet0, changed state to up *Dec 16 04:20:46.543
CST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
TenGigabitEthernet4/1/2, changed state to down *Dec 16 04:20:46.546
CST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
TenGigabitEthernet4/1/3, changed state to down *Dec 16 04:20:46.548
CST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
TenGigabitEthernet4/1/4, changed state to down *Dec 16 04:20:46.551
CST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
TenGigabitEthernet4/1/5, changed state to down *Dec 16 04:20:46.571
CST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
TenGigabitEthernet4/1/6, changed state to down *Dec 16 04:20:46.574
CST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
TenGigabitEthernet4/1/7, changed state to down *Dec 16 04:20:46.576
CST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
TenGigabitEthernet5/1/0, changed state to down *Dec 16 04:20:46.578
```

```
CST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
TenGigabitEthernet5/1/1, changed state to down *Dec 16 04:20:46.580
CST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
TenGigabitEthernet5/1/2, changed state to down *Dec 16 04:20:46.582
CST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
TenGigabitEthernet5/1/3, changed state to down *Dec 16 04:20:46.584
CST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
TenGigabitEthernet5/1/4, changed state to down *Dec 16 04:20:46.586
CST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
TenGigabitEthernet5/1/5, changed state to down *Dec 16 04:20:46.588
CST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
TenGigabitEthernet5/1/6, changed state to down *Dec 16 04:20:46.590
CST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
TenGigabitEthernet5/1/7, changed state to down *Dec 16 04:20:46.641
CST: %SYS-6-BOOTTIME: Time taken to reboot after reload =  374 seconds
*Dec 16 04:20:53.697 CST: %IOSXE-1-PLATFORM: R0/0: kernel: Raptor MAC
image download wrote 55917152 bytes *Dec 16 04:21:23.432 CST:
%TRANSCEIVER-6-INSERTED: CLC4: iomd:
transceiver module inserted in TenGigabitEthernet4/1/0 *Dec 16
04:21:23.435 CST: %TRANSCEIVER-6-INSERTED: CLC4: iomd:
transceiver module inserted in TenGigabitEthernet4/1/1 *Dec 16
04:21:23.440 CST: %TRANSCEIVER-6-INSERTED: CLC4: iomd:
transceiver module inserted in TenGigabitEthernet4/1/4 *Dec 16
04:21:29.430 CST: %CBRDTI-5-DTISLOT: DTI slot 4/1: card role changed to
Active

*Dec 16 04:21:29.454 CST: %SPA_OIR-6-ONLINECARD: SPA (CBR-SUPPIC-8X10G)
online in subslot 4/1 *Dec 16 04:21:31.403 CST: %LINK-3-UPDOWN:
Interface TenGigabitEthernet4/1/0, changed state to up *Dec 16
04:21:31.405 CST: %CBR_SPA-7-RAPTOR_ESI_EGRESS_HDR_LO_INTERRUPT:
CLC4: iomd:  LOCAL RAPTOR, DP 0, channel_not_found_err *Dec 16
04:21:31.412 CST: %LINK-3-UPDOWN: Interface TenGigabitEthernet4/1/1,
changed state to up *Dec 16 04:21:32.403 CST: %LINEPROTO-5-UPDOWN: Line
protocol on Interface TenGigabitEthernet4/1/0, changed state to up *Dec
16 04:21:32.412 CST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
TenGigabitEthernet4/1/1, changed state to up *Dec 16 04:21:41.171 CST:
%IOSXE-3-PLATFORM: R0/0: kernel: i801_smbus
0000:00:1f.3: Transaction timeout
*Dec 16 04:21:41.174 CST: %IOSXE-3-PLATFORM: R0/0: kernel:
/nobackup/ram/ece5-bk/binos/os/linux/drivers/binos/i2c/max3674/max3674_
mai n.c:show_reg_pll (line 88): show_reg_pll failed *Dec 16
04:21:58.237 CST: %IOSXE-5-PLATFORM: CLC6: cdman: Basestar FPGA rev_id
0x00000002, fpga_rev_id 0x00000032 *Dec 16 04:21:59.074 CST:
%CMRP-3-BAD_ID_HW: R0/0: cmand:  Failed Identification Test in CBR
linecard. The module linecard slot 6 in this router may not be a
genuine Cisco product. Cisco warranties and support programs only apply
to genuine Cisco products. If Cisco determines that your insertion of
non-Cisco memory, WIC cards, AIM cards,  Network Modules, SPA cards,
GBICs or other modules into a  Cisco product is the cause of a support
issue, Cisco may  deny support under your warranty or under a Cisco
support  pro *Dec 16 04:21:59.075 CST: %IOSXE_OIR-6-ONLINECARD: Card
(cc) online in slot 6 *Dec 16 04:22:08.825 CST:
%ASR1000_INFRA-3-EOBC_SOCK: CLC6:
ubrclc-k9lc-ms:  Socket event for  EO6/0/1, fd 11, failed to bind;
Address already in use success *Dec 16 04:22:09.605 CST:  SNMP IPC
session up(RP <-> slot 6)!
*Dec 16 04:22:09.605 CST:  CMTS IPC session up!
*Dec 16 04:22:14.564 CST: %SNMP-5-LINK_UP: LinkUp:Interface
Cable6/0/0-upstream0 changed state to up *Dec 16 04:22:14.565 CST:
%SNMP-5-LINK_UP: LinkUp:Interface
Cable6/0/0-upstream1 changed state to up *Dec 16 04:22:14.566 CST:
%SNMP-5-LINK_UP: LinkUp:Interface
Cable6/0/2-upstream0 changed state to up *Dec 16 04:22:14.566 CST:
%SNMP-5-LINK_UP: LinkUp:Interface
```

```
Cable6/0/2-upstream1 changed state to up *Dec 16 04:22:15.051 CST:
%SNMP-5-LINK_UP: LinkUp:Interface Cable6/0/0 changed state to up *Dec
16 04:22:15.258 CST: %SNMP-5-LINK_UP: LinkUp:Interface Cable6/0/1
changed state to up *Dec 16 04:22:15.258 CST: %SNMP-5-LINK_UP:
LinkUp:Interface Cable6/0/2 changed state to up *Dec 16 04:22:15.259
CST: %SNMP-5-LINK_UP: LinkUp:Interface Cable6/0/3 changed state to up
*Dec 16 04:22:15.259 CST: %SNMP-5-LINK_UP: LinkUp:Interface Cable6/0/4
changed state to up *Dec 16 04:22:15.411 CST: %SNMP-5-LINK_UP:
LinkUp:Interface Cable6/0/5 changed state to up *Dec 16 04:22:15.411
CST: %SNMP-5-LINK_UP: LinkUp:Interface Cable6/0/6 changed state to up
*Dec 16 04:22:15.411 CST: %SNMP-5-LINK_UP: LinkUp:Interface Cable6/0/7
changed state to up *Dec 16 04:22:15.411 CST: %SNMP-5-LINK_UP:
LinkUp:Interface Cable6/0/8 changed state to up *Dec 16 04:22:15.432
CST: %SNMP-5-LINK_UP: LinkUp:Interface Cable6/0/9 changed state to up
*Dec 16 04:22:15.432 CST: %SNMP-5-LINK_UP: LinkUp:Interface Cable6/0/10
changed state to up *Dec 16 04:22:15.433 CST: %SNMP-5-LINK_UP:
LinkUp:Interface Cable6/0/11 changed state to up *Dec 16 04:22:15.433
CST: %SNMP-5-LINK_UP: LinkUp:Interface Cable6/0/12 changed state to up
*Dec 16 04:22:15.433 CST: %SNMP-5-LINK_UP: LinkUp:Interface Cable6/0/13
changed state to up *Dec 16 04:22:15.433 CST: %SNMP-5-LINK_UP:
LinkUp:Interface Cable6/0/14 changed state to up *Dec 16 04:22:15.433
CST: %SNMP-5-LINK_UP: LinkUp:Interface Cable6/0/15 changed state to up
*Dec 16 04:22:15.677 CST: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Cable6/0/8, changed state to up *Dec 16 04:22:15.678 CST:
%LINEPROTO-5-UPDOWN: Line protocol on Interface Cable6/0/9, changed
state to up *Dec 16 04:22:15.901 CST: %LINEPROTO-5-UPDOWN: Line
protocol on Interface Cable6/0/10, changed state to up *Dec 16
04:22:15.902 CST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Cable6/0/11, changed state to up *Dec 16 04:22:15.902 CST:
%LINEPROTO-5-UPDOWN: Line protocol on Interface Cable6/0/12, changed
state to up *Dec 16 04:22:15.903 CST: %LINEPROTO-5-UPDOWN: Line
protocol on Interface Cable6/0/13, changed state to up *Dec 16
04:22:15.903 CST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Cable6/0/14, changed state to up *Dec 16 04:22:15.904 CST:
%LINEPROTO-5-UPDOWN: Line protocol on Interface Cable6/0/15, changed
state to up *Dec 16 04:22:17.046 CST: %LINEPROTO-5-UPDOWN: Line
protocol on Interface Cable6/0/0, changed state to up *Dec 16
04:22:17.047 CST: %LINK-3-UPDOWN: Interface Cable6/0/0, changed state
to up *Dec 16 04:22:17.256 CST: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Cable6/0/1, changed state to up *Dec 16 04:22:17.257 CST:
%LINK-3-UPDOWN: Interface Cable6/0/1, changed state to up *Dec 16
04:22:17.259 CST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Cable6/0/2, changed state to up *Dec 16 04:22:17.260 CST:
%LINK-3-UPDOWN: Interface Cable6/0/2, changed state to up *Dec 16
04:22:17.260 CST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Cable6/0/3, changed state to up *Dec 16 04:22:17.260 CST:
%LINK-3-UPDOWN: Interface Cable6/0/3, changed state to up *Dec 16
04:22:17.260 CST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Cable6/0/4, changed state to up *Dec 16 04:22:17.260 CST:
%LINK-3-UPDOWN: Interface Cable6/0/4, changed state to up *Dec 16
04:22:17.411 CST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Cable6/0/5, changed state to up *Dec 16 04:22:17.411 CST:
%LINK-3-UPDOWN: Interface Cable6/0/5, changed state to up *Dec 16
04:22:17.411 CST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Cable6/0/6, changed state to up *Dec 16 04:22:17.411 CST:
%LINK-3-UPDOWN: Interface Cable6/0/6, changed state to up *Dec 16
04:22:17.411 CST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Cable6/0/7, changed state to up *Dec 16 04:22:17.412 CST:
%LINK-3-UPDOWN: Interface Cable6/0/7, changed state to up *Dec 16
04:22:16.714 CST: %IOSXE-5-PLATFORM: CLC6: cdman: DS-JIB:ILK Interrupts
Enabled. (Init:20539, Check:9566 1stPKO:8942) *Dec 16 04:22:17.809 CST:
%CMRP-3-IDPROM_SENSOR: R0/0: cmand:  One or more sensor fields from the
idprom failed to parse properly because Invalid argument.
Dec 16 04:22:57.161 CST: %SNMP-5-LINK_DOWN: LinkDown:Interface
```

```
Integrated-Cable6/0/0-downstream0 changed state to down Dec 16
04:22:57.161 CST: %SNMP-5-LINK_DOWN: LinkDown:Interface
Integrated-Cable6/0/0-downstream1 changed state to down Dec 16
04:22:57.161 CST: %SNMP-5-LINK_DOWN: LinkDown:Interface
Integrated-Cable6/0/0-downstream2 changed state to down Dec 16
04:22:57.162 CST: %SNMP-5-LINK_DOWN: LinkDown:Interface
Integrated-Cable6/0/0-downstream3 changed state to down Dec 16
04:22:57.162 CST: %SNMP-5-LINK_DOWN: LinkDown:Interface
Integrated-Cable6/0/0-downstream4 changed state to down Dec 16
04:22:57.162 CST: %SNMP-5-LINK_DOWN: LinkDown:Interface
Integrated-Cable6/0/0-downstream5 changed state to down Dec 16
04:22:57.162 CST: %SNMP-5-LINK_DOWN: LinkDown:Interface
Integrated-Cable6/0/0-downstream6 changed state to down Dec 16
04:22:57.162 CST: %SNMP-5-LINK_DOWN: LinkDown:Interface
Integrated-Cable6/0/0-downstream7 changed state to down Dec 16
04:22:57.163 CST: %SNMP-5-LINK_DOWN: LinkDown:Interface
Integrated-Cable6/0/0-downstream8 changed state to down Dec 16
04:22:57.163 CST: %SNMP-5-LINK_DOWN: LinkDown:Interface
Integrated-Cable6/0/0-downstream9 changed state to down Dec 16
04:22:57.163 CST: %SNMP-5-LINK_DOWN: LinkDown:Interface
Integrated-Cable6/0/0-downstream10 changed state to down Dec 16
04:22:57.163 CST: %SNMP-5-LINK_DOWN: LinkDown:Interface
Integrated-Cable6/0/1-downstream0 changed state to down Dec 16
04:22:57.164 CST: %SNMP-5-LINK_DOWN: LinkDown:Interface
Integrated-Cable6/0/1-downstream1 changed state to down Dec 16
04:22:57.164 CST: %SNMP-5-LINK_DOWN: LinkDown:Interface
Integrated-Cable6/0/1-downstream2 changed state to down Dec 16
04:22:57.164 CST: %SNMP-5-LINK_DOWN: LinkDown:Interface
Integrated-Cable6/0/1-downstream3 changed state to down Dec 16
04:22:57.164 CST: %SNMP-5-LINK_DOWN: LinkDown:Interface
Integrated-Cable6/0/1-downstream4 changed state to down Dec 16
04:22:57.164 CST: %SNMP-5-LINK_DOWN: LinkDown:Interface
Integrated-Cable6/0/1-downstream5 changed state to down Dec 16
04:22:57.183 CST: %SNMP-5-LINK_UP: LinkUp:Interface
Integrated-Cable6/0/0-downstream0 changed state to up Dec 16
04:22:57.184 CST: %SNMP-5-LINK_UP: LinkUp:Interface
Integrated-Cable6/0/0-downstream1 changed state to up Dec 16
04:22:57.189 CST: %SNMP-5-LINK_UP: LinkUp:Interface
Integrated-Cable6/0/0-downstream2 changed state to up Dec 16
04:22:57.211 CST: %SNMP-5-LINK_UP: LinkUp:Interface
Integrated-Cable6/0/0-downstream3 changed state to up Dec 16
04:22:57.212 CST: %SNMP-5-LINK_UP: LinkUp:Interface
Integrated-Cable6/0/0-downstream4 changed state to up Dec 16
04:22:57.212 CST: %SNMP-5-LINK_UP: LinkUp:Interface
Integrated-Cable6/0/0-downstream6 changed state to up Dec 16
04:22:57.213 CST: %SNMP-5-LINK_UP: LinkUp:Interface
Integrated-Cable6/0/0-downstream7 changed state to up Dec 16
04:22:57.213 CST: %SNMP-5-LINK_UP: LinkUp:Interface
Integrated-Cable6/0/0-downstream8 changed state to up Dec 16
04:22:57.213 CST: %SNMP-5-LINK_UP: LinkUp:Interface
Integrated-Cable6/0/0-downstream9 changed state to up Dec 16
04:22:57.213 CST: %SNMP-5-LINK_UP: LinkUp:Interface
Integrated-Cable6/0/0-downstream10 changed state to up Dec 16
04:22:57.214 CST: %SNMP-5-LINK_UP: LinkUp:Interface
Integrated-Cable6/0/1-downstream0 changed state to up Dec 16
04:22:57.424 CST: %SNMP-5-LINK_UP: LinkUp:Interface
Integrated-Cable6/0/1-downstream1 changed state to up Dec 16
04:22:57.426 CST: %SNMP-5-LINK_UP: LinkUp:Interface
Integrated-Cable6/0/1-downstream2 changed state to up Dec 16
04:22:57.435 CST: %SNMP-5-LINK_UP: LinkUp:Interface
Integrated-Cable6/0/1-downstream3 changed state to up Dec 16
04:22:57.437 CST: %SNMP-5-LINK_UP: LinkUp:Interface
Integrated-Cable6/0/1-downstream4 changed state to up Dec 16
04:22:57.449 CST: %SNMP-5-LINK_UP: LinkUp:Interface
```

```
Integrated-Cable6/0/1-downstream5 changed state to up Dec 16
04:22:59.219 CST: %LINEPROTO-5-UPDOWN: Line protocol on Interface
Integrated-Cable6/0/1:0, changed state to up Dec 16 04:22:59.219 CST:
%LINK-3-UPDOWN: Interface Integrated-Cable6/0/1:0, changed state to up
Dec 16 04:22:59.427 CST: %LINEPROTO-5-UPDOWN: Line protocol on
Interface Integrated-Cable6/0/1:1, changed state to up Dec 16
04:22:59.427 CST: %LINK-3-UPDOWN: Interface Integrated-Cable6/0/1:1,
changed state to up Dec 16 04:22:59.449 CST: %LINEPROTO-5-UPDOWN: Line
protocol on Interface Wideband-Cable6/0/0:0, changed state to up Dec 16
04:22:59.450 CST: %LINK-3-UPDOWN: Interface Wideband-Cable6/0/0:0,
changed state to up Dec 16 04:22:59.450 CST: %LINK-3-UPDOWN: Interface
Wideband-Cable6/0/0:1, changed state to up Dec 16 04:22:59.450 CST:
%LINK-3-UPDOWN: Interface Wideband-Cable6/0/0:2, changed state to up
Dec 16 04:22:59.450 CST: %LINK-3-UPDOWN: Interface
Wideband-Cable6/0/0:3, changed state to up Dec 16 04:22:59.450 CST:
%LINK-3-UPDOWN: Interface Wideband-Cable6/0/0:4, changed state to up
Dec 16 04:22:59.450 CST: %LINK-3-UPDOWN: Interface
Wideband-Cable6/0/0:5, changed state to up Dec 16 04:22:59.451 CST:
%LINK-3-UPDOWN: Interface Wideband-Cable6/0/0:6, changed state to up
Dec 16 04:22:59.451 CST: %LINK-3-UPDOWN: Interface
Wideband-Cable6/0/0:7, changed state to up Dec 16 04:22:59.451 CST:
%LINEPROTO-5-UPDOWN: Line protocol on Interface Wideband-Cable6/0/1:0,
changed state to up Dec 16 04:22:59.451 CST: %LINK-3-UPDOWN: Interface
Wideband-Cable6/0/1:0, changed state to up Dec 16 04:22:59.451 CST:
%LINEPROTO-5-UPDOWN: Line protocol on Interface Wideband-Cable6/0/1:1,
changed state to up Dec 16 04:22:59.452 CST: %LINK-3-UPDOWN: Interface
Wideband-Cable6/0/1:1, changed state to up Dec 16 04:22:59.452 CST:
%LINK-3-UPDOWN: Interface Wideband-Cable6/0/2:0, changed state to up
Dec 16 04:23:27.352 CST: %IOSXE-5-PLATFORM: CLC6: cdman: DSPHY Gemini
module  1 was not present Dec 16 04:26:59.885 CST:
%ENVIRONMENTAL-1-ALERT: Temp: INLET, Location:
6, State: Critical, Reading: 53 Celsius sig-cbr#]]></aml-block:Data>
</aml-block:Attachment> </aml-block:Attachments> </aml-block:Block>
</soap-env:Body> </soap-env:Envelope>
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS XE commands	Cisco IOS Master Commands List, All Releases
Smart Call Home site page on Cisco.com for access to all related product information.	Cisco Smart Call Home site
Explains how the Smart Call Home service offers web-based access to important information on select Cisco devices and offers higher network availability, and increased operational efficiency by providing real-time alerts.	Smart Call Home User Guide
Call Home Quick Start Guide	Smart Call Home Quick Start Configuration Guide for Cisco cBR Series Routers

MIBs

MIB	MIBs Link
CISCO-CALLHOME-MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

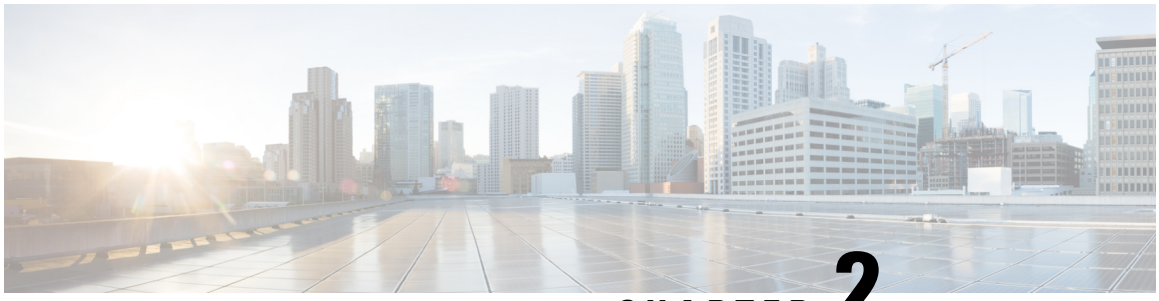
Feature Information for Call Home

Use Cisco Feature Navigator to find information about the platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to the www.cisco.com/go/cfn link. An account on the Cisco.com page is not required.

Note The following table lists the software release in which a given feature is introduced. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 11: Feature Information for Call Home

Feature Name	Releases	Feature Information
Smart Call Home	Cisco IOS XE Everest 16.6.1	This feature was integrated into Cisco IOS XE Everest 16.6.1 on the Cisco cBR Series Converged Broadband Routers.



CHAPTER 2

SNMP Support over VPNs—Context-Based Access Control

The SNMP Support over VPNs--Context-Based Access Control feature provides the infrastructure for multiple Simple Network Management Protocol (SNMP) context support in Cisco software and VPN-aware MIB infrastructure using the multiple SNMP context support infrastructure.

- Finding Feature Information, on page 67
- Hardware Compatibility Matrix for the Cisco cBR Series Routers, on page 67
- Restrictions for SNMP Support over VPNs—Context-Based Access Control, on page 68
- Information About SNMP Support over VPNs—Context-Based Access Control, on page 68
- How to Configure SNMP Support over VPNs—Context-Based Access Control, on page 71
- Configuration Examples for SNMP Support over VPNs—Context-Based Access Control, on page 75
- Additional References, on page 76
- Feature Information for SNMP Support over VPNs—Context-Based Access Control, on page 78

Finding Feature Information

Finding Feature Information

Your software release may not support all the features that are documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. The Feature Information Table at the end of this document provides information about the documented features and lists the releases in which each feature is supported.

Hardware Compatibility Matrix for the Cisco cBR Series Routers

Note The hardware components that are introduced in a given Cisco IOS-XE Release are supported in all subsequent releases unless otherwise specified.

Table 12: Hardware Compatibility Matrix for the Cisco cBR Series Routers

Cisco CMTS Platform	Processor Engine	Interface Cards
Cisco cBR-8 Converged Broadband Router	**Cisco IOS-XE Release 16.5.1 and Later Releases** Cisco cBR-8 Supervisor: • PID—CBR-SUP-250G • PID—CBR-CCAP-SUP-160G • PID—CBR-CCAP-SUP-60G • PID—CBR-SUP-8X10G-PIC	**Cisco IOS-XE Release 16.5.1 and Later Releases** Cisco cBR-8 CCAP Line Cards: • PID—CBR-LC-8D30-16U30 • PID—CBR-LC-8D31-16U30 • PID—CBR-RF-PIC • PID—CBR-RF-PROT-PIC • PID—CBR-CCAP-LC-40G • PID—CBR-CCAP-LC-40G-R Cisco cBR-8 Downstream PHY Modules: • PID—CBR-D30-DS-MOD • PID—CBR-D31-DS-MOD Cisco cBR-8 Upstream PHY Modules: • PID—CBR-D30-US-MOD • PID—CBR-D31-US-MOD

Restrictions for SNMP Support over VPNs—Context-Based Access Control

- If you delete an SNMP context using the **no snmp-server context** command, all SNMP instances in that context are deleted.
- Not all MIBs are VPN-aware.

Information About SNMP Support over VPNs—Context-Based Access Control

SNMP Versions and Security

Cisco software supports the following versions of SNMP:

- SNMPv1—Simple Network Management Protocol: a full Internet standard, defined in RFC 1157. (RFC 1157 replaces the earlier versions that were published as RFC 1067 and RFC 1098.) Security is based on community strings.
- SNMPv2c—The community string-based Administrative Framework for SNMPv2. SNMPv2c (the "c" is for "community") is an experimental Internet protocol defined in RFC 1901, RFC 1905, and RFC 1906. SNMPv2c is an update of the protocol operations and data types of SNMPv2p (SNMPv2 Classic) and uses the community-based security model of SNMPv1.

For more information about SNMP Versions, see the " Configuring SNMP Support " module in the *Cisco Network Management Configuration Guide*.

SNMPv1 or SNMPv2 Security

Cisco IOS software supports the following versions of SNMP:

- SNMPv1—Simple Network Management Protocol: a full Internet standard, defined in RFC 1157. (RFC 1157 replaces the earlier versions that were published as RFC 1067 and RFC 1098.) Security is based on community strings.
- SNMPv2c—The community string-based Administrative Framework for SNMPv2. SNMPv2c (the "c" is for "community") is an experimental Internet protocol defined in RFC 1901, RFC 1905, and RFC 1906. SNMPv2c is an update of the protocol operations and data types of SNMPv2p (SNMPv2 Classic) and uses the community-based security model of SNMPv1.

SNMPv1 and SNMPv2 are not as secure as SNMPv3. SNMP version 1 and 2 use plain text communities and do not perform the authentication or security checks that SNMP version 3 performs. To configure the SNMP Support over VPNs—Context-Based Access Control feature when using SNMP version 1 or SNMP version 2, you need to associate a community name with a VPN. This association causes SNMP to process requests coming in for a particular community string only if it comes in from the configured VRF. If the community string contained in the incoming packet does not have an associated VRF, it is processed only if it came in through a non-VRF interface. This process prevents users outside the VPN from snooping a clear text community string to query the VPN's data. These methods of source address validation are not as secure as using SNMPv3.

SNMPv3 Security

If you are using SNMPv3, the security name should always be associated with authentication or privileged passwords. Source address validation is not performed on SNMPv3 users. To ensure that a VPN's user has access only to context associated to the VPN and cannot see the MIB data of other VPNs, you must configure a minimum security level of AuthNoPriv.

On a provider edge (PE) router, a community can be associated with a VRF to provide source address validation. However, on a customer edge (CE) router, if source address validation is to be provided, you must associate a source address with the community list by using an access control list.

If you are using SNMPv3, the security name or security password of the users of a VPN should be unknown to users of other VPNs. Cisco recommends not to use SNMPv3 nonauthorized users if you need security of management information.

SNMP Notification Support over VPNs

The SNMP Notification Support over VPNs feature allows the sending and receiving of SNMP notifications (traps and informs) using VPN routing and forwarding (VRF) instance tables. In particular, this feature adds support to Cisco software for the sending and receiving of SNMP notifications (traps and informs) specific to individual VPNs.

SNMP is an application-layer protocol that provides a message format for communication between SNMP managers and agents.

A VPN is a network that provides high-connectivity transfers on a shared system with the same usage guidelines as a private network. A VPN can be built on the Internet over IP, Frame Relay, or ATM networks.

A VRF stores per-VPN routing data. It defines the VPN membership of a customer site attached to the network access server (NAS). A VRF consists of an IP routing table, a derived Cisco Express Forwarding (formerly known as CEF) table, and guidelines and routing protocol parameters that control the information that is included in the routing table.

The SNMP Support for VPNs—Context-Based Access Control feature provides configuration commands that allow users to associate SNMP agents and managers with specific VRFs. The associated VRF is used for the sending of SNMP notifications (traps and informs) and responses between agents and managers. If a VRF is not specified, the default routing table for the VPN is used.

VPN-Aware SNMP

The SNMP Support for VPNs—Context-Based Access Control feature extends the capabilities of the SNMP Notification Support for VPNs feature and enables SNMP to differentiate between incoming packets from different VPNs.

When the SNMP Support for VPNs—Context-Based Access Control feature is configured, SNMP accepts requests on any configured VRF and returns responses to the same VRF. A trap host also can be associated with a specific VRF. The configured VRF is then used for sending out traps; otherwise, the default routing table is used. You also can associate a remote user with a specific VRF. You also can configure the VRFs from which SNMP should accept requests. Any requests coming from VRFs that are not specified are dropped.

IP access lists can be configured and associated with SNMP community strings. This feature enables you to configure an association between VRF instances with SNMP community strings. When a VRF instance is associated with an SNMP community string, SNMP processes the requests coming in for a particular community string only if the requests are received from the configured VRF. If the community string contained in the incoming packet does not have a VRF associated with it, the community string will be processed only if it came in through a non-VRF interface.

You also can enable or disable authentication traps for SNMP packets dropped due to VRF mismatches. By default if SNMP authentication traps are enabled, VRF authentication traps are also enabled.

VPN Route Distinguishers

A route distinguisher (RD) creates routing and forwarding tables and specifies the default route distinguisher for a VPN. The RD is added to the beginning of the customer's IPv4 prefixes to change them into globally unique VPN-IPv4 prefixes.

The RD is either an autonomous system number (ASN)-relative RD, in which case it comprises an autonomous system number and an arbitrary number, or it is an IP-address-relative RD, in which case it comprises an IP address and an arbitrary number.

You can enter an RD in either of these formats:

- 16-bit ASN: your 16-bit number: For example, 101:3.
- 32-bit IP address: your 32-bit number: For example, 192.168.122.15:1.

SNMP Contexts

SNMP contexts provide VPN users with a secure way of accessing MIB data. When a VPN is associated with a context, that VPN's specific MIB data exists in that context. Associating a VPN with a context enables service providers to manage networks with multiple VPNs. Creating and associating a context with a VPN enables a provider to prevent the users of one VPN from accessing information about other VPN userss on the same networking device.

VPN-aware SNMP requires an agreement between SNMP manager and agent entities operating in a VPN environment on a mapping between the SNMP security name and the VPN ID. This mapping is created by using multiple contexts for the SNMP data of different VPNs through the configuration of the SNMP-VACM-MIB. The SNMP-VACM-MIB is configured with views so that a user on a VPN with a security name is allowed access to the restricted object space associated with a user's access type in the context associated with the user of that VPN.

SNMP request messages undergo three phases of security and access control before a response message is sent back with the object values in the context of a VPN:

- In the first phase, the username is authenticated. This phase ensures that the user is authenticated and authorized for SNMP access.
- In the second phase, the user is authorized for the SNMP access requested to the group objects under consideration of the configured SNMP context. This phase is called the access control phase.
- In the third phase, access is made to a particular instance of a table entry. With this third phase, complete retrieval can be based on the SNMP context name.

How to Configure SNMP Support over VPNs—Context-Based Access Control

Configuring an SNMP Context and Associating the SNMP Context with a VPN

Perform this task to configure an SNMP context and to associate the SNMP context with a VPN.

Note

- Only the following MIBs are context-aware. All the tables in these MIBs can be polled:
  - CISCO-IPSEC-FLOW-MONITOR-MIB
  - CISCO-IPSEC-MIB
  - CISCO-PING-MIB
  - IP-FORWARD-MIB
  - MPLS-LDP-MIB
- Only two SNMP variables in the IP-FORWARD-MIB can be polled: 1.3.6.1.2.1.4.24.3 (ipCidrRouteNumber - Scalar) and 1.3.6.1.2.1.4.24.4.1 (ipCidrRouteEntry - Table).

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**snmp-server context** *context-name* **Example:** `Device(config)# snmp-server context context1`	Creates and names an SNMP context.
Step 4	**vrf definition** *vrf-name* **Example:** `Device(config)# vrf definition vrf1`	Configures a VRF routing table and enters VRF configuration mode.
Step 5	**rd** *route-distinguisher* **Example:** `Device(config-vrf)# rd 100:120`	Creates a VPN route distinguisher.
Step 6	**context** *context-name* **Example:** `Device(config-vrf)# context context1`	Associates an SNMP context with a particular VRF. **Note** Depending on your release, the **context** command is replaced by the **snmp context** command. See the *Cisco IOS Network Management Command Reference* for more information.

	Command or Action	Purpose
Step 7	**route-target** {**import** | **export** | **both**} *route-target-ext-community* **Example:** `Device(config-vrf)# route-target export 100:1000`	(Optional) Creates a route-target extended community for a VRF.
Step 8	**end** **Example:** `Device(config-vrf)# end`	Exits interface mode and enters global configuration mode.
Step 9	**end** **Example:** `Device(config)# end`	Exits global configuration mode.

Configuring SNMP Support and Associating an SNMP Context

Perform this task to configure SNMP support and associate it with an SNMP context.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server user** *username group-name* [**remote** *host* [**udp-port** *port*] [**vrf** *vrf-name*]] { **v1** | **v2c** | **v3** [**encrypted**] [**auth** { **md5** | **sha** } *auth-password*]} [**access** [**ipv6** *nacl*] [**priv** { **des** | **3des** | **aes** { **128** | **192** | **256** }} *privpassword*] { *acl-number* | *acl-name* }]
4. **snmp-server group** *group-name* { **v1** | **v2c** | **v3** { **auth** | **noauth** | **priv** }} [**context** *context-name*] [**read** *read-view*] [**write** *write-view*] [**notify** *notify-view*] [**access** [**ipv6** *named-access-list*] [*acl-number* | *acl-name*]]
5. **snmp-server view** *view-name oid-tree* { **included** | **excluded** }
6. **snmp-server enable traps** [*notification-type*] [**vrrp**]
7. **snmp-server community** *string* [**view** *view-name*] [**ro** | **rw**] [**ipv6** *nacl*] [*access-list-number* | *extended-access-list-number* | *access-list-name*]
8. **snmp-server host** { *hostname* | *ip-address* } [**vrf** *vrf-name*] [**traps** | **informs**] [**version** { **1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port** *port*] [*notification-type*]
9. **snmp mib community-map** *community-name* [**context** *context-name*] [**engineid** *engine-id*] [**security-name** *security-name*] [**target-list** *upn-list-name*]
10. **snmp mib target list** *vpn-list-name* { **vrf** *vrf-name* | **host** *ip-address* }
11. **no snmp-server trap authentication vrf**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:**	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
	`Device> enable`	
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**snmp-server user** *username group-name* [**remote** *host* [**udp-port** *port*] [**vrf** *vrf-name*]] { **v1** | **v2c** | **v3** [**encrypted**] [**auth** { **md5** | **sha** } *auth-password*]} [**access** [**ipv6** *nacl*] [**priv** { **des** | **3des** | **aes** { **128** | **192** | **256** }} *privpassword*] { *acl-number* | *acl-name* }] **Example:** `Device(config)# snmp-server user customer1 group1 v1`	Configures a new user to an SNMP group.
Step 4	**snmp-server group** *group-name* { **v1** | **v2c** | **v3** { **auth** | **noauth** | **priv** }} [**context** *context-name*] [**read** *read-view*] [**write** *write-view*] [**notify** *notify-view*] [**access** [**ipv6** *named-access-list*] [*acl-number* | *acl-name*]] **Example:** `Device(config)# snmp-server group group1 v1 context context1 read view1 write view1 notify view1`	Configures a new SNMP group or a table that maps SNMP users to SNMP views. • Use the **context** *context-name* keyword argument pair to associate the specified SNMP group with a configured SNMP context.
Step 5	**snmp-server view** *view-name oid-tree* { **included** | **excluded** } **Example:** `Device(config)# snmp-server view view1 ipForward included`	Creates or updates a view entry.
Step 6	**snmp-server enable traps** [*notification-type*] [**vrrp**] **Example:** `Device(config)# snmp-server enable traps`	Enables all SNMP notifications (traps or informs) available on your system.
Step 7	**snmp-server community** *string* [**view** *view-name*] [**ro** | **rw**] [**ipv6** *nacl*] [*access-list-number* | *extended-access-list-number* | *access-list-name*] **Example:** `Device(config)# snmp-server community public view view1 rw`	Sets up the community access string to permit access to the SNMP.

	Command or Action	Purpose
Step 8	**snmp-server host** { *hostname* | *ip-address* } [**vrf** *vrf-name*] [**traps** | **informs**] [**version** { **1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *community-string* [**udp-port** *port*] [*notification-type*] **Example:** `Device(config)# snmp-server host 10.0.0.1 vrf vrf1 public udp-port 7002`	Specifies the recipient of an SNMP notification operation.
Step 9	**snmp mib community-map** *community-name* [**context** *context-name*] [**engineid** *engine-id*] [**security-name** *security-name*] [**target-list** *upn-list-name*] **Example:** `Device(config)# snmp mib community-map community1 context context1 target-list commAVpn`	Associates an SNMP community with an SNMP context, Engine ID, or security name.
Step 10	**snmp mib target list** *vpn-list-name* { **vrf** *vrf-name* | **host** *ip-address* } **Example:** `Device(config)# snmp mib target list commAVpn vrf vrf1`	Creates a list of target VRFs and hosts to associate with an SNMP community.
Step 11	**no snmp-server trap authentication vrf** **Example:** `Device(config)# no snmp-server trap authentication vrf`	(Optional) Disables all SNMP authentication notifications (traps and informs) generated for packets received on VRF interfaces. • Use this command to disable authentication traps only for those packets on VRF interfaces with incorrect community associations.

Configuration Examples for SNMP Support over VPNs—Context-Based Access Control

Example: Configuring Context-Based Access Control

The following configuration example shows how to configure the SNMP Support over VPNs—Context-Based Access Control feature for SNMPv1 or SNMPv2:

Note Depending on your releases, the **context** command is replaced by the **snmp context** command. See the *Cisco IOS Network Management Command Reference* for more information.

```
snmp-server context A
snmp-server context B
ip vrf Customer_A
 rd 100:110
 context A
 route-target export 100:1000
 route-target import 100:1000
!
ip vrf Customer_B
 rd 100:120
 context B
 route-target export 100:2000
 route-target import 100:2000
!
interface TenGigabitEthernet4/1/0
 description Belongs to VPN A
 ip vrf forwarding CustomerA
 ip address 192.168.2.1 255.255.255.0

interface TenGigabitEthernet4/1/1
 description Belongs to VPN B
 ip vrf forwarding CustomerB
 ip address 192.168.2.2 255.255.255.0
snmp-server user commA grp1A v1
snmp-server user commA grp2A v2c
snmp-server user commB grp1B v1
snmp-server user commB grp2B v2c
snmp-server group grp1A v1 context A read viewA write viewA notify viewA
snmp-server group grp1B v1 context B read viewB write viewB notify viewB
snmp-server view viewA ipForward included
snmp-server view viewA ciscoPingMIB included
snmp-server view viewB ipForward included
snmp-server view viewB ciscoPingMIB included
snmp-server enable traps
snmp-server host 192.168.2.3 vrf CustomerA commA udp-port 7002
snmp-server host 192.168.2.4 vrf CustomerB commB udp-port 7002
snmp mib community-map commA context A target-list commAvpn
! Configures source address validation
snmp mib community-map commB context B target-list commBvpn
! Configures source address validation
snmp mib target list commAvpn vrf CustomerA
! Configures a list of VRFs or from which community commA is valid
snmp mib target list commBvpn vrf CustomerB
! Configures a list of VRFs or from which community commB is valid
```

Additional References

Related Documents

Related Topic	Document Title
Cisco software commands	Cisco IOS Master Command List, All Releases
Cisco Network Management commands	*Cisco IOS Network Management Command Reference*
SNMP configuration	" Configuring SNMP Support " chapter in the *Cisco Network Management Configuration Guide*

Related Topic	Document Title
SNMP Support for VPNs	SNMP Notification Support for VPNs

Standards

Standard	Title
None	--

MIBs

MIB	MIBs Link
• CISCO-PING-MIB • IP-FORWARD-MIB • SNMP-VACM-MIB, *The View-based Access Control Model (ACM) MIB for SNMP*	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 1441	*Introduction to version 2 of the Internet-standard Network Management Framework*
RFC 1442	*Structure of Management Information for version 2 of the Simple Network Management Protocol (SNMPv2)*
RFC 1443	*Textual Conventions for version 2 of the Simple Network Management Protocol (SNMPv2)*
RFC 1444	*Conformance Statements for version 2 of the Simple Network Management Protocol (SNMPv2)*
RFC 1445	*Administrative Model for version 2 of the Simple Network Management Protocol (SNMPv2)*
RFC 1446	*Security Protocols for version 2 of the Simple Network Management Protocol (SNMPv2)*
RFC 1447	*Party MIB for version 2 of the Simple Network Management Protocol (SNMPv2)*
RFC 1448	*Protocol Operations for version 2 of the Simple Network Management Protocol (SNMPv2)*
RFC 1449	*Transport Mappings for version 2 of the Simple Network Management Protocol (SNMPv2)*
RFC 1450	*Management Information Base for version 2 of the Simple Network Management Protocol (SNMPv2)*
RFC 2571	*An Architecture for Describing SNMP Management Frameworks*
RFC 2576	*Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework*

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

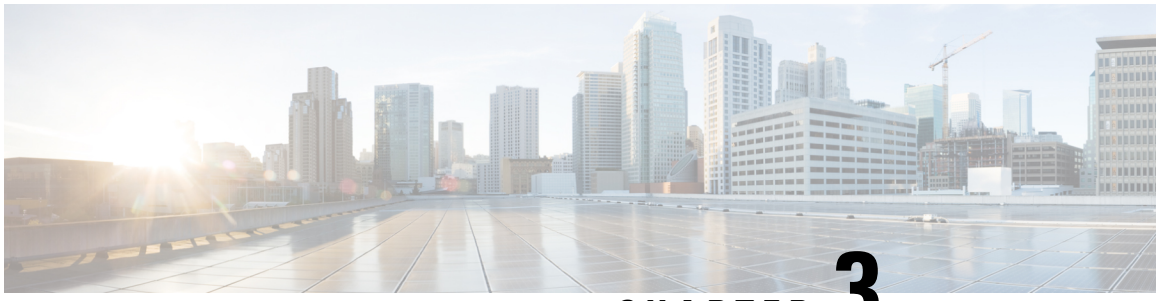
Feature Information for SNMP Support over VPNs—Context-Based Access Control

Use Cisco Feature Navigator to find information about the platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to the www.cisco.com/go/cfn link. An account on the Cisco.com page is not required.

Note The following table lists the software release in which a given feature is introduced. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 13: Feature Information for SNMP Support over VPNs—Context-Based Access Control

Feature Name	Releases	Feature Information
SNMP Support over VPNs—Context-Based Access Control	Cisco IOS XE Everest 16.6.1	This feature was integrated into Cisco IOS XE Everest 16.6.1 on the Cisco cBR Series Converged Broadband Routers.



CHAPTER 3

SNMP Engine Enhancement

The SNMP Cache Engine Enhancement feature caches the SNMP information on the Supervisor.

Finding Feature Information

Your software release may not support all the features that are documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. The Feature Information Table at the end of this document provides information about the documented features and lists the releases in which each feature is supported.

Contents

- Hardware Compatibility Matrix for the Cisco cBR Series Routers, on page 79
- Restrictions for SNMP Cache Engine Enhancement, on page 80
- Information About SNMP Cache Engine Enhancement, on page 80
- How to Configure SNMP Cache Engine Enhancement, on page 81
- Verifying the SNMP Cache Engine Status, on page 82
- Additional References, on page 83
- Feature Information for SNMP Cache Engine Enhancement, on page 83

Hardware Compatibility Matrix for the Cisco cBR Series Routers

Note The hardware components that are introduced in a given Cisco IOS-XE Release are supported in all subsequent releases unless otherwise specified.

Table 14: Hardware Compatibility Matrix for the Cisco cBR Series Routers

Cisco CMTS Platform	Processor Engine	Interface Cards
Cisco cBR-8 Converged Broadband Router	**Cisco IOS-XE Release 16.5.1 and Later Releases** Cisco cBR-8 Supervisor: • PID—CBR-SUP-250G • PID—CBR-CCAP-SUP-160G • PID—CBR-CCAP-SUP-60G • PID—CBR-SUP-8X10G-PIC	**Cisco IOS-XE Release 16.5.1 and Later Releases** Cisco cBR-8 CCAP Line Cards: • PID—CBR-LC-8D30-16U30 • PID—CBR-LC-8D31-16U30 • PID—CBR-RF-PIC • PID—CBR-RF-PROT-PIC • PID—CBR-CCAP-LC-40G • PID—CBR-CCAP-LC-40G-R Cisco cBR-8 Downstream PHY Modules: • PID—CBR-D30-DS-MOD • PID—CBR-D31-DS-MOD Cisco cBR-8 Upstream PHY Modules: • PID—CBR-D30-US-MOD • PID—CBR-D31-US-MOD

Restrictions for SNMP Cache Engine Enhancement

The time interval for which the cached information is available on the Supervisor is 5 seconds.

Information About SNMP Cache Engine Enhancement

The SNMP Cache Engine Enhancement feature caches the information on the Supervisor for the MIB tables, which need to retrieve the data from the interface cards. When a MIB table item is queried from the interface card, the next *N* items are retrieved and cached on the Supervisor.

For example, if SNMP client queries the docsIf3CmtsCmRegStatusMacAddr.1, the interface card bundles docsIf3CmtsCmRegStatusMacAddr.1, docsIf3CmtsCmRegStatusMacAddr.2, docsIf3CmtsCmRegStatusMacAddr.3, to docsIf3CmtsCmRegStatusMacAddr.N together in one IPC response, and sends it to the Supervisor. The Supervisor caches all the items locally. When the SNMP client queries the docsIf3CmtsCmRegStatusMacAddr.2 later, the information is available in the Supervisor cache directly instead of sending another IPC message to interface card. The number *N* depends on the single MIB item size and maximum IPC message buffer size.

The MIB table information for following MIBs are retrieved and cached on the Supervisor:

- DOCS-IF-MIB
- DOCS-IFEXT2-MIB
- DOCS-QOS-MIB
- DOCS-IF3-MIB
- DOCS-IF31-MIB
- DOCS-QOS3-MIB
- DOCS-IETF-QOS-MIB
- DOCS-BPI-PLUS-MIB
- DOCS-LOADBALANCING-MIB
- DOCS-LOADBAL3-MIB
- DOCS-DSG-IF-MIB
- CISCO-DOCS-EXT-MIB
- CISCO-CABLE-WIDEBAND-MIB
- CISCO-CABLE-SPECTRUM-MIB

This feature is enabled by default on the Cisco cBR routers. The time interval for which the SNMP cache information is stored on the Supervisor is known as *age* and set to 5 seconds.

How to Configure SNMP Cache Engine Enhancement

Before you begin

You must configure the **service internal** command in global configuration mode to enable or disable SNMP Cache Engine Enhancement.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable snmp cache active** **Example:**	Sets the SNMP cache status to active.

	Command or Action	Purpose
	`Router(config)# cable snmp cache active`	**Note** Use the **no** form of the command to disable the SNMP cache status.
Step 4	**exit** **Example:** `Router(config)# exit`	Exits the global configuration mode and enters the privileged EXEC mode.

Verifying the SNMP Cache Engine Status

Use the **show cable snmp cache-status** command to display the current SNMP cache engine status.

Important You must configure the **service internal** command in global configuration mode to verify the SNMP cache engine status.

Following is a sample output of the command.

```
Router# show cable snmp cache-status

    Cache engine is ON, age: 5 seconds
```

Use the **test cable snmp counter-show** command to display the cache counters information.

```
Router# test cable snmp counter-show
========== cache counters ==========
ubrcce_snmp_cache_hit_counter:0.
ubrcce_snmp_cache_get_from_lc_counter:1.
ubrcce_snmp_cache_miss_counter:0.
ubrcce_snmp_cache_ipc_fail_counter:0.
ubrcce_snmp_cache_buffer_full_counter:0.
```

hit and *mis* are the historic information for the SNMP cache after the system bootup. *hit* indicates the number of times the SNMP queries are hit in the cache and *mis* indicates the number of times the SNMP queries are missed in the SNMP cache.

Additional References

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

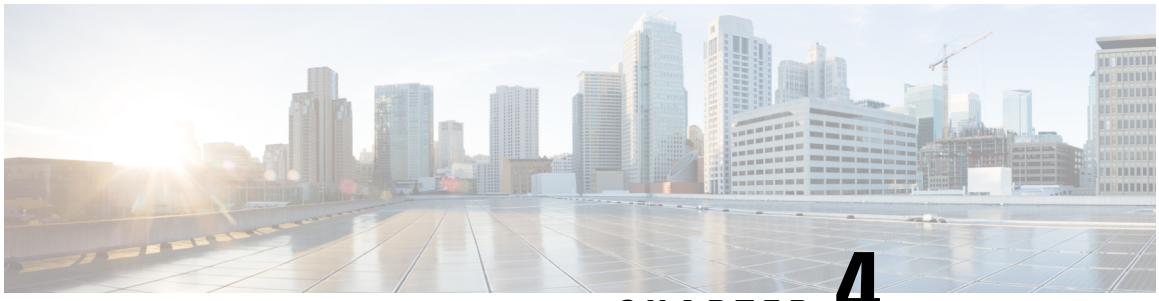
Feature Information for SNMP Cache Engine Enhancement

Use Cisco Feature Navigator to find information about the platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to the www.cisco.com/go/cfn link. An account on the Cisco.com page is not required.

Note The following table lists the software release in which a given feature is introduced. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 15: Feature Information for SNMP Cache Engine Enhancement

Feature Name	Releases	Feature Information
SNMP Cache Engine Enhancement	Cisco IOS XE Everest 16.6.1	This feature was integrated into Cisco IOS XE Everest 16.6.1 on the Cisco cBR Series Converged Broadband Routers.



CHAPTER 4

Onboard Failure Logging

Onboard Failure Logging (OBFL) captures and stores hardware failure and environmental information into nonvolatile memory. OBFL permits improved accuracy in hardware troubleshooting and root cause isolation analysis. Stored OBFL data can be retrieved in the event of a router crash or failure.

- Finding Feature Information, on page 85
- Hardware Compatibility Matrix for the Cisco cBR Series Routers, on page 85
- Understanding OBFL, on page 86
- Configuring OBFL, on page 87
- Displaying OBFL Logging Information, on page 87
- Clearing OBFL Logging, on page 87
- Configuration and Verification Examples, on page 88
- Feature Information for Onboard Failure Logging, on page 90

Finding Feature Information

Finding Feature Information

Your software release may not support all the features that are documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. The Feature Information Table at the end of this document provides information about the documented features and lists the releases in which each feature is supported.

Hardware Compatibility Matrix for the Cisco cBR Series Routers

Note The hardware components that are introduced in a given Cisco IOS-XE Release are supported in all subsequent releases unless otherwise specified.

Table 16: Hardware Compatibility Matrix for the Cisco cBR Series Routers

Cisco CMTS Platform	Processor Engine	Interface Cards
Cisco cBR-8 Converged Broadband Router	**Cisco IOS-XE Release 16.5.1 and Later Releases** Cisco cBR-8 Supervisor: • PID—CBR-SUP-250G • PID—CBR-CCAP-SUP-160G • PID—CBR-CCAP-SUP-60G • PID—CBR-SUP-8X10G-PIC	**Cisco IOS-XE Release 16.5.1 and Later Releases** Cisco cBR-8 CCAP Line Cards: • PID—CBR-LC-8D30-16U30 • PID—CBR-LC-8D31-16U30 • PID—CBR-RF-PIC • PID—CBR-RF-PROT-PIC • PID—CBR-CCAP-LC-40G • PID—CBR-CCAP-LC-40G-R Cisco cBR-8 Downstream PHY Modules: • PID—CBR-D30-DS-MOD • PID—CBR-D31-DS-MOD Cisco cBR-8 Upstream PHY Modules: • PID—CBR-D30-US-MOD • PID—CBR-D31-US-MOD

Understanding OBFL

OBFL provides a mechanism to store hardware, software, and environment related critical data in a non-volatile memory, such as flash EPROM or EEPROM on routers. The logging information is used by the TAC team to troubleshoot and fix hardware issues.

OBFL collects data like temperatures and voltages. It stores the data in a dedicated area of the flash memory of the router. This data is retrieved by TAC personnel to troubleshoot routers. It can also be analyzed by back-end software to detect failure patterns, and possibly to recommend specific quality improvements.

Retrieval of the OBFL message

If the hardware is defective and the system cannot boot up, any data in flash is inaccessible. In that case, use any one of the following methods to recover OBFL data:

- Read the flash through JTAG: this requires provisions in hardware design and back-end hardware and software support tools.
- Repair the system; boot it; use the OBFL CLI commands.

Configuring OBFL

Use the **hw-module** {**all**|**slot**|**module**} {*slotnumber*/*subslotnumber*|*modulenumber*} **logging onboard** {**disable** | **enable**} command to enable or disable OBFL on a specified hardware module.

Note OBFL is enabled by default.

```
Router# hw-module slot R0 logging onboard enable
```

Displaying OBFL Logging Information

Use the **show logging onboard** {**slot**|**module**|**bay**} {*slotnumber*/*subslotnumber*|*modulenumber*} {**dram** | **message** | **serdes** | **status** | **temperature** | **uptime** | **voltage**] command to view the OBFL log information.

Note OBFL is enabled by default on the Cisco cBR series router.

For the card PICs, use the **show logging onboard bay** *slotnumber*/*subslotnumber* {**dram** | **message** | **serdes** | **status** | **temperature** | **uptime** | **voltage**] command to view its OBFL information.

Clearing OBFL Logging

Use the **clear logging onboard** {**slot**|**module**} {*slotnumber*/*subslotnumber*|*modulenumber*} {**dram** | **message** | **serdes** | **temperature** | **voltage**} command to clear OBFL logging.

Following example shows how to clear DRAM ECC error log:

```
Router# clear logging onboard slot R0 dram
```

Following example shows how to clear OBFL error message:

```
Router# clear logging onboard slot R0 message
```

Following example shows how to clear onboard serdes log:

```
Router# clear logging onboard slot R0 serdes
```

Following example shows how to clear onboard temperature log:

```
Router# clear logging onboard slot R0 temperature
```

Following example shows how to clear onboard voltage log:

```
Router# clear logging onboard slot R0 voltage
```

Configuration and Verification Examples

Example—Verifying OBFL Configuration Status

```
Router#show logging onboard slot R1 status
Status: Enabled

Router#show logging onboard slot 5 status
Status: Disabled
```

Example—Displaying OBFL Logs

```
Router#show logging onboard slot R1 message
timestamp            module    sev  message

------------------------------------------------------------------------------------------------------------------------

01/01/12 12:00:23    SUP_PSOC  3    SUP MB PSOC alert interrupt

01/01/12 12:00:23    SUP_PSOC  3    SUP MB PSOC alert interrupt

01/01/12 12:00:23    SUP_PSOC  3    SUP MB PSOC alert interrupt

01/01/12 12:00:23    SUP_PSOC  3    SUP MB PSOC alert interrupt

01/01/12 12:01:15    SUP_PSOC  3    SUP MB PSOC alert interrupt
```

```
Router#show logging onboard slot R1 voltage
Name              Id    Data (mV)  Poll      Last Update
-------------------------------------------------------------------------
PSOC-MB2_20: VO   40         1791  1         01/01/12 17:03:03
PSOC-MB2_21: VO   41         3290  1         01/01/12 17:03:03
PSOC-MB2_22: VO   42         3293  1         01/01/12 17:03:03
PSOC-MB2_23: VO   43         3299  1         01/01/12 17:03:03
PSOC-MB2_24: VO   44         4958  1         01/01/12 17:03:03
PSOC-MB2_25: VO   45         4508  1         01/01/12 17:03:03
PSOC-MB3_0: VOU   46         4999  1         01/01/12 17:03:03
PSOC-MB3_1: VOU   47         4982  1         01/01/12 17:03:03
PSOC-MB3_2: VOU   48         1499  1         01/01/12 17:03:03
PSOC-MB3_3: VOU   49         1193  1         01/01/12 17:03:03
PSOC-MB3_4: VOU   50          708  1         01/01/12 17:03:03
PSOC-MB3_5: VOU   51          757  1         01/01/12 17:03:03
PSOC-MB3_6: VOU   52          585  1         01/01/12 17:03:03
PSOC-MB3_7: VOU   53         1501  1         01/01/12 17:03:03
```

```
Router#show logging onboard slot R1 temperature
Name              Id     Data (C)  Poll      Last Update
-------------------------------------------------------------------------
Temp: BB_DIE      159          25  1         01/02/12 23:04:19
Temp: VP_DIE      160          21  1         01/02/12 23:04:19
Temp: RT-E_DIE    161          29  1         01/02/12 23:04:19
Temp: INLET_1     162          20  1         01/02/12 23:04:19
Temp: INLET_2     163          18  1         01/02/12 23:04:19
Temp: OUTLET_1    164          22  1         01/02/12 23:04:19
Temp: 3882_1      165          44  1         01/02/12 23:04:19
```

```
Temp: 3882_1A     166          38  1         01/02/12 23:04:19
Temp: 3882_1B     167          36  1         01/02/12 23:04:19
Temp: 3882_2      168          38  1         01/02/12 23:04:19
Temp: 3882_2A     169          37  1         01/02/12 23:04:19
Temp: 3882_2B     170          35  1         01/02/12 23:04:19
Temp: 3882_3      171          38  1         01/02/12 23:04:19
```

```
Router#show logging onboard slot R1 uptime latest
 Slot              Reset reason  Power On
-------------------------------------------------------
    1      reset local software  01/02/12 23:02:46
```

```
Router#show logging onboard slot R1 uptime
 Slot              Reset reason  Power On
-------------------------------------------------------
    0      reset local software  01/06/12 01:52:26
    4      reset local software  01/06/12 01:52:42
    0      reset local software  01/06/12 01:52:45
    0      reset local software  01/06/12 02:20:27
    4      reset local software  01/06/12 02:20:43
    0      reset local software  01/06/12 02:20:46
    0      reset local software  01/06/12 05:12:02
    4      reset local software  01/06/12 05:12:19
    0      reset local software  01/06/12 05:12:22
    0      reset local software  01/06/12 05:17:31
    4      reset local software  01/06/12 05:17:48
    0      reset local software  01/06/12 05:17:51
    0            reset power on  01/01/12 08:56:44
    4            reset power on  01/01/12 08:57:00
```

```
Router#show logging onboard bay 4/3 message
timestamp            module    sev  message

-------------------------------------------------------------------------------------------------------------------

01/02/12 08:14:22    RFSW-PIC  6    CAT1836E07Q:7.13:Initialize:3/1

01/02/12 08:20:42    RFSW-PIC  6    CAT1836E07Q:7.13:Initialize:3/1

01/02/12 09:13:23    RFSW-PIC  6    CAT1836E07Q:7.13:Initialize:3/1

01/02/12 09:42:33    RFSW-PIC  6    CAT1836E07Q:7.13:Initialize:3/1

01/02/12 11:56:09    RFSW-PIC  6    CAT1836E07Q:7.13:Initialize:3/1

01/02/12 12:27:23    RFSW-PIC  6    CAT1836E07Q:7.13:Initialize:3/1
```

```
Router#show logging onboard bay 5/3 message
timestamp            module    sev  message

-------------------------------------------------------------------------------------------------------------------

01/22/15 01:06:05    RFSW-PIC  6    JAB092709EL:7.35:Init--stby:3/1

01/22/15 01:19:01    RFSW-PIC  6    JAB092709EL:7.35:Init--stby:3/1

01/22/15 01:31:47    RFSW-PIC  6    JAB092709EL:7.35:Init--stby:3/1

01/22/15 01:44:38    RFSW-PIC  6    JAB092709EL:7.35:Init--stby:3/1

01/22/15 01:59:04    RFSW-PIC  6    JAB092709EL:7.35:Init--stby:3/1
```

```
01/22/15 02:12:07    RFSW-PIC  6    JAB092709EL:7.35:Init--stby:3/1


Router#show logging onboard bay 4/4 message
timestamp            module    sev  message

------------------------------------------------------------------------------------------------------------------------

01/01/12 10:01:44    SUP-PIC   0    TEST1122334:0.130:PLL-LOS:1[04]

01/01/12 10:01:45    SUP-PIC   0    TEST1122334:0.130:PLL-LOS:2[04]

01/01/12 10:01:46    SUP-PIC   0    TEST1122334:0.130:PLL-LOS:3[04]

01/01/12 10:01:49    SUP-PIC   0    TEST1122334:0.130:PLL-LOS:4[04]

01/01/12 10:01:50    SUP-PIC   0    TEST1122334:0.130:PLL-LOS:5[04]

01/01/12 10:01:51    SUP-PIC   0    TEST1122334:0.130:PLL-LOS:6[04]


Router#show logging onboard bay 5/5 message
timestamp            module    sev  message

------------------------------------------------------------------------------------------------------------------------

01/03/12 13:52:55    SUP-PIC   0    TEST8877665:0.130:PLL-LOS:1[04]

01/03/12 13:52:56    SUP-PIC   0    TEST8877665:0.130:PLL-LOS:2[04]

01/03/12 13:52:57    SUP-PIC   0    TEST8877665:0.130:PLL-LOS:3[04]

01/03/12 13:53:00    SUP-PIC   0    TEST8877665:0.130:PLL-LOS:4[04]

01/03/12 13:53:01    SUP-PIC   0    TEST8877665:0.130:PLL-LOS:5[04]
```

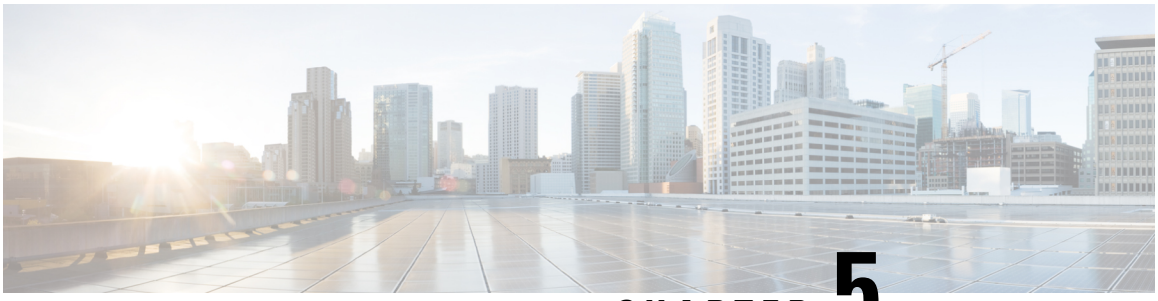
Feature Information for Onboard Failure Logging

Use Cisco Feature Navigator to find information about the platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to the www.cisco.com/go/cfn link. An account on the Cisco.com page is not required.

Note The following table lists the software release in which a given feature is introduced. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 17: Feature Information for Onboard Failure Logging

Feature Name	Releases	Feature Information
Onboard Failure Logging	Cisco IOS XE Everest 16.6.1	This feature was integrated into Cisco IOS XE Everest 16.6.1 on the Cisco cBR Series Converged Broadband Routers.



CHAPTER 5

Control Point Discovery

This document describes the Control Point Discovery (CPD) feature. This feature, along with Network Layer Signaling (NLS), enables automatic discovery of any control point associated with an end point.

Finding Feature Information

Your software release may not support all the features that are documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. The Feature Information Table at the end of this document provides information about the documented features and lists the releases in which each feature is supported.

Contents

- Hardware Compatibility Matrix for the Cisco cBR Series Routers, on page 91
- Prerequisites for Control Point Discovery, on page 92
- Restrictions for Control Point Discovery, on page 92
- Information About Control Point Discovery, on page 93
- How to Configure CPD, on page 95
- Additional References, on page 99
- Feature Information for Control Point Discovery, on page 100

Hardware Compatibility Matrix for the Cisco cBR Series Routers

Note The hardware components that are introduced in a given Cisco IOS-XE Release are supported in all subsequent releases unless otherwise specified.

Table 18: Hardware Compatibility Matrix for the Cisco cBR Series Routers

Cisco CMTS Platform	Processor Engine	Interface Cards
Cisco cBR-8 Converged Broadband Router	**Cisco IOS-XE Release 16.5.1 and Later Releases** Cisco cBR-8 Supervisor: • PID—CBR-SUP-250G • PID—CBR-CCAP-SUP-160G • PID—CBR-CCAP-SUP-60G • PID—CBR-SUP-8X10G-PIC	**Cisco IOS-XE Release 16.5.1 and Later Releases** Cisco cBR-8 CCAP Line Cards: • PID—CBR-LC-8D30-16U30 • PID—CBR-LC-8D31-16U30 • PID—CBR-RF-PIC • PID—CBR-RF-PROT-PIC • PID—CBR-CCAP-LC-40G • PID—CBR-CCAP-LC-40G-R Cisco cBR-8 Downstream PHY Modules: • PID—CBR-D30-DS-MOD • PID—CBR-D31-DS-MOD Cisco cBR-8 Upstream PHY Modules: • PID—CBR-D30-US-MOD • PID—CBR-D31-US-MOD

Prerequisites for Control Point Discovery

No special equipment or software is needed to use the Control Point Discovery feature.

Restrictions for Control Point Discovery

- The CPD feature does not sync any dynamic CPD/NLS related data between the route processors (RPs). After sending a NLS challenge to the controller, the new active PRE will ignore the NLS response as a result of any RP switchover.
- The CPEs become inaccessible for a small duration during line card switchovers. During this interval, any CPD request received on CMTS will be responded to as if the endpoint is not connected or as if the control relationship is not supported.
- The CPD functionality is restricted to default VPN table id (0).
- Only manual configuration of NLS authentication pass phrase would be supported for CPD/NLS security.
- For NLS authentication, HMAC SHA1 (no configuration option) is used with MAC length truncated to 96 bits.

Information About Control Point Discovery

To configure the Control Point Discovery feature, you should understand the following concepts:

Control Points

Control points are points in a network that can be used to apply certain functions and controls for a media stream. In a cable environment, the control points are Cable Modem Termination Systems (CMTS) and devices that utilizes these control points are referred to as CPD Requestors (or controllers).

Cable CPD Requestors include the following:

- Call Management Server (CMS)
- Policy Server (PS)
- Mediation Device for Lawful Intercept (MD)

Network Layer Signaling (NLS)

Network Layer Signaling (NSL) is an on-path request protocol used to carry topology discovery and other requests in support of various applications. In the CPD feature, NLS is used to transport CPD messages.

NLS for CPD

NLS is used to transport CPD messages. The CPD data is carried under an application payload of the NLS and contains a NLS header with flow id. The NLS flow id is used during NLS authentication to uniquely identify the CPD requests and responses for an end point of interest.

NLS Flags

All NLS headers contain bitwise flags. The CMTS expects the following NLS flag settings for CPD applications:

- HOP-BY-HOP = 0
- BUILD-ROUTE = 0
- TEARDOWN = 0
- BIDIRECTOINAL = 0
- AX_CHALLANGE = 0/1
- AX_RESPONSE = 0/1

Note Any requests with flags other then AX flags, set to one will be rejected with an error indicating a poorly formed message.

NLS TLVs

The following NLS TLVs are supported for all CPD applications:

- APPLICATION_PAYLOAD
- IPV4_ERROR_CODE
- IPV6_ERROR_CODE

- AGID
- A_CHALLENGE
- A_RESPONSE
- B_CHALLENGE
- B_RESPONSE
- AUTHENTICATION
- ECHO

The following NLS TLVs are not supported for CPD applications:

- NAT_ADDRESS
- TIMEOUT
- IPV4_HOP
- IPV6_HOP

Control Point Discovery

The control point discovery feature allows CPD Requestors to determine the control point IP address between the CPD Requestor and the media endpoint.

Using Networking Layer Signaling (NLS), the control point discovery feature sends a CPD message towards the end point (MTA). The edge/aggregation device (CMTS), located between the requestor and the endpoint, will respond to the message with its IP address.

Note For Lawful Intercept, it is important that the endpoint does not receive the CPD message. In this instance, the CMTS responds to the message without forwarding it to its destination.

CPD Protocol Hierarchy

CPD messages are sent over the NLS.

The CPD Protocol Hierarchy is as follows:

1. CPD
2. NLS
3. UDP
4. IP

Note Since NLS is implemented on the UDP protocol, there is a potential of message loss. If messages are lost, the controller will re-send the CPD request in any such event.

Control Relationship

A control relationship between a control point and a controller is identified as a function on a media flow that passes through a control point. A control relationship is uniquely defined by a control relationship type (CR TYPE) and control relationship ID (CR ID). The CR ID is provisioned on CMTS as well as the controller.

The table lists the supported CR TYPEs and corresponding pre-defined CR IDs

Table 19: Supported Control Relationship Types and Corresponding Control Relationship IDs

Control Relationship Type	Pre-Defined Corresponding Control Relationship ID
CR TYPE = 1 (Lawful Intercept)	CR ID = 1: CMTS
	CR ID = 2: Aggregation router or switch in front of CMTS
	CR ID = 3: Aggregation router or switch in front of Media Services
	CR ID = 4: Media Gateway
	CR ID = 5: Conference Server
	CR ID = 6: Other
CR TYPE = 2 (DQoS)	CR ID = 1: CMTS
CR TYPE = 3 (PCMM)	CR ID = 1: CMTS

How to Configure CPD

Enabling CPD Functionality

To enable the CPD functionality, use the cpd command in global configuration mode. The CPD message authentication is determined by NLS configuration.

Before you begin

The CPD message authentication is determined by NLS configuration.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cpd** **Example:**	Enables CPD functionality • Us the “no” form of this command to disable CPD functionality.

	Command or Action	Purpose
	`Router (config)# cpd`	
Step 4	**end** **Example:** `Router# end`	Exits global configuration mode and enters privileged EXEC mode.

Examples for CPD Enable

The following example shows the cpd enabled on a router:

```
Router (config)# cpd
```

Debugging CPD Functionality

To debug the CPD feature, use the **debug cpd** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

Configuring Control Relationship Identifier

To configure a Control relationship identifier (CR ID) for CMTS, use the cpd cr-id command. When CPD request comes with a wild-card CR ID, the CMTS will respond with this configured value.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cpd cr-id** **Example:** `Router (config)# cpd cr-id 100`	Configures a control relationship identifier (CR ID) for CMTS.

	Command or Action	Purpose
Step 4	**end** **Example:** `Router# end`	Exits global configuration mode and enters privileged EXEC mode.

Examples

The following example shows the cpd cr-id command configured with a cr-id number of 100 on a router.

```
Router (config)# cpd cr-id 100
```

Enabling NLS Functionality

To enable the NLS functionality, use the nls command in global configuration mode. It is recommended that NLS message authentication be enabled at all times.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**nls** **Example:** `Router (config)# nls`	Enables NLS functionality. • NLS authentication is optional. • It is recommended that NLS message authentication be enabled at all times.
Step 4	**end** **Example:** `Router# end`	Exits global configuration mode and enters privileged EXEC mode.

Examples

The following example shows the nls command enbaled on a router.

```
Router (config)# nls
```

Debugging NLS Functionality

To debug the NLS feature, use the **debug nls** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

Configuring Authorization Group Identifier and Authentication Key

The Authorization Group Identifier (AG ID) and corresponding authorization key are provisioned on CMTS, as well as on controller/CPD requester.

To configure the Authorization Group Identifier and Authentication Key, use the nls ag-id command in global configuration mode. It is recommended that NLS message authentication be enabled at all times.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**nls ag-id** **Example:** `Router (config)# nls ag-id 100 auth-key 20`	Configures the Authorization Group Identifier and Authentication Key.
Step 4	**end** **Example:** `Router# end`	Exits global configuration mode and enters privileged EXEC mode.

Examples

The following example shows the nls ag-id command with an Authorization Group ID of 100 and Authentication Key of 20.

```
Router (config)# nls ag-id 100 auth-key 20
```

Configuring NLS Response Timeout

The NLS response timeout governs the time CMTS will wait for getting a response for a NLS authentication request.

To configure the NLS response timeout, use the nls ag-id command in global configuration mode. It is recommended that NLS message authentication be enabled at all times.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**nls resp-timeout** **Example:** `Router (config)# nls resp-timeout 60`	Configures the NLS response time.
Step 4	**end** **Example:** `Router# end`	Exits global configuration mode and enters privileged EXEC mode.

Examples

The following example shows the nls resp-timeout command with a response timeout setting of 60 seconds.

```
Router (config)# nls resp-timeout 60
```

Additional References

The following sections provide references related to the CPD feature.

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

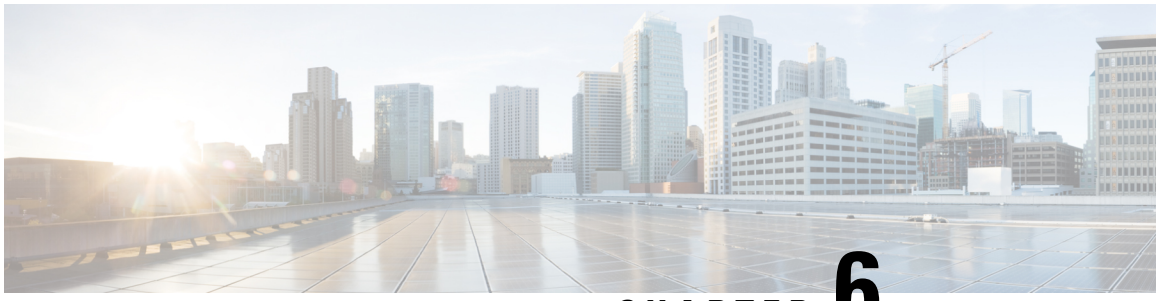
Feature Information for Control Point Discovery

Use Cisco Feature Navigator to find information about the platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to the www.cisco.com/go/cfn link. An account on the Cisco.com page is not required.

Note The following table lists the software release in which a given feature is introduced. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 20: Feature Information for Control Point Discovery

Feature Name	Releases	Feature Information
Control Point Discovery	Cisco IOS XE Everest 16.6.1	This feature was integrated into Cisco IOS XE Everest 16.6.1 on the Cisco cBR Series Converged Broadband Routers.



CHAPTER 6

IPDR Streaming Protocol

The Cisco cBR Series Converged Broadband Routersupports the Internet Protocol Detail Record (IPDR) streaming protocol feature that provides high volume data exported from the network equipment to mediation systems such as the Operations Support Systems (OSS) or Business Support Systems (BSS). IPDR provides information about IP-based service usage and other activities that are used by OSS and BSS. This protocol provides a mechanism to collect data from various network elements or equipment using a push model as opposed to the conventional Simple Network Management Protocol (SNMP) polling mechanism.

Based on the DOCSIS 3.0 specifications, the IPDR feature optimizes time and resource efficiency in the transfer of large amounts of performance metrics to the management systems. DOCSIS 3.0 introduces five management features or the FCAPS model. FCAPS represents Fault, Configuration, Accounting, Performance and Security.

Finding Feature Information

Your software release may not support all the features that are documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. The Feature Information Table at the end of this document provides information about the documented features and lists the releases in which each feature is supported.

Contents

- Restrictions for Configuring IPDR Streaming Protocol, on page 101
- Information About IPDR Streaming Protocol, on page 102
- How to Configure IPDR Streaming Protocol, on page 103
- Configuration Examples for IPDR Streaming Protocol, on page 107
- Verifying IPDR Streaming Protocol, on page 108
- Additional References, on page 110
- Feature Information for IPDR Streaming Protocol , on page 110

Restrictions for Configuring IPDR Streaming Protocol

- An IPDR exporter can be connected to many collectors, but it will only send data to the highest priority operating collector at any given time.
- Each IPDR session can be associated to one active (zero) or more standby collector with priority.

Information About IPDR Streaming Protocol

IPDR Streaming Protocol is designed to address the need for a reliable, fast, efficient, and flexible export process of high volume data records such as billing, performance and diagnostic data.

The IPDR/SP process communicates with IPDR collectors. The IPDR streaming protocol supports multiple IPDR sessions. The architecture supports primary and secondary collectors for failover purposes. At any time, data is sent to only one collector. If the exporter to primary collector connection fails due to any reason, the data is sent to the secondary collector. Depending on the network configuration, you can have only one primary collector for each session, while for different sessions, you can have different primary collectors. For example, there may be a billing collector, a diagnostic collector, and so on.

Note IPDR exporter refers to the Cable Modem Termination System (CMTS) and the IPDR collector refers to the network equipment.

Data Collection Methodologies

IPDR is the data generated or collected for various performance related metrics such as billing information, diagnostics, network topology, signal quality monitoring, and other management data. These data are based on the FCAPS model (Fault, Configuration, Accounting, Performance and Security.)

The IPDR client application communicates with the IPDR exporter using the IPDR_GET_SESSIONS message to identify the streams provided by the exporter, and the exporter sends responses to the client using the IPDR_GET_SESSIONS_RESPONSE message. This data collection method is based on the *Operations Support System Interface Specification* (CM-SP-OSSIv3.0-I13-101008).

The IPDR_GET_SESSIONS_RESPONSE message includes the SessionBlock.reserved attribute to identify the IPDR session ID. This attribute helps the Cisco CMTS router define an IPDR session ID for each data collection mechanism supported for each IPDR service definition. This attribute was not used in Cisco IOS Releases earlier to Cisco IOS Release 12.2(33)SCE.

The IPDR feature defines methods for the collectors or network elements to collect data from the CMTS. Below is the list of collection methodologies:

Time Interval Session: In this method, the CMTS follows a schedule-based session to stream data at a periodic time interval. A time interval is the time gap between two adjacent sessions' start messages. This method is managed by the CMTS in controlling the start and stop operation of a session. The time interval session terminates after the CMTS exports the records.

Note During the course of a one-time interval when the CMTS is streaming records, if another time interval is expected, the CMTS will ignore the new time interval and continue exporting the data until the previous time interval ends.

Event-based Session: In this method, the CMTS can export records at any time, when the session is open. In other words, this method works on an open-ended session.

Ad-hoc Session: In this method, the CMTS creates a session, allows data streaming, and closes the session when the data export is complete or when a closing command is generated.

A new session is created by issuing the **ipdr session** command. After, the CMTS receives the FLOW_START message from the collector, the CMTS exporter sends a SESSION_START message to start exporting the IPDR data from the collector. After all data is transported, the exporter receives a ACK message from the collector, and then sends a SESSION_STOP message to the collector. This method is known as the Ad-hoc session.

How to Configure IPDR Streaming Protocol

This section describes the configuration tasks that are performed when using the IPDR streaming protocol feature on the Cisco CMTS platforms.

Note Use no ipdr command to remove the IPDR configuration.

Configuring the IPDR Session

To enable the CMTS application to add a session to the IPDR exporter, use the ipdr session command in global configuration mode.

Use the no form of the command to remove the IPDR session.

Note
- The session ID must be unique.
- To remove an active session, you must deactivate it before removing it.

>

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	ipdr session session_id session_name session_descr **Example:** `Router(config)# ipdr session 1 samis_sxn test`	Enables the CMTS application to add a session to the IPDR exporter.

Configuring the IPDR Type

To configure the IPDR session type, use the ipdr type command in global configuration mode. The IPDR session types that can be defined using this command are event type, time-interval type, and the ad hoc type.

Use the no form of the command to reset the session type to the default "event" type.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	ipdr type session_id [ad-hoc | event | time-interval value] **Example:** `Router(config)# ipdr type 1 time-interval 15`	Enables the CMTS application to configure an IPDR session type.

What to do next

Note Once the IPDR session type is configured, only the templates supported by this IPDR type are allowed be associated with it. Also, the console provides information about those templates that are not supported by this IPDR session type when the type is changed.

Configuring the IPDR Collector

To configure the IPDR collector details, use the ipdr collector command in global configuration mode. The port number is used when an exporter creates an active connection.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ipdr collector** **Example:** `Router(config)# ipdr collector federal 192.168.6.5`	Enables the CMTS application to configure an IPDR collector and authenticate the IPDR protocol. **Note** Configure the NAT address in case of an IPDR collector that is operating in a NAT enabled network.

Configuring the IPDR Associate

To associate the collector with a session, use the ipdr associate command in global configuration mode.

Before you begin

- You must deactivate the session before configuring the associate.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ipdr associate session_id collector_name priority** **Example:** `Router(config)# ipdr associate 1 federal 1`	Associates the collector with a session.

Configuring the IPDR Template

To add an IPDR template to the IPDR session, use the ipdr template command in global configuration mode. The template list can be viewed by entering a “?” at the command prompt.

Note
- You can add only the system-supported templates.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ipdr template session_id template_name** **Example:** `Router(config)# ipdr template 1 SAMIS`	Adds an IPDR template to the IPDR session.

Configuring the IPDR Exporter

IPDR exporter parameters such as keepalive timer count, the maximum number of unacknowledged records, and unacknowledged timeout interval value can be configured using the following commands.

- **ipdr exporter keepalive**—Sets the keepalive timer count value on the IPDR Exporter.
- **ipdr exporter max-unacked**—Sets the maximum number of unacknowledged records on the IPDR Exporter.
- **ipdr exporter ack-timeout**—Sets the time interval for acknowledged records on the IPDR Exporter.

Note The default value for DataAckTimeInterval is 60 seconds and the default value for DataAckSequenceInterval is 200 seconds.

You can set the values for the IPDR parameters to customize exporter for the collectors used in the facility. However, these commands are optional, so if not configured, the default values of the commands are used when **ipdr exporter start** command is executed.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:**	Enables privileged EXEC mode. Enter your password if prompted.

	Command or Action	Purpose
	`Router> enable`	
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ipdr exporter keepalive** *time_interval* **Example:** `Router(config)# ipdr exporter keepalive 300`	(Optional) Sets the keepalive timer count for the IPDR Exporter. The valid range is from 5 to 300 seconds. The default value is 300.
Step 4	**ipdr exporter max-unacked** *records* **Example:** `Router(config)# ipdr exporter max-unacked 200`	(Optional) Sets the number of maximum unacknowledged records on the IPDR Exporter. The valid range is from 5 to 200 records. The default value is 200.
Step 5	**ipdr exporter ack-timeout** *time_interval* **Example:** `Router(config)# ipdr exporter ack-timeout 60`	(Optional) Sets the acknowledged records timeout interval on the IPDR Exporter. The valid range is from 5 to 60 seconds. The default value is 60.
Step 6	ipdr exporter start **Example:** `Router(config)# ipdr exporter start`	Enables the CMTS application to start the IPDR exporter process to connect the exporter and the collector.

Configuration Examples for IPDR Streaming Protocol

Example: Configuring the IPDR Session

The following example shows how to configure the IPDR session.

```
Router> enable
Router# configure terminal
Router(config)# ipdr session 1 test no_descr
```

Example: Configuring the IPDR Type

The following example shows how to configure the IPDR “time-interval” session type for a time interval of 15 minutes.

```
Router> enable
Router# configure terminal
Router(config)# ipdr type 1 time-interval 15
```

Example: Configuring the IPDR Collector

The following example shows how to configure the IPDR collector.

```
Router> enable
Router# configure terminal
Router(config)# ipdr collector federal 209.165.200.225
```

Example for Configuring the IPDR Collector with NAT Address

This example shows the **nat-address** keyword used to configure the NAT address for an IPDR collector:

```
Router(config)#ipdr collector federal 192.0.2.225 nat-address 192.0.2.51
```

Example: Configuring the IPDR Associate

The following example shows how to associate the collector with a session.

```
Router> enable
Router# configure terminal
Router(config)# ipdr associate 1 federal 1
```

Example: Configuring the IPDR Template

The following example shows how to add an IPDR template to the IPDR session.

```
Router> enable
Router# configure terminal
Router(config)# ipdr template 1 SAMIS-TYPE1
```

Example: Configuring the IPDR Exporter

The following example shows how to configure the IPDR exporter process to connect the exporter and the collector.

```
Router> enable
Router# configure terminal
Router(config)# ipdr exporter keepalive 300
Router(config)# ipdr exporter max-unacked 200
Router(config)# ipdr exporter ack_timeout 60
Router(config)# ipdr exporter start
```

Verifying IPDR Streaming Protocol

This section describes the commands used for verification of the IPDR streaming protocol feature on the Cisco CMTS platforms.

Verifying the IPDR Collector

The **show ipdr collector** command displays the collector information, message statistics, and event for all the sessions that are associated with the collector.

The following example shows the sample output for the **show ipdr collector** command.

```
Router# show ipdr collector federal
Collector Name: federal, IP: 192.0.2.0, Port: 0
2001-07-05T19:28:22 Collector in session 1 Statistics:
 Transmitted 12658 Acknowledged 12658 Enqueued 12658 Lost 0
 Last Event: Event Id 1 IPDR_EVENT_SERVER_CONNECTED - INCOMING
Router(config)#
```

Verifying IPDR exporter

The **show ipdr exporter** command displays information about the IPDR Exporter state as listed below.

- started
- not started
- not initialized

The following example shows the sample output for the **show ipdr exporter** command:

```
Router# show ipdr exporter
IPDR exporter is started.
Current parameters:
        KeepAliveInterval   :300
        AckTimeInterval     :60
        AckSequenceInterval :200
Router#
```

Verifying IPDR session

The **show ipdr session** command displays the session details such as the session ID, description, and the session state for all sessions as well as for a specific session.

The following example shows the sample output for the **all** keyword for the **show ipdr session** command.

```
Router# show ipdr session all
Session ID: 1, Name: utilsta, Descr: test, Started: False
```

The following example shows the sample output for the **session_id** keyword for the **show ipdr session** command.

```
Router# show ipdr session 1
Session ID: 1, Name: utilsta, Descr: test, Started: False
2001-07-05T19:36:28 Statistics:
Transmitted 0 Acknowledged 0 Enqueued 0 Lost 0
queuedOutstanding 0 queuedUnacknowledged 0
1 Collectors in the session:
Name: federal, IPAddr: 192.0.2.0, Port: 0, Priority: 1
```

Verifying IPDR Session Collector

The **show ipdr session collector** command displays the details of a collector that is associated with a specific session. Because there can be multiple collectors associated to a session, this command is used to show a specific session-collector pair.

The following example shows the sample output for the **show ipdr session collector** command.

```
Router# show ipdr session 1 collector federal
Session ID: 1, Name: utilsta, Descr: test, Started: False
Collecotr Name: federal, IP: 192.0.2.0, Port: 0
2001-07-05T19:38:02 Collector in session 1 Statistics:
 Transmitted 0 Acknowledged 0 Enqueued 0 Lost 0
 Last Event: Event Id 0 WRONG_EVENT_ID
```

Verifying IPDR Session Template

The **show ipdr session template** command displays the list of all active templates supported by a specific session.

The following example shows the sample output for the **show ipdr session template** command.

```
Router# show ipdr session 1 template
Template ID: 2, Name:
http://www.cablelabs.com/namespaces/DOCSIS/3.0/xsd/ipdr/DOCSIS-CMTS-CMSERVICE-FLOW-TYPE,
Type: DOCSIS-Type, KeyNumber: 22
Session 1 has totally 1 templates.
```

Additional References

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/support

Feature Information for IPDR Streaming Protocol

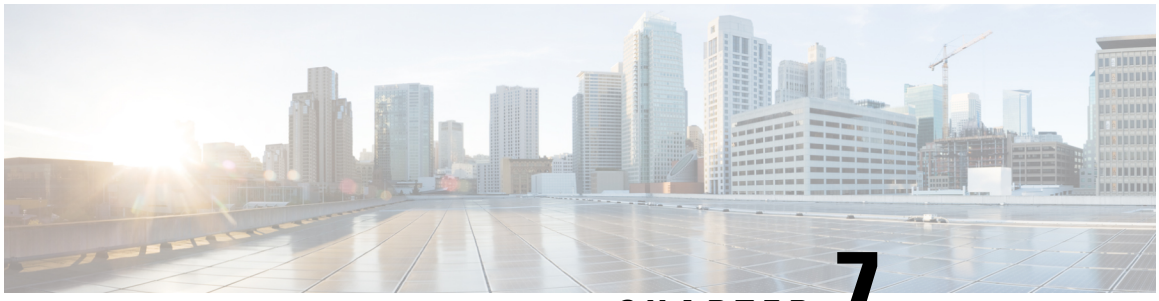
Use Cisco Feature Navigator to find information about the platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release,

feature set, or platform. To access Cisco Feature Navigator, go to the www.cisco.com/go/cfn link. An account on the Cisco.com page is not required.

Note The following table lists the software release in which a given feature is introduced. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 21: Feature Information for Downstream Interface Configuration

Feature Name	Releases	Feature Information
IPDR Streaming Protocol	Cisco IOS XE Everest 16.6.1	This feature was integrated into Cisco IOS XE Everest 16.6.1 on the Cisco cBR Series Converged Broadband Router.



CHAPTER 7

Usage-Based Billing (SAMIS)

This document describes the Usage-based Billing feature for the Cisco Cable Modem Termination System (CMTS) routers, which provides subscriber account and billing information in the Subscriber Account Management Interface Specification (SAMIS) format. The SAMIS format is specified by the Data-over-Cable Service Interface Specifications (DOCSIS) Operations Support System Interface (OSSI) specification.

Finding Feature Information

Your software release may not support all the features that are documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. The Feature Information Table at the end of this document provides information about the documented features and lists the releases in which each feature is supported.

Contents

- Hardware Compatibility Matrix for the Cisco cBR Series Routers, on page 113
- Prerequisites for Usage-Based Billing (SAMIS), on page 114
- Restrictions for Usage-based Billing, on page 115
- Information About Usage-based Billing, on page 116
- How to Configure the Usage-based Billing Feature, on page 126
- Monitoring the Usage-based Billing Feature, on page 151
- Configuration Examples for Usage-based Billing, on page 153

Hardware Compatibility Matrix for the Cisco cBR Series Routers

Note The hardware components that are introduced in a given Cisco IOS-XE Release are supported in all subsequent releases unless otherwise specified.

Table 22: Hardware Compatibility Matrix for the Cisco cBR Series Routers

Cisco CMTS Platform	Processor Engine	Interface Cards
Cisco cBR-8 Converged Broadband Router	**Cisco IOS-XE Release 16.5.1 and Later Releases** Cisco cBR-8 Supervisor: • PID—CBR-SUP-250G • PID—CBR-CCAP-SUP-160G • PID—CBR-CCAP-SUP-60G • PID—CBR-SUP-8X10G-PIC	**Cisco IOS-XE Release 16.5.1 and Later Releases** Cisco cBR-8 CCAP Line Cards: • PID—CBR-LC-8D30-16U30 • PID—CBR-LC-8D31-16U30 • PID—CBR-RF-PIC • PID—CBR-RF-PROT-PIC • PID—CBR-CCAP-LC-40G • PID—CBR-CCAP-LC-40G-R Cisco cBR-8 Downstream PHY Modules: • PID—CBR-D30-DS-MOD • PID—CBR-D31-DS-MOD Cisco cBR-8 Upstream PHY Modules: • PID—CBR-D30-US-MOD • PID—CBR-D31-US-MOD

Prerequisites for Usage-Based Billing (SAMIS)

The Usage-based Billing feature has the following prerequisites:

- Cable modems must be compliant with DOCSIS 1.0 or DOCSIS 2.0, OSSI version 3.0 and DOCSIS 3.0.
- Cable modems that are being monitored should use a DOCSIS configuration file that defines upstream and downstream primary service flows using Service Class Naming (SCN [TLV 24/25, subTLV 4]). If dynamically-created service flows are to be monitored, they should also be created with SCN names.
- When the feature is operating in File mode, an external billing server must log into the Cisco CMTS to copy the billing records to the external server, using either Secure Copy (SCP) or Trivial File Transfer Protocol (TFTP). The Cisco CMTS cannot operate as a FTP or secure FTP (SFTP) server.
- When the feature is operating in Streaming mode in non-secure mode, an external billing server must be configured to receive the billing records at a configurable TCP port.
- When the feature is operating in Streaming mode in secure mode, the following are required:
  - The external billing server must be configured to receive the billing records at a configurable TCP port using a secure socket layer (SSL) connection.

Tip Several third-party solutions for SSL support on the billing application server are available http://www.openssl.org/index.html.

- • A Certificate Authority (CA) must be configured and available to provide the required digital certificates to the billing application and Cisco CMTS router. The CA can be a public CA, such as Verisign, or a server on your private management network that is running software such as the Cisco Provisioning Center (CPC).

- To use the **full-records** keyword, the Cisco CMTS router must be running the Cisco IOS-XE releases.
- To use the **flow-aggregate** keyword for ipdr/ipdr-d3 the Cisco CMTS router must be running the Cisco IOS-XE releases.

When **flow-aggregate** is enabled, the service flows are combined into one record per cable modem:

- • ServiceClassName element always returns a null value in IPDR records, even when service flows on the cable modem have a valid service class name.
  - ServiceIdentifier element always returns a zero value.

Restrictions for Usage-based Billing

The Usage-based Billing feature has the following restrictions and limitations:

- SNMP commands can be used to display or modify the Usage-based Billing configuration, and SNMP traps can be used to notify the billing application system when a billing record is available. However, SNMP commands cannot be used to retrieve billing records.
- Enabling IPDR mode through SNMP is not supported.

During a line card switchover, the items in the line card side are lost. Similarly, during a PRE switchover, those items in the RP side of the sflog file are lost.

If the user uses the SAMIS file destination, a PRE switchover also reinitializes that output file

- Billing records do not include information about multicast service flows and traffic counters.
- The packet counters displayed by CLI commands are reset to zero whenever the Cisco CMTS router is rebooted. The packet counters displayed by SNMP commands are not retained across router reloads, and SNMP MIB counters cannot be preserved during reloads. These counters are 64-bit values and could roll over to zero during periods of heavy usage.
- When configuring cable metering in the usage-based billing File Mode, the source-interface cannot be specified immediately after using the cable metering filesystem command. Once the cable metering filesystem command is used, the cable metering file will write to the bootflash. Until this operation is complete, no cable metering configuration will be allowed. After the file write operation is complete, the source-interface command (cable metering source-interface) can then be configured; and the metering file in the bootflash would need to be removed so that billing packets have the source-interface's IP address.

Note This cable metering restriction will not be a problem during reload.

- When configuring cable metering in the usage-based billing Streaming Mode, make sure that the loopback interface is accessible from the collector server. Telnetting to the IP address of the loopback interface from the collector server is a good method of testing whether the loopback interface is accessible from the collector server or not.

Information About Usage-based Billing

Feature Overview

The Usage-based Billing feature provides a standards-based, open application approach to recording and retrieving traffic billing information for DOCSIS networks. When enabled, this feature provides the following billing information about the cable modems and customer premises equipment (CPE) devices that are using the cable network:

- IP and MAC addresses of the cable modem.
- Service flows being used (both upstream and downstream service flows are tracked).
- IP addresses for the CPE devices that are using the cable modem.
- Total number of octets and packets received by the cable modem (downstream) or transmitted by the cable modem (upstream) during the collection period.
- Total number of downstream packets for the cable modem that the CMTS dropped or delayed because they would have exceeded the bandwidth levels allowed by the subscriber's service level agreement (SLA).

Billing records are maintained in a standardized text format that the service provider can easily integrate into their existing billing applications. Service providers can use this information to determine which users might be potential customers for service upgrades, as well as those customers that might be trying to exceed their SLA limits on a regular basis.

Usage-Based Billing and DOCSIS Support on the Cisco CMTS Routers

The usage-based billing feature supports these DOCSIS features on the Cisco CMTS routers:

- DOCSIS 1.0, DOCSIS 2.0, and DOCSIS 3.0 compliant cable modems are supported.
- Best Effort service flows are supported for DOCSIS-compliant cable modems.
- Secondary service flows are supported for DOCSIS-compliant cable modems.
- Dynamic service flows are supported for DOCSIS-compliant cable modems.
- Information about deleted service flows is available only for DOCSIS 1.1 service flows but not for DOCSIS 1.0 service flows.
- Support for terminated service flows must be enabled using the **cable sflog** command in global mode.

Standards

The Usage-based Billing feature is based on several open standards, allowing it to be supported by a wide range of commercial and custom-written billing applications. The following standards provide the major guidelines for writing and using the billing records that the CMTS produces:

- Extensible Markup Language (XML)—A metalanguage that in turn can easily define other markup languages to contain any kind of structured information, such as billing records. An XML-based approach allows the collected billing information to be used by and distributed among many different billing applications from different vendors. It also allows the format to be easily updated and customized to meet the needs of different providers.
- IP Detail Record (IPDR)—An open, vendor-independent standard, defined in the *Network Data Management—Usage (NDM-U) For IP-Based Services* specification, to simplify billing and usage record-keeping for any type of services that can be delivered over an IP-based network. Service providers can use IPDR to create unified billing applications for all of their services, such as DOCSIS or Voice-over-IP, even though those services use different protocols and application servers.
- DOCSIS Operations Support System Interface (OSSI) specification—A DOCSIS specification that defines the requirements for the network management of a DOCSIS network, including a Subscriber Account Management Interface Specification (SAMIS) for a billing record interface. The DOCSIS 2.0 version of this specification states that a CMTS is not required to provide a billing interface, but if the CMTS does provide a billing interface, it must be based on the IPDR/XML standards.

Tip For further information about these standards, see the documents listed in the “Standards” section on page 38.

IPDR Service Definition Schemas

To standardize the management of objects, service definition schemas are associated with IPDR just as MIBs are associated to SNMP.

For more information, see the OSSI specification document at http://www.cablelabs.com/wp-content/uploads/specdocs/CM-SP-OSSIv3.0-I02-070223.pdf.

The schemas are supported on Cisco IOS-XE releases.

Table 23: IPDR Schema List for DOCSIS 3.0

Category	Service Definition	Schema Definition	Collection Method
SAMIS	SAMIS-TYPE-1	DOCSIS-SAMIS-TYPE-1_3.5.1-A.1.xsd	time interval, ad-hoc
	SAMIS-TYPE-2	DOCSIS-SAMIS-TYPE-2_3.5.1-A.1.xsd	time interval, ad-hoc

Category	Service Definition	Schema Definition	Collection Method
Diagnostic Log Service Definition Schemas	DIAG-LOG-TYPE	DOCSIS-DIAG-LOG-TYPE_3.5.1-A.1.xsd	ad-hoc
	DIAG-LOG-EVENT-TYPE	DOCSIS-DIAG-LOG-EVENT-TYPE_3.5.1-A.1.xsd	event
	DIAG-LOG-DETAIL-TYPE	DOCSIS-DIAG-LOG-DETAIL-TYPE_3.5.1-A.1.xsd	time interval, ad-hoc, event
Spectrum Management	SPECTRUM-MEASUREMENT-TYPE	DOCSIS-SPECTRUM-MEASUREMENT-TYPE_3.5.1-A.1.xsd	time interval, ad-hoc
CMTS CM Registration Status Information	CMTS-CM-REG-STATUS-TYPE	DOCSIS-CMTS-CM-REG-STATUS-TYPE_3.5.1-A.1.xsd	time interval, ad-hoc, event
CMTS CM Upstream Status Information	CMTS-CM-US-STATS-TYPE	DOCSIS-CMTS-CM-US-STATS-TYPE_3.5.1-A.1.xsd	time interval, ad-hoc
CMTS Topology	CMTS-TOPOLOGY-TYPE	DOCSIS-CMTS-TOPOLOGY-TYPE_3.5.1-A.1.xsd	ad-hoc, event
CPE Information	CPE-TYPE	DOCSIS-CPE-TYPE_3.5.1-A.1.xsd	ad-hoc, event
CMTS Utilization Statistics	CMTS-US-UTIL-STATS-TYPE	DOCSIS-CMTS-US-UTIL-STATS-TYPE_3.5.1-A.1.xsd	event
	CMTS-DS-UTIL-STATS-TYPE	DOCSIS-CMTS-DS-UTIL-STATS-TYPE_3.5.1-A.1.xsd	event

The schemas listed in the table are supported by implementing the respective Collectors, which work as SNMP agents to generate these IPDR records according to management information of the system.

IPDR CM-STATUS-2008

Cisco IOS-XE Release 16.5.1 supports the IPDR CM-STATUS 2008 version for forward compatibility to support old IPDR collectors. In the IPDR CM-STATUS 2008 version, the CmtsRcsId and CmtsTcsId objects are 16 bits in length whereas in the CM-STATUS version both these objects are 32 bits in length.

The CmtsRcsId object in the CM-STATUS-2008 version returns the lower 16 bits of value from the CM-STATUS version. But, the CmtsTcsId object returns the same value for both the CM-STATUS-2008 and CM-STATUS version since the value does not exceed 16 bits in both the schemas.

DOCSIS SAMIS Service Definitions

SAMIS for DOCSIS 3.0 service definitions are well structured and has two versions—SAMIS-TYPE-1 and SAMIS-TYPE-2 and provide a different level of information details than SAMIS.

DOCSIS 2.0 SAMIS supports only event session (default type) and DOCSIS 3.0 SAMIS TYPE 1 and DOCSIS 3.0 SAMIS TYPE 2 support only interval and ad-hoc sessions.

SAMIS is collected based on configurable time intervals. Each interval is a different document and the Exporter stops and starts a new session for a new interval. The interval starts from the last metering that has either succeeded or failed, unlike the time-interval session that has a fixed starting point and an interval.

Note The SAMIS schema can be configured with the **cable metering ipdr session** command SAMIS-TYPE-1 and SAMIS-TYPE-2 schemas can be configured through the **cable metering ipdr-d3** command. These schemas are mutually exclusive of each other.

Limitation To DOCSIS SAMIS

- Only schemas that are consistent with the **cable metering ipdr| ipdr-d3** command works. If none of the schemas are consistent, none of them work.
- Changing the SAMIS IPDR type cancels exporting IPDR data.

DOCSIS Diagnostic Log Service Definitions

This service definition defines the IPDR Streaming using a two-step process:

- SNMP or other configuration management interface, such as the CLI is used to configure the Diagnostic Log.
- IPDR/SP is used to stream the Diagnostic Log instances.

These Diagnostic Log service definition schemas support the following collection methods:

- The Cisco CMTS supports streaming of the DIAG-LOG-TYPE record collections as an ad-hoc session.
- The Cisco CMTS supports streaming of DIAG-LOG-EVENT-TYPE record collections as an event session. For event-based Diagnostic Log records, the Cisco CMTS streams the record when the event is logged in the Diagnostic Log and an IPDR message is transmitted to the Collector.
- The DOCSIS-DIAG-LOG-DETAIL-TYPE supports the following collection methods:
  - Time interval—Follows a schedule based on session configuration to export data on a periodic time interval. When a given time interval end is reached, the Exporter collects the diagnostic log, then streams the record to the Collector associated with this session. For time interval based Diagnostic Log records, the Cisco CMTS streams a snapshot of the Diagnostic Log at the scheduled collection time.
  - Ad-hoc—When the Exporter receives a "FlowStart" message, it triggers the application to collect the diagnostic record and send the data to the Collector.
  - Event—When a diagnostic log record is created, an ipdr message is transmitted to the Collector. For more information, see the Operations Support System Interface (OSSI) Specification.

DOCSIS Spectrum Measurement Service Definition

This service definition schema defines the IPDR schema for the enhanced signal quality monitoring feature.

The DOCSIS-SPECTRUM-MEASUREMENT-TYPE schema supports the following collection methods:

- Time interval—Follows a schedule based on session configuration to export data on a periodic time interval. When a given time interval end is reached, the Exporter collects the spectrum information, then streams the records to the Collector.
- Ad-hoc—When the Exporter receives a "FlowStart" message, it triggers the application to collect the spectrum information and send the data to the Collector.

DOCSIS CMTS CM Registration Status Service Definition

This service definition schema defines the IPDR service definition schema for the CMTS CM Registration Status information.

The DOCSIS-CMTS-CM-REG-STATUS-TYPE schema supports the following collection methods:

- Time interval—Follows a schedule based on session configuration to export data on a periodic time interval. When a given time interval end is reached, the Exporter collects the CM status information, then streams the records to the Collector.
- Ad-hoc—When the Exporter receives a "FlowStart" message, it triggers the application to collect all status information of the cable modems and send the data to the Collector.
- Event—When a cable modem goes from "offline" status to "online" or changes to "offline" from "online" (not including intermediate state changes), the Exporter invokes the application to collect the cable modem status information and sends the data to the Collector. For more information, see the Operations Support System Interface (OSSI) Specification.

DOCSIS CMTS CM Upstream Status Service Definition

This service definition schema define the cable modem registration status objects and upstream status objects from the cable modem and the Cisco CMTS perspective. In the CmtsCmUsEqData IPDR schema field, configure the **cable upstream equalization-coefficient** command under the corresponding MAC domain to enable the feature to have data. For more information on this command, see the Cisco IOS CMTS Cable Command Reference Guide .

The DOCSIS-CMTS-CM-US-STATS-TYPE schema support the following collection methods:

- Time interval—Follows a schedule based on session configuration to export data on a periodic time interval. When a given time interval end is reached, the Exporter collects the cable modem upstream status information, then streams the records to the Collector.
- Ad-hoc—When the Exporter receives a "FlowStart" message, it triggers the application to collect all upstream status information of the cable modem and send the data to the Collector.

DOCSIS CMTS Topology Service Definition

In the case of an event session, the event means a change of the topology.

This service definition schema defines the IPDR service definition schema for the CMTS Topology information.

The DOCSIS-CMTS-TOPOLOGY-TYPE schema supports the following collection methods:

- Ad-hoc—Sends the entire picture of all fiber-nodes.
- Event—Sends only the updated channels status of the fiber nodes.

DOCSIS CPE Service Definition

The DOCSIS-CPE-TYPE schema supports the following collection methods:

- Ad-hoc—Follows a schedule based on session configuration to export data on a periodic time interval. When a given time interval end is reached, the Exporter collects the CPE status information, then transfers the records to the Collector.
- Event—When new CPE is added, the status of the CPE changes (including change in IP address), or a new CPE replaces an old one (in this case, two messages are displaced— removal of the old CPE and addition of the new CPE). For more information, see the Operations Support System Interface (OSSI) Specification.

DOCSIS CMTS Utilization Statistics Service Definition

The CMTS Utilization Statistics mainly focuses on channel utilization. It covers CMTS MAC Domain, channel identifier, and the upstream or downstream utilization attributes and counters.

The DOCSIS-CMTS-US-UTIL-STATS-TYPE schemas defines upstream utilization statistics for a specified upstream logical channel interface for the specified Cisco CMTS. The interval can be configured through Channel Utilization Interval.

The DOCSIS-CMTS-DS-UTIL-STATS-TYPE schema defines downstream utilization statistics for a specified downstream interface for the specified Cisco CMTS. The interval can be configured through Channel Utilization Interval.

For more information, see the IPDR Streaming Protocol on the Cisco CMTS Routers guide at the following URL:

IPDR Streaming Protocol

These schemas support only interval-driven event session for the entire downstream and upstream. The interval is defined in the docsIfCmtsChannelUtilizationInterval MIB and it creates document for every exporting.

Note The UsUtilTotalCntnReqDataMslots, UsUtilUsedCntnReqDataMslots, and UsUtilCollCntnReqDataMslots MIBs are not supported on the Cisco CMTS implementation.

The DsUtilTotalBytes MIB for RF Gateway RF channels is the maximum counter of bytes this RF channel can pass during an interval.

Modes of Operation

The Usage-based Billing feature can operate in three modes:

- File Mode—In file mode, the CMTS collects the billing record information and writes the billing records to a file on a local file system, using a file name that consists of the router's hostname followed by a timestamp of when the file was written. A remote application can then log into the CMTS and transfer the billing record file to an external server where the billing application can access it.

The remote application can use the Secure Copy Protocol (SCP) or the Trivial File Transfer Protocol (TFTP) to transfer the file. After a successful transfer, the remote application then deletes the billing record file, which signals the CMTS that it can create a new file. The remote application can either periodically log into the CMTS to transfer the billing record file, or it can wait until the CMTS sends an SNMPv2 trap to notify the application that a billing record file is available.

- Streaming Mode—In streaming mode, the CMTS collects the billing record information and then regularly transmits the billing record file to an application on an external server, using either a non-secure TCP

connection or a secure sockets layer (SSL) connection. The billing record data collected is streamed in real time; and if streaming is unsuccessful, then the SAMIS data is sent only at the next interval.

If the CMTS fails to establish a successful connection with the external server, it retries the connection between one to three times, depending on the configuration. If the CMTS continues to fail to connect with the external server, the Cisco CMTS sends an SNMPv2 trap to notify the SNMP manager that this failure occurred.

In streaming mode, you can configure the CMTS to transmit the billing record file at regular intervals. Typically, the interval chosen would depend on the number of cable modems and the size of the billing record files that the CMTS produces.

- IPDR Mode—In the IPDR mode, the IPDR export process communicates with IPDR Collectors. The architecture supports multiple Collectors distinguished by priority value for failover purposes. The smaller the number of Collectors, the higher is the priority value. Associating one session to two or more Collectors with the same priority value is regarded as random priority. At any given time, data is sent to only the available highest priority Collector. If the highest priority Collector connection fails due to any reason, the data is sent to the next available highest priority Collector. After a higher priority Collector comes back online, it will fail over again. Depending on the network configuration, you can have different primary Collectors for different IPDR sessions. For example, there may be a billing Collector or a diagnostic Collector.

Billing Record Format

Each billing record is an ASCII text file using XML formatting to encode the billing record objects that are required by the DOCSIS specifications. This file can be read by any billing application that can be configured to parse XML data files.

The table lists the objects that are contained in each billing record that the CMTS generates. This table shows the object's name, as it appears in the billing record, and a description of that object.

Table 24: Billing Record Objects

Object Name	Description
IPDRcreationTime	(Appears in header of billing record) Date and time that the CMTS created the billing created.
serviceClassName	Service Class Name (SCN) identifying the service flow (for example, BronzeDS).
CMmacAddress	MAC Address of the cable modem, expressed as six hexadecimal bytes separated by dashes (for example, 00-00-0C-01-02-03).
CMipAddress	IP address for the cable modem, expressed in dotted decimal notation (for example, 192.168.100.101).
CMdocsisMode	Version of DOCSIS QoS provision that the cable modem is currently using (DOCSIS 1.0 or 1.1).
CPEipAddress	IP address for each CPE device that is using this cable modem, expressed in dotted decimal notation. This object is optional and can be suppressed to improve performance by reducing the size of the billing record files.
CMTSipAddress	IP address for the CMTS, expressed in dotted decimal notation.

Object Name	Description
CMTShostName	Fully qualified hostname for the CMTS (for example, cmts01.cisco.com).
CMTSsysUpTime	Amount of time, in hundredths of a second, since the last initialization of the CMTS management interface, expressed as a 32-bit decimal number (0 to 4,294,967,296).
RecType (SFType renamed to RecType in Cisco IOS Release 12.3(17a)BC)	Type of service flow being described: • **Interim**—the service flow was active throughout the collection period and should be reported as 1. • **Stop**—the service flow was deleted at some point during the collection period and should be reported as 2.
serviceIdentifier	Service flow ID assigned to this service flow by the CMTS, expressed as a decimal number. **Note** For DOCSIS 1.0 cable modems, the SFID field always shows the primary service flow for the upstream or downstream.
serviceDirection	Direction for the service flow (**Downstream** or **Upstream**).
serviceOctetsPassed	Total number of octets received by the cable modem (downstream service flows) or transmitted by the cable modem (upstream service flows) during the collection period, expressed as a 64-bit decimal number.
servicePktsPassed	Total number of packets received by the cable modem (downstream service flows) or transmitted by the cable modem (upstream service flows) during the collection period, expressed as a 64-bit decimal number.
SLAdropPkts	(Downstream service flows only) Total number of downstream packets for the cable modem that the CMTS dropped because otherwise they would have exceeded the bandwidth levels allowed by the subscriber's service level agreement (SLA), expressed as a 64-bit decimal number.
SLAdelayPkts	(Downstream service flows only) Total number of packets that the CMTS delayed transmitting on the downstream to the cable modem because otherwise they would have exceeded bandwidth levels allowed by the subscriber's service level agreement (SLA), expressed as a 64-bit decimal number.
CMTScatvIfIndex	The ifIndex of the MAC interface.
CMTScatvIfName	The ifName of the CMTS CATV (MAC) interface associated with this cable modem.
CMTSupIfName	The ifName of the CMTS Upstream interface associated with this cable modem.
CMTSdownIfName	The ifName of the CMTS Downstream interface associated with this cable modem.
CMcpeFqdn	FQDNs for cable modem associated CPEs.

Object Name	Description
serviceTimeCreated	Timestamp for SF creation (consistent with QoS MIB model).
serviceTimeActive	The active time of the SF in seconds.

Note Because the byte and packet counters are 64-bit values, it is possible for them to wrap around to zero during a billing period. The billing application should use the sysUpTime value along with the counters to determine whether the counters have wrapped since the last billing period. If a counter appears to regress, and if the current sysUpTime indicates this billing cycle is the next scheduled cycle for this particular cable modem, you can assume that the counter has wrapped during the billing cycle.

Note These billing record objects are defined in Appendix B, *IPDR Standards Submission for Cable Data Systems Subscriber Usage Billing Records* , in the *DOCSIS 2.0 OSSI Specification* (SP-OSSIv2.0-IO3-021218).

The following example shows a sample IPDR billing record for a downstream service flow:

```
<?xml version="1.0" encoding="UTF-8"?>
<IPDRDoc xmlns="http://www.ipdr.org/namespaces/ipdr"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="DOCSIS-3.1-B.0.xsd"
docId="C341A679-0000-0000-0000-000BBF54D000"
creationTime="2002-05-25T14:41:29Z"
IPDRRecorderInfo="CMTS01"
version="3.1">
</IPDR>
<IPDR xsi:type="DOCSIS-Type">
<IPDRcreationTime>2003-09-18T16:52:34Z</IPDRcreationTime>
<CMTShostname>R7519-UBR7246.cisco.com</CMTShostname>
<CMTSipAddress>1.8.8.21</CMTSipAddress>
<CMTSsysUpTime>287315    </CMTSsysUpTime>
<CMTScatvIfName>Cable8/0/0</CMTScatvIfName>
<CMTScatvIfIndex>13</CMTScatvIfIndex>
<CMTSupIfName>Ca8/0/0-upstream0</CMTSupIfName>
<CMTSupIfType>129</CMTSupIfType>
<CMTSdownIfName>Ca8/0/0-downstream</CMTSdownIfName>
<CMmacAddress>00-00-39-AB-D4-53</CMmacAddress>
<CMdocsisMode>1.0</CMdocsisMode>
<CMipAddress>3.8.21.3</CMipAddress>
<CPEipAddress></CPEipAddress>
<RecType>1</SFtype>
<serviceIdentifier>3</serviceIdentifier>
<serviceClassName></serviceClassName>
<serviceDirection>2</serviceDirection>
<serviceOctetsPassed>23457</ServiceOctetsPassed>
<servicePktsPassed>223</ServicePktsPassed>
<serviceSlaDropPkts>2</serviceSlaDropPkts>
<serviceSlaDelayPkts>0</serviceSlaDelayPkts>
<serviceTimeCreated>11000</serviceTimeCreated>
<serviceTimeActive>15890</serviceTimeActive>
</IPDR>
</IPDRDoc>
```

The following example shows a sample IPDR billing record for an upstream service flow:

<?xml version="1.0" encoding="UTF-8"?>

```
<IPDRDoc xmlns="http://www.ipdr.org/namespaces/ipdr"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="DOCSIS-3.1-B.0.xsd"
docId="docId="C3146152-0000-0000-0000-000BBF7D5800"
creationTime="2003-09-18T16:52:34Z"
IPDRRecorderInfo="CMTS01-UBR7246.cisco.com"
version="3.1">
<IPDR xsi:type=" DOCSIS-Type">
<IPDRcreationTime>2003-09-18T16:52:34Z</IPDRcreationTime>
<CMTShostname>R7519-UBR7246.cisco.com</CMTShostname>
<CMTSipAddress>1.8.8.21</CMTSipAddress>
<CMTSsysUpTime>287315    </CMTSsysUpTime>
<CMTScatvIfName>Cable8/0/0</CMTScatvIfName>
<CMTScatvIfIndex>13</CMTScatvIfIndex>
<CMTSupIfName>Ca8/0/0-upstream0</CMTSupIfName>
<CMTSupIfType>129</CMTSupIfType>
<CMTSdownIfName>Ca8/0/0-downstream</CMTSdownIfName>
<CMmacAddress>00-00-39-18-8A-4D</CMmacAddress>
<CMdocsisMode>1.0</CMdocsisMode>
<CMipAddress>3.8.21.14</CMipAddress>
<CPEipAddress></CPEipAddress>
<RecType>1</SFtype>
<serviceIdentifier>3</serviceIdentifier>
<serviceClassName></serviceClassName>
<serviceDirection>1</serviceDirection>
<serviceOctetsPassed>1404</ServiceOctetsPassed>
<servicePktsPassed>6</ServicePktsPassed>
<serviceSlaDropPkts>0</serviceSlaDropPkts>
<serviceSlaDelayPkts>0</serviceSlaDelayPkts>
<serviceTimeCreated>11000</serviceTimeCreated>
<serviceTimeActive>15890</serviceTimeActive>
</IPDR>
</IPDRDoc>
```

SNMP Support

Cisco cBR Series Converged Broadband Routers support the following MIBs that provide SNMPv2 support for the Usage-based Billing feature:

CISCO-CABLE-METERING-MIB

- Supports configuration of the usage-based billing feature using SNMPv2 commands.
- Displays the current usage-based billing configuration using SNMPv2 commands.
- Sends SNMPv2 traps based on the following usage-based billing events:
  - The Cisco CMTS reports that a new billing record is available.
  - The Cisco CMTS reports that a failure occurred in writing the most recent billing record (for example, the disk is full).
  - The Cisco CMTS reports that it could not successfully open a secure SSL connection to stream a billing record to the billing server.

CISCO-CABLE-WIDEBAND-MIB

Sets the polling interval for calculating the utilization of an RF channel by using the **ccwbRFChanUtilInterval** object.

DOCS-QOS-MIB

- Sets the load and utilization of both upstream and downstream physical channels through the **docsIfCmtsChannelUtilizationInterval** object. This information may be used for capacity planning and incident analysis, and may be particularly helpful in provisioning high value QoS.
- Displays information about all service flows (DOCSIS 1.1 service flows only) including multicast service flow is maintained in the **docsQosServiceFlowLogTable** in DOCS-QOS-MIB, **docsIetfQosServiceFlowLogTable** in DOCS-IETF-QOS-MIB, and **docsQos3ServiceFlowLogTable** in DOCS-QOS3-MIB.

To view information about deleted service flows, enable logging of deleted service flows using the **cable sflog** global configuration command.

Benefits

The usage-based billing feature provides the following benefits to cable service providers and their partners and customers:

- Allows service providers to integrate their billing applications for DOCSIS services with their other XML-capable billing applications.
- Standards-based approach that supports existing networks and services, such as DOCSIS and PacketCable, and is easily extensible to support future services as they are supported on the Cisco CMTS.

How to Configure the Usage-based Billing Feature

This section describes the following tasks that are required to implement the Usage-based Billing feature:

Enabling Usage-based Billing Feature File Mode Using CLI Commands

This section describes how to enable and configure the Usage-based Billing feature so that it operates in file mode, where it writes the billing record files to a local file system. The billing application must then log into the Cisco CMTS and retrieve the billing record files on a regular basis.

Procedure

	Command or Action	Purpose

Step 1	**enable**
	Example:
	`Router> enable`
	Example:
	`Router#`
		Enables privileged EXEC mode. Enter your password if prompted.

	Command or Action	Purpose

Step 2	**configure terminal**
	Example:
	`Router# configure terminal`
	Example:
	`Router(config)#`
		Enters global configuration mode.

Step 3	**cable metering filesystem** *filesys* [**flow-aggregate**] [**cpe-list-suppress**] [**full-records**]
	Example:
	`Router(config)# cable metering filesystem harddisk:`
	Example:
	`Router(config)#`
		Enables the Usage-based Billing feature for file mode and configures it.
		The system will write the billing records on this file system using a file name that contains the hostname of the router followed by a timestamp when the record was written.

Step 4	**snmp-server enable traps cable metering**
	Example:
	`Router(config)# snmp-server enable traps cable metering`
	Example:
	`Router(config)#`
		(Optional) Enables SNMP traps for usage-based billing events. Traps are sent when a new billing record is available, or when the system encountered a failure (such as insufficient disk space) in writing the new billing record.

Step 5	**cable sflog max-entry** *number* **entry-duration** *time*
	Example:
	`Router(config)# cable sflog max-entry 2000 entry-duration 7200`
	Example:
	`Router(config)#`
		(Optional) Enables logging for deleted SNMP service flows, which allows the billing feature to include information about deleted service flows.

Step 6	**cable metering source-interface** *interface*
	Example:
	`Router(config)# cable metering source-interface loopback100`
	Example:
	`Router(config)#`
		(Optional) Enables specification of the source-interface for the billing packets, usually a loopback interface.

	Command or Action	Purpose

Step 7	**end**
	Example:
	`Router(config)# end`
	Example:
	`Router#`
		Exits global configuration mode and returns to privileged EXEC mode.

Enabling Usage-based Billing Feature File Mode Using SNMP Commands

This section describes how to enable and configure the Usage-based Billing feature so that it operates in file mode and writes the billing record files to a local file system. The billing application must then log into the Cisco CMTS and retrieve the billing record files on a regular basis.

To configure the Cisco CMTS for Usage-based Billing feature in file mode, you must set a number of objects in the CISCO-CABLE-METERING-MIB.

In addition, to include information about deleted service flows in the billing records (supported for DOCSIS 1.1 service flows), you must enable the logging of deleted service flows, using the **cable sflog** global configuration command.

Table 25: SNMP Objects to be Configured for File Mode

Object	Type	Description
ccmtrCollectionType	Integer	Enables or disables the Usage-based Billing feature. The valid values are: • 1—none. The Usage-based Billing feature is disabled (default). • 2—local. The Usage-based Billing feature is enabled and configured for file mode. • 3—stream. The Usage-based Billing feature is enabled and configured for streaming mode. Set ccmtrCollectionType to 2 (local) to enable the feature for file mode.
ccmtrCollectionFilesystem	DisplayString	Specifies the file system where the billing record file should be written. This object has a maximum length of 25 characters and must specify a valid file system on the router (such as slot0, disk1, or flash). **Note** The Cisco CMTS writes the billing records to this file system using a file name that consists of the router's hostname followed by a timestamp when the record was written.
ccmtrCollectionCpeList	TruthValue	(Optional) Indicates whether IP addresses for customer premises equipment (CPE) devices are omitted from the billing records, so as to reduce the size of the billing records and to improve performance. The valid values are the following: • true—CPE information is present (default). • false—CPE information is omitted. **Note** When set to true, a maximum of 5 CPE IP addresses for each cable modem.

Object	Type	Description
ccmtrCollectionAggregate	TruthValue	(Optional) Indicates whether all information for an individual cable modem is combined into one record. Separate counters are maintained for upstream and downstream traffic, but those counters include all service flows in that direction. The valid values are as follows: • true—All service flow information for each cable modem is aggregated into a single billing record. In this configuration, the service flow ID (SFID) for the billing record is set to 0 and the service class name (SCN) is blank. • false—Information for each cable modem is not aggregated into a single billing record, but instead each service flow is recorded into its own record (default).
ccmtrCollectionSrcIfIndex	TruthValue	(Optional) Specifies the source-interface for the billing packets.

Note The following steps use the standard SNMP commands that are available on many Unix and Linux systems. For each step, replace *ip-address* with the IP address of the Cisco CMTS, and replace *rw-community-string* with an SNMP community string that provides read-write access to the router.

Step 1 Set the ccmtrCollectionType object to 2, to enable the Usage-based Billing feature and to configure it for file mode:

Example:

```
workstation# setany -v2c

ip-address rw-community-string

ccmtrCollectionType.0 -i 2

workstation#
```

Step 2 Set the ccmtrCollectionFilesystem object to the local file system where the Cisco CMTS should write the billing records:

Example:

```
workstation# setany -v2c

ip-address rw-community-string
 ccmtrCollectionFilesystem.0 -D disk0:

workstation#
```

Step 3 (Optional) To omit the IP addresses of CPE devices from the billing records, set the ccmtrCollectionCpeList object to 2 (false). The default is to include the CPE information.

Example:

```
workstation# setany -v2c

ip-address rw-community-string
 ccmtrCollectionCpeList.0 -i 2
workstation#
```

Step 4 (Optional) To aggregate all service flow information for each cable modem in a single record, set the ccmtrCollectionAggregate object to 1 (true). The default is for each service flow to be written in a separate record:

Example:

```
workstation# setany -v2c

ip-address rw-community-string
 ccmtrCollectionAggregate.0 -i 1
workstation#
```

Step 5 (Optional) To specify the source-interface for the billing packets, set the ccmtrtrCollectionSrcIfIndex object to 1 (true). The default is for the billing packets to automatically select a source-interface.

Example:

```
workstation# setany -v2c

ip-address rw-community-string
 ccmtrtrCollectionSrcIfIndex.0 -i 1
workstation#
```

Examples for Enabling Usage Billing using SNMP Mode

The following example shows the Usage-based Billing feature being configured using SNMP commands. The following display shows that a Cisco CMTS router at IP address 10.8.8.21 is configured with the default configuration (the Usage-based Billing feature is disabled):

```
workstation# getmany -v2c 10.8.8.21 rw-string ciscoCableMeteringMIB

ccmtrCollectionType.0 = none(1)
ccmtrCollectionFilesystem.0 =
ccmtrCollectionCpeList.0 = true(1)
ccmtrCollectionAggregate.0 = false(2)
ccmtrCollectionStatus.0 = 0
ccmtrCollectionDestination.0 =
ccmtrCollectionTimestamp.0 = 00 00  00 00   00 00  00 00
ccmtrCollectionNotifEnable.0 = true(1)
workstation#
```

The following SNMP commands are then given to enable the Usage-based Billing feature and to configure it for file mode:

```
workstation# setany -v2c 10.8.8.21 rw-string ccmtrCollectionType.0 -i 2
workstation# setany -v2c 10.8.8.21 rw-string
ccmtrCollectionFilesystem
.0 -D disk1:
workstation#
```

These commands add the following line to the router's running configuration file:

```
Router# show running-config | include metering

cable metering filesystem disk1:
```

```
Router#
```

The following SNMP display shows the new configuration, after the Cisco CMTS has successfully written a billing record:

```
workstation# getmany -v2c 10.8.8.21 rw-string ciscoCableMeteringMIB

ccmtrCollectionType.0 = local(2)
ccmtrCollectionFilesystem.0 = disk1:
ccmtrCollectionCpeList.0 = true(1)
ccmtrCollectionAggregate.0 = false(2)
ccmtrCollectionStatus.0 = success(1)
ccmtrCollectionDestination.0 = disk1:UBR7246.cisco.com-20030925-185827
ccmtrCollectionTimestamp.0 = 07 d3  09 19   12 3a  1c 00
ccmtrCollectionNotifEnable.0 = true(1)
workstation#
```

Enabling Usage-based Billing Feature Streaming Mode Using CLI Commands

This section describes how to enable and configure the Usage-based Billing feature so that it operates in streaming mode, where it regularly transmits the billing records to an external server for use by the billing application.

Procedure

	Command or Action	Purpose

Step 1	**enable**
	Example:
	`Router> enable`
	Example:
	`Router#`
		Enables privileged EXEC mode. Enter your password if prompted.

Step 2	**configure terminal**
	Example:
	`Router# configure terminal`
	Example:
	`Router(config)#`
		Enters global configuration mode.

Step 3	**cable metering destination** *ip-address port* [*ip-address2 port2*] *retries minutes* {**non-secure** | **secure**} [**flow-aggregate**] [**cpe-list-suppress**] [**full-records**] **Example:** `Router(config)# cable metering destination 10.10.21.3 5300 10.10.21.4 5300 2 30 secure`	Enables the Usage-based Billing feature for streaming mode and configures it with the following parameters:

	Command or Action	Purpose
	Example: `Router(config)#`	

Step 4	**snmp-server enable traps cable metering**
	Example:
	`Router(config)# snmp-server enable traps cable metering`
	Example:
	`Router(config)#`
		(Optional) Enables SNMP traps for usage-based billing events. Traps are sent when a new billing record is available, or when the system encountered a failure (such as insufficient disk space) in writing the new billing record.

Step 5	**cable sflog max-entry** *number* **entry-duration** *time*
	Example:
	`Router(config)# cable sflog max-entry 2000 entry-duration 7200`
	Example:
	`Router(config)#`
		(Optional) Enables logging for deleted SNMP service flows, which allows the billing feature to include information about deleted service flows.

Step 6	**cable metering source-interface** *interface*
	Example:
	`Router(config)# cable metering source-interface loopback100`
	Example:
	`Router(config)#`
		(Optional) Enables specification of the source-interface for the billing packets, usually a loopback interface.

Step 7	**end**
	Example:
	`Router(config)# end`
	Example:
	`Router#`
		Exits global configuration mode and returns to privileged EXEC mode.

Enabling Usage-based Billing Feature Streaming Mode Using SNMP Commands

This section describes how to use SNMP commands to enable and configure the Usage-based Billing feature so that it operates in streaming mode, where it regularly transmits the billing records to an external server for use by the billing application.

To configure the Cisco CMTS for Usage-based Billing feature in streaming mode, you must set a number of objects in the CISCO-CABLE-METERING-MIB.

Note In addition, to include information about deleted service flows (DOCSIS 1.1 service flows only) in the billing records, you must enable the logging of deleted service flows, using the **cable sflog** global configuration command. See the *Cisco IOS CMTS Cable Command Reference Guide* on Cisco.com:

Cisco CMTS Cable Command Reference

Table 26: SNMP Objects to be Configured for Streaming Mode

Object	Type	Description
ccmCollectionType	Integer	Enables or disables the Usage-based Billing feature. The valid values are: • 1—none. The Usage-based Billing feature is disabled (default). • 2—local. The Usage-based Billing feature is enabled and configured for file mode. • 3—stream. The Usage-based Billing feature is enabled and configured for streaming mode. Set ccmCollectionType to 3 (stream) to enable the feature for streaming mode.
ccmCollectionIpAddress	InetAddress	IP address for the external collection server. This value must be specified.
ccmCollectionPort	Unsigned32	TCP port number at the external collection server to which the billing records should be sent. The valid range is 0 to 65535, but you should not specify a port in the well-known range of 0 to 1024. This value must be specified.
Note You can configure the ccmCollectionIpAddress and ccmCollectionPort objects twice, to specify a primary collection server and a secondary collection server.		
ccmCollectionIpAddrType	InetAddressType	(Optional) Type of IP address being used for the collection server. The only valid value is ipv4, which is the default value.
ccmCollectionInterval	Unsigned32	(Optional) Specifies how often, in minutes, the billing records are streamed to the external server. The valid range is 2 to 1440 minutes (24 hours), with a default of 30 minutes. (We recommend a minimum interval of 30 minutes.)
ccmCollectionRetries	Unsigned32	(Optional) Specifies the number of retry attempts that the CMTS will make to establish a secure connection with the external server before using the secondary server (if configured) and sending an SNMP trap about the failure. The valid range for *n* is 0 to 5, with a default of 0.
Note The ccmCollectionInterval and ccmCollectionRetries parameters are optional when configuring usage-based billing for streaming mode with SNMP commands, but these parameters are required when configuring the feature with CLI commands.		

Object	Type	Description
ccmCollectionSecure	TruthValue	(Optional) Specifies whether the Cisco CMTS should use a secure socket layer (SSL) connection when connecting with the billing application on the external server. The valid values are: • true(1)—The Cisco CMTS uses a SSL connection. This option is available only on CMTS software images that support Baseline Privacy Interface (BPI) encryption. • false(2)—The Cisco CMTS uses an unencrypted TCP connection. This is the default value.
ccmCollectionCpeList	TruthValue	(Optional) Indicates whether IP addresses for customer premises equipment (CPE) devices are omitted from the billing records, so as to reduce the size of the billing records and to improve performance. The valid values are the following: • true—CPE information is present (default). • false—CPE information is omitted. **Note** When set to true, a maximum of 5 CPE IP addresses for each cable modem.
ccmCollectionAggregate	TruthValue	(Optional) Indicates whether all information for an individual cable modem is combined into one record. Separate counters are maintained for upstream and downstream traffic, but those counters include all service flows in that direction. The valid values are as follows: • true—All service flow information for each cable modem is aggregated into a single billing record. In this configuration, the service flow ID (SFID) for the billing record is set to 0 and the service class name (SCN) is blank. • false—Information for each cable modem is not aggregated into a single billing record, but instead each service flow is recorded into its own record (default).
ccmtrCollectionSrcIfIndex	TruthValue	(Optional) Specifies the source-interface for the billing packets.

Note The following steps use the standard SNMP commands that are available on many Unix and Linux systems. For each step, replace *ip-address* with the IP address of the Cisco CMTS, and replace *rw-community-string* with an SNMP community string that provides read-write access to the router.

Step 1 Set the ccmCollectionType object to 3, to enable the Usage-based Billing feature and to configure it for streaming mode:

Example:

```
workstation# setany -v2c
ip-address rw-community-string
 ccmCollectionType.0 -i 3
workstation#
```

Step 2 Set the ccmCollectionIpAddress and ccmCollectionPort objects to the IP address of the external collection server and the TCP port number to which billing records should be sent:

Example:

```
workstation# setany -v2c
ip-address rw-community-string
 ccmCollectionIpAddress.1 -o '0a 08 06 0b'

workstation# setany -v2c
ip-address rw-community-string
 ccmCollectionPort.1 -g 6789

workstation#
```

Step 3 (Optional) Set the ccmCollectionIpAddress and ccmCollectionPort objects a second time to specify the IP address and TCP port number of a second external collection server to which billing records should be sent, in the case that the Cisco CMTS cannot connect to the primary collection server:

Example:

```
workstation# setany -v2c
ip-address rw-community-string
 ccmCollectionIpAddress.1 -o '0a 08 06 0c'

workstation# setany -v2c
ip-address rw-community-string
 ccmCollectionPort.1 -g 7000

workstation#
```

Step 4 (Optional) To change any of the other default parameters, set the appropriate objects to the desired values. For example, the following lines configure the Usage-based Billing feature for a non-secure connection, with a collection interval of 45 minutes, and a maximum number of 3 retries.

Example:

```
workstation# setany -v2c
ip-address rw-community-string
 ccmCollectionSecure.1 -i 2
workstation# setany -v2c
ip-address rw-community-string
 ccmCollectionInterval.1 -i 45
workstation# setany -v2c
ip-address rw-community-string
 ccmCollectionRetries.1 -i 3
workstation#
```

Step 5 (Optional) To omit the IP addresses of CPE devices from the billing records, set the ccmCollectionCpeList object to 2 (false). The default is to include the CPE information.

Example:

```
workstation# setany -v2c

ip-address rw-community-string
 ccmCollectionCpeList.0 -i 2
workstation#
```

Step 6 (Optional) To aggregate all service flow information for each cable modem in a single record, set the ccmCollectionAggregate object to 1 (true). The default is for each service flow to be written in a separate record:

Example:

```
workstation# setany -v2c

ip-address rw-community-string
 ccmCollectionAggregate.0 -i 1
workstation#
```

Step 7 (Optional) To specify the source-interface for the billing packets, set the ccmtrCollectionSrcIfIndex object to 1 (true). The default is for the billing packets to automatically select a source-interface.

Example:

```
workstation# setany -v2c

ip-address rw-community-string
 ccmtrCollectionSrcIfIndex.0 -i 1
workstation#
```

Examples for SNMP Commands

The following example shows the Usage-based Billing feature being configured using SNMP commands. The following display shows that a Cisco CMTS router at IP address 10.8.8.21 is configured with the default configuration (the Usage-based Billing feature is disabled):

```
workstation# getmany -v2c 10.8.8.21 rw-string ciscoCableMeteringMIB

ccmCollectionType.0 = none(1)
ccmCollectionFilesystem.0 =
ccmCollectionCpeList.0 = true(1)
ccmCollectionAggregate.0 = false(2)
ccmCollectionStatus.0 = 0
ccmCollectionDestination.0 =
ccmCollectionTimestamp.0 = 00 00  00 00   00 00  00 00
ccmCollectionNotifEnable.0 = true(1)
workstation#
```

The following SNMP commands are then given to enable the Usage-based Billing feature and to configure it for streaming mode:

```
workstation# setany -v2c 10.8.8.21 rw-string ccmCollectionType.0 -i 3
workstation# setany -v2c 10.8.8.21 rw-string ccmCollectionIpAddress.1 -o '0a 08 06 0b'

workstation# setany -v2c 10.8.8.21 rw-string ccmCollectionPort.1 -g 6789

workstation# setany -v2c 10.8.8.21 rw-string ccmCollectionSecure.1 -i 2
workstation# setany -v2c 10.8.8.21 rw-string ccmCollectionRetries.1 -i 3
workstation# setany -v2c 10.8.8.21 rw-string ccmCollectionInterval.1 -i 45
workstation#
```

These commands add the following line to the router's running configuration file:

```
Router# show running-config | include metering

cable metering destination 10.8.6.11 6789 3 45 non-secure
Router#
```

The following SNMP display shows the new configuration:

```
workstation# getmany -v2c 10.8.8.21 rw-string ciscoCableMeteringMIB

ccmCollectionType.0 = stream(3)
ccmCollectionFilesystem.0 =
ccmCollectionIpAddrType.1 = ipv4(1)
ccmCollectionIpAddress.1 = 0a 08  06 0b
ccmCollectionPort.1 = 6789
ccmCollectionInterval.1 = 45
ccmCollectionRetries.1 = 3
ccmCollectionSecure.1 = false(2)
ccmCollectionRowStatus.1 = active(1)
ccmCollectionCpeList.0 = true(1)
ccmCollectionAggregate.0 = false(2)
ccmCollectionStatus.0 = 0
ccmCollectionDestination.0 =
ccmCollectionTimestamp.0 = 00 00  00 00   00 00  00 00
ccmCollectionNotifEnable.0 = true(1)
workstation#
```

Enabling and Configuring the Secure Copy Protocol (optional)

This section describes how to configure the Cisco CMTS for the Secure Copy Protocol (SCP), which allow an external server to log in to the Cisco CMTS and copy the billing records from the Cisco CMTS to the external server.

Procedure

	Command or Action	Purpose

Step 1	**enable**
	Example:
	`Router> enable`
	Example:
	`Router#`
		Enables privileged EXEC mode. Enter your password if prompted.

Step 2	**configure terminal** **Example:** `Router# configure terminal` **Example:**	Enters global configuration mode.

	Command or Action	Purpose
	`Router(config)#`	

Step 3	**aaa new-model**
	Example:
	`Router(config)# aaa new-model`
	Example:
	`Router(config)#`
		Enables the Authentication, Authorization, and Accounting (AAA) access control model.

Step 4	**aaa authentication login** {**default** | *list-name* } *method1* [*method2 ...*]
	Example:
	`Router(config)# aaa authentication login default enable`
	Example:
	`Router(config)#`
		Enables AAA access control authentication at login, using the following parameters:
		Valid methods include **enable**, **line**, and **local**.

Step 5	**aaa authorization exec** {**default** | *list-name* } *method1* [*method2 ...*]
	Example:
	`Router(config)# aaa authorization exec default local`
	Example:
	`Router(config)#`
		Configures the CMTS to allow users to run an EXEC shell and access the CLI to run the Secure Copy commands.
		Valid methods include **local**.

Step 6	**username** *name* **privilege** *level* **password** *encryption-type password*
	Example:
	`Router(config)# username billingapp privilege 15 password 7 billing-password`
	Example:
	`Router(config)#`
		(Optional) Creates a user account for login access and specifies the privilege level and password for that account:
		Note This step is optional but for the purposes of security and management, Cisco recommends creating a unique account for the billing application to use when logging into the CMTS.

Step 7	**ip ssh time-out** *seconds* **Example:** `Router(config)# ip ssh time-out 120` **Example:**	Enables Secure Shell (SSH) access on the Cisco CMTS, which is required for SCP use. The *seconds* parameter specifies the maximum time allowed for SSH authentication, in seconds, with a valid range of 0 to 120 seconds, with a default of 120 seconds.

	Command or Action	Purpose
	`Router(config)#`	

Step 8	**ip ssh authentication-retries** *n*
	Example:
	`Router(config)# ip ssh authentication-retries 3`
	Example:
	`Router(config)#`
		Specifies the maximum number of login attempts a user is allowed before the router disconnects the SSH session. The valid range is 1 to 5, with a default of 3 attempts.

Step 9	**ip scp server enable**
	Example:
	`Router(config)# ip scp server enable`
	Example:
	`Router(config)#`
		Enables SCP access on the Cisco CMTS.

Step 10	**end**
	Example:
	`Router(config)# end`
	`Router#`
		Exits global configuration mode and returns to privileged EXEC mode.

Configuring the Cisco CMTS for SSL Operation

This section describes the procedures to configure the Cisco CMTS for secure socket layer (SSL) operation, so that the Usage-based Billing feature can use an SSL connection to transfer the billing record files in streaming mode.

Note This procedure is required only when using the **secure** option with the **cable metering destination** command.

Prerequisites for CA

- The billing application server must be configured for SSL operations.
- A Certificate Authority (CA) must be configured to provide the required digital certificates to the billing application and Cisco CMTS router. The CA can be a public CA, such as Verisign, or a server on your private management network that is running software such as the Cisco Provisioning Center (CPC).

SUMMARY STEPS

To prepare the Cisco CMTS router for SSL operation, you must perform the following configuration steps:

- Configuring the router's host name and IP domain name, if not already done.
- Generating an RSA key pair.
- Declaring a Certification Authority.

- Configuring a Root CA (Trusted Root).
- Authenticating the CA.
- Requesting the Certificates.

For the detailed steps in performing these procedures, see the Configuring Certification Authority Interoperability

Retrieving Records from a Cisco CMTS in File Mode

When the Usage-based Billing feature is enabled and configured for File mode, the billing application server must regularly retrieve the billing records from the Cisco CMTS. This is typically done by a script that either logs in to the Cisco CMTS and uses CLI commands to transfer the file, or by a script that uses SNMP commands to transfer the file.

When using CLI commands, the procedure is typically as follows:

1. The billing application server receives an SNMP trap from the Cisco CMTS when a billing record is written. This notification contains the file name of the billing record that should be retrieved.
2. The billing application server starts a custom-written script to retrieve the billing record. This script would do one of the following:
   a. If using CLI commands, the script logs in to the Cisco CMTS using a telnet connection, and then transfers the billing record to the billing application server, using the **copy** CLI command. The transfer can be done using either the Secure Copy Protocol (SCP) or the Trivial File Transfer Protocol (TFTP).

Note You could also use the File Transfer Protocol (FTP) to transfer files from the Cisco CMTS to an external FTP server, but this is not recommended, because the FTP protocol transmits the login username and password in cleartext.

   b. If using SNMP commands, the script sets the ciscoFlashCopyEntry objects in the CISCO-FLASH-MIB to transfer the billing record to the application server, using TFTP.
3. After transferring the billing record, the script deletes it on the Cisco CMTS file system, so that the Cisco CMTS can begin writing a new billing record.

The following sections show examples of how this can be done, using each method.

Tip The following examples are given for illustration only. Typically, these commands would be incorporated in automated scripts that would retrieve the billing records.

Using SCP

To transfer billing records using SCP, you must first enable and configure the router for SCP operation, using the procedure given in the “Enabling and Configuring Secure Copy (optional)” section on page 21 . Then, the application server must log in to the Cisco CMTS and use the **copy** command at the privileged EXEC prompt. The **copy** command needs to specify the location of the billing record on the local filesystem and the destination server for the SCP transfer.

The following example shows a typical session where a billing record on slot0 is transferred to an FTP server with the hostname of billserver.mso-example.com:

```
CMTS01# copy slot0:CMTS01_20030211-155025 scp://billingapp-server.mso-example.com/

Address or name of remote host [billingapp-server.mso-example.com]?
Destination username [billing-app]?
Destination filename [CMTS01_20030211-155025]?
Writing CMTS01_20030211-155025
Password: billing-password

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 1403352/1024 bytes]
1403352 bytes copied in 17.204 secs (85631 bytes/sec)
CMTS01# delete slot0:CMTS01_20030211-155025

CMTS01# squeeze slot0:

CMTS01#
```

Note The billing application must delete the billing record after it has been successfully transferred, so that the Cisco CMTS can write the next record. The **squeeze** command frees up the deleted disk space on Flash Memory and old-style PCMCIA cards (bootflash, flash, slot0, slot1). It is not needed on the newer ATA-style PCMCIA cards (disk0, disk1, disk2). However, because the **squeeze** command takes several seconds to complete, it should be given only when insufficient disk space exists for a new billing record. To avoid this problem, Cisco recommends using a 64 MB (or larger) ATA-style PCMCIA memory card, which automatically reclaims disk space for deleted files.

Using TFTP

To transfer billing records using TFTP, you must first configure an external workstation to be a TFTP server. For security, the TFTP server should be isolated from the Internet or any external networks, so that only authorized TFTP clients, such as the Cisco CMTS router, can access the server.

To transfer the billing records, the application server must log in to the Cisco CMTS and use the **copy** command at the privileged EXEC prompt. The **copy** command needs to specify the location of the billing record on the local filesystem and the destination server for the TFTP transfer.

The following example shows a typical session where a billing record on slot0 is transferred to an TFTP server with the hostname of billserver.mso-example.com.

```
Router# copy slot0:CMTS01_20030211-155025 tftp://billingapp-server.mso-example.com/incoming

Address or name of remote host [billingapp-server.mso-example.com]?
Destination username [billing-app]?
Destination filename [CMTS01_20030211-155025]?
Writing CMTS01_20030211-155025
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 1102348/1024 bytes]
1102348 bytes copied in 14.716 secs (63631 bytes/sec)
Router# delete slot0:CMTS01_20030211-155025

Router# squeeze slot0:

Router#
```

Note The billing application must delete the billing record after it has been successfully transferred, so that the Cisco CMTS can write the next record. The **squeeze** command frees up the deleted disk space on Flash Memory and old-style PCMCIA cards (bootflash, flash, slot0, slot1). It is not needed on the newer ATA-style PCMCIA cards (disk0, disk1, disk2). However, because the **squeeze** command takes several seconds to complete, it should be given only when insufficient disk space exists for a new billing record. To avoid this problem, Cisco recommends using a 64 MB (or larger) ATA-style PCMCIA memory card, which automatically reclaims disk space for deleted files.

Using SNMP

To transfer billing record file using SNMP commands, you must set a number of objects in the CISCO-FLASH-MIB to transfer the file to a TFTP server. After the file has been successfully transferred, you can then use SNMp commands to delete the billing record file.

Note Before proceeding with these steps, ensure that the TFTP server is properly configured to receive to receive the billing records. At the very least, this means creating a directory that is readable and writable by all users. On some servers, the TFTP server software also requires that you create a file with the same name as the file that is to be received, and this file should also be readable and writable by all users.

To transfer a billing record file to a TFTP server, using SNMP commands, you must set a number of objects in the CISCO-FLASH-MIB.

Table 27: Transferring a File to a TFTP Server Using SNMP Commands

Object	Type	Description
ciscoFlashCopyEntryStatus	RowStatus	Status of this table entry. Typically, this object is first set to 5 (create-and-wait). Then after all other parameters are specified, it is set to Active (1) to execute the command.
ciscoFlashCopyCommand	INTEGER	Type of copy command to be performed. To copy a billing record file to a TFTP server, set this object to 3 (copyFromFlash).
ciscoFlashCopyServerAddress	IpAddress	IP address of the TFTP server. **Note** This parameter defaults to the broadcast address of 255.255.255.255, which means it will transfer the billing record file to the first TFTP server that responds. For security, this object should always be set to the IP address of the authorized TFTP server.
ciscoFlashCopySourceName	DisplayString	Name of the billing record file to be transferred, including the Flash device on which it is stored.

Object	Type	Description
ciscoFlashCopyDestinationName	DisplayString	(Optional) Name for the billing record, including path, on the TFTP server. If not specified, the copy operation defaults to saving the billing record at the top-most directory on the TFTP server, using the original file name. **Note** A file with the destination file name should already exist on the TFTP server. This file should be readable and writable by all users, so that it can be replaced with the billing record file.
ciscoFlashCopyProtocol	INTEGER	(Optional) Specifies the protocol to be used when copying the file. For a TFTP transfer, set this object to 1 (tftp), which is the default.
ciscoFlashCopyNotifyOnCompletion	TruthValue	(Optional) Specifies whether the Cisco CMTS should generate a trap upon the completion of the copy operation. The default is false (no trap is generated).

After transferring the billing records file, you must then set a number of objects in the CISCO-FLASH-MIB to delete the file, so that the Cisco CMTS can begin writing a new file. If the Flash memory is not ATA-compatible, you must also set a number of objects to squeeze the Flash memory to make the deleted space available for new files. Table 28: Deleting a File Using SNMP Commands , on page 143 describes each of these objects, and whether they are required or optional.

Table 28: Deleting a File Using SNMP Commands

Object	Type	Description
ciscoFlashMiscOpCommand	INTEGER	Specifies the operation to be performed: • 3—Delete the file. • 5—Squeeze the Flash memory, so as to recover the deleted space and make it available for new files.
ciscoFlashMiscOpDestinationName	DisplayString	When deleting a file, the name of the file to be deleted, including the name of the file system, up to a maximum of 255 characters. When squeezing a file system, the name of the file system to be squeezed (slot0:, slot1:, flash:, or bootflash:).
ciscoFlashMiscOpEntryStatus	RowStatus	Status of this table entry. Typically, this object is first set to 5 (create-and-wait). Then after all other parameters are specified, it is set to Active (1) to execute the command.
ciscoFlashMiscOpNotifyOnCompletion	TruthValue	(Optional) Specifies whether the Cisco CMTS should generate a trap upon the completion of the operation. The default is false (no trap is generated).

DETAILED STEPS

Note The following steps use the standard SNMP commands that are available on many Unix and Linux systems. For each step, replace *ip-address* with the IP address of the Cisco CMTS, and replace *rw-community-string* with an SNMP community string that provides read-write access to the router.

Copying the Billing Record File to the TFTP Server

Step 1 The script performing the copy should generate a 32-bit number to be used as the index entry for this copy command. The script can generate this number in any convenient way, so long as the index number is not currently being used for another operation.

Step 2 Create the table entry for the copy command, by using the number that was generated in Step 1 and setting the ciscoFlashCopyEntryStatus object to the create-and-wait state (5):

Example:

```
workstation# setany -v2c ip-address rw-community-string ciscoFlashCopyEntryStatus.582 -i 5

workstation#
```

Step 3 Set the ciscoFlashCopyCommand to 3 (copyFromFlash) to specify that the billing record file should be copied from the router's Flash file system:

Example:

```
workstation# setany -v2c ip-address rw-community-string ciscoFlashCopyCommand
.582

-i 3
workstatioN#
```

Step 4 Set the ciscoFlashCopyServerAddress object to the IP address of the TFTP server:

Example:

```
workstation# setany -v2c ip-address rw-community-string ciscoFlashCopyServerAddress
.582

-a "172.20.12.193"

workstatioN#
```

Step 5 Set the ciscoFlashCopySourceName object to the file name, including the device name, of the billing record file to be transferred:

Example:

```
workstation# setany -v2c ip-address rw-community-string ciscoFlashCopySourceName
.582
-D
"slot0:CMTS01_20030211-155025
"
workstation#
```

Step 6 (Optional) To specify a specific destination on the TFTP server, set the ciscoFlashCopyDestinationName object to the path name and file name for the billing record file on the TFTP server. (Typically, the path name and file name should already exist on the TFTP server.)

Example:

```
workstation# setany -v2c ip-address rw-community-string ciscoFlashCopyDestinationName
.582
-D
```

```
"/cmts01-billing/billing-file
"
workstation#
```

Step 7 To execute the command, set the ciscoFlashCopyEntryStatus object to the active state (1):

Example:

```
workstation# setany -v2c ip-address rw-community-string ciscoFlashCopyEntryStatus.582 -i 1

workstation#
```

Step 8 Periodically poll the ciscoFlashCopyStatus object until the file transfer completes:

Example:

```
workstation# getmany -v2c ip-address rw-community-string ciscoFlashCopyStatus
.582
  ciscoFlashCopyStatus.582 = copyInProgress(1)
workstation# getmany -v2c ip-address rw-community-string ciscoFlashCopyStatus
.582
  ciscoFlashCopyStatus.582 = copyInProgress(1)
workstation# getmany -v2c ip-address rw-community-string ciscoFlashCopyStatus
.582
  ciscoFlashCopyStatus.582 = copyOperationSuccess(2)
workstation#
```

If the file transfer fails, the most common status values that are reported by the ciscoFlashCopyStatus object are:

- 3—copyInvalidOperation. This indicates that the operation failed on the TFTP server, typically because the destination file name and path name do not exist on the TFTP server, or they exist but are not writable by all users.
- 5—copyInvalidSourceName. The file name for the billing record, as specified in ciscoFlashCopySourceName does not exist. Verify that you specified the correct device name and that no spaces exist in the file name.
- 6—copyInvalidDestName. The destination path name and file name specified in ciscoFlashCopyDestinationName is not accessible on the TFTP server. This could be because the path name does not exist or is not configured to allow write-access. This error could also occur if a file with the same path name and file name already exists on the TFTP server.
- 7—copyInvalidServerAddress. The IP address of the TFTP server specified in ciscoFlashCopyServerAddress is invalid, or the TFTP server is not responding.
- 14—copyFileTransferError. A network error occurred that prevented the file transfer from completing.

Step 9 After the file transfer has completed successfully, set the ciscoFlashCopyEntryStatus object to 6 (delete) to delete the row entry for this copy command:

Example:

```
workstation# setany -v2c ip-address rw-community-string ciscoFlashCopyEntryStatus.582 -i 6

workstation#
```

What to do next

Deleting the Billing Record File

Using SNMP

After the billing record file has been successfully transferred, use the following procedure to delete the billing record on the Cisco CMTS flash file system, so that the Cisco CMTS can write the new billing record.

Step 1 Generate another random number to be used as an index entry and configure the following objects in the ciscoFlashMiscOpTable:

Example:

```
workstation# setany -v2c ip-address rw-community-string ciscoFlashMiscOpEntryStatus
.31 -i 5

workstation# setany -v2c ip-address rw-community-string ciscoFlashMiscOpCommand
.31 -i 3
workstation# setany -v2c ip-address rw-community-string ciscoFlashMiscOpDestinationName
.31 -D
"/cmts01-billing/CMTS01_20030211-155025
"
workstation# setany -v2c ip-address rw-community-string ciscoFlashMiscOpEntryStatus
.31 -i 1

workstation#
```

Step 2 Periodically poll the ciscoFlashMiscOpStatus object until the file transfer completes:

Example:

```
workstation# getmany -v2c ip-address rw-community-string ciscoFlashMiscOpStatus
.31
  ciscoFlashCopyStatus.31 = miscOpInProgress(1)
workstation# getmany -v2c ip-address rw-community-string ciscoFlashMiscOpStatus
.31
  ciscoFlashCopyStatus.582 = miscOpOperationSuccess(2)
workstation#
```

Step 3 If the Flash memory system is not ATA-compatible (slot0:, slot1:, flash:, or bootflash:), configure the following objects in the ciscoFlashMiscOpTable to squeeze the Flash file system to recover the deleted file space:

Example:

```
workstation# setany -v2c ip-address rw-community-string ciscoFlashMiscOpEntryStatus
.32
-i 5

workstation# setany -v2c ip-address rw-community-string ciscoFlashMiscOpCommand
.32 -i 5
workstation# setany -v2c ip-address rw-community-string ciscoFlashMiscOpDestinationName
.32 -D slot0:
workstation# setany -v2c ip-address rw-community-string ciscoFlashMiscOpEntryStatus
.32
-i 1

workstation#
```

Examples To Transfer Using SNMP

The following SNMP commands transfer a file named CMTS01_20030211-155025 to a TFTP server at the IP address 10.10.31.3. After the file is successfully transferred, the row entry for this copy command is deleted.

```
workstation# setany -v2c 10.8.8.21 rw-string
 ciscoFlashCopyEntryStatus.582 -i 5

workstation# setany -v2c 10.8.8.21 rw-string
 ciscoFlashCopyCommand
.582
 -i 3
workstation# setany -v2c 10.8.8.21 rw-string
 ciscoFlashCopyServerAddress
.582
 -a "10.10.31.3"

workstation# setany -v2c 10.8.8.21 rw-string
 ciscoFlashCopySourceName
.582 -D
"slot0:CMTS01_20030211-155025
"
workstation# setany -v2c 10.8.8.21 rw-string
 ciscoFlashCopyDestinationName
.582 -D
"/cmts01-billing/CMTS01_20030211-155025
"
workstation# setany -v2c 10.8.8.21 rw-string
 ciscoFlashCopyEntryStatus.582 -i 1

workstation# getmany -v2c 10.8.8.21 rw-string
 ciscoFlashCopyStatus
.582
  ciscoFlashCopyStatus.582 = copyInProgress(1)
workstation# getmany -v2c 10.8.8.21 rw-string
 ciscoFlashCopyStatus
.582
  ciscoFlashCopyStatus.582 = copyOperationSuccess(2)
workstation# setany -v2c 10.8.8.21 rw-string
 ciscoFlashCopyEntryStatus.582 -i 6

workstation#
```

The following commands show a billing record file being deleted on the Cisco CMTS file system, and the deleted file space being recovered by a squeeze operation:

```
workstation# setany -v2c 10.8.8.21 rw-string
 ciscoFlashMiscOpEntryStatus
.31 -i 5

workstation# setany -v2c 10.8.8.21 rw-string
 ciscoFlashMiscOpCommand
.31 -i 3
workstation# setany -v2c 10.8.8.21 rw-string
 ciscoFlashMiscOpDestinationName
.31 -D
"/cmts01-billing/CMTS01_20030211-155025
"
workstation# setany -v2c 10.8.8.21 rw-string
 ciscoFlashMiscOpEntryStatus
.31 -i 1
```

```
workstation# getmany -v2c 10.8.8.21 rw-string
 ciscoFlashMiscOpStatus
.31
  ciscoFlashCopyStatus.31 = miscOpInProgress(1)
workstation# getmany -v2c 10.8.8.21 rw-string
 ciscoFlashMiscOpStatus
.31
  ciscoFlashCopyStatus.582 = miscOpOperationSuccess(2)
workstation# setany -v2c 10.8.8.21 rw-string
 ciscoFlashMiscOpEntryStatus
.32 -i 5

workstation# setany -v2c 10.8.8.21 rw-string
 ciscoFlashMiscOpCommand
.32 -i 5
workstation# setany -v2c 10.8.8.21 rw-string
 ciscoFlashMiscOpDestinationName
.32 -D slot0:
workstation# setany -v2c 10.8.8.21 rw-string
 ciscoFlashMiscOpEntryStatus
.32 -i 1

workstation#
```

Disabling the Usage-based Billing Feature

This section describes how to disable the Usage-based Billing. Giving this command immediately stops the collection of billing information. If a billing record is currently written or being streamed to an external server, the CMTS completes the operation before disabling the usage-based billing feature.

Procedure

	Command or Action	Purpose

Step 1	**enable**
	Example:
	`Router> enable`
	Example:
	`Router#`
		Enables privileged EXEC mode. Enter your password if prompted.

Step 2	**configure terminal**
	Example:
	`Router# configure terminal`
	Example:
	`Router(config)#`
		Enters global configuration mode.

Step 3	**no cable metering** **Example:**	Immediately disables the Usage-based Billing feature and stops the collection of billing information.

	Command or Action	Purpose

	`Router(config)# no cable metering`
	Example:
	`Router(config)#`	

Step 4	**no snmp-server enable traps cable metering**
	Example:
	`Router(config)# no snmp-server enable traps cable metering`
	Example:
	`Router(config)#`
		(Optional) Disables SNMP traps for usage-based billing events.

Step 5	**no cable sflog**
	Example:
	`Router(config)# no cable sflog`
	Example:
	`Router(config)#`
		(Optional) Disables the logging of deleted service flows.

Step 6	**no cable metering source-interface**
	Example:
	`Router(config)# no cable metering source-interface`
	Example:
	`Router(config)#`
		(Optional) Disables a specified source-interface for the billing packets.

Step 7	**exit**
	Example:
	`Router(config)# exit`
	Example:
	`Router#`
		Exits global configuration mode.

Configuring Certified SSL Servers for Usage-Based Billing

Cisco introduces adds support for the Secure Socket Layer (SSL) Server, used with the usage-based billing feature of the Cisco CMTS. Usage-based billing implements the DOCSIS Subscriber Account Management Interface Specification (SAMIS) format.

This new capability enables the configuration of the SSL server between the Cisco CMTS and a collection server. Certificate creation steps and **debug** commands are added or enhanced to support the SSL Server and certificates. This section describes general steps.

Refer also to the Configuring the Cisco CMTS for SSL Operation, on page 139 section.

Generating SSL Server Certification

These general steps describe the creation and implementation of certification for the Secure Socket Layer (SSL) Server.

1. Generate the CA key.
2. Set up the open SSL environment, to include directory and sub-directory.
3. Copy files to the appropriate directories.
4. Generate the SSL Server certification request.
5. Grant the SSL Server certification request.
6. Convert the SSL Server certification to DER format.
7. Copy the SSL certification to Bootflash memory (write mem).
8. Start the SSL server.

Configuring and Testing the Cisco CMTS for Certified SSL Server Support

Perform the following steps to configure the Cisco router to support the SSL Server and certification.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip domain name** *domain* **Example:** `Router(config)# ip domain name Cisco.com`	Defines a default domain name that the Cisco IOS software uses to complete unqualified host names (names without a dotted-decimal domain name). Do not include the initial period that separates an unqualified name from the domain name. **Note** See the Domain Name System (DNS) document on Cisco.com for additional DNS information.
Step 4	**crypto key generate rsa** **Example:** `Router(config)# crypto key generate rsa`	Generates RSA key pairs.

	Command or Action	Purpose

Step 5	Ctrl-Z
	Example:
	`Router(config)# Ctrl-Z`
	Example:
	`Router#`
		Returns to privileged EXEC mode.

Step 6	**test cable read certificate** **Example:** `Router# test cable read certificate`	Verifies the certificate is valid and operational on the Cisco CMTS.
Step 7	**show crypto ca certificate** **Example:** `Router# show crypto ca certificate`	Displays the available certificates on the Cisco CMTS.

Step 8	**configure terminal**
	Example:
	`Router# configure terminal`
	Example:
	`Router(config)#`
		Enters global configuration mode.

Step 9	**cable metering destination** *ip-addr num-1 num-2 num-3* **secure** **Example:** `Router(config)# cable metering destination 1.7.7.7 6789 0 15 secure`	Defines the destination IP address for cable metering, to be used with the certificate.
Step 10	test cable metering **Example:** `Router# test cable metering`	Tests cable metering in light of the supported SSL server and metering configuration.

Monitoring the Usage-based Billing Feature

To display the most current billing record, use the **show cable metering-status** command. The following example shows typical output when usage-based billing is configured to write the billing records to a local file system:

```
CMTS01# show cable metering-status
```

```
destination                          complete-time   flow   cpe     status
                                                    aggr suppress
disk0:R7519-UBR7246-20000308-004428 Jun 12 09:33:05  No     No     success
CMTS01#
```

The following example shows a typical output for the **show cable metering-status** command when usage-based billing is configured to stream the billing records to an external server:

```
Router# show cable metering-status

destination                      complete-time   flow cpe  full status
                                                 aggr supp rec
10.11.37.2 :1234                 Jun 12 09:33:05  No   No  No success
Router#
```

The following example shows a typical output for the **show cable metering-status** command using verbose option:

```
Router# show cable metering-status verbose
Last export status
Destination : disk0:sunethra10k-20070129-190423
Complete Time : Jan29 19:04:38
Flow Aggregate : No
Full records : No
Cpe list suppression : No
Source interface : FastEthernet0/0/0
Status of last export : success
Current export status : In progress
```

The following example shows a typical output for the **show cable metering-status** command when usage-based billing is configured to use the IPDR Exporter to stream the billing records to an external server:

```
Router# show cable metering-status
destination                 complete-time   flow  cpe   full    status
              aggr  supp  rec
IPDR_Session2               Apr12 16:51:15  No    No    No    success
```

The following example shows a typical output for the verbose form of the **show cable metering-status** command when usage-based billing is configured to use the IPDR Exporter to stream the billing records to an external server:

```
Router# show cable metering-status
 verbose

Last export status
Destination               : IPDR_Session2
Complete Time          : Apr12 16:51:15
Flow Aggregate         : No
Full records               :No
Cpe list suppression   : No
Source interface       : Not defined
Status of last export  : success
```

Note If the **show cable metering-status** command displays the status of a streaming operation as "success" but the records were not received on the billing application server, verify that the Cisco CMTS and server are configured for the same type of communications (non-secure TCP or secure SSL). If the Cisco CMTS is configured for non-secure TCP and the server is configured for secure SSL, the Cisco CMTS transmits the billing record successfully, but the server discards all of the data, because it did not arrive in a secure SSL stream.

Tip The **show cable metering-status** command continues to show the status of the last billing record operation, until that billing record is deleted. If the record is not deleted, no new records are created.

To display information about the state of the IPDR Exporter, use the show ipdr Exporter command. The following example shows typical output:

```
Router#configure terminal
Router#show ipdr exporter
```

IPDR exporter is started.

Configuration Examples for Usage-based Billing

This section lists the following sample configurations for the Usage-based Billing feature:

File Mode Configuration (with Secure Copy)

The following excerpt from a configuration file shows a typical configuration for the Usage-based Billing feature when operating in file mode and enabling Secure Copy (SCP) for file transfers.

```
!
cable metering filesystem disk1:
snmp-server enable traps cable metering
...
aaa new-model
aaa authentication login default group tacacs+
aaa authorization exec default group tacacs+
username billingapp level 15 password 7 billing-password
ip ssh time-out 120
ip ssh authentication-retries 3
ip scp server enable
```

Non-Secure Streaming Mode Configuration

The following excerpt from a configuration file shows a typical configuration for the Usage-based Billing feature when operating in streaming mode and specifying both a primary and a secondary external server. The data is sent using standard TCP packets, without any security.

```
cable metering destination 10.10.10.171 5321 10.10.10.173 5321 2 30 non-secure
```

```
snmp-server enable traps cable metering
```

The following excerpt from a configuration file shows a typical configuration for the Usage-based Billing feature when operating in streaming mode and specifying only a primary external server:

```
cable metering destination 10.10.11.181 6789 2 30 non-secure
snmp-server enable traps cable metering
```

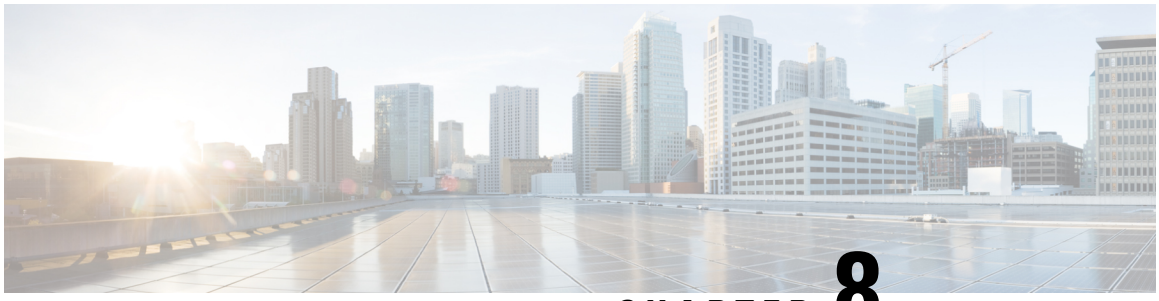
Note You must ensure that the billing application server is configured for standard TCP communications. If the billing application server is configured for SSL communications when the Cisco CMTS is configured for standard TCP, the Cisco CMTS is able to send the billing records to the server, but the server discards all of that information because it is not arriving in a secure stream.

Secure Streaming Mode Configuration

The following excerpt from a configuration file shows a typical configuration for the Usage-based Billing feature when operating in streaming mode and specifying only a primary external server. Secure socket layer (SSL) TCP connections are used to transmit the data, which requires the configuration of a digital certificate.

```
cable metering destination 10.10.11.181 6789 2 30 secure cpe-list-suppress
snmp-server enable traps cable metering
...
crypto ca trustpoint SSL-CERT
!
crypto ca certificate chain SSL-CERT
 certificate ca 00
  308204A6 3082038E A0030201 02020100 300D0609 2A864886 F70D0101 04050030
  8198310B 30090603 55040613 02555331 13301106 03550408 130A4361 6C69666F
  726E6961 3111300F 06035504 07130853 616E204A 6F736531 1C301A06 0355040A
  13134369 73636F20 53797374 656D732C 20496E63 2E311130 0F060355 040B1308
  4361626C 65204255 310E300C 06035504 03130553 65656D61 3120301E 06092A86
...
  3E65DBBA 337627E8 589980D6 C8836C7E 3D3C3BC1 F21973BF 7B287D7A 13B16DA2
  02B2B180 C2A125C7 368BDA4C 0B8C81B7 7D5BEFF9 A6618140 1E95D19E BD0A84F5
  B43702AB 39B5E632 87BA36AC A3A8A827 C5BAC0F1 B24B8F4D 55615C49 5B6E4B61
  B15CC48A 8EF566C8 6E449B49 BF8E9165 317C1734 9A48A240 78A356B5 403E9E9B
  88A51F5B 0FE38CC2 F431
  quit
!
```

Note You must ensure that the billing applications server is also configured for SSL communications.



CHAPTER 8

Frequency Allocation Information for the Cisco CMTS Routers

- Frequency Allocation for the Cisco CMTS Routers, on page 155

Frequency Allocation for the Cisco CMTS Routers

The table below provides information about the NTSC 6-MHz channel bands:

Table 29: NTSC Cable Television Channels and Relative Frequencies in MHz

Channel Number	Bandwidth	Video Carrier	Color Carrier	Audio Carrier
T 7	5.75 - 11.75	7	10.58	11.5
T 8	11.75 - 17.75	13	16.58	17.5
T9	17.75-23.75	19	22.58	23.5
T10	23.75-29.75	25	28.58	29.5
T11	29.75-35.75	31	34.58	35.5
T12	35.75-41.75	37	40.58	41.5
T13	41.75-47.75	43	46.58	47.5
TV-IF	40.0-46.0	45.75	42.17	41.25
2-2	54.0-60.0	55.25	58.83	59.75
3-3	60.0-66.0	61.25	64.83	65.75
4-4	66.0-72.0	67.25	70.83	71.75
5-5	76.0-82.0	77.25	80.83	81.75
6-6	82.0-88.0	83.25	86.83	87.75

Channel Number	Bandwidth	Video Carrier	Color Carrier	Audio Carrier
FM	88.0-108.0			
A-5-95	90.0-96.0	91.25	94.83	95.75
A-4-96	96.0-102.0	97.25	100.83	101.75
A-3-97	102.0-108.0	103.25	106.83	107.75
A-2-98	108.0-114.0	109.25	112.83	113.75
A-1-99	114.0-120.0	115.25	118.83	119.75
A-14	120.0-126.0	121.25	124.83	125.75
B-15	126.0-132.0	127.25	130.83	131.75
C-16	132.0-138.0	133.25	136.83	137.75
D-17	138.0-144.0	139.25	142.83	143.75
E-18	144.0-150.0	145.25	148.83	149.75
F-19	150.0-156.0	151.25	154.83	155.75
G-20	156.0-162.0	157.25	160.83	161.75
H-21	162.0-168.0	163.25	166.83	167.75
I-22	168.0-174.0	169.25	172.83	173.75
7-7	174.0-180.0	175.25	178.83	179.75
8-8	180.0-186.0	181.25	184.83	185.75
9-9	186.0-192.0	187.25	190.83	191.75
10-10	192.0-198.0	193.25	196.83	197.75
11-11	198.0-204.0	199.25	202.83	203.75
12-12	204.0-210.0	205.25	208.83	209.75
13-13	210.0-216.0	211.25	214.83	215.75
J-23	216.0-222.0	217.25	220.83	221.75
K-24	222.0-228.0	223.25	226.83	227.75
L-25	228.0-234.0	229.25	232.83	233.75
M-26	234.0-240.0	235.25	238.83	239.75
N-27	240.0-246.0	241.25	244.83	245.75

Channel Number	Bandwidth	Video Carrier	Color Carrier	Audio Carrier
O-28	246.0-252.0	247.25	250.83	251.75
P-29	252.0-258.0	253.25	256.83	257.75
Q-30	258.0-264.0	259.25	262.83	263.75
R-31	264.0-270.0	265.25	268.83	269.75
S-32	270.0-276.0	271.25	274.83	275.75
T-33	276.0-282.0	277.25	280.83	281.75
U-34	282.0-288.0	283.25	286.83	287.75
V-35	288.0-294.0	289.25	292.83	293.75
W-36	294.0-300.0	295.25	298.83	299.75
AA-37	300.0-306.0	301.25	304.83	305.75
BB-38	306.0-312.0	307.25	310.83	311.75
CC-39	312.0-318.0	313.25	316.83	317.75
DD-40	318.0-324.0	319.25	322.83	323.75
EE-41	324.0-330.0	325.25	328.83	329.75
FF-42	330.0-336.0	331.25	334.83	335.75
GG-43	336.0-342.0	337.25	340.83	341.75
HH-44	342.0-348.0	343.25	346.83	347.75
II-45	348.0-354.0	349.25	352.83	353.75
JJ-46	354.0-360.0	355.25	358.83	359.75
KK-47	360.0-366.0	361.25	364.83	365.75
LL-48	366.0-372.0	367.25	370.83	371.75
MM-49	372.0-378.0	373.25	376.83	377.75
NN-50	378.0-384.0	379.25	382.83	383.75
OO-51	384.0-390.0	385.25	388.83	389.75
PP-52	390.0-396.0	391.25	394.83	395.75
QQ-53	396.0-402.0	397.25	400.83	401.75
RR-54	402.0-408.0	403.25	406.83	407.75

Channel Number	Bandwidth	Video Carrier	Color Carrier	Audio Carrier
SS-55	408.0-414.0	409.25	412.83	413.75
TT-56	414.0-420.0	415.25	418.83	419.75
UU-57	420.0-426.0	421.25	424.83	425.75
VV-58	426.0-432.0	427.25	430.83	431.75
WW-59	432.0-438.0	433.25	436.83	437.75
XX-60	438.0-444.0	439.25	442.83	443.75
YY-61	444.0-450.0	445.25	448.83	449.75
ZZ-62	450.0-456.0	451.25	454.83	455.75
AAA-63	456.0-462.0	457.25	460.83	461.75
BBB-64	462.0-468.0	463.25	466.83	467.75
CCC-65	468.0-474.0	469.25	472.83	473.75
DDD-66	474.0-480.0	475.25	478.83	479.75
EEE-67	480.0-486.0	481.25	484.83	485.75
FFF-68	486.0-492.0	487.25	490.83	491.75
GGG-69	492.0-498.0	493.25	496.83	497.75
HHH-70	498.0-504.0	499.25	502.83	503.75
III-71	504.0-510.0	505.25	508.83	509.75
JJJ-72	510.0-516.0	511.25	514.83	515.75
KKK-73	516.0-522.0	517.25	520.83	521.75
LLL-74	522.0-528.0	523.25	526.83	527.75
MMM-75	528.0-534.0	529.25	532.83	533.75
NNN-76	534.0-540.0	535.25	538.83	539.75
OOO-77	540.0-546.0	541.25	544.83	545.75
PPP-78	546.0-552.0	547.25	550.83	551.75
QQQ-79	552.0-558.0	553.25	556.83	557.75
RRR-80	558.0-564.0	559.25	562.83	563.75
SSS-81	564.0-570.0	565.25	568.83	569.75

Channel Number	Bandwidth	Video Carrier	Color Carrier	Audio Carrier
TTT-82	570.0-576.0	571.25	574.83	575.75
UUU-83	576.0-582.0	577.25	580.83	581.75
VVV-84	582.0-588.0	583.25	586.83	587.75
WWW-85	588.0-594.0	589.25	592.83	593.75
XXX86	594.0-600.0	595.25	598.83	599.75
YYY-87	600.0-606.0	601.25	604.83	605.75
ZZZ-88	606.0-612.0	607.25	610.83	611.75
89-89	612.0-618.0	613.25	616.83	617.75
90-90	618.0-624.0	619.25	622.83	623.75
91-91	624.0-630.0	625.25	628.83	629.75
92-92	630.0-636.0	631.25	634.83	635.75
93-93	636.0-642.0	637.25	640.83	641.75
94-94	642.0-648.0	643.25	646.83	647.75
100-100	648.0-654.0	649.25	652.83	653.75
101-101	654.0-660.0	655.25	658.83	659.75
102-102	660.0-666.0	661.25	664.83	665.75
103-103	666.0-672.0	667.25	670.83	671.75
104-104	672.0-678.0	673.25	676.83	677.75
105-105	678.0-684.0	679.25	682.83	683.75
106-106	684.0-690.0	685.25	688.83	689.75
107-107	690.0-696.0	691.25	694.83	695.75
108-108	696.0-702.0	697.25	700.83	701.75
109-109	702.0-708.0	703.25	706.83	707.75
110-110	708.0-714.0	709.25	712.83	713.75
111-111	714.0-720.0	715.25	718.83	719.75
112-112	720.0-726.0	721.25	724.83	725.75
113-113	726.0-732.0	727.25	730.83	731.75

Channel Number	Bandwidth	Video Carrier	Color Carrier	Audio Carrier
114-114	732.0-738.0	733.25	736.83	737.75
115-115	738.0-744.0	739.25	742.83	743.75
116-116	744.0-750.0	745.25	748.83	749.75
117-117	750.0-756.0	751.25	754.83	755.75
118-118	756.0-762.0	757.25	760.83	761.75
119-119	762.0-768.0	763.25	766.83	767.75
120-120	768.0-674.0	769.25	772.83	773.75
121-121	774.0-780.0	775.25	778.83	779.75
122-122	780.0-786.0	781.25	784.83	785.75
123-123	786.0-792.0	787.25	790.83	791.75
124-124	792.0-798.0	793.25	796.83	797.75
125-125	798.0-804.0	799.25	802.83	803.75
126-126	804.0-810.0	805.25	808.83	809.75
127-127	810.0-816.0	811.25	814.83	815.75
128-128	816.0-822.0	817.25	820.83	821.75
129-129	822.0-828.0	823.25	826.83	827.75
130-130	828.0-834.0	829.25	832.83	833.75
131-131	834.0-840.0	835.25	838.83	839.75
132-132	840.0-846.0	841.25	844.83	845.75
133-133	846.0-852.0	847.25	850.83	851.75
134-134	852.0-858.0	853.25	856.83	857.75
135-135	858.0-864.0	859.25	862.83	863.75
136-136	864.0-870.0	865.25	868.83	869.75
137-137	870.0-876.0	871.25	874.83	875.75
138-138	876.0-882.0	877.25	880.83	881.75
139-139	882.0-888.0	883.25	886.83	887.75
140-140	888.0-894.0	889.25	892.83	893.75

Channel Number	Bandwidth	Video Carrier	Color Carrier	Audio Carrier
141-141	894.0-900.0	895.25	898.83	899.75
142-142	900.0-906.0	901.25	904.83	905.75
143-143	906.0-912.0	907.25	910.83	911.75
144-144	912.0-918.0	913.25	916.83	917.75
145-145	918.0-924.0	919.25	922.83	923.75
146-146	924.0-930.0	925.25	928.83	929.75
147-147	930.0-936.0	931.25	934.83	935.75
148-148	936.0-942.0	937.25	940.83	941.75
149-149	942.0-948.0	943.25	946.83	947.75
150-150	948.0-954.0	949.25	952.83	953.75
151-151	954.0-960.0	955.25	958.83	959.75
152-152	960.0-966.0	961.25	964.83	965.75
153-153	966.0-972.0	967.25	970.83	971.75
154-154	972.0-978.0	973.25	976.83	977.75
155-155	978.0-984.0	979.25	982.83	983.75
156-156	984.0-990.0	985.25	988.83	989.75
157-157	990.0-996.0	991.25	994.83	995.75
158-158	996.0-1002.0	997.25	1000.83	1001.75

The table below provides information on the Phase Alternating Line (PAL) and Systeme Electronique Couleur Avec Memoire (SECAM) 8-MHz channel bands:

Table 30: European Cable Television Channels and Relative Frequencies in MHz

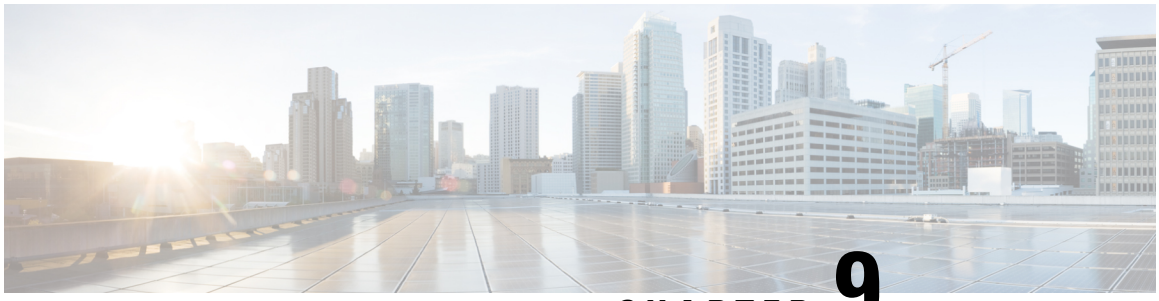
Channel Number	Bandwidth	Video Carrier	Audio Carrier
2	47-54	48.25	48.25
3	54-61	55.25	55.25
4	61-68	62.25	62.25
S2	111-118	112.25	112.25
S3	118-125	119.25	119.25

Channel Number	Bandwidth	Video Carrier	Audio Carrier
S4	125-132	126.25	126.25
S5	132-139	133.25	133.25
S6	139-146	140.25	140.25
S7	146-153	147.25	147.25
S8	153-160	154.25	154.25
S9	160-167	161.25	161.25
S10	167-174	168.25	168.25
5	174-181	175.25	175.25
6	181-188	182.25	182.25
7	188-195	189.25	189.25
8	195-202	196.25	196.25
9	202-209	203.25	203.25
10	209-216	210.25	210.25
11	216-223	217.25	217.25
12	223-230	224.25	224.25
S11	230-237	231.25	231.25
S12	237-244	238.25	238.25
S13	244-251	245.25	245.25
S14	251-258	252.25	252.25
S15	258-265	259.25	259.25
S16	265-272	266.25	266.25
S17	272-279	273.25	273.25
S18	279-286	280.25	280.25
S19	286-293	287.25	287.25
S20	293-300	294.25	294.25
S21	302-310	303.25	303.25
S22	310-318	311.25	311.25

Channel Number	Bandwidth	Video Carrier	Audio Carrier
S23	318-326	319.25	319.25
S24	326-334	327.25	327.25
S25	334-342	335.25	335.25
S26	342-350	343.25	343.25
S27	350-358	351.25	351.25
S28	358-366	359.25	359.25
S29	366-374	367.25	367.25
S30	374-382	375.25	375.25
S31	382-390	383.25	383.25
S32	390-398	391.25	391.25
S33	398-406	399.25	399.25
S34	406-414	407.25	407.25
S35	414-422	415.25	415.25
S36	422-430	423.25	423.25
S37	430-438	431.25	431.25
S38	438-446	439.25	439.25
21	470-478	471.25	471.25
22	478-486	479.25	479.25
23	486-494	487.25	487.25
24	494-502	495.25	495.25
25	502-510	503.25	503.25
26	510-518	511.25	511.25
27	518-526	519.25	519.25
28	526-534	527.25	527.25
29	534-542	535.25	535.25
30	542-550	543.25	543.25
31	550-558	551.25	551.25

Channel Number	Bandwidth	Video Carrier	Audio Carrier
32	558-566	559.25	559.25
33	566-574	567.25	567.25
34	574-582	575.25	575.25
35	582-590	583.25	583.25
36	590-598	591.25	591.25
37	598-606	599.25	599.25
38	606-614	607.25	607.25
39	614-622	615.25	615.25
40	622-630	623.25	623.25
41	630-638	631.25	631.25
42	638-646	639.25	639.25
43	646-654	647.25	647.25
44	654-662	655.25	655.25
45	662-670	663.25	663.25
46	670-678	671.25	671.25
47	678-686	679.25	679.25
48	686-694	687.25	687.25
49	694-702	695.25	695.25
50	702-710	703.25	703.25
51	710-718	711.25	711.25
52	718-726	719.25	719.25
53	726-734	727.25	727.25
54	734-742	735.25	735.25
55	742-750	743.25	743.25
56	750-758	751.25	751.25
57	758-766	759.25	759.25
58	766-774	767.25	767.25

Channel Number	Bandwidth	Video Carrier	Audio Carrier
59	774-782	775.25	775.25
60	782-790	783.25	783.25
61	790-798	791.25	791.25
62	798-806	799.25	799.25
63	806-814	807.25	807.25
64	814-822	815.25	815.25
65	822-830	823.25	823.25
66	830-838	831.25	831.25
67	838-846	839.25	839.25
68	846-854	847.25	847.25
69	854-862	855.25	855.25



CHAPTER 9

Flap List Troubleshooting

This document describes how to configure and use the Flap List Troubleshooting feature on the Cisco Cable Modem Termination System (CMTS) routers. The flap list is a patented tool for the Cisco CMTS routers to diagnose potential problems with a particular cable modem or with a particular cable interface. The flap list tracks "flapping" cable modems, which are cable modems that have intermittent connectivity problems. Excessive flapping could indicate a problem with a particular cable modem or with the upstream or downstream portion of the cable plant.

- Finding Feature Information, on page 167
- Hardware Compatibility Matrix for the Cisco cBR Series Routers, on page 167
- Prerequisites for Flap List Troubleshooting, on page 168
- Restrictions for Flap List Troubleshooting, on page 168
- Information About Flap List Troubleshooting, on page 169
- How to Configure Flap List Troubleshooting, on page 171
- How to Monitor and Troubleshoot Using Flap Lists, on page 176
- Configuration Examples for Flap List Troubleshooting, on page 183
- Additional References, on page 183
- Feature Information for Flap List Troubleshooting, on page 184

Finding Feature Information

Finding Feature Information

Your software release may not support all the features that are documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. The Feature Information Table at the end of this document provides information about the documented features and lists the releases in which each feature is supported.

Hardware Compatibility Matrix for the Cisco cBR Series Routers

Note The hardware components that are introduced in a given Cisco IOS-XE Release are supported in all subsequent releases unless otherwise specified.

Table 31: Hardware Compatibility Matrix for the Cisco cBR Series Routers

Cisco CMTS Platform	Processor Engine	Interface Cards
Cisco cBR-8 Converged Broadband Router	**Cisco IOS-XE Release 16.5.1 and Later Releases** Cisco cBR-8 Supervisor: • PID—CBR-SUP-250G • PID—CBR-CCAP-SUP-160G • PID—CBR-CCAP-SUP-60G • PID—CBR-SUP-8X10G-PIC	**Cisco IOS-XE Release 16.5.1 and Later Releases** Cisco cBR-8 CCAP Line Cards: • PID—CBR-LC-8D30-16U30 • PID—CBR-LC-8D31-16U30 • PID—CBR-RF-PIC • PID—CBR-RF-PROT-PIC • PID—CBR-CCAP-LC-40G • PID—CBR-CCAP-LC-40G-R Cisco cBR-8 Downstream PHY Modules: • PID—CBR-D30-DS-MOD • PID—CBR-D31-DS-MOD Cisco cBR-8 Upstream PHY Modules: • PID—CBR-D30-US-MOD • PID—CBR-D31-US-MOD

Prerequisites for Flap List Troubleshooting

- To configure and access the flap list using SNMP commands, you must be using an SNMPv3 manager and have configured the Cisco CMTS router for SNMP operations.

Restrictions for Flap List Troubleshooting

- The Flap List Troubleshooting feature can be used only with two-way cable modems. The flap-list does not support telco-return cable modems or set-top boxes.

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 can go offline faster than the frequency hop period, which can cause the frequency to stay fixed while cable modems go offline. To compensate for this, reduce the hop period to 10 seconds.

Information About Flap List Troubleshooting

This section describes the following information about the Flap List Troubleshooting feature:

Feature Overview

The Flap List Troubleshooting is a patented tool that is incorporated in the Cisco IOS software for the Cisco Cable Modem Termination System (CMTS) routers. The flap list tracks "flapping" cable modems, which are cable modems that have intermittent connectivity problems. A flapping cable modem can indicate either a problem with that particular cable modem, or it could indicate an RF noise problem with the upstream or downstream portion of the cable plant.

The flap-list feature supports any cable modem that conforms to the Data-over-Cable Service Interface Specifications (DOCSIS) because it does use any special messaging to poll cable modems or to request any special information from them. Instead, this feature monitors the normal registration and station maintenance activity that is already performed over a DOCSIS cable network.

This allows the Cisco CMTS to collect the flap-list data without generating additional packet overhead and without impacting network throughput and performance. It also means that although the Flap List Troubleshooting feature is a proprietary feature for Cisco CMTS routers, it is compatible with all DOCSIS-compliant cable modems. In addition, unlike other monitoring methods that use the Simple Network Management Protocol (SNMP), the flap list uses zero bandwidth.

Information in the Flap List

The Flap List Troubleshooting feature tracks the following situations:

- Reinsertions—A reinsertion occurs when the cable modem re-registers more frequently than the user-specified insertion time. A pattern of reinsertions can indicate either potential problems in the downstream or that the cable modem is being improperly provisioned.
- Hits and Misses—A hit occurs when a cable modem successfully responds to the station maintenance messages (MAC-layer "keepalive" messages) that the Cisco CMTS sends out to conform to the DOCSIS standard. A miss occurs when the cable modem does not respond to the request within the user-specified timeout period. A pattern of misses can indicate a potential problem in either the downstream or upstream path, or that a problem can be occurring in the registration process.
- Power Adjustments—DOCSIS cable modems can adjust their upstream transmission power levels to adjust to unstable cable plant signal levels, up to a maximum allowable power level. Repeated power adjustments usually indicate a problem with an amplifier in the upstream return path.

The flap-list feature is automatically enabled, but to use the flap list effectively, the cable system administrator should also typically do the following:

- Set up a script to periodically poll the flap list, for example, every 15 minutes.
- Examine the resulting data and perform trend analysis to identify cable modems that are consistently in the flap list.
- Query the billing and administrative database for cable modem MAC address-to-street address translation and generate a report. The reports can be given to the customer service department or the cable plant's operations and maintenance department. Using these reports, maintenance personnel can quickly discern how characteristic patterns of flapping cable modems, street addresses, and flap statistics indicate which

amplifier or feeder lines are faulty. The reports also help to quickly discern whether problems exist in your downstream or upstream path and whether the problem is ingress noise or equipment related.

The flap list provides a quick way to quickly diagnose a number of possible problems. For example, if a subscriber reports a problem, but the flap list for the cable interface that is providing services to them shows little or no flap-list activity, the cable technician can assume that the Cisco CMTS and cable plant are communicating reliably. The problem, therefore, is probably in the subscriber's computer equipment or in the local connection to the cable modem.

Similarly, a cable technician can use the pattern of reinsertions, hits and misses, and power adjustments to quickly troubleshoot the following types of problems:

- If a subscriber's cable modem shows a lot of flap-list activity, it is having some kind of communication problem. Either the cable modem’s hardware is faulty, its installation is faulty, the coaxial cable being used is faulty, or some portion of the cable plant that services this cable modem is faulty.
- Focus on the top 10 percent of cable modems that are most active in the flap list, since these are the most likely to indicate consistent and pervasive plant or equipment problems that will continue to disrupt communication 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 problem with the provisioning servers.
- Cable modems with high cyclic redundancy check (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.

In addition, the cable network administrators can use the flap list to collect quality control and upstream performance data. Typically, the network operations center (NOC) saves the flap list to a database on a local computer on a daily basis, providing the ability to generate reports that track upstream performance and installation quality control, as well as to provide trend reports on cable plant problems.

Tip The system supports automatic power adjustments. The show cable flap-list and show cable modem commands indicate when the headend cable router 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 modem when a power adjustment has been made; an exclamation point (!) appears when the modem has reached its maximum power-transmit level and cannot increase its power level any further.

Cisco Cable Manager and Cisco Broadband Troubleshooter

The Flap List Troubleshooting feature is supported by Cisco Cable Manager (CCM), Release 2.0 or later, which is a UNIX-based software suite that manages routers and DOCSIS-compliant cable modems, generates performance reports, troubleshoots connectivity problems, views the network graphically, and edits DOCSIS configuration files. You can access the CCM locally from the CCM server console or remotely from a UNIX workstation or a PC.

The Flap List Troubleshooting feature also works together with the Cisco Broadband Troubleshooter (CBT), which is a graphical-based application to manage and diagnose problems on the hybrid fiber-coaxial (HFC)

network. Radio frequency (RF) technicians can quickly isolate plant and provisioning problems and characterize upstream and downstream trouble patterns, including analyzing flapping modems.

Benefits

The Flap List Troubleshooting feature is a proactive way to manage and troubleshoot problems on an HFC network. Its use of passive monitoring is more scalable and efficient than techniques that send special messages to cable modems or that regularly poll the cable modems using Simple Network Management Protocol (SNMP) commands. Because it uses mechanisms that already exist in a DOCSIS network, it can be used with any DOCSIS-certified cable modem or set-top box.

The flap list provides a cable technician with both real-time and historical cable health statistics for quick, accurate problem isolation and network diagnosis. Using the flap list, a cable technician is able to do the following:

- Quickly learn how to characterize trouble patterns in the hybrid fiber-coaxial (HFC) network.
- Determine which amplifier or feeder line is faulty.
- Distinguish an upstream path problem from a downstream one.
- Isolate an ingress noise problem from a plant equipment problem.

How to Configure Flap List Troubleshooting

This section describes how to configure the flap list operation on the Cisco CMTS. You can use either the command-line interface (CLI) commands or Simple Network Management Protocol (SNMP) commands to configure the flap list, to remove a cable modem from the list, or to clear the flap-list counters.

Configuring Flap List Operation Using the CLI (optional)

To configure the operation of the flap list, use the following procedure, beginning in EXEC mode. This procedure is optional, unless you want to change the default values for the flap list.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 3	**cable flap-list insertion-time** *seconds* **Example:** `Router(config)# cable flap-list insertion-time 3600`	(Optional) Specifies the minimum insertion (registration) time interval in seconds. Any cable modem that makes a registration request more frequently than this period of time is placed in the flap list.
Step 4	**cable flap-list power-adjust threshold** *db* **Example:** `Router(config)# cable flap-list power-adjust threshold 5`	(Optional) Specifies the minimum power adjustment, in dB, that constitutes a flap-list event. **Note** A threshold of less than 2 dB can cause excessive flap-list event recording. If you need to change this parameter from its default, Cisco recommends setting it to 3 dB or higher.
Step 5	**cable flap-list miss-threshold** *misses* **Example:** `Router(config)# cable flap-list miss-threshold 10`	(Optional) Specifies the number of MAC-layer station maintenance (keepalive) messages that can be missed in succession before the CMTS places the cable modem in the flap list. **Note** A high miss rate indicates potential plant problems, such as intermittent upstream problems, fiber laser clipping, or common-path distortion.
Step 6	**cable flap-list aging** *minutes* **Example:** `Router(config)# cable flap-list aging 20160`	(Optional) Specifies how long, in minutes, the Cisco CMTS should keep information for cable modems in the flap list.
Step 7	**cable flap-list size** *number* **Example:** `Router(config)# cable flap-list size 4000`	Specifies the maximum number of cable modems that can be kept in the flap list. **Tip** To avoid wasting processor memory, do not set this value beyond the actual number of cable modems being serviced by the Cisco CMTS.
Step 8	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.

Clearing the Flap List and Counters Using the CLI (optional)

To clear one or more cable modems from the flap list, or to clear the flap list counters for one or more cable modems (while still keeping the modems in the flap list), use the following procedure, beginning in EXEC mode.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

Step 2	**clear cable flap-list** *mac-addr* | **all**} [**save-counters**]
	Example:
	`Router# clear cable flap-list 0102.0304.0506 save-counters`
	Example:
	`Router# clear cable flap-list 000C.0102.0304`
		Clears one or all cable modems from the flap list.

Step 3	**clear cable modem** {*mac-addr* | *ip-addr* | [**cable** *interface*] **all** | **oui***string* | **reject**} } **counters**
	Example:
	`Router# clear cable modem 172.12.23.45 counters`
	Example:
	`Router# clear cable modem oui Cisco counters`
	Example:
	`Router# clear cable modem reject counters`
	Example:
	`Router# clear cable modem c4/0 counters`
	Example:
		Sets the flap-list counters to zero for one or more CMs.

Enabling or Disabling Power Adjustment Using the CLI (optional)

The Cisco CMTS can automatically monitor a cable modem's power adjustments and determine whether a particular cable modem requires a chance in the power adjustment method. To enable a cable interface to make automatic power adjustments, and to set the frequency threshold for when those adjustments are made, use the following procedure, beginning in EXEC mode.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface cable** *x/y* **Example:** `Router(config)# interface cable 4/0`	Enters cable interface configuration mode for the specified cable interface.

Step 4	**cable upstream** *n* **power-adjust** {**continue** *pwr-level* | **noise** *perc-pwr-adj* | **threshold value**}
	Example:
	`Router(config-if)# cable upstream 0 power-adjust threshold 2`
	Example:
	`Router(config-if)# cable upstream 0 power-adjust noise 50`
		Enables automatic power adjustment on an upstream port for this cable interface.
		Note Repeat 4 for each upstream port on the cable interface.

Step 5	**cable upstream** *n* **freq-adj averaging** *percent* **Example:** `Router(config-if)# cable upstream 0 freq-adj averaging 50`	Specifies the percentage of frequency adjustment packets needed to change the adjustment method from the regular power-adjustment method to the automatic power adjustment method.
Step 6	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode.
Step 7	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.

What to do next

Caution The default settings are adequate for system operation. Amplitude averaging is an automatic procedure. In general, Cisco does not recommend that 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 for the **cable upstream power-adjust** command: If CMs cannot complete ranging because they have reached maximum power levels, increase the **continue** *pwr-level* parameter beyond the default value of 2 dB. Values larger than 10 dB on "C" versions of cable interface line cards, or 5 dB on FPGA versions, are not recommended. If the flap list shows CMs with a large number of power adjustments, but the CMs are not detected as "noisy," decrease the **noise** *perc-pwr-adj* value. If too many CMs are unnecessarily detected as "noisy," increase the percentage.

Configuring Flap List Operation Using SNMP (optional)

To configure the Flap List Troubleshooting feature on the Cisco CMTS using SNMP, set the appropriate cssFlapObjects attributes in the CISCO-CABLE-SPECTRUM-MIB. the table lists each of the configurable attributes:

Table 32: Flap-List Configuration Attributes

Attribute	Type	Range	Description
ccsFlapListMaxSize	Integer32	1 to 65536[1]	The maximum number of modems that a flap list can support per line card. The default is 100.[2]
ccsFlapListCurrentSize	Integer32	1 to 65536	The current number of modems in the flap list.[3]
ccsFlapAging	Integer32	1 to 86400	The flap entry aging threshold in minutes. The default is 10080 minutes (180 hours or 7 days).
ccsFlapInsertionTime	Integer32	60 to 86400	The worst-case insertion time, in seconds. If a cable modem has not completed the registration stage within this interval, the cable modem is inserted into the flap list. The default value is 90 seconds.
ccsFlapPowerAdjustThreshold	Integer32	1 to 10	When the power of the modem is adjusted beyond the power adjust threshold, the modem is inserted into the flap list.
ccsFlapMissThreshold	Unsigned32	1 to 12	When a cable modem does not acknowledge this number of consecutive MAC-layer station maintenance (keepalive) messages, the cable modem is placed in the flap list.

[1] The allowable range when using SNMP for these parameters is 1 to 65536 (a 32-bit value), but the valid operational range is 1 to 8191.

[2] This value is the same as set by the **cable flap-list size** command and is applied only to the command output. The flap list entries displayed via SNMP are not affected by this.

[3] The number of SNMP entries is the same as this value. The number of the CLI entries depends on the value set by **ccsFlapListMaxSize**.

Note **ccsFlapListMaxSize** controls the display of the flap list per downstream cable interface. As long as the number of flap list entries per line card does not exceed 8191, these entries will be stored in the system, and will not be displayed via CLI.

ccsFlapListCurrentSize reflects the number of flap list entries of all the line cards that in the system, regardless of their visibility to the CLI.

Clearing the Flap List and Counters Using SNMP (optional)

To remove a cable modem from the flap list or to clear one or all of the flap-list counters, set the appropriate cssFlapObjects attributes in the CISCO-CABLE-SPECTRUM-MIB. the table lists the attributes that clear the SNMP counters.

Table 33: Attributes to Clear the Flap List

Attribute	Type	Description
ccsFlapResetAll	Boolean	Setting this object to True (1) resets all flap-list counters to zero.
ccsFlapClearAll	Boolean	Setting this object to True (1) removes all cable modems from the flap list, and destroys all entries in the ccsFlapTable. If a modem keeps flapping, the modem is added again into the flap list as a new entry.

Note The ccsFlapLastClearTime attribute contains the date and time that the entries in the ccsFlapTable table were last cleared.

How to Monitor and Troubleshoot Using Flap Lists

Displaying the Flap List Using the show cable flap-list Command

To display the current contents of the flap list, use the show cable flap-list command in privileged EXEC mode. This command has the following syntax:

- **show cable flap-list**—Displays the complete flap list.
- **show cable flap-list sort-interface**—Displays the complete flap list sorted by cable interface.
- **show cable flap-list cable** *interface* **upstream** *port*—Displays the flap list for a specific cable interface, or for a specific upstream port on that cable interface.

To change the way the output is sorted, add one of the following optional keywords:

- **sort-flap**—Sorts the output by the number of times that the cable modem has flapped.
- **sort-time**—Sorts the output by the most recent time that the cable modem flapped.

The following example shows typical output of the **show cable flap-list** command.

```
Router# show cable flap-list
Mac Addr       CableIF Ins    Hit   Miss    CRC  P-Adj   Flap    Time
0010.9500.461f C1/0 U1 56  18857    887      0      1    116 Jun 1  14:09:12
0010.9500.446e C1/0 U1 38  18686   2935      0      1     80 Jun 2  19:03:57
0010.9500.38ec C1/0 U2 63  18932   1040      0      8    138 Jun 2  23:50:53
0010.9500.4474 C1/0 U2 65  18913   1053      0      3    137 Jun 2  09:30:09
0010.9500.4672 C1/0 U2 56  18990   2327      0      6    124 Jun 2  10:44:14
0010.9500.38f0 C1/0 U2 50  18964   2083      0      5    111 Jun 2  20:46:56
0010.9500.e8cb C1/0 U2  0   6537    183      0      1      5 Jun 2  22:35:48
0010.9500.38f6 C1/0 U3 50  19016   2511      0      2    104 Jun 2  07:46:31
0010.9500.4671 C1/0 U3 43  18755   3212      1      1     89 Jun 1  19:36:20
0010.9500.38eb C1/0 U0 57  36133   1608      0      6    126 Jun 2  20:04:58
0010.9500.3ce2 C1/0 U0 44  35315   1907      0      4     99 Jun 2  16:42:47
0010.9500.e8d0 C1/0 U2  0  13213    246      0      1      5 Jun 3  04:15:30
0010.9500.4674 C1/0 U2 56  36037   2379      0      4    121 Jun 3  00:34:12
0010.9500.4677 C1/0 U2 40  35781   2381      0      4     91 Jun 2  12:14:38
0010.9500.4614 C1/0 U2 40  21810   2362      0    502    586 Jun 2  21:43:02
0010.9500.3be9 C1/0 U2 63  22862    969      0      0    128 Jun 1  14:09:03
0010.9500.4609 C1/0 U2 55  22723   2127      0      0    112 Jun 1  14:08:02
0010.9500.3cb8 C1/0 U2 49  22607   1378      0      0    102 Jun 1  14:08:58
0010.9500.460d C1/0 U3 46  22477   2967      0      2     96 Jun 2  17:03:48
0010.9500.3cba C1/0 U3 39  22343   3058      0      0     81 Jun 1  14:13:16
0010.9500.3cb4 C1/0 U3 38  22238   2936      0      0     79 Jun 1  14:09:26
0010.9500.4612 C1/0 U3 38  22306   2928      0      0     79 Jun 1  14:09:29
Router#
```

Displaying the Flap List Using the show cable modem flap Command

To display the contents of the flap list for a specific cable modem, use the **show cable modem flap** command in privileged EXEC mode. This command has the following syntax:

- **show cable modem** [*ip-address* | *mac-address*] **flap**—Displays the flap list for a specific cable modem, as identified by its IP address or MAC address.
- **show cable modem cable***interface* [**upstream** *port*] **flap**—Displays the flap list for all cable modems on a specific cable interface.

Note The **show cable modem flap** command displays information similar to that shown by the **show cable flap-list** command, except it displays this information on a per-modem basis.

The following example shows sample output for the **show cable modem flap** command for a particular cable modem:

```
Router# show cable modem 0010.7bb3.fcd1 flap
MAC Address    I/F       Ins   Hit   Miss  CRC   P-Adj   Flap  Time
0010.7bb3.fcd1 C5/0/U5   0     36278 92    0     369     372   Jun 1  13:05:23 (18000msec)
```

The following example shows sample output for the **show cable modem flap** command for all cable modems on a specific cable interface:

```
Router# show cable modem cable 6/0/0 flap
MAC Address    I/F           Ins   Hit   Miss  CRC   P-Adj   Flap  Time
0025.2e34.4386 C6/0/0/U0     0     46778 3980  0      0      0     (14212 msec)
0025.2e2f.d4b6 C6/0/0/U0     0     48002 1899  0      0      0     (18000 msec)
```

```
0025.2e2f.d4de C6/0/0/U0     0     48098 1889  0      0      0     (19552 msec)
0023.bee1.e96b C6/0/0/U0     0     46658 4351  0      0      0     (22432 msec)
0025.2e2f.d4d8 C6/0/0/U0     0     21979 781   0      0      0     ( -- )
0025.2e2f.d48c C6/0/0/U0     0     48048 1835  0      0      0     ( -- )
0025.2e2f.d490 C6/0/0/U0     0     48029 1819  0      0      0     ( -- )
```

Displaying the Flap List Using SNMP

To display the contents of the flap list using SNMP, query the ccsFlapTable table in the CISCO-CABLE-SPECTRUM-MIB. This table contains an entry for each cable modem. the table briefly describes each attribute in this table.

Table 34: cssFlapTable Attributes

Attribute	Type	Description
cssFlapMacAddr	MacAddress	MAC address of the cable modem's cable interface. Identifies a flap-list entry for a flapping cable modem.
ccsFlapUpstreamIfIndex	InterfaceIndex	Upstream being used by the flapping cable modem.
ccsFlapDownstreamIfIndex	InterfaceIndex	Downstream being used by the flapping cable modem.
ccsFlapLastFlapTime	DateAndTime	Time stamp for the last time the cable modem flapped.
ccsFlapCreateTime	DateAndTime	Time stamp that this entry was added to the table.
ccsFlapRowStatus	RowStatus	Control attribute for the status of this entry.
ccsFlapInsertionFailNum	Unsigned32	Number of times the CM comes up and inserts itself into the network. This counter is increased when the time between initial link establishment and a reestablishment was less than the threshold parameter configured using the **cable flap-list insertion-time** command or ccsFlapInsertionTime attribute. When the cable modem cannot finish registration within the insertion time (ccsFlapInsertionTime), it resends the Initial Maintenance packet. When the CMTS receives the packet sooner than expected, the CMTS increments this counter.
ccsFlapHitNum	Unsigned32	Number of times the CM responds to MAC-layer station maintenance (keepalive) messages. (The minimum hit rate is once per 30 seconds.)
ccsFlapMissNum	Unsigned32	Number of times the CM misses and does not respond to a MAC-layer station maintenance (keepalive) message. An 8 percent miss rate is normal for the Cisco cable interface line cards. If the CMTS misses a ranging request within 25 msec, then the miss number is incremented.
ccsFlapCrcErrorNum	Unsigned32	Number of times the CMTS upstream receiver flagged a packet with a CRC error. A high value indicates that the cable upstream may have a high noise level. The modem may not be flapping yet, but this could become a possible problem.
ccsFlapPowerAdjustmentNum	Unsigned32	Number of times the cable modem upstream transmit power is adjusted during station maintenance. When the adjustment is greater than the power-adjustment threshold, the number is incremented.

Attribute	Type	Description
ccsFlapTotalNum	Unsigned32	Number of times a modem has flapped, which is the sum of the following: • When ccsFlapInsertionFailNum is increased • When the CMTS receives a miss followed by a hit • When ccsFlapPowerAdjustmentNum is increased
ccsFlapResetNow	Boolean	Setting this object to True (1) resets all flap-list counters to zero.
ccsFlapLastResetTime	DateAndTime	Time stamp for when all the counters for this particular entry were reset to zero.

Displaying Flap-List Information for Specific Cable Modems

To use SNMP requests to display flap-list information for a specific cable modem, use the cable modem's MAC address as the index to retrieve entries from the ccsFlapTable. Use the following procedure to retrieve flap-list entries for a particular cable modem.

Step 1 Convert the cable modem's MAC address into a dotted decimal string. For example, the MAC address 000C.64ff.eb95 would become 0.12.100.255.235.149.

Step 2 Use the dotted decimal version of the MAC address as the instance for requesting information from the ccsFlapTable. For example, to retrieve the ccsFlapHits, ccsFlapMisses, and ccsFlapPowerAdjustments values for this cable modem, you would make an SNMP request for the following objects:

- ccsFlapHits.0.12.100.255.235.149
- ccsFlapMisses.0.12.100.255.235.149
- ccsFlapPowerAdjustments.0.12.100.255.235.149

Example

Assume that you want to retrieve the same flap-list information as the **show cable flap-list** command for a cable modem with the MAC address of 000C.64ff.eb95:

```
Router# show cable flap-list
MAC Address     Upstream     Ins   Hit   Miss  CRC   P-Adj Flap  Time
000C.64ff.eb95  Cable3/0/U4  3314  55605 50460 0    *42175 47533 Jan 27 02:49:10
Router#
```

Use an SNMP tool to retrieve the ccsFlapTable and filter it by the decimal MAC address. For example, using the standard Unix **getone** command, you would give the following command:

```
csh% getmany -v2c 192.168.100.121 public ccsFlapTable | grep 0.12.100.255.235.149

ccsFlapUpstreamIfIndex.0.12.100.255.235.149 = 15
ccsFlapDownstreamIfIndex.0.12.100.255.235.149 = 17
ccsFlapInsertionFails.0.12.100.255.235.149 = 3315
ccsFlapHits.0.12.100.255.235.149 = 55608
ccsFlapMisses.0.12.100.255.235.149 = 50460
ccsFlapCrcErrors.0.12.100.255.235.149 = 0
```

```
ccsFlapPowerAdjustments.0.12.100.255.235.149 = 42175
ccsFlapTotal.0.12.100.255.235.149 = 47534
ccsFlapLastFlapTime.0.12.100.255.235.149 = 07 d4  01 1b   02 33  1a 00
ccsFlapCreateTime.0.12.100.255.235.149 = 07 d4  01 16   03 23  22 00
ccsFlapRowStatus.0.12.100.255.235.149 = active(1)
ccsFlapInsertionFailNum.0.12.100.255.235.149 = 3315
ccsFlapHitNum.0.12.100.255.235.149 = 55608
ccsFlapMissNum.0.12.100.255.235.149 = 50460
ccsFlapCrcErrorNum.0.12.100.255.235.149 = 0
ccsFlapPowerAdjustmentNum.0.12.100.255.235.149 = 42175
ccsFlapTotalNum.0.12.100.255.235.149 = 47534
ccsFlapResetNow.0.12.100.255.235.149 = false(2)
ccsFlapLastResetTime.0.12.100.255.235.149 = 07 d4  01 16   03 20  18 00
csh%
```

To request just one particular value, use the decimal MAC address as the instance for that object:

```
csh% getone -v2c 172.22.85.7 public ccsFlapMisses.0.12.100.255.235.149

ccsFlapMisses.0.12.100.255.235.149 = 50736
csh %
```

Troubleshooting Suggestions

This section provides tips on how to interpret the flap-list counters, as well as how to determine the optimum power level for a flapping cable modem.

Troubleshooting Tips

This section includes suggestions on how to interpret different network conditions based on the flap-list statistics:

- Condition 1: Low miss or hit ratio, low insertion, low P-Adj, low flap counter, and old time stamp. Analysis: This exhibits an optimal network situation.
- Condition 2: High ratio of misses over hits (> 10 percent). Analysis: Hit and 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, the upstream can be experiencing noise. If the miss count is greater, then the modem is probably dropping out frequently and not completing registration. The upstream or downstream might not be 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 that the power-adjustment threshold is probably set at default value of 2 dB. The modem transmitter step size is 1.5 dB, but the headend can 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 can be set using cable flap power threshold <0-10 dB> in the Cisco IOS global configuration mode. A properly operating HFC network with short amplifier cascades can use a 2 to 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 modems with the highest CRC count first. If the modems are not going offline (Ins = 0), this is not noticed by subscribers. However, they could receive slower service due to dropped IP packets in the upstream. This condition also results in input errors on the Cisco CMTS router cable interface.

- Condition 5: High insertion rate. Analysis: If link reestablishment happens too frequently, the modem is usually having a registration problem. This is indicated by a high Ins counter, which tracks the Flap counter.

Performing Amplitude Averaging

The CMTS 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—known as flapping. To avoid dropping flapping cable modems, the CMTS averages a configurable number of RNG-REQ messages before it makes power adjustments. By compensating for a potentially unstable return path, the CMTS 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 to which paths the CMTS 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  Cable1/0/U1  0     2792  281   0     *45    58    Jul 27 16:54:50
 0010.7bb3.fcfc  Cable1/0/U1  0     19    4     0     !43    43    Jul 27 16:55:01
 0010.7bb3.fcdd  Cable1/0/U1  0     19    4     0     *3     3     Jul 27 16:55:01
```

The asterisk (*) indicates that the CMTS is using the power-adjustment method on this modem. An exclamation point (!) indicates that the modem has reached maximum transmit power.

Output of the **show cable modem** command appears below:

```
Router# show cable modem
 Interface   Prim Online     Timing Rec    QoS CPE IP address      MAC address
             Sid  State      Offset Power
 Cable1/0/U0 1    online     2257    0.00  3   0   10.30.128.142   0090.8330.0217
 Cable1/0/U0 2    online     2262  *-0.50  3   0   10.30.128.145   0090.8330.020f
 Cable1/0/U0 3    online     2260    0.25  3   0   10.30.128.146   0090.8330.0211
 Cable1/0/U0 4    online     2256   *0.75  3   0   10.30.128.143   0090.8330.0216
 Cable1/0/U0 5    online     2265   *0.50  3   0   10.30.128.140   0090.8330.0214
 Cable1/0/U0 6    online     2256    0.00  3   0   10.30.128.141   0090.8330.0215
 Cable1/0/U0 7    online     4138  !-1.00  3   1   10.30.128.182   0050.7366.124d
 Cable1/0/U0 8    online     4142  !-3.25  3   1   10.30.128.164   0050.7366.1245
 Cable1/0/U0 9    online     4141  !-3.00  3   1   10.30.128.185   0050.7366.17e3
 Cable1/0/U0 10   online     4142  !-2.75  3   0   10.30.128.181   0050.7366.17ab
 Cable1/0/U0 11   online     4142  !-3.25  3   1   10.30.128.169   0050.7366.17ef
```

Similar to the **show cable flap-list** command display, the * symbol in the **show cable modem** command output indicates that the CMTS is using the power-adjustment method on this CM. The ! symbol indicates that the CM has reached maximum transmit power.

Using Other Related Commands

The following related Cisco IOS commands can be used to do maintenance on or display information about a cable modem.

- The following clears the counters for a cable modem (or all cable modems) in the station maintenance list:

```
clear cable modem {mac-addr | ip-addr | all} counters
```

- The following displays the QoS, modem status, In and Out octets, IP and MAC addresses per SID:

```
show int cable slot/port sid
```

- The following drops the modem's RF link by removing a modem from the keepalive polling list. This forces the modem to reset. Note the warning below.

```
clear cable-modem {mac-addr | ip-addr | all} reset
```

Tip The **clear cable-modem** *all* **reset** command causes all modems to go offline and disrupt service for your users. It is best used in a test or nonproduction environment.

- The following uses a MAC-layer ping to determine if the cable modem is online. It uses smaller data units on the wire than a standard IP ping, resulting in lower overhead. This command works even if the IP layer in the modem is down or has not completed registration:

```
ping DOCSIS cable-modem mac-addr | IP address
```

- The following displays the timing offset, receive power, and QoS values by cable interface, SID, and MAC address:

```
show cable modem [ip-address | MAC-address]
```

- The following displays the current allocation table and frequency assignments:

```
show cable spectrum-group [spectrum group number]
```

- The following displays maximum, average, and minimum percent of online time and offline time for a given SID on a given cable router interface:

```
show int slot/port sid connectivity
```

- The following command displays input and output rates, input errors, CRC, frames, overruns, underruns, collisions, interface resets. High input errors in the CMTS retrieved from this query suggest noisy upstream. In older versions of the chassis, loose midplane and line card screws caused a similar problem:

```
show interface slot/downstream-port
```

- The following command displays upstream packet discards, errors, error-free packets, correctable and uncorrectable errors, noise, and micro-reflection statistics.

```
show interface slot/downstream-port upstream
```

Configuration Examples for Flap List Troubleshooting

The following excerpt from a configuration file shows a typical flap-list configuration:

```
!
cable flap-list insertion-time 120
cable flap-list power-adjust threshold 3
cable flap-list miss-threshold 4
cable flap-list aging 8
cable flap-list size 8191
...
```

Additional References

For additional information related to the Flap List Troubleshooting feature, refer to the following references:

Related Documents

Related Topic	Document Title
CMTS Command Reference	Cisco CMTS Cable Command Reference
Cisco Broadband Troubleshooter	http://www.cisco.com/c/en/us/support/cloud-systems-management/broadband-trou

Standards

Standards[4]	Title
ANSI/SCTE 22-1 2012 (formerly SP-RFI-C01-011119)	Data-Over-Cable Service Interface Specification DOCSIS 1.0 Radio Frequency Interface (RFI)
SP-RFIv1.1-I08-020301	Data-over-Cable Service Interface Specifications Radio Frequency Interface Specification
SP-BPI+-I08-020301	DOCSIS Baseline Privacy Interface Plus Specification

[4] Not all supported standards are listed.

MIBs

MIBs[5]	MIBs Link
CISCO-CABLE-SPECTRUM-MIB	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://tools.cisco.com/ITDIT/MIBS/servlet/index

[5] Not all supported MIBs are listed.

RFCs

Description	Link
No new or modified RFCs are supported by this feature.	To locate and download Request for Comments (RFCs) and Internet Drafts, see the Internet Engineering Task Force (IETF) web site at the following URL: http://www.ietf.org/index.html

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

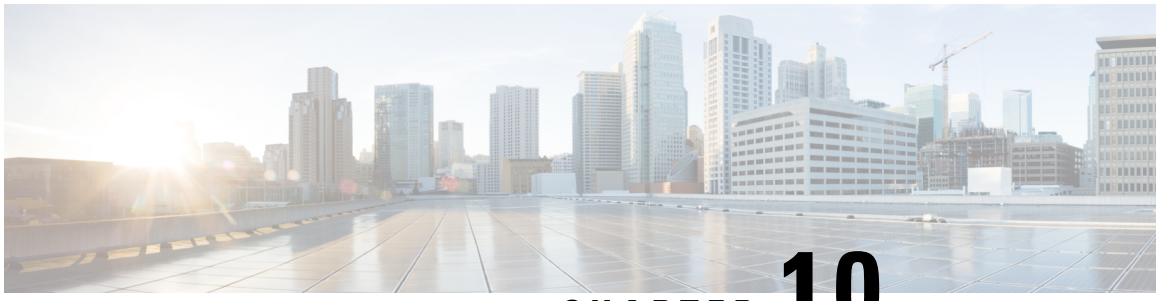
Feature Information for Flap List Troubleshooting

Use Cisco Feature Navigator to find information about the platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to the www.cisco.com/go/cfn link. An account on the Cisco.com page is not required.

Note The following table lists the software release in which a given feature is introduced. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 35: Feature Information for Flap List Troubleshooting

Feature Name	Releases	Feature Information
Flap List Troubleshooting	Cisco IOS XE Everest 16.6.1	This feature was integrated intoCisco IOS XE Everest 16.6.1 on the Cisco cBR Series Converged Broadband Routers.



CHAPTER 10

Maximum CPE and Host Parameters

This document describes how to use different methods to control subscriber access that are allowed by the Data-over-Cable Service Interface Specifications (DOCSIS) for use on cable networks.

- Finding Feature Information, on page 185
- Hardware Compatibility Matrix for the Cisco cBR Series Routers, on page 185
- Information About the MAX CPE and Host Parameters, on page 186
- How to Configure the MAX CPE and Host Parameters, on page 190
- Configuration Examples, on page 192
- Additional References, on page 193
- Feature Information for Maximum CPE and Host Parameters, on page 194

Finding Feature Information

Finding Feature Information

Your software release may not support all the features that are documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. The Feature Information Table at the end of this document provides information about the documented features and lists the releases in which each feature is supported.

Hardware Compatibility Matrix for the Cisco cBR Series Routers

Note The hardware components that are introduced in a given Cisco IOS-XE Release are supported in all subsequent releases unless otherwise specified.

Table 36: Hardware Compatibility Matrix for the Cisco cBR Series Routers

Cisco CMTS Platform	Processor Engine	Interface Cards
Cisco cBR-8 Converged Broadband Router	**Cisco IOS-XE Release 16.5.1 and Later Releases** Cisco cBR-8 Supervisor: • PID—CBR-SUP-250G • PID—CBR-CCAP-SUP-160G • PID—CBR-CCAP-SUP-60G • PID—CBR-SUP-8X10G-PIC	**Cisco IOS-XE Release 16.5.1 and Later Releases** Cisco cBR-8 CCAP Line Cards: • PID—CBR-LC-8D30-16U30 • PID—CBR-LC-8D31-16U30 • PID—CBR-RF-PIC • PID—CBR-RF-PROT-PIC • PID—CBR-CCAP-LC-40G • PID—CBR-CCAP-LC-40G-R Cisco cBR-8 Downstream PHY Modules: • PID—CBR-D30-DS-MOD • PID—CBR-D31-DS-MOD Cisco cBR-8 Upstream PHY Modules: • PID—CBR-D30-US-MOD • PID—CBR-D31-US-MOD

Information About the MAX CPE and Host Parameters

The DOCSIS specification includes a number of provisions to allow service providers to control the number of subscribers who can access the network through any particular cable modem.

The following are the parameters that controls the number of CPE that can access the network:

Note In addition, the DOCSIS configuration file contains a Network Access parameter that specifies whether the CPE devices behind the cable modem can access the cable network. If the Network Access parameter is set to Disabled, no CPE devices behind a cable modem are able to access the network.

Tip Also, the Cisco CMTS lists offline cable modems in its internal database for 24 hours. The CMTS does not reset the CPE counts for these offline cable modems until the 24 hour period expires and the cable modems come back online. If the cable modems come back online before the 24 hour period expires, the CMTS continues to use the existing CPE counts.

All of these methods are similar in purpose, but they are configured differently and have a different impact on cable modems and their CPE devices.

The cable modem enforces the MAX CPE value, the CMTS enforces the MAX Host, MAX CPE IP, and MAX CPE IPv6 values.

Note The MAX CPE parameter provides Layer 2 control of CPE devices. The MAX CPE IP and MAX CPE IPv6 parameters provide Layer 3 control of CPE devices. The two methods are complimentary but not otherwise related.

MAX CPE

The MAX CPE is a required parameter and used to control the number of CPE devices that can access the network during the current session. In DOCSIS 1.0 cable networks, the MAX CPE parameter is the primary means of controlling the number of CPE devices that can connect to the cable network using any particular cable modem. This parameter is configured in the DOCSIS configuration file (TLV 18). If this parameter is not specified in the DOCSIS configuration file, it defaults to a value of 1.

Note In DOCSIS 1.1 cable networks, the CMTS ignores the MAX CPE parameter that is specified in the DOCSIS configuration file, and uses the MAX Host parameter instead.

Each time a new CPE device attempts to connect to the cable network, the cable modem logs the hardware (MAC) address. If the cable modem has not reached the MAX CPE number of MAC addresses, the new CPE device is allowed to access the network. If the cable modem has reached the MAX CPE limit, it drops the traffic from any additional CPE devices.

By default, the cable modem learns new MAC addresses on a first-come, first-served basis. You can also preconfigure the allowable MAC addresses for CPE devices by entering those MAC addresses in the DOCSIS configuration file (TLV 14). These cable modem gives these preconfigured MAC addresses preference in connecting to the network.

The DOCSIS specification does not allow cable modems to age out MAC addresses, so a MAC address stays in the log table of the cable modem until the cable modem is reset. You should therefore think of this parameter as specifying the maximum number of CPE devices that can connect during any particular session, instead of the maximum number of CPE devices that can simultaneously connect to the cable network.

For example, if you set MAX CPE to 2, a customer could use their cable modem to connect a maximum of two CPE devices (two MAC addresses) to the cable network. A customer could choose to connect two PCs simultaneously to their cable modem and use both to access the network.

However, if the customer then disconnected these PCs and connected two new PCs, the cable modem would not allow the new PCs to come online, because they would be the third and fourth MAC addresses that are connected to the cable modem. The customer would have to reset the cable modem before being able to use the new PCs.

Note The MAX CPE value, if present, must be a positive integer in DOCSIS 1.0 configuration files. This parameter can be zero in DOCSIS 1.1 configuration files, but if so, the cable modem uses a MAX CPE value of 1. If the MAX CPE parameter is not present in either type of DOCSIS configuration file, it defaults to 1.

MAX Host

The MAX Host parameter is an optional parameter and is configured on the Cisco CMTS and specifies the maximum number of CPE devices (MAC addresses) that the CMTS will allow to have network access. You can control this parameter for individual cable modems, for all cable modems on a particular cable interface, or for all cable modems on the Cisco CMTS, depending on the CLI command being used:

- **cable modem max-cpe**—Configures MAX Host for all cable modems on the Cisco CMTS. You can use the **unlimited** keyword to specify that the Cisco CMTS should not enforce a MAX Host limit for cable modems.

When this is enabled, the Cisco CMTS learns a MAC address the first time that the CPE device accesses the cable network. After the Cisco CMTS has logged the maximum number of MAC addresses specified by a MAX Host parameter, it drops all traffic from CPE devices that have any other MAC address.

Tip In DOCSIS 1.1 cable networks, when both the MAX CPE IP and MAX Host parameters are configured, the Cisco CMTS uses the lesser value to determine the maximum number of CPE devices that are allowed behind each cable modem. By default, MAX Host is set to 16.

Note The entire MAX Host address table is cleared whenever the Cisco TS is reset. You can also clear an entry for a particular CPE device using the **clear cable host** command.

Specifying an Unlimited Value for Max Host

The **cable modem max-cpe** command, which affects all cable modems on the CMTS, supports the **unlimited** keyword, which specifies that the CMTS should not enforce any limit on CPE devices. When you configure the CMTS with the unlimited **keyword**, this setting, you are allowing cable modems to support any number of CPE devices.

Do not use the **unlimited** option without also specifying the proper value for MAX CPE in the DOCSIS configuration file, so that each cable modem can control the maximum number of CPE devices it supports. In addition, to prevent users from requesting an unlimited number of IP address, be sure to configure the DHCP servers so that they control how many IP addresses are assigned to the CPE devices behind each cable modem.

MAX CPE IP

The MAX CPE IP parameter is applicable only in DOCSIS 1.1 cable networks and is an optional parameter. This parameter specifies whether the cable modem should perform IP address filtering on the CPE devices.

If so, this attribute also specifies the maximum number of simultaneous IP addresses that are permitted behind the modem at any one time.

The MAX CPE IP parameter is configured in the DOCSIS configuration file (TLV 35), or by using SNMP commands to set the docsDevCpeIpMax attribute (in DOCS-CABLE-DEVICE-MIB) for the cable modem. By default, this parameter is not enabled and the Cisco CMTS does not actively manage CPE devices, unless you enable the use of the MAX CPE IP parameter by using the **cable submgmt default active** command. The **cable submgmt default max-cpe** command can be used to limit the number of IP addresses behind the cable modem.

If this feature is enabled, the cable modem learns the allowable IP addresses the first time that the CPE device sends an IP packet out into the network. The IP addresses are added to the docsDevFilterCpeTable table. This address table is cleared automatically when the cable modem is reset or powered off, or you can manually clear the IP address table by setting the docsSubMgtCpeControlReset attribute in the appropriate table entry for this cable modem.

Tip The CMTS uses the MAX CPE IP value as part of its own filtering process, but the two filters operate independently on the cable modem and CMTS.

MAX CPE IPv6

The MAX CPE IPv6 parameter is an optional parameter and specifies the maximum number of simultaneous IPv6 addresses that are permitted for a cable modem at any time.

The MAX CPE IPv6 parameter is configured in the DOCSIS 3.0 configuration file (TLV 63), or by using the SNMP commands to set the docsSubmgt3BaseCpeMaxIpv6PrefixDef attribute (in DOCS-SUBMGT3-MIB) for the cable modem. By default, this parameter is not enabled and the Cisco CMTS does not actively manage CPE devices, unless the use of the MAX CPE IPv6 parameter is enabled by using the **cable submgmt default active** command. The **cable submgmt default max-ipv6-cpe** command can be used to limit the number of IPv6 addresses allowed behind a cable modem.

When the MAX CPE IPv6 feature is enabled, the cable modem learns the allowable IPv6 addresses the first time that the CPE device sends an IPv6 packet out into the network. The IPv6 addresses are added to the IPv6 address table. The address table is cleared automatically when the cable modem is reset or powered off.

Interoperation of the Maximum CPE Parameters

The different methods of CPE control can all be active simultaneously. They can interact with one another but do not conflict with one another. The table lists each method and compares their characteristics.

Table 37: Comparison of the Different Max CPE and Max Host Control Mechanisms

CM Configuration Parameter	Function	CMTS Equivalent	CMTS Enforcement Priority
Network Access Control	Prevents all network access for CPE devices	Cable submgmt default learnable	CMTS overrides CM Config File
MAX CPE	Limits MAC addresses per CM	Cable modem max-hosts	Least restrictive is enforced

CM Configuration Parameter	Function	CMTS Equivalent	CMTS Enforcement Priority
MAX CPE IP	Limits IP addresses per CM	Cable submgmt default max-cpe	Most restrictive is enforced
MAX CPE IPv6	Limits IPv6 addresses per CM	Cable submgmt default max-ipv6-cpe	Most restrictive is enforced

The table lists the MAX CPE parameters in order of priority. For example, the Network Access Control and MAX CPE parameters interact as follows:

- If the Network Access Control field for a cable modem is set to Disabled, none of that modem's CPE devices will be able to access the network, regardless of how the other parameters are set.
- If Network Access Control is Enabled and MAX CPE is set to 1 for a cable modem, then a maximum of one CPE device will be able to access the network, no matter how the remaining parameters are configured.

Benefits

- CMTS flexibility allows multiple service operator provisioners, service providers, and other users to synchronize between the CMTS and the cable modem, the maximum number of CPE devices, maximum number of IPv4 addresses, and maximum number of IPv6 addresses that can be connected behind a cable modem.
- Changes can be made by using CLI commands or by using SNMP commands.

How to Configure the MAX CPE and Host Parameters

To reset the maximum number of permitted CPE devices recognized by the CMTS, use one of the following configuration commands. All procedures are optional, depending on the requirements.

Note The CMTS assigns the MAX Host value to a cable modem at the time that the cable modem registers with the CMTS. Changing any of the MAX Host commands affects only cable modems that register after the change.

Configuring the Maximum Number of CPE Devices on the Cisco CMTS

To configure the maximum number of CPE devices per cable modem, use the following procedure:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:**	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
	`Router> enable`	
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable modem max-cpe** [*number* | **unlimited**] **Example:** `Router(config)# cable modem max-cpe 8`	Sets the value of the MAX CPE parameter on the Cisco CMTS for all cable interfaces. The **show cable modem subscriber** displays the MAXIMUM value of cable modem max-cpe and the MAX CPE value in the DOCSIS configuration file of the cable modem. The number of the CPE that can be online is determined based on one of the following aspects: • If the number of the CPE is lower than the MAX CPE value in the DOCSIS configuration file of the cable modem, then the **cable modem max-cpe** command overrides the configuration file value. • If number of the CPE is higher than the MAX CPE value in the DOCSIS configuration file of the cable modem or is set as unlimited, then the value set in the configuration file takes precedence. **Note** If the value in the configuration file is zero and **no cable modem max-cpe** is configured, then no CPE device is able to obtain an IP address.
Step 4	**cable submgmt default active** **Example:** `Router(config)# cable submgmt default active`	Specifies that the CMTS should actively manage CPE devices. The default is the **no** version of this command, so that the CMTS does not actively manage CPE devices.
Step 5	**cable submgmt default max-cpe** *cpe-ip* **Example:** `Router(config)# cable submgmt default max-cpe 4`	(Optional) Specifies the default value for the MAX CPE IP.
Step 6	**cable submgmt default max-ipv6-cpe** *ipv6-num* **Example:** `Router(config)# cable submgmt default max-ipv6-cpe`	(Optional) Specifies the default value for the MAX IPv6 CPE.

	Command or Action	Purpose
	4	
Step 7	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.

What to do next

Note Use of the **cable modem max-cpe unlimited** command can open a security hole in the system by enabling denial of service attacks. It could allow a single user to obtain a large number of IP addresses, and thereby cause the entire network to go down after this single user has reserved all available IP addresses.

Configuration Examples

To display the current configuration and status of a cable interface, use the **show running-config** command in privileged EXEC mode. The following is sample output that shows that the CMTS permits up to five CPE devices to use the specified cable interface to pass traffic.

```
interface Cable3/0
 ip address 192.168.1.1 255.255.255.0 secondary
 ip address 10.1.1.1 255.255.255.0
 load-interval 30
 no keepalive
 cable downstream annex B
 cable downstream modulation 256qam
 cable downstream interleave-depth 32
 cable downstream frequency 507000000
 cable upstream 0 frequency 27008000
 cable upstream 0 power-level 0
 cable upstream 0 minislot-size 32
 cable upstream 0 modulation-profile 2
 no cable upstream 0 shutdown
 cable upstream 1 frequency 29008000
 cable upstream 1 power-level 0
 cable upstream 1 channel-width 3200000
 cable upstream 1 minislot-size 4
 no cable upstream 1 shutdown
 cable dhcp-giaddr policy
 cable helper-address 172.17.110.131
end
```

You can also use the **more system:running-config** command to verify the maximum number of permitted CPE devices for a cable interface.

```
CMTS01# more system:running-config
Building configuration...
Current configuration:
!
```

```
interface Cable6/0
 ip address 10.1.1.1 255.255.255.0
 no keepalive
 cable insertion-interval 2000
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream symbol-rate 5056941
 cable upstream 0 frequency 15008000
 cable upstream 0 fec
 cable upstream 0 scrambler
 no cable upstream 0 shutdown
```

Additional References

For additional information related to configuring the MAX CPE and Host parameters on the Cisco CMTS, refer to the following references:

Related Documents

Related Topic	Document Title
Cisco CMTS Commands	Cisco CMTS Cable Command Reference
Interaction of MAX CPE Parameters	Using the max-cpe Command in the DOCSIS and CMTS

Standards

Standards[6]	Title
SP-RFIv1.1-I08-020301	*Data-Over-Cable Service Interface Specifications Radio Frequency Interface Specification* , *version 1.1* (http://www.cablelabs.com/cablemodem/)

[6] Not all supported standards are listed.

MIBs

MIBs[7]	MIBs Link
DOCS-CABLE-DEVICE-MIB DOCS-SUBMGT-MIB DOCS-SUBMGT3-MIB	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

[7] Not all supported MIBs are listed.

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

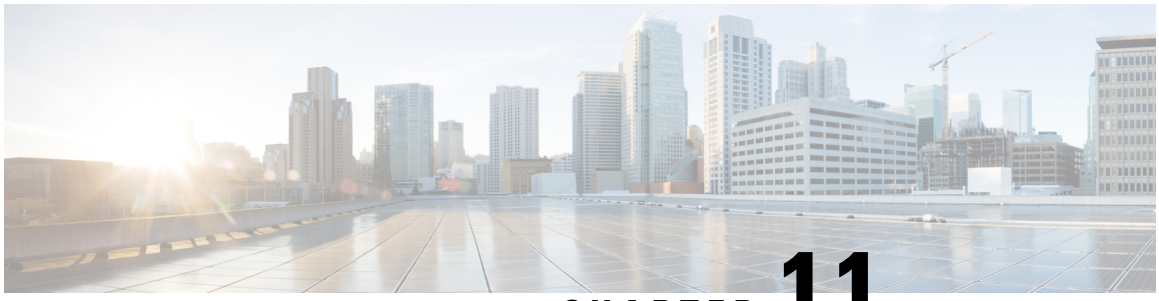
Feature Information for Maximum CPE and Host Parameters

Use Cisco Feature Navigator to find information about the platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to the www.cisco.com/go/cfn link. An account on the Cisco.com page is not required.

Note The following table lists the software release in which a given feature is introduced. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 38: Feature Information for Maximum CPE and Host Parameters

Feature Name	Releases	Feature Information
Maximum CPE and Host Parameters	Cisco IOS XE Everest 16.6.1	This feature was integrated into Cisco IOS XE Everest 16.6.1 on the Cisco cBR Series Converged Broadband Routers.



CHAPTER 11

SNMP Background Synchronization

The SNMP Background Synchronization features provides periodic background synchronization of DOCSIS MIB data from line card to Supervisor in order to improve the performance of the SNMP polling of these MIB tables.

Finding Feature Information

Your software release may not support all the features that are documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. The Feature Information Table at the end of this document provides information about the documented features and lists the releases in which each feature is supported.

Contents

- Information About SNMP Background Synchronization, on page 195
- How to Configure SNMP Background Synchronization, on page 196
- Configuring Example for SNMP Background Synchronization, on page 203
- Feature Information for SNMP Background Synchronization, on page 203

Information About SNMP Background Synchronization

To improve SNMP performance, SNMP background synchronization feature is introduced to synchronize the SNMP MIB information between the line card and the Supervisor. It is based on raw socket and uses TCP protocol. The benefits of the SNMP Background Synchronization include:

- Bundles small packets together before sending out, increases IPC channel utilization.
- Use pre-allocated static buffer to send/receive message, avoid buffer allocation at run time.
- In order not to burden CPU when the system is in high load, SNMP background synchronization receive process can sleep based on CPU utilization, so it will not compete with other priority processes.
- Significantly improve SNMP polling performance for supported MIB tables, and reduce the CPU utilization in both Supervisor and line card.

The following MIB tables are supported in SNMP background synchronization:

- docsQosParamSetEntry
- docsIetfQosParamSetEntry

- docsQos3ParamSetEntry
- docsIf3CmtsCmUsStatusEntry
- docsIfCmtsCmStatusEntry
- docsSubMgtCpeControlEntry
- docsSubMgtCmFilterEntry
- cdxCmtsCmStatusExtEntry
- docsLoadBalCmtsCmStatusEntry
- docsIf3CmtsCmRegStatusTable
- docsIfSignalQualityTable
- docsifCmtsServiceTable
- cdxCmtsServiceExtEntry

How to Configure SNMP Background Synchronization

Enabling SNMP Background Synchronization

Before you begin

To use the **cable bgsync** command, you must configure the **service internal** command in global configuration mode.

SNMP background synchronization is enabled by default, use **no cable bgsync active** to disable this feature, and use **cable bgsync active** to enable it again. The following procedure lists detailed steps to enable SNMP background synchronization:

```
enable
configure terminal
cable bgsync active
exit
```

Setting Data Interval

Before you begin

To use the **cable bgsync** command, you must configure the **service internal** command in global configuration mode. Use the **cable bgsync** command carefully as it can impact the CPU utilization.

To set the data intervals for the background synchronization of SNMP MIB data on the Cisco cBR routers, use the **cable bgsync** {**itime** *i-interval*|**ptime** *p-interval*} command in global configuration mode. To disable background synchronization, use the **no** form of this command. The following procedure lists detailed steps to set data interval:

```
enable
configure terminal
```

```
service internal
cable bgsync itime i-interval
cable bgsync ptime p-interval
exit
```

itime is the interval of synchronizing all related MIB tables from line card to Supervisor. The valid range is from 5 to 31536000. The default value is 86400. **ptime** is the interval of synchronizing the changed MIB content from line card to Supervisor.

Verifying SNMP Background Synchronization

- To display the current status of the SNMP background synchronization, use the **show cable bgsync** command as shown in the example below:

```
Router#show cable bgsync
Background Sync is active, uptime is 5 minutes, 14 seconds.
Background Sync last active time is 5 minutes, 14 seconds. ago.
I-packet interval time is 1 day,  P-packet interval time is 5 senconds.
Line Card with bg-sync: 3/0
Line Card working on I syncing:
Last clear cable bg sync counters Time:
Total bytes: 85864
Total background sync packets: 2109
  Ack packets: 0
  Run Ctrl Msg packets: 2
  Data packets: 0
Interval packets: 2002
  I Type packets: 230
  P Type packets: 1772
Bg sync data IPC lost packets: 0

Background Sync statistics for the last 00:07:34
============================================================
 ipc packets 0-30k:      105
 ipc packets 30-60k:     0
 ipc packets 60-100k:    0
 msg per packet average: 20
 msg per packet max:     113
 msg per packet min:     1
 msg per packet under 3: 60
============================================================
type       packets        cpu-total(ms)    avg(us)   max(us)
serv flow  904            3                3         1000
sflog      0              0                0         0
cm         17             0                0         0
cmtx       296            0                0         0
paramset   112            0                0         0
DXIF       298            0                0         0
sid        208            0                0         0
uschan     167            1                5         1000
------------------------------------------------------------
IPC PKTs   105            4                0      ms 1      ms
================================================================================================
slot type       packets        bytes            pps        Bps        wrong_len_pkts
0    serv flow  0              0                0.0        0.0        0

0    sflog      0              0                0.0        0.0        0

0    cm         0              0                0.0        0.0        0
```

0	cmtx	0	0	0.0	0.0	0
0	paramset	0	0	0.0	0.0	0
0	DXIF	0	0	0.0	0.0	0
0	sid	0	0	0.0	0.0	0
0	uschan	0	0	0.0	0.0	0
1	serv flow	0	0	0.0	0.0	0
1	sflog	0	0	0.0	0.0	0
1	cm	0	0	0.0	0.0	0
1	cmtx	0	0	0.0	0.0	0
1	paramset	0	0	0.0	0.0	0
1	DXIF	0	0	0.0	0.0	0
1	sid	0	0	0.0	0.0	0
1	uschan	0	0	0.0	0.0	0
2	serv flow	0	0	0.0	0.0	0
2	sflog	0	0	0.0	0.0	0
2	cm	0	0	0.0	0.0	0
2	cmtx	0	0	0.0	0.0	0
2	paramset	48	7680	0.0	0.0	0
2	DXIF	0	0	0.0	0.0	0
2	sid	16	512	0.0	0.0	0
2	uschan	0	0	0.0	0.0	0
3	serv flow	904	25104	4.4	115.4	0
3	sflog	0	0	0.0	0.0	0
3	cm	17	981	0.0	2.0	0
3	cmtx	296	8607	0.7	20.6	0
3	paramset	64	8368	0.0	0.0	0
3	DXIF	298	21876	0.9	74.3	0
3	sid	192	4756	0.1	6.8	0
3	uschan	167	5832	0.3	10.7	0
6	serv flow	0	0	0.0	0.0	0
6	sflog	0	0	0.0	0.0	0
6	cm	0	0	0.0	0.0	0

```
6    cmtx       0              0              0.0        0.0        0
6    paramset   0              0              0.0        0.0        0
6    DXIF       0              0              0.0        0.0        0
6    sid        0              0              0.0        0.0        0
6    uschan     0              0              0.0        0.0        0
7    serv flow  0              0              0.0        0.0        0
7    sflog      0              0              0.0        0.0        0
7    cm         0              0              0.0        0.0        0
7    cmtx       0              0              0.0        0.0        0
7    paramset   0              0              0.0        0.0        0
7    DXIF       0              0              0.0        0.0        0
7    sid        0              0              0.0        0.0        0
7    uschan     0              0              0.0        0.0        0
8    serv flow  0              0              0.0        0.0        0
8    sflog      0              0              0.0        0.0        0
8    cm         0              0              0.0        0.0        0
8    cmtx       0              0              0.0        0.0        0
8    paramset   0              0              0.0        0.0        0
8    DXIF       0              0              0.0        0.0        0
8    sid        0              0              0.0        0.0        0
8    uschan     0              0              0.0        0.0        0
9    serv flow  0              0              0.0        0.0        0
9    sflog      0              0              0.0        0.0        0
9    cm         0              0              0.0        0.0        0
9    cmtx       0              0              0.0        0.0        0
9    paramset   0              0              0.0        0.0        0
9    DXIF       0              0              0.0        0.0        0
9    sid        0              0              0.0        0.0        0
9    uschan     0              0              0.0        0.0        0
```

- To display all the SNMP background sync data on Supervisor side or line card side, use the **show cable bgsync sync-info cable** command as shown in the example below:

```
Router#show cable bgsync sync-info cable 9/0/1
```

```
 part1 for srv template:
srv_tmp_id   min_rate    max_rate    max_burst
0           0           0           0
1           0           64000       0
2           0           1000000     0
3           0           1000000     3044
4           0           0           3044
5           0           110000000   30000
6           0           0           3044
7           0           2000000000  5000000
8           0           0           3044
 part2 for srv flow:
sfid     prov_qos   adm_qos    act_qos    wb_mode    octets    pkts    delay_pkts
drop_pkts    gate_id    create_time    total_active_time
1        0          0          0          0          0         0          0
0          0              0              0
2        0          0          0          0          0         0          0
0          0              0              0
3        0          0          0          0          0         0          0
0          0              0              0
4        0          0          0          0          0         0          0
0          0              0              0
5        0          0          0          0          0         0          0
0          0              0              0
6        0          0          0          0          0         0          0
0          0              0              0
7        0          0          0          0          0         0          0
0          0              0              0
8        0          0          0          0          0         0          0
0          0              0              0
9        0          0          0          0          0         0          0
0          0              0              0
10       0          0          0          0          0         0          0
0          0              0              0
11       0          0          0          0          0         0          0
0          0              0              0
12       0          0          0          0          0         0          0
0          0              0              0
13       0          0          0          0          0         0          0
0          0              0              0
14       0          0          0          0          0         0          0
0          0              0              0
15       3          3          3          0          0         0          0
0          0              3600           179
16       3          3          3          0          0         0          0
0          0              3600           179
17       3          3          3          0          0         0          0
0          0              3600           179
18       3          3          3          0          0         0          0
0          0              3600           179
19       3          3          3          0          0         0          0
0          0              3600           179
20       3          3          3          0          0         0          0
0          0              3600           179
21       3          3          3          0          0         0          0
0          0              3600           179
22       3          3          3          0          0         0          0
0          0              3600           179
23       3          3          3          0          0         0          0
0          0              3600           179
24       3          3          3          0          0         0          0
0          0              3600           179
25       3          3          3          0          0         0          0
0          0              3600           179
```

```
26       3          3          3          0          0          0          0
0          0             3600          179
27       4          5          5          0          8925       42         0
0          0             12700         88
28       6          7          7          3          0          0          0
0          0             12700         88
29       4          5          5          3          3855       21         0
0          0             11500         100
30       6          7          7          3          0          0          0
0          0             11500         100
31       8          8          8          3          222        3          0
0          0             11500         100
32       4          5          5          3          1277       11         0
0          0             12100         94
33       6          7          7          0          0          0          0
0          0             12100         94
34       4          5          5          0          3851       21         0
0          0             12300         92
35       6          7          7          3          0          0          0
0          0             12300         92
36       8          8          8          0          148        2          0
0          0             12100         94
37       4          5          5          0          3855       21         0
0          0             12700         88
38       6          7          7          3          0          0          0
0          0             12700         88
39       8          8          8          3          222        3          0
0          0             12300         92
40       4          5          5          3          3281       20         0
0          0             13100         84
41       6          7          7          3          0          0          0
0          0             13100         84
42       8          8          8          3          222        3          0
0          0             12700         88
43       8          8          8          3          222        3          0
0          0             12700         88
44       4          5          5          3          3308       21         0
0          0             13100         84
45       6          7          7          3          0          0          0
0          0             13100         84
46       8          8          8          3          296        4          0
0          0             13100         84
47       8          8          8          3          296        4          0
0          0             13100         84
48       4          5          5          3          73         2          0
0          0             14500         70
49       6          7          7          3          0          0          0
0          0             14500         70
50       8          8          8          3          74         1          0
0          0             14500         70
 part3 for sid
 sid_entry[1] sid 1 service_class 2 create_time 127 total_octets 8925
 sid_entry[2] sid 2 service_class 2 create_time 115 total_octets 3855
 sid_entry[3] sid 3 service_class 2 create_time 121 total_octets 1277
 sid_entry[4] sid 4 service_class 2 create_time 123 total_octets 3851
 sid_entry[5] sid 5 service_class 2 create_time 127 total_octets 3855
 sid_entry[6] sid 6 service_class 2 create_time 131 total_octets 3281
 sid_entry[7] sid 7 service_class 2 create_time 131 total_octets 3308
 sid_entry[8] sid 8 service_class 2 create_time 145 total_octets 73
 part4 for cm and cmtx
 cm_mac: 68ee.9633.0699, tcsbmp: 0x1, admin_status 1, md_sg_id 0x1510505, rcc_status_id
 0x4, rcs_id 0x1520005, tcs_id 0x1 last_reg_time 1444372688, RCP ID:00 10 00 00 10
 usch 1, modulation_type 2, rx_power -5, signal_noise 390, time_offset 2085
 cm_mac: e448.c70c.96e7, tcsbmp: 0x4, admin_status 1, md_sg_id 0x1510505, rcc_status_id
```

```
 0x4, rcs_id 0x1520005, tcs_id 0x3 last_reg_time 1444372678, RCP ID:00 10 00 00 08
 usch 3, modulation_type 2, rx_power -15, signal_noise 381, time_offset 1785
 cm_mac: 0019.474a.c126, tcsbmp: 0x1, admin_status 1, md_sg_id 0x1510505, rcc_status_id
 0x0, rcs_id 0x22, tcs_id 0x1 last_reg_time 1444372682, RCP ID:00 00 00 00 00
 usch 1, modulation_type 2, rx_power -15, signal_noise 390, time_offset 1792
 cm_mac: e448.c70c.982b, tcsbmp: 0x1, admin_status 1, md_sg_id 0x1510505, rcc_status_id
 0x4, rcs_id 0x1520005, tcs_id 0x1 last_reg_time 1444372685, RCP ID:00 10 00 00 08
 usch 1, modulation_type 2, rx_power -10, signal_noise 390, time_offset 1786
 cm_mac: e448.c70c.96d5, tcsbmp: 0x2, admin_status 1, md_sg_id 0x1510505, rcc_status_id
 0x4, rcs_id 0x1520005, tcs_id 0x2 last_reg_time 1444372688, RCP ID:00 10 00 00 08
 usch 2, modulation_type 2, rx_power -15, signal_noise 381, time_offset 1786
 cm_mac: e448.c70c.9819, tcsbmp: 0x1, admin_status 1, md_sg_id 0x1510505, rcc_status_id
 0x4, rcs_id 0x1520005, tcs_id 0x1 last_reg_time 1444372692, RCP ID:00 10 00 00 08
 usch 1, modulation_type 2, rx_power -10, signal_noise 390, time_offset 1789
 cm_mac: e448.c70c.980d, tcsbmp: 0x4, admin_status 1, md_sg_id 0x1510505, rcc_status_id
 0x4, rcs_id 0x1520005, tcs_id 0x3 last_reg_time 1444372695, RCP ID:00 10 00 00 08
 usch 3, modulation_type 2, rx_power -10, signal_noise 390, time_offset 1783
 cm_mac: e448.c70c.96f3, tcsbmp: 0x1, admin_status 1, md_sg_id 0x1510505, rcc_status_id
 0x4, rcs_id 0x1520005, tcs_id 0x1 last_reg_time 1444372723, RCP ID:00 10 00 00 04
 usch 1, modulation_type 2, rx_power 0, signal_noise 420, time_offset 1798
 part5 for dxif info ifnum 1
 basedata[1][1]: cmstatusindex 2375681, cm_mac 68ee.9633.0699, cm_ip 0x5011961F, cm_ds_if
 59881, cm_us_if 204952
 cmregmode 2, cmmodultype 2, cmdocmode 2
 basedata[1][2]: cmstatusindex 2375682, cm_mac e448.c70c.96e7, cm_ip 0x5011961D, cm_ds_if
 59882, cm_us_if 204954
 cmregmode 2, cmmodultype 2, cmdocmode 2
 basedata[1][3]: cmstatusindex 2375683, cm_mac 0019.474a.c126, cm_ip 0x50119602, cm_ds_if
 59914, cm_us_if 204952
 cmregmode 2, cmmodultype 2, cmdocmode 2
 basedata[1][4]: cmstatusindex 2375684, cm_mac e448.c70c.982b, cm_ip 0x50119612, cm_ds_if
 59881, cm_us_if 204952
 cmregmode 2, cmmodultype 2, cmdocmode 2
 basedata[1][5]: cmstatusindex 2375685, cm_mac e448.c70c.96d5, cm_ip 0x5011960D, cm_ds_if
 59881, cm_us_if 204953
 cmregmode 2, cmmodultype 2, cmdocmode 2
 basedata[1][6]: cmstatusindex 2375686, cm_mac e448.c70c.9819, cm_ip 0x5011961E, cm_ds_if
 59881, cm_us_if 204952
 cmregmode 2, cmmodultype 2, cmdocmode 2
 basedata[1][7]: cmstatusindex 2375687, cm_mac e448.c70c.980d, cm_ip 0x5011961A, cm_ds_if
 59882, cm_us_if 204954
 cmregmode 2, cmmodultype 2, cmdocmode 2
 basedata[1][8]: cmstatusindex 2375688, cm_mac e448.c70c.96f3, cm_ip 0x5011960E, cm_ds_if
 59882, cm_us_if 204952
 cmregmode 2, cmmodultype 2, cmdocmode 2
 part6 uschan for ifnum 1
usport 1 micro_reflections 0 us_snr 390 snmp_sigq_unerroreds 0 snmp_sigq_correcteds 0
 snmp_sigq_uncorrectables 0
usport 2 micro_reflections 0 us_snr 381 snmp_sigq_unerroreds 0 snmp_sigq_correcteds 0
 snmp_sigq_uncorrectables 0
usport 3 micro_reflections 0 us_snr 390 snmp_sigq_unerroreds 0 snmp_sigq_correcteds 0
 snmp_sigq_uncorrectables 0
usport 4 micro_reflections 0 us_snr 0 snmp_sigq_unerroreds 0 snmp_sigq_correcteds 0
snmp_sigq_uncorrectables 0
```

- To display raw socket interprocess communication (IPC) infrastructure statistics for specified field replaceable unit (FRU), use the **show platform software ios** *slot-id* **socket statistics** command as shown in the example below:

```
Router#show platform software ios R0 socket statistics 0
-----------------------------------------------

Session Slot             : 2
```

```
Socket FD               : 93
Client ID               : 0
Message Receive Count   : 0
Message Receive Bytes   : 0

-----------------------------------------

Session Slot            : 2
Socket FD               : 93
Client ID               : 1
Message Receive Count   : 30155
Message Receive Bytes   : 1326820

-----------------------------------------

Session Slot            : 3
Socket FD               : 86
Client ID               : 0
Message Receive Count   : 0
Message Receive Bytes   : 0

-----------------------------------------

Session Slot            : 3
Socket FD               : 86
Client ID               : 1
Message Receive Count   : 29611
Message Receive Bytes   : 69782901
```

Configuring Example for SNMP Background Synchronization

The following example shows how to configure SNMP background synchronization:

```
enable
configure terminal
cable bgsync active
service internal
cable bgsync itime 200
cable bgsync ptime 500
exit
```

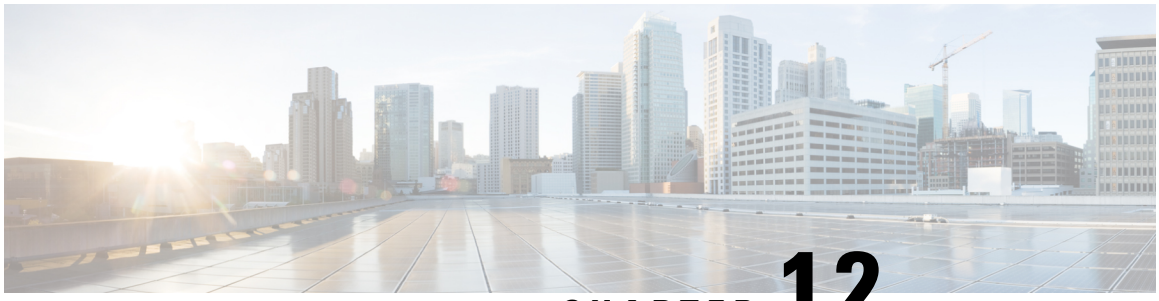
Feature Information for SNMP Background Synchronization

Use Cisco Feature Navigator to find information about the platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to the www.cisco.com/go/cfn link. An account on the Cisco.com page is not required.

Note The following table lists the software release in which a given feature is introduced. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 39: Feature Information for SNMP Background Synchronization

Feature Name	Releases	Feature Information
SNMP Background Synchronization	Cisco IOS XE Everest 16.6.1	This feature was integrated into Cisco IOS XE Everest 16.6.1 on the Cisco cBR Series Converged Broadband Routers.



CHAPTER 12

Online Offline Diagnostics

Online Offline Diagnostics (OOD) Field Diagnostics feature allows the customer to test and verify hardware-related issues on a line card deployed in the field. The test results can be used to verify whether a line card is fault and troubleshoot network issues.

- Overview of Online Offline Diagnostics, on page 205
- How to Configure Online Offline Diagnostics, on page 206
- Configuration Example for Online Offline Diagnostics, on page 207
- Feature Information for Online Offline Diagnostics, on page 207

Overview of Online Offline Diagnostics

The Online Offline Diagnostics is a field diagnostic mechanism that allows the customers to test and verify the line card hardware problems.

To perform a hardware diagnostic test on a line card in the Cisco cBR universal broadband router, download an OOD Field Diagnostic image for free from Cisco.com and use it to verify if the line card problems are due to hardware failure. The customer can run field diagnostic tests on the standby line card at any time without interrupting service. Testing the standby line card improves high availability of the system by ensuring the standby line card is ready for a switchover.

Field Diagnostic Image Information

Field Diagnostic image is used to run diagnostic tests on a line card and is available from Cisco.com.

First, download it from Cisco.com to one of the flash file systems on the router. Then move it to the line card, and the line card is automatically taken offline. Once field diagnostic tests are complete and the test results are gathered, the Field Diagnostic image must be unloaded from the line card. Normal line card operation will automatically resume after the Field Diagnostic image is unloaded from the line card.

Benefits of Online Offline Diagnostics

- **Improved Troubleshooting**. Field diagnostics verifies whether a line card problem is hardware-related or not. If the problem is software-related, the Field Diagnostic image allows customer to quickly rule out hardware related cause and focus on fixing the software issue causing the problem.
- **Pre-installation Line Card Hardware Verification**. Field diagnostics verifies whether a line card has hardware problems before installing the line card in a Cisco cBR Series router.

- **Onsite Fault Detection**. Field diagnostics helps to confirm if the problem is hardware-related and if it is necessary to replace the line card.
- **Additional Uptime**. Field diagnostics ensures that line cards are not mistakenly taken offline if the problem is not hardware-related, thereby increasing network uptime.

Prerequisites for Online Offline Diagnostics

- Before running the OOD Field Diagnostic tests on the working (active) line card in an N + 1 redundancy setup, it is advisable to switch over to the protect (standby) line card before loading the Field Diagnostic image to the line card to avoid service interruption.
- After an OOD Field Diagnostic image is loaded to the line card, the line card goes offline. Therefore, schedule a downtime for the line card to be tested before performing field diagnostic tests.
- Before performing any field diagnostic test, unplug all cables on the device that connect to other interfaces. If the cables that connect interfaces are not unplugged, some field diagnostic tests may send packets to connected devices, which increments packet counters on the receiving interfaces.

Restrictions for Online Offline Diagnostics

- When accessing a router through Telnet while running an OOD Field Diagnostic test, testing progress messages do not appear on the screen.
- If supervisor switchover occurs during a field diagnostic test, the test stops immediately and the line card run-time image automatically replaces the Field Diagnostic image on the line card.
- This feature is supported on CBR-CCAP-LC-40G line card in Cisco IOS-XE release 3.18.0S and later releases.
- It is suggested to run OOD on one line card at a time to avoid service impact.
- To run OOD on multiple line cards, leave 5 to 10 minutes gap before loading the OOD image to the next line card.

How to Configure Online Offline Diagnostics

Configuring Field Diagnostic Test

To load the field diagnostic image and start field diagnostic test, complete the following procedure:

```
copy tftp:image-file {harddisk: | bootflash: | flash:}
request platform hardware diagnostic load slot slot-id image-file autostart
```

Verifying the Testing Process

To verify whether the field diagnostic tests are running, use the **show platform hardware diagnostic status slot** *slot-id* command as shown in the example below:

```
Router# show platform hardware diagnostic status slot 0
Online Offline Diagnostic Status (P=Passed, F=Failed, U=Untested)
State                 Overall Test Num        Test Done Num          Test Result

--------------------------------------------------------------------------------
Running Auto Test     75                      70                     P:69 F:1 U:5
```

Note If the test result shows that the failed test number is not 0, please copy the full log and contact Cisco TAC team for support. You can use **dir harddisk:ood/** command to list the log files.

Removing the Field Diagnostic Image from a Line Card

To unload the Field Diagnostic image, use the **request platform hardware diagnostic unload slot** *slot-id* command as below:

request platform hardware diagnostic unload slot *slot-id*

Then the line card will be reloaded to run-time image.

Note To retain the results of a diagnostic test, copy and paste the **show platform hardware diagnostic status slot** command output into a separate file before unloading the Field Diagnostic image. The output of the **show platform hardware diagnostic status slot** command cannot be gathered after unloading the Field Diagnostic image from the line card.

Configuration Example for Online Offline Diagnostics

The following example shows running output for Online Offline Diagnostics:

```
copy tftp:field_diag harddisk:
request platform hardware diagnostic load slot 0 harddisk:field_diag autostart

Mar 2 16:00:51.933 CST: %IOSXE_OIR-6-REMCARD: Card (cc) removed from slot x
Mar 2 16:00:51.934 CST: %CABLE_CLC-5-LOGGER_LC_REMOVED: Carrier Card x removed
```

Feature Information for Online Offline Diagnostics

Use Cisco Feature Navigator to find information about the platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to the www.cisco.com/go/cfn link. An account on the Cisco.com page is not required.

Note The following table lists the software release in which a given feature is introduced. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 40: Feature Information for Online Offline Diagnostics

Feature Name	Releases	Feature Information
Online Offline Diagnostics	Cisco IOS XE Everest 16.6.1	This feature was integrated into Cisco IOS XE Everest 16.6.1 on the Cisco cBR Series Converged Broadband Routers.

INDEX

B

benefits **171, 190**
  flap-list troubleshooting **171**
  maximum CPE or host parameters **190**

C

Cable Manager 2.0flap-list troubleshooting **170**
  Cable Manager 2.0 **170**
commands, configuration **190**
  cable modem max-cpe command **190**
configuration examples **183**
  flap-list troubleshootingexamples, configuration **183**
    flap-list troubleshooting **183**
configuration tasks **171, 190**
  cable modem max-cpe command **190**
  flap-list troubleshooting **171**
  maximum CPE or host parameters **190**
  reset max permitted CPE devices **190**
CPE **186**
  set max number **186**
customer premises equipment devices **186**
  customer premises equipment. See CPE. **186**

D

DOCSIS configuration file **186**
  set max permitted CPE devices on CMTSCPE **186**
    maximum number **186**

F

flap-list troubleshooting **176–178, 180–181**
  monitoring and troubleshooting **176**
  performing amplitude averaging **181**
  troubleshooting suggestions **180**
  using CLI **176–177**
  using SNMP API **176**
  using SNMPflap-list troubleshooting **178**
    troubleshooting suggestions **178**

O

overview **169, 186, 189**
  cable modem max-cpe commandoverview **189**
    cable max-hosts command **189**
  cable modem max-hosts command **189**
  flap-list troubleshootingflap-list troubleshooting **169**
  maximum CPE or host parameters **186**

R

restrictions and limitations **168**
  flap-list troubleshooting **168**