Cisco cBR Converged Broadband Routers Video Configuration Guide for Cisco IOS XE Dublin 17.12

First Published: 2023-07-31

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

© 2023 Cisco Systems, Inc. All rights reserved.

CONTENTS

PART I **Basic Configuration and Provisioning Construct** 17

CHAPTER 1 **Video Services Provisioning Model** 1

Information about Video Services Provisioning 1

Video Provisioning Constructs 1

Feature Information for Video Services Provisioning 2

CHAPTER 2 **Video Virtual Carrier Group and Virtual Edge Input** 5

Information about Virtual Carrier Group and Virtual Edge Input 5

Virtual Carrier Group 5

Virtual Edge Input 6

How to Configure Virtual Carrier Group and Virtual Edge Input 6

Configuring Virtual Carrier Group 6

Overriding the Default TSID 7

Verifying Virtual Carrier Group Configuration 7

Configuring Virtual Edge Input under Logical Edge Device 7

Verifying Virtual Edge Input Configuration 8

Configuration Examples for Virtual Carrier Group and Virtual Edge Input 9

Example: Configuring Virtual Carrier Group 9

Example: Configuring Virtual Edge Input 9

Example: Overriding the Default TSID 10

Feature Information for Virtual Carrier Group and Virtual Edge Input 10

CHAPTER 3 **Service Distribution Group** 11

Information About Service Distribution Group 11

How to Configure the Service Distribution Group 12

Defining the Physical Slot/Bay/Port 12
Configuring QAM Replication 12
Overriding the Default ONID 13
Overriding the Default PSI Value 13
Configuring the Serving Area 13
Verifying the Serving Area Configuration 13
Verifying Service Distribution Group Configuration 15
Troubleshooting Tips 15
Configuration Examples 15
Configuring a Service Distribution Group 15
Feature Information for Service Distribution Group 16

CHAPTER 4 **QAM Profile 17**
QAM Profile 17
How to Configure the Video QAM Carriers 17
Configuring the Video QAM Profile 17
Configuring the Video QAM Carriers 18
Verify the configuration of the RF Channel 19
Configuration Examples 19
Video QAM Carriers 19
Feature Information for QAM Video Carriers 20
How to Configure the Video QAM Carriers 20
Configuring the Video QAM Profile 20
Configuring the Video QAM Carriers 21
Verify the configuration of the RF Channel 22
Configuration Examples 22
Video QAM Carriers 22
Feature Information for QAM Video Carriers 23

CHAPTER 5 **PSIP and EAS Support for Broadcast QAM 25**
Hardware Compatibility Matrix for the Cisco cBR Series Routers 25
Information About PSIP and EAS Support 27
Prerequisites for PSIP and EAS Support 27
How to Configure PSIP and EAS Sessions 27

Configuring PSIP and EAS Sessions 27
Verifying the PSIP and EAS Configurations 28
Verifying the PSIP Session Configuration 28
Verifying EAS Session Configuration 29
Configuration Example 30
Example: PSIP and EAS Configuration 30
Troubleshooting Tips 30
Feature Information for PSIP and EAS Support 31

CHAPTER 6 **NIT Reference Support for Broadcast QAM** 33
Hardware Compatibility Matrix for the Cisco cBR Series Routers 33
Information About NIT Reference Support 35
How to Configure NIT Reference 35
Configuring NIT Reference 35
Verifying the NIT Reference Configuration 36
Removing the NIT Reference 36
Configuration Example 36
Example: NIT Reference Configuration 36
Troubleshooting Tips 36
Feature Information for NIT Reference Support 37

CHAPTER 7 **Logical Edge Devices** 39
Information about Logical Edge Devices 39
How to Configure the Logical Edge Devices 39
Configuring Session-Based (Dynamic) Logical Edge Devices 39
Verifying the Session-Based (Dynamic) Logical Edge Devices Configuration 41
Configuring the D6 Discovery Protocol 44
Verifying the D6 Configuration 46
Configuration Examples 46
Example: GQI LED Configuration 46
Feature Information for Logical Edge Devices 47

CHAPTER 8 **Cisco Smart Licensing for Video** 49
Video Smart Licensing 49

Information About Video Smart Licensing 49
Benefits of Smart Licensing 49
Prerequisites for Video Smart Licensing 49
Restrictions for Video Smart Licensing 50
How to Verify Video Smart Licensing 50
Verifying Video Smart Licensing Using Show Commands 50
Configuration Examples 51
Use Cases or Deployment Scenarios 52
Feature Information for Video Smart Licensing 54

CHAPTER 9 **Physical to Virtual Binding** 55
Information About Physical to Virtual Binding 55
How to Configure VPME Encryption 55
Configuring Physical to Virtual Binding 55
Configuring QAM Replication 56
Configuration Examples 56
Example 1: Physical to Virtual Binding Configuration 56
Example 2: Physical to Virtual Binding Configuration 56
Example 3: QAM Replication Configuration 57
Feature Information for Physical to Virtual Binding 57

CHAPTER 10 **Table Based Configuration** 59
Information About Table Based Configuration 59
Configuring Table Based Session 59
Configuration Example 60
Virtual Edge Input Bundling 60
Verifying Virtual Edge Input Data 60
Verifying VEI Bundles 61
Configuration Example 61
10-6 UDP Port Mapping 62
Restrictions for 10-6 UDP Port Mapping 62
Configuring 10-6 UDP Port Mapping 62
Verifying 10-6 UDP Port Mapping Configuration 63
10-6 UDP Port Mapping Configuration Example 63

Feature Information for Table Based Configuration 64

CHAPTER 11 **Management IP Interface** 65

Information About Management IP Interface 65

How to Configure the Management IP Interface 65

Configuring the VirtualPortGroup Interface 66

Configuring the Cable Video Management Interface 67

Configuring the LED Management Interface 67

Configuration Examples 68

Management IP Interface 68

Feature Information for Management IP Interface 68

CHAPTER 12 **Video Encryption** 71

Information About Encryption 71

Prerequisites for Encryption 72

How to Configure Encryption for the Data Stream 72

Enforcing Data Stream Encryption Type 72

Configuring Virtual Carrier Group 72

Verifying Encryption Configuration 73

Configuration Examples for Encryption 73

Example: Enforcing Data Stream Encryption Type 73

Example: Configuring Virtual Carrier Group 73

Configuring Privacy Mode Encryption 73

Configuring VODS-ID 74

Configuring CEM IP and Port 74

Configuring Management IP 74

Verifying PME Connection Status 75

Verifying PME Version 75

Verifying PME Sessions on a Line Card 75

Troubleshooting Video Encryption Issues 76

New Events and Alarms for Video Encryption Debugging 76

Example Logs 79

Feature Information for Encryption 80

CHAPTER 13 **Global Video Configuration** 81

Configuring the Default ONID 81

Configuring the Default PSI interval 81

Configuring Video Session Timeouts 82

Configure Video Interface IP 82

Configure Virtual Routing and Forwarding 83

Configuration Examples 83

Example: Global Video Configuration 83

Feature Information for Global Video Configuration 84

CHAPTER 14 **Advanced Video MPEG Features** 85

Information about Advanced Video MPEG Features 85

Reserved Output PID Range 85

How to Configure Advanced Video MPEG Features 85

Configuring Reserved Output PID Range 85

Verifying Reserved Output PID Range Configuration 85

Configuration Examples for Advanced Video MPEG Features 86

Example: Configuring Reserved Output PID Range 86

Feature Information for Advanced Video MPEG Features 86

CHAPTER 15 **Important Notes** 87

Video Packet Routing Requirements 87

CHAPTER 16 **Cisco cBR-8 as Auxiliary Video Core** 89

Information About cBR-8 as Auxiliary Video Core 89

Limitations 90

How to Configure cBR-8 as Auxiliary Video Core 90

Configure DOCSIS Principal Core 91

Configure cBR-8 as Auxiliary Video Core 91

Configuration Examples for cBR-8 as Auxiliary Video Core 91

Feature Information for cBR-8 as Auxiliary Video Core 92

PART II Cisco cBR Converged Broadband Routers Video Features 93

CHAPTER 17 PowerKEY VOD 95

Information About PowerKEY VOD 95

Overview of PowerKEY VOD 95

How to Configure PowerKEY VOD 95

Configuring the Encryption Type on the Line Card 96

Configuring the Encrypted Virtual Carrier Groups 96

Configuring the Service Distribution Groups and Binding 97

Configuring the Logical Edge Device and GQI Protocol 97

Verifying the PowerKEY VOD Configuration 98

Troubleshooting Tips 100

Configuration Examples 101

Example: Configuring Encryption Type on the Line Card 102

Example: Configuring Encrypted Virtual Carrier Groups 102

Example: Configuring Service Distribution Groups and Binding 102

Feature Information for PowerKEY VOD 102

CHAPTER 18 DOCSIS Downstream Controllers 105

Configure Video Controllers 105

Configure Video Controller-Profile 106

Configure RF Channel Type 106

Bind Video Controller to RPD DS Port 106

Verify Video Controller-Profile 106

Examples of Video Configuration 109

CHAPTER 19 Simple Content Protection Video Session Support 111

Support for SCP Conditional Access System 111

Prerequisites 111

Configure Cisco cBR Routers for SCP 112

Create SDG and VCG 112

Example: Creating SDG and VCG 112

Create a Table-based LED for SCP 112

Example: Creating a Table-based LED for SCP 112
Configure Table-based and PSIP Sessions 113
Example: Configuring Table-based and PSIP Sessions 113
Feature Information for SCP Video Session Support 113

CHAPTER 20 **Table-Based Video and VPME Encryption 115**
Overview of VPME 115
Prerequisites for VPME 115
Restrictions for VPME 116
How to Configure Table-Based Video Session 116
Configuring Table-Based Video 116
Configuring Table-Based Session : VEI Input Port-Based 116
Configuring Table-Based Session :VEI Bundle-Based 117
Verifying Table-Based Video Configuration 118
Output State is OFF 119
Output Status is Idle or Pending 121
Input State is Active and not Active PSI 122
Abnormalities on the Output 123
Configuring CEM Connectivity for PME Encryption 124
Verifying CEM Connectivity 125
Connectivity with CEM is Lost 125
How to Configure VPME Encryption 126
Enforcing Data Stream Encryption Type 126
Configuring Virtual Carrier Group 126
Verifying VPME Encryption Configuration 126
No PMT at the Output 128
Configuration Examples For VPME Encryption 129
Use Cases or Deployment Scenarios 129
Feature Information for Table-Based Video and VPME Encryption 130

CHAPTER 21 **PMV Support for Table-Based Videos 131**
Information About the PMV Support for Table-Based Videos 131
Overview of PMV 131
Prerequisites for Configuring PMV 132

Restrictions for Configuring PMV 132
How to Configure PMV 133
Enabling PMV Allocation Scheme for LED 133
Verifying the PMV Configuration on LED 133
How to Configure Sessions with PMV Value 134
Verifying the PMV on RF Channel Sessions 135
Troubleshooting Tips 135
Disabling PMV Allocation Scheme for LED 135
Verifying the Disabled PMV Configuration 135
Configuration Examples 136
Feature Information for PMV Support 139

CHAPTER 22 **Video QAM Replication** 141
QAM Replication 141
Information About Replication 141
Overview of QAM Replication 141
Benefits of QAM Replication 142
Prerequisites for Replication 142
Restrictions for QAM Replication 143
Configuring Replication for Table-Based or Session-Based Video 143
Verifying Replication of Table Based Video Sessions 143
Configuration Examples 144
Feature Information for Replication 145

CHAPTER 23 **D6 Discovery Protocol** 147
Information About D6 Discovery Protocol 147
Overview of the D6 Discovery Protocol 147
Prerequisites for D6 Discovery Protocol 148
How to Configure the D6 Discovery Protocol 149
Configuring the Mandatory D6 Discovery Protocol Parameters 149
Verifying the D6 Discovery Protocol Configurations 150
Troubleshooting the D6 Mandatory Parameters Configuration 151
Configuring the D6 Discovery Protocol Optional Parameters 152
Verifying the Hold Time and Timeout Settings 153

Troubleshooting the D6 Optional Parameters Configuration 153
Example: D6 Discovery Protocol Configuration 153
Deployment Scenario for the D6 Discovery Protocol 154
Feature Information for D6 Discovery Protocol 155

CHAPTER 24 **Switched Digital Video 157**
Switched Digital Video Services 157
Session Cloning 157
Redundant Multicast Sources 158
Benefits of Switched Digital Video 159
Prerequisites for Switched Digital Video 159
Restrictions for Switched Digital Video 159
QAM Sharing 159
QAM Replication 159
MPTS Pass-through Session 160
Configuring Multicast Routing 160
Configuring Multicast Label 161
Configuring Multicast Table-based Sessions 161
Configuring Source Switching 162
Verifying Switched Digital Video Configuration 162
Configuration Examples for Switched Digital Video 163
Troubleshooting Switched Digital Video Configuration 167
Feature Information for Switched Digital Video 167

CHAPTER 25 **DVB Video on Demand 169**
Information About DVB VOD 169
Overview of DVB VOD 169
Session based Scrambling Setup 169
Fail-to-Clear 170
Tier based Scrambling Setup 170
Restrictions for DVB 171
How to Configure DVB 171
Configuring DVB 171
Verifying the DVB Configuration 173

Troubleshooting Tips 174
Configuration Examples 175
Example 1: Basic Session-based Scrambling Configuration 175
Example 2: Basic Tier-based Scrambling Configuration 176
Additional References 177
Feature Information for Low Latency VOD Support 177

CHAPTER 26 DualCrypt Encryption Mode Support 179
Hardware Compatibility Matrix for the Cisco cBR Series Routers 179
Information about DualCrypt Encryption Mode 181
Prerequisites for Dualcrypt Encryption Mode 181
Restrictions for DualCrypt Encryption Mode 182
How to Configure Dualcrypt Encryption Mode 182
Configuring DVB Session for DualCrypt Encryption 182
Verifying DVB Session for DualCrypt Encryption 183
Verifying the GQI Configuration 184
Verifying the GQI Sessions for Encryption 184
Verifying ONID and TSID of the QAMs Configured for Specific LED 185
Troubleshooting Tips 186
Configuration Examples 187
Example: Basic Session-based Scrambling Configuration 187
Example: Session-based Configuration with EIS Binding to LED using LED ID 188
Example: Configuration with EIS Binding to LED using LED Name 188
Example: EIS Binding to IP Address Other than Default DVB Management IP Address 189
Example: Session-based Configuration with VRF 189
Feature Information for DualCrypt Encryption Mode 190

CHAPTER 27 Low Latency VOD Support 191
Information About Low Latency VOD Support 191
Overview of Low Latency VOD Support 191
How to Configure Low Latency VOD Support 192
Configuring the Low Latency Virtual Carrier Group 192
Verifying the Low Latency Virtual Carrier Group Configuration 192
Verifying the Low Latency in Linecard 192

Configuring the Jitter Buffer Size for Table Based Session 193
Configuring the Jitter Buffer Size for GQI 193
Verifying Jitter Buffer Size for GQI 193
Verifying the Low Latency Sessions 194
Feature Information for Low Latency VOD Support 194

CHAPTER 28 **Video MIBs** 197
SCTE-HMS-MPEG-MIB 197
SCTE-HMS-QAM-MIB 198
CISCO-ENTITY-ALARM-MIB 199

CHAPTER 29 **Expanded GQI Protocol Support** 201
Hardware Compatibility Matrix for the Cisco cBR Series Routers 201
Information About GQI Protocol Support 203
GQI Announce Event Messages 203
Supported Announce Events 203
Blocking Announce Event Messages 204
GQI Announce Event Profile 205
Prerequisites for Configuring GQI Announce Event Profile 205
Restrictions for Configuring GQI Announce Event Profile 205
How to Configure GQI Announce Events 205
Verifying the Logical Edge Device 205
Verifying the GQI Connection 206
Configuration Example for Announce Event 206
Disabling Announce Event Profile 206
Filtering Announce Events 207
Verifying the Announce Event Profile Configuration 207
Configuration Example for Announce Event 208
Example: GQI Announce Event Profile Configuration 208
Feature Information for Expanded GQI Protocol Support 208

CHAPTER 30 **Advanced MPEG Features** 209
Advanced MPEG Features 209
Information About Advanced MPEG Features 209

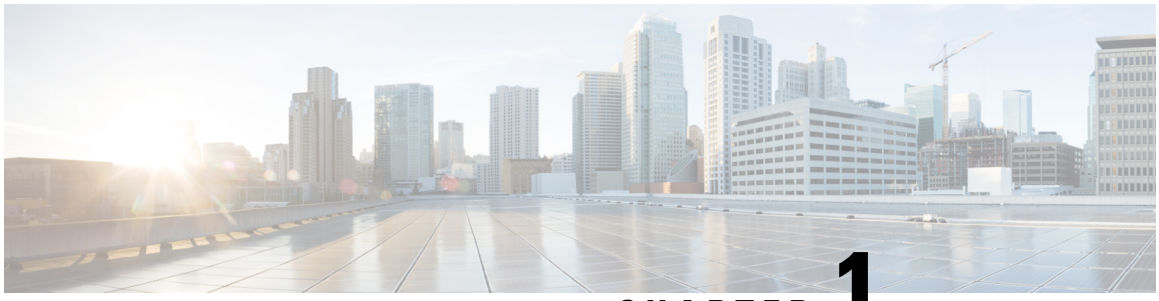
Overview of PID Filtering, Program Filtering, and PID Remapping 210
Rules for Configuring PID Filtering and PID Remapping 210
Benefits of Using PID Filtering and PID Remapping 210
Restrictions for PID Remapping 210
Remapping PAT or SI from External Data Stream 211
Blocking Unreferenced PIDs 211
Overview of Enhanced Input Source Switching 211
Benefits of Using Enhanced Input Source Switching 211
Overview of MPTS Remuxing 212
How to Configure Advanced MPEG Features 212
Configuring PID Filtering 212
Configuring Program Filtering 212
Configuring PID Remapping 213
Configuring Remapping Data PID to PAT PID 213
Configuring Enhanced Input Source Switching 214
Configuring MPTS Remuxing 214
Verifying PID Filtering, Program Filtering, and PID Remapping 214
Verifying MPTS Remuxing 215
Troubleshooting Tips for Possible Configuration Errors 216
Configuration Examples for Advanced MPEG Features 217
Feature Information for Advanced MPEG Features 220

CHAPTER 31 **Video Notifications** 221
Information About Video Notifications 221
Overview of Video Notifications 221
How to Configure Video Notifications 222
Configuring SNMP Notification Host 222
Configuring SNMP Notification Message Queue Length 222
Configuring Video Notification 223
Viewing Active Video Notifications 223
Disabling Video Notification 224
Configuration Examples for Video Notifications 224
Configuring CC-ERROR Reporting 225
Feature Information for Video Notifications 226

PART I

Basic Configuration and Provisioning Construct

- Video Services Provisioning Model, on page 1
- Video Virtual Carrier Group and Virtual Edge Input, on page 5
- Service Distribution Group, on page 11
- QAM Profile, on page 17
- PSIP and EAS Support for Broadcast QAM, on page 25
- NIT Reference Support for Broadcast QAM, on page 33
- Logical Edge Devices, on page 39
- Cisco Smart Licensing for Video , on page 49
- Physical to Virtual Binding , on page 55
- **Table Based Configuration**, on page 59
- Management IP Interface, on page 65
- Video Encryption, on page 71
- Global Video Configuration, on page 81
- Advanced Video MPEG Features, on page 85
- Important Notes, on page 87
- Cisco cBR-8 as Auxiliary Video Core, on page 89



CHAPTER 1

Video Services Provisioning Model

The Cisco cBR-8 router offers the next generation CCAP platform supporting converged CMTS and EQAM functionality. The redesigned video data model supports the creation of virtual edge devices within the platform. This data model simplifies the provisioning procedure and enables seamless migration to virtualized video service management in the future.

The video provisioning constructs of the new data model provide hardware abstraction and divides services into virtual edge devices for easier provisioning at scale. It also provides isolation between the service applications at the software layer. A bind-operation connects these constructs to the physical resources.

- Information about Video Services Provisioning , on page 1
- Feature Information for Video Services Provisioning, on page 2

Information about Video Services Provisioning

Video Provisioning Constructs

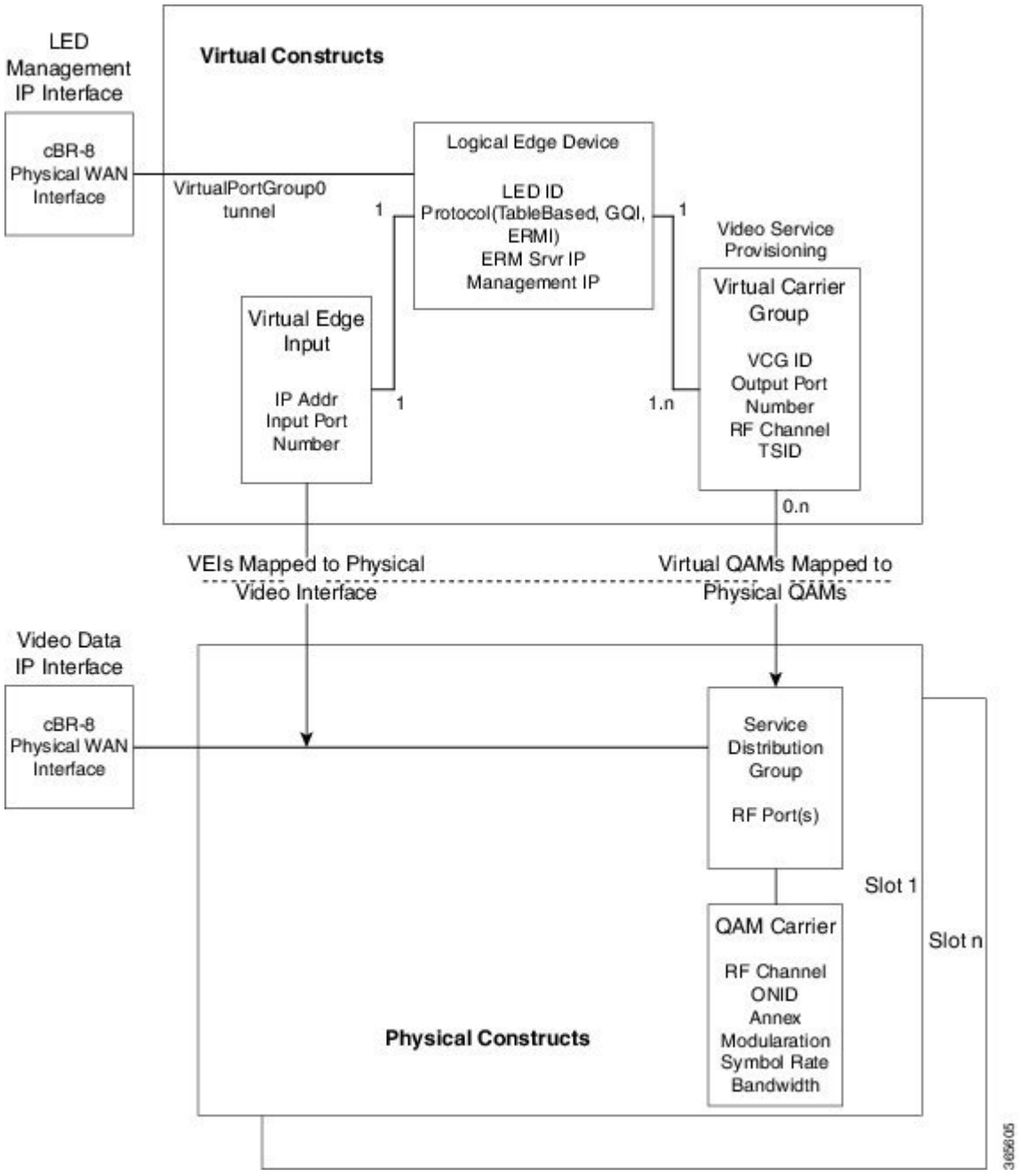
The Video Services Provisioning Model has the following elements:

- **Logical Edge Device (LED)**—a virtual edge device in the Cisco cBR-8 chassis that can be provisioned for static or dynamic sessions.
- **Virtual Carrier Group (VCG)**—a collection of Virtual QAM Carriers (RF channels) provisioned on an LED.
- **Virtual Edge Input (VEI)**—assigned either globally to all VCGs in the LED or optionally assigned uniquely to an individual VCG.
- **Service Distribution Group (SDG)**—a collection of one or more RF ports that define the physical slot/bay/port to be used in a video service.

Connection of Virtual and Physical Constructs

The VCGs are bound to an SDG using a bind command (bind-vcg). This connects the virtual carriers to the physical ports listed in the SDG. After binding, a path from the VEI is mapped to the RF ports.

The image below shows the elements in the Video Provisioning Construct.



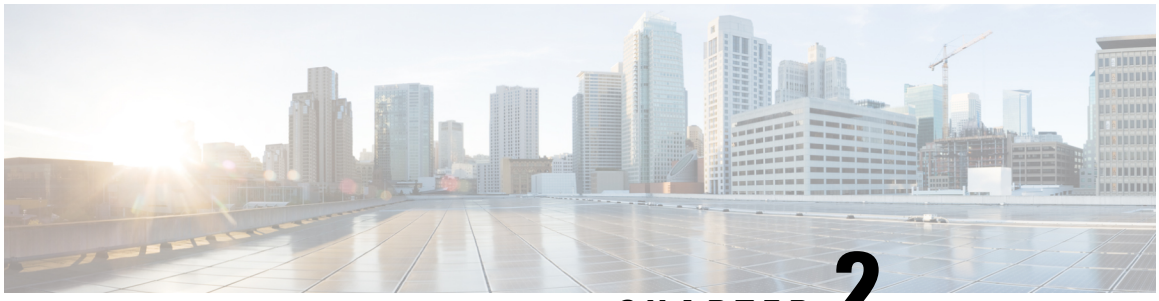
Feature Information for Video Services Provisioning

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 https://cfnng.cisco.com/ 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 1: Feature Information for Video Services Provisioning

Feature Name	Releases	Feature Information
Video Services Provisioning	Cisco IOS XE Everest 16.6.1	This feature was integrated on the Cisco cBR Series Converged Broadband Routers.



CHAPTER 2

Video Virtual Carrier Group and Virtual Edge Input

A Virtual Carrier Group (VCG) is a collection of virtual QAM carriers (RF channels) provisioned on a Logical Edge Device (LED). A Virtual Edge Input (VEI) is a customer assigned IP address that is used, from the Head End, as a destination IP address for unicast video IP packets.

- Information about Virtual Carrier Group and Virtual Edge Input, on page 5
- How to Configure Virtual Carrier Group and Virtual Edge Input, on page 6
- Configuration Examples for Virtual Carrier Group and Virtual Edge Input, on page 9
- Feature Information for Virtual Carrier Group and Virtual Edge Input, on page 10

Information about Virtual Carrier Group and Virtual Edge Input

Virtual Carrier Group

A Virtual Carrier Group (VCG) is a collection of virtual QAM carriers (RF channels) provisioned on a Logical Edge Device (LED).

Each VCG must have a unique name and ID, since it also assigns attributes such as TSID and output port number to the virtual QAM carriers. The output port number only needs to be unique per LED. However, TSID/ONID pair must be unique for the chassis.

Duplicate TSIDs can be assigned to multiple QAM carriers by overriding the default TSID. Overriding the default TSID does not affect the unique TSID/ONID pair on the cBR router. The duplicate TSID overrides the unique TSID on the PAT header.

For more information, see Overriding the Default TSID section.

The service type must be designated in each VCG and the encrypt command must be entered if the carriers are to be encrypted. Enabling the VCG to use encryption and service type designates that each QAM carrier listed in the VCG will consume a QAM encryption license and video service type license. The actual number of licenses consumed will be done at VCG binding operation and is also dependent on the QAM replication requirements.

For more information on how the licenses are consumed, see Cisco Smart Licensing for Video.

Virtual Edge Input

A Virtual Edge Input (VEI) is a customer assigned IP address that is used, from the Head End, as a destination IP address for unicast video IP packets. Each VEI will need to be configured with a routable IP address from within the customer's network.

A VEI is assigned within a Logical Edge Device. Each Virtual Carrier Group (VCG) is associated with one or more IP addresses that represent VEIs.

For GQI protocol, VEI must be configured under the LED, since GQI expects VEI to be able to reach any Virtual QAM carrier listed in the same LED. Again, for GQI protocol, there is a limit of five VEIs per LED.

For the table based protocol, VEI may be configured under the LED or under a VCG. If the VEI is configured under a VCG, it can only reach the virtual QAM carriers associated with that particular VCG.

During the VCG binding operation, each VEI IP address will be bound to a single Video IP interface.

You can isolate the video traffic from other network traffic using MPLS (Multiprotocol Label Switching) and VRF (Virtual Routing and Forwarding), by configuring the VRF name parameter in video-edge-input command.

Note Do not use the same VEI IP address in multiple VRFs, as Head End video session management servers are not MPLS or VRF aware.

How to Configure Virtual Carrier Group and Virtual Edge Input

Configuring Virtual Carrier Group

Before you begin

Since each VEI needs to be configured with a routable IP address from within the customer’s network, choose the IP addresses to use prior to configuring the VEIs.

Error messages for problems with the VCG configuration will become evident during the bind operation. Errors include overlapping rf-channels.

In virtual-edge-input-ip command line configuration, vrf is an optional parameter and can be used for MPLS routing or to make VEI private from other parts of the network.

To configure virtual carrier group, follow the steps below:

```
enable
configure terminal
cable video
virtual-carrier-group name [id number]
virtual-edge-input-ip ip-address [vrf vrf-name] input-port-number port-number
encrypt
service-type narrowcast
rf-channel start_channel-end_channel tsid start_tsid-end_tsid output-port-number
start_number-end_number
```

Overriding the Default TSID

To assign duplicate TSIDs to multiple QAM carriers, you can override the default TSID by using the **override-tsid** command as shown in the example below.

```
enable
configure terminal
cable video
virtual-carrier-group name [id number]
override-tsid TSID
```

Verifying Virtual Carrier Group Configuration

To verify the virtual carrier group configuration, use the **show cable video virtual-carrier-group** command as shown in the example below.

```
Router# show cable video virtual-carrier-group all
Number of Virtual Carrier Groups: 1

ID Name Service        Logical      ServiceType Encrypted Low      Override Total Total
        -Distribution  -Edge                              Latency  TSID     VEI   RF-
        -Group Name    -Device Name                                          Channel

-------------------------------------------------------------------------------------------
1  vcg1 sdg1           led1         narrowcast   N          N        -      0      1
```

Configuring Virtual Edge Input under Logical Edge Device

Before you begin

Since each VEI will need to be configured with a routable IP address from within the customer's network, choose the IP addresses to use prior to configuring the VEIs.

To configure virtual edge input, follow the steps below:

```
enable
configure terminal
cable video
virtual-carrier-group name [id] number
virtual-edge-input-ip ip-address [vrf vrf-name] input-port-number port-number
vcg vcg-name
active
```

To configure virtual edge input under logical edge device, follow the steps below:

```
enable
configure terminal
cable video
logical-edge-device name [id] number
protocol table-based
virtual-edge-input-ip ip-address [vrf vrf-name] input-port-number port-number
vcg vcg-name
active
```

Verifying Virtual Edge Input Configuration

To verify the virtual edge input configuration, use the **show cable video logical-edge-device** command as shown in the example below.

```
Router# show cable video logical-edge-device id 1
Logical Edge Device: led
Id: 1
Protocol: GQI
Service State: Active
Discovery State: Disable
Management IP: 1.33.2.10
MAC Address: c414.3c17.6000
Number of Servers: 2
  Server 1: 1.200.1.193
  Server 2: 1.200.1.183
Reset Interval: 5
Keepalive Interval: 5
Retry Count:3
Number of Virtual Carrier Groups: 2
Number of Share Virtual Edge Input: 1
Number of Physical Qams: 94
Number of Sessions: 240
No Reserve PID Range

Virtual Edge Input:
Input Port    VEI          Slot/Bay Bundle Gatewayy
ID            IP                     ID     IP
-------------------------------------------------
1             174.102.1.1  7/0      -      - --

Virtual Carrier Group:
ID Name  Total Total       Service-Distribution-Group Service-Distribution-Groupup
         VEI   RF-channel  Name                       ID
-------------------------------------------------------------------------------

1  vcg   0     28          sdg                        1
2  vcg-2 0     19          sdg                        1

Integrated Physical Admin Operational TSID ONID Output VCG SDG Encryption
Cable      QAM ID   State State                 Port   ID  ID  Capable
-------------------------------------------------------------------------

7/0/0:1    1        ON    UP          29   1000 30     2   1   powerkey
7/0/0:2    2        ON    UP          30   1000 30     2   1   powerkey
7/0/0:3    3        ON    UP          31   1000 30     2   1   powerkey
7/0/0:4    4        ON    UP          32   1000 30     2   1   powerkey
7/0/0:5    5        ON    UP          33   1000 30     2   1   powerkey
7/0/0:6    6        ON    UP          34   1000 30     2   1   powerkey
7/0/0:7    7        ON    UP          35   1000 30     2   1   powerkey
7/0/0:8    8        ON    UP          36   1000 30     2   1   powerkey
7/0/0:9    9        ON    UP          37   1000 30     2   1   powerkey
```

To verify the VEI configuration with MPLS-VPN VRF, use the **show ip arp vrf** command as shown in the example below:

```
Router# show ip arp vrf Video-VOD-Vrf
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  174.102.1.1            -   12ab.0007.ce01  ARPA   Video7/0/0
```

Configuration Examples for Virtual Carrier Group and Virtual Edge Input

This section provides configuration examples for the Virtual Carrier Group and Virtual Edge Input:

Example: Configuring Virtual Carrier Group

The following example shows how to configure virtual carrier group:

```
enable
configure terminal
cable video
virtual-carrier-group vcg-0 id 1
virtual-edge-input-ip 174.101.1.1 input-port-number 1
virtual-edge-input-ip 174.102.1.1 vrf Video-VOD-Vrf input-port-number 2
encrypt
service-type narrowcast
rf-channel 0-10 tsid 1-11 output-port-number 1-11
```

Example: Configuring Virtual Edge Input

The following example shows how to configure virtual edge input:

```
enable
configure terminal
cable video
logical-edge-device led_bc1 id 1
protocol table-based
virtual-edge-input-ip 174.102.1.1 input-port-number 1
vcg vcg_bc1
active
```

You can also configure VEI to be associated with a MPLS-VPN VRF:

```
enable
configure terminal
cable video
virtual-carrier-group vcg1 id 1
virtual-edge-input-ip 174.102.1.1 vrf Video-VOD-Vrf input-port-number 1
vcg vcg-name
active
```

Under logical edge device, follow the steps below:

```
enable
configure terminal
cable video
logical-edge-device led_bc1 id 1
protocol table-based
virtual-edge-input-ip 174.102.1.1 vrf Video-VOD-Vrf input-port-number 1
```

```
vcg vcg_bc1
active
```

Example: Overriding the Default TSID

The following example shows how to override the default TSID:

```
enable
configure terminal
cable video
virtual-carrier-group vcg1 id 1
override-tsid 100
%%Configuring this will regenerate the PAT with overridden TSID value for all QAM channels
 under this VCG.
Do you want to continue? [Yes/No][confirm]y
```

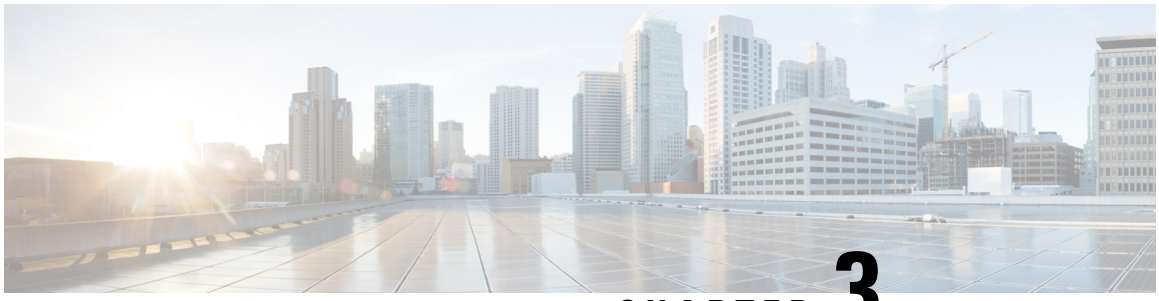
Feature Information for Virtual Carrier Group and Virtual Edge Input

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 https://cfnng.cisco.com/ 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 2: Feature Information for Virtual Carrier Group and Virtual Edge Input

Feature Name	Releases	Feature Information
Virtual Carrier Group and Virtual Edge Input	Cisco IOS XE Everest 16.6.1	This feature was integrated on the Cisco cBR Series Converged Broadband Routers.
Using VRF for Video Session Traffic	Cisco IOS XE Everest 16.6.1	This feature was integrated on the Cisco cBR Series Converged Broadband Routers.



CHAPTER 3

Service Distribution Group

The Service Distribution Group (SDG) is a collection of one or more RF ports and defines the physical slot/bay/port to be used in a video service.

Contents

- Information About Service Distribution Group, on page 11
- How to Configure the Service Distribution Group, on page 12
- Troubleshooting Tips, on page 15
- Configuration Examples, on page 15
- Feature Information for Service Distribution Group, on page 16

Information About Service Distribution Group

The following are the required components for configuring an SDG:

- Multiple Ports—Multiple ports in an SDG replicate all QAMs from the Virtual Carrier Group (VCG) to every port.
- Unicast—Unicast (VoD) services cannot be replicated across line cards.
- TSID—The TSIDs should always be unique (North American MSO). Non-unique TSIDs can be used if the ONID is changed from the default value of zero (0).

The convention slot/bay/port represents the following:

- Slot—Slot is the line card slot number. Slot can be configured 0–3 or 6–9. Slots 4 and 5 are the supervisor slots.
- Bay—Bay is the Cisco cBR-8 chassis number. This parameter is always configured as 0.
- Port—Port is the RF port number. This parameter can be configured 1–8.

Note

- For a Remote PHY line card, the SDG does not describe a collection of RF ports. SDG specifies the line card, bay, and downstream cable controller where the video will be destined. Use **rpd downstream-cable** *slot/bay/controller* command instead of **rf-port integrated-cable** *slot/bay/port* command. Only one downstream cable controller can be specified for an SDG, so QAM replication is not supported. (However, the controller can be multicast to multiple remote PHY devices which is similar to QAM replication but occurs external to the cBR-8.)
- Cisco Remote PHY Device 1x2 can join up to 30 multicast streams simultaneously for video.
- Cisco HA Shelf can join up to 30 multicast streams simultaneously per RPD for video.

How to Configure the Service Distribution Group

This section describes how to configure SDGs for the video session on Cisco cBR-8.

Defining the Physical Slot/Bay/Port

To define the Service Distribution Group (SDG), you must define the physical *slot*/*bay*/*port* to be used in a video service.

Before You Begin

Make sure that the controller type is **video** for the *slot*/*bay*/*port* that you use for the SDG. Errors due to the incorrect controller type used in the SDG appear during the bind operation.

To define the physical *slot*/*bay*/*port*, complete the following procedure:

```
configure terminal
cable video
service-distribution-group sdg name
rf-port integrated-cable slot/bay/port
```

Configuring QAM Replication

To configure QAM replication for service group size alignment between the DOCSIS and video services to one or more ports, you can add more ports into the service distribution group configuration.

Before You Begin

Make sure that the controller type is video for the slot/bay/port that you would use for the SDG. For more information, see the **Video QAM Carriers** section. Errors due to the incorrect controller type used in the SDG appear during the bind operation.

To configure QAM replication, complete the following procedure:

```
configure terminal
cable video
service-distribution-group service distribution group name
rf-port  integrated-cable  slot/bay/port
rf-port  integrated-cable  slot/bay/port
```

Overriding the Default ONID

You can override the default ONID, by defining a new ONID value in the SDG configuration. If you perform this configuration, all channels associated with the configured SDG will have the new ONID value. By default, the system ONID is 0, which is commonly used in North America.

To override the default ONID, complete the following procedure:

```
configure terminal
cable video
service-distribution-group service distribution group name
onid onid number
```

Overriding the Default PSI Value

To override the default PSI value, complete the following procedure:

```
configure terminal
cable video
service-distribution-group  service distribution group name
psi-interval psi-interval  msec
```

Configuring the Serving Area

Configure the serving area to enable the set tops to discover VOD content.

```
configure terminal
cable video
service-distribution-group service distribution group name id id
serving-area value
```

To configure the service descriptor default, complete the following procedure:

```
configure terminal
cable video
service-descriptor-default
service-id id
service-name string
service-type id
provider-name string
```

If the serving area is specified and there are no defaults specified, the service name should be set as **VOD** and provider name should be set as **VOD-SERVER**, service id set as **1**, service type set as **1**.

Verifying the Serving Area Configuration

If the serving area is configured, session detail output will list the SDT information.

```
Router# show cable video session logical-edge-device id 2 session-id 270532608
Session Name        : mpts1.2.199
Session Id          : 270532608
Creation Time       : Fri Oct 12 22:07:03 2018

Output Port         : 41
```

```
TSID                : 41
Override TSID       : not specified
ONID                : 2
Number of Sources   : 1
  Source IP         : 176.51.1.2
  Group IP          : 238.11.1.106
  UDP Port          : 0
Config Bitrate      : not specified
Jitter              : 100 ms
Processing Type     : Passthru
Stream Rate         : CBR
Program Number      : -
Idle Timeout        : 2000 msec
Init Timeout        : 2000 msec
Off Timeout         : 60 sec
Encryption Type     : Pre-encrypted
Encryption Status   : Encrypted

Input Session Stats:
====================
  State: ACTIVE-PSI, Uptime: 0 days 02:50:59
  IP Packets: In 2569416, RTP 0, Drop 0
  TP Packets: In 16910560, PCR 262629, PSI 292104, Null 1075352
              Unreference 102351, Discontinuity 0
  Errors: Sync loss 0, CC error 0, PCR Jump 4,
          Underflow 2, Overflow 0, Block 0
  Bitrate: Measured 2463450 bps, PCR 2637379 bps

Output Session Stats:
=====================
  State: ON, Uptime: 0 days 02:50:59
  TP Packets: In 17056642, PCR 262628, PSI 292102,
              Drop 0, Forward 16764540, Insert 0
  Errors: Info Overrun 0, Info Error 0, Block 0, Overdue 0,
          Invalid Rate 0, Underflow 0, Overflow 0
  Bitrate: Measured 2439152 bps

SDT Info:
=========
  Version 2, TSID 10, len 41, carousel 450

PAT Info:
=========
  Version 18, TSID 1, len 16, section 0/0
  Program 1: PMT 16

Input PMT Info:
===============
  Program 1, Version 1, PCR 17, Info len 0
  PID 17: Type 2, Info len 9, (CA SYS-ID 3584, PID 1, Private data: 010101)
  PID 18: Type 4, Info len 15, (lang eng), (CA SYS-ID 3584, PID 1, Private data: 010102)
  PID 19: Type 4, Info len 15, (lang spa), (CA SYS-ID 3584, PID 1, Private data: 010103)
  PID 20: Type 4, Info len 15, (lang fre), (CA SYS-ID 3584, PID 1, Private data: 010104)

Output PMT Info:
================
  Program 1, Version 1, PCR 17, Info len 0
  PID 17: Type 2, Info len 9, (CA SYS-ID 3584, PID 1, Private data: 010101)
  PID 18: Type 4, Info len 15, (lang eng), (CA SYS-ID 3584, PID 1, Private data: 010102)
  PID 19: Type 4, Info len 15, (lang spa), (CA SYS-ID 3584, PID 1, Private data: 010103)
  PID 20: Type 4, Info len 15, (lang fre), (CA SYS-ID 3584, PID 1, Private data: 010104)
```

To verify the service descriptor default value, use the command as shown in the following example:

```
Router# show run | s service-descriptor-default
  Service-descriptor-default
    Service-id 200
    Service-name HD-Service
    Service-type 1
    Provider-name NEWS-channel
```

Verifying Service Distribution Group Configuration

To verify the SDG configuration, use the **show cable video service-distribution-group** command as shown in the example below:

```
Router# show cable video service-distribution-group all
Number of Service Distribution Groups: 1
ID Name   Virtual-Carrier-Group  Logical-Edge-Device RF-Port  ONID   PSI       Serving
          Name                   Name                         Interval  Area
-------------------------------------------------------------------------------------
1  sdg1   vcg1                   table-based         9/0/0    0      100       10


Router# show cable video service-distribution-group id 1
Name:  sdg1
       Id:  1
      ONID:  0
      PSI Interval:  100
      Serving Area:  10

      RF Ports:
          Integrated-Cable 9/0/0

      Number of Virtual Carrier Groups:  1
      VCG ID         VCG Name               LED ID      LED Name
      ---------------------------------------------------------------------
      1              vcg 1                  1           table-based
```

Troubleshooting Tips

To undo any configuration, use the **no** form of the command. This command is useful if you have configured something by mistake. The errors are not apparent until you perform the bind operation.

Configuration Examples

This section provides example configurations for the service distribution group.

Configuring a Service Distribution Group

```
configure terminal
cable video
service-distribution-group vod id 1
 onid 100
 rf-port integrated-cable 7/0/0
 rf-port integrated-cable 7/0/1
```

```
rf-port integrated-cable 7/0/2
rf-port integrated-cable 7/0/3
```

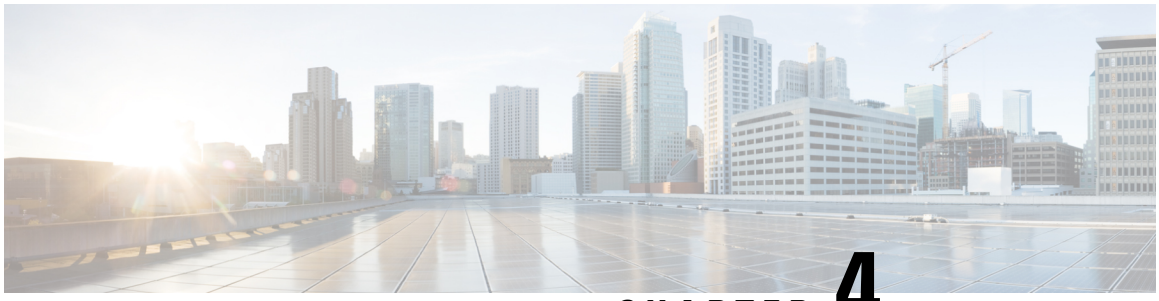
Feature Information for Service Distribution Group

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 https://cfnng.cisco.com/ 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 3: Feature Information for Service Distribution Group

Feature Name	Releases	Feature Information
Service Distribution Group	Cisco IOS XE Everest 16.6.1	This feature was integrated on the Cisco cBR Series Converged Broadband Routers.
SDT	Cisco IOS XE Gibraltar 16.10.1c	Thisfeature was introduced on the Cisco cBR Series Converged Broadband Routers.



CHAPTER 4

QAM Profile

A QAM profile describes the common downstream channel modulator settings, referred to as physical layer parameters. This includes QAM constellation, symbol rate, interleaver-depth, spectrum-inversion, and annex.

For more information about the downstream interface configuration, see Downstream Interface Configuration.

But be aware that, if you configure annex A 6MHz or 7MHz in a QAM profile, then this QAM profile cannot be applied to a DOCSIS channel.

- QAM Profile, on page 17
- How to Configure the Video QAM Carriers, on page 17
- Configuration Examples, on page 19
- Feature Information for QAM Video Carriers, on page 20
- How to Configure the Video QAM Carriers, on page 20
- Configuration Examples, on page 22
- Feature Information for QAM Video Carriers, on page 23

QAM Profile

A QAM profile describes the common downstream channel modulator settings, referred to as physical layer parameters. This includes QAM constellation, symbol rate, interleaver-depth, spectrum-inversion, and annex.

For more information about the downstream interface configuration, see Downstream Interface Configuration.

But be aware that, if you configure annex A 6MHz or 7MHz in a QAM profile, then this QAM profile cannot be applied to a DOCSIS channel.

How to Configure the Video QAM Carriers

Configuring the Video QAM Profile

To configure the video QAM profile, complete the following procedure:

```
configure terminal
cable downstream qam-profile id
annex {A freq_spacing|B|C}
modulation value
```

```
interleaver-depth value
symbol-rate value
spectrum-inversion {on|off} [interop]
description line
```

The frequency spacing of 6MHz, 7MHz and 8 MHz can be selected or annex A. In this case, the QAM profile can only be applied to a video channel.

Spectrum Inversion

Spectrum inversion happens because of mixing processes in RF or IF electronics. Spectrum inversion allows for the adaptation of older equipment with the new plant. The mixing of I and Q are used to create a quadrant profile. For some set-tops, the inversion of the quadrant profile is needed where the axis are flipped such that I represents the X and Q represents the Y-axis. Most modern equipment can detect and resolve the inversion split.

You can change this spectrum inversion configuration on a user-defined qam-profile. It cannot be changed on a system generated qam-profile from 0 to 5.

Currently, spectrum inversion configuration in QAM profile has different results between Cisco RPD and the RPD from other vendors. Starting from Cisco IOS XE Bengaluru 17.6.1w release, a new option **interop** is added to the **spectrum-inversion** configuration command. If you configure the interop keyword, cBR-8 sends a vendor specific TLV to reverse the spectrum inversion inside the RPD. You can configure a single profile for both Cisco RPD and other vendor's RPD using this configuration. This enables legacy set-up boxes to detect the spectrum inversion automatically.

To configure spectrum inversion on single QAM profile:

```
cable downstream qam-profile id
spectrum-inversion {on|off} interop
```

Configuration Example

```
cable downstream qam-profile 10
spectrum-inversion off interop
```

When using the inversion flag in combination with different **annex** types, the following table shows the spectrum inversion output on a Cisco RPD:

Table 4: Spectrum Inversion Output on a Cisco RPD

spectrum-inversion command option	annex A	annex B	annex B
on	normal	inverted	normal
off	inverted	normal	inverted
on interop	inverted	inverted	inverted
off interop	normal	normal	normal

Configuring the Video QAM Carriers

To configure the Video QAM carriers, complete the following procedure:

```
configure terminal
controller integrated-cable slot/bay/port
rf-channel start-channel - end-channel
type video
start-frequency frequency
rf-output normal
power-adjust number
qam-profile qam-profile number
```

Note For video provisioning, the carriers must be of type “video” in the controller integrated-cable configuration.

Verify the configuration of the RF Channel

To verify the RF channel configuration, use the Show controller integrated-cable rf-chan command as shown in the example below:

```
Router#show controllers integrated-Cable 9/0/7 rf-channel 0-10
Load for five secs: 6%/0%; one minute: 5%; five minutes: 5%
Chan State Admin Frequency  Type   Annex Mod  srate Interleaver  dcid  power  output
0     UP   UP    100000000  VIDEO   A    256   5361  I12-J17      -    34.0   NORMAL
1     UP   UP    106000000  VIDEO   A    256   5361  I12-J17      -    34.0   NORMAL
2     UP   UP    112000000  VIDEO   A    256   5361  I12-J17      -    34.0   NORMAL
3     UP   UP    118000000  VIDEO   A    256   5361  I12-J17      -    34.0   NORMAL
4     UP   UP    124000000  VIDEO   A    256   5361  I12-J17      -    34.0   NORMAL
5     UP   UP    130000000  VIDEO   A    256   5361  I12-J17      -    34.0   NORMAL
6     UP   UP    136000000  VIDEO   A    256   5361  I12-J17      -    34.0   NORMAL
7     UP   UP    142000000  VIDEO   A    256   5361  I12-J17      -    34.0   NORMAL
8     UP   UP    148000000  VIDEO   A    256   5361  I12-J17      -    34.0   NORMAL
9     UP   UP    154000000  VIDEO   A    256   5361  I12-J17      -    34.0   NORMAL
10    UP   UP    160000000  VIDEO   A    256   5361  I12-J17      -    34.0   NORMAL
```

Configuration Examples

This section provides configuration examples for the QAM video carrier.

Video QAM Carriers

The following is a sample for the Video QAM carrier configuration:

```
Router#enable
Router(config)#cable downstream qam-profile 4
Router(config-qam-prof)#annex A 6MHz
Router(config-qam-prof)#modulation 256
Router(config-qam-prof)#interleaver-depth I32-J4
Router(config-qam-prof)#symbol-rate 5361
Router(config-qam-prof)#spectrum-inversion off
Router(config-qam-prof)#description default-annex-a-256-qam
Router(config-qam-prof)#exit
Router(config)#controller Integrated-Cable 3/0/0
Router(config-controller)#max-carrier 128
Router(config-controller)#base-channel-power 34
Router(config-controller)#freq-profile 0
Router(config-controller)#rf-chan 0 95
```

```
Router(config-rf-chan)#type video
Router(config-rf-chan)#frequency 93000000
Router(config-rf-chan)#rf-output NORMAL
Router(config-rf-chan)#power-adjust 0
Router(config-rf-chan)#docsis-channel-id 1
Router(config-rf-chan)#qam-profile 1
```

Feature Information for QAM Video Carriers

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 https://cfnng.cisco.com/ 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 5: Feature Information for QAM Video Carriers

Feature Name	Releases	Feature Information
QAM Video Carriers	Cisco IOS XE Everest 16.6.1	This feature was integrated on the Cisco cBR Series Converged Broadband Routers.
Annex A Variable Channel Witdh	Cisco IOS XE Everest 16.6.1	This feature was integrated on the Cisco cBR Series Converged Broadband Routers.

How to Configure the Video QAM Carriers

Configuring the Video QAM Profile

To configure the video QAM profile, complete the following procedure:

```
configure terminal
cable downstream qam-profile id
annex {A freq_spacing|B|C}
modulation value
interleaver-depth value
symbol-rate value
spectrum-inversion {on|off} [interop]
description line
```

The frequency spacing of 6MHz, 7MHz and 8 MHz can be selected or annex A. In this case, the QAM profile can only be applied to a video channel.

Spectrum Inversion

Spectrum inversion happens because of mixing processes in RF or IF electronics. Spectrum inversion allows for the adaptation of older equipment with the new plant. The mixing of I and Q are used to create a quadrant profile. For some set-tops, the inversion of the quadrant profile is needed where the axis are flipped such that I represents the X and Q represents the Y-axis. Most modern equipment can detect and resolve the inversion split.

You can change this spectrum inversion configuration on a user-defined qam-profile. It cannot be changed on a system generated qam-profile from 0 to 5.

Currently, spectrum inversion configuration in QAM profile has different results between Cisco RPD and the RPD from other vendors. Starting from Cisco IOS XE Bengaluru 17.6.1w release, a new option **interop** is added to the **spectrum-inversion** configuration command. If you configure the interop keyword, cBR-8 sends a vendor specific TLV to reverse the spectrum inversion inside the RPD. You can configure a single profile for both Cisco RPD and other vendor's RPD using this configuration. This enables legacy set-up boxes to detect the spectrum inversion automatically.

To configure spectrum inversion on single QAM profile:

```
cable downstream qam-profile id
spectrum-inversion {on|off} interop
```

Configuration Example

```
cable downstream qam-profile 10
spectrum-inversion off interop
```

When using the inversion flag in combination with different **annex** types, the following table shows the spectrum inversion output on a Cisco RPD:

Table 6: Spectrum Inversion Output on a Cisco RPD

spectrum-inversion command option	annex A	annex B	annex B
on	normal	inverted	normal
off	inverted	normal	inverted
on interop	inverted	inverted	inverted
off interop	normal	normal	normal

Configuring the Video QAM Carriers

To configure the Video QAM carriers, complete the following procedure:

```
configure terminal
controller integrated-cable slot/bay/port
rf-channel start-channel - end-channel
type video
start-frequency frequency
rf-output normal
power-adjust number
qam-profile qam-profile number
```

Note For video provisioning, the carriers must be of type “video” in the controller integrated-cable configuration.

Verify the configuration of the RF Channel

To verify the RF channel configuration, use the Show controller integrated-cable rf-chan command as shown in the example below:

```
Router#show controllers integrated-Cable 9/0/7 rf-channel 0-10
Load for five secs: 6%/0%; one minute: 5%; five minutes: 5%
Chan State Admin Frequency  Type   Annex Mod  srate Interleaver  dcid  power  output
0     UP   UP    100000000  VIDEO   A    256   5361  I12-J17      -    34.0   NORMAL
1     UP   UP    106000000  VIDEO   A    256   5361  I12-J17      -    34.0   NORMAL
2     UP   UP    112000000  VIDEO   A    256   5361  I12-J17      -    34.0   NORMAL
3     UP   UP    118000000  VIDEO   A    256   5361  I12-J17      -    34.0   NORMAL
4     UP   UP    124000000  VIDEO   A    256   5361  I12-J17      -    34.0   NORMAL
5     UP   UP    130000000  VIDEO   A    256   5361  I12-J17      -    34.0   NORMAL
6     UP   UP    136000000  VIDEO   A    256   5361  I12-J17      -    34.0   NORMAL
7     UP   UP    142000000  VIDEO   A    256   5361  I12-J17      -    34.0   NORMAL
8     UP   UP    148000000  VIDEO   A    256   5361  I12-J17      -    34.0   NORMAL
9     UP   UP    154000000  VIDEO   A    256   5361  I12-J17      -    34.0   NORMAL
10    UP   UP    160000000  VIDEO   A    256   5361  I12-J17      -    34.0   NORMAL
```

Configuration Examples

This section provides configuration examples for the QAM video carrier.

Video QAM Carriers

The following is a sample for the Video QAM carrier configuration:

```
Router#enable
Router(config)#cable downstream qam-profile 4
Router(config-qam-prof)#annex A 6MHz
Router(config-qam-prof)#modulation 256
Router(config-qam-prof)#interleaver-depth I32-J4
Router(config-qam-prof)#symbol-rate 5361
Router(config-qam-prof)#spectrum-inversion off
Router(config-qam-prof)#description default-annex-a-256-qam
Router(config-qam-prof)#exit
Router(config)#controller Integrated-Cable 3/0/0
Router(config-controller)#max-carrier 128
Router(config-controller)#base-channel-power 34
Router(config-controller)#freq-profile 0
Router(config-controller)#rf-chan 0 95
Router(config-rf-chan)#type video
Router(config-rf-chan)#frequency 93000000
Router(config-rf-chan)#rf-output NORMAL
Router(config-rf-chan)#power-adjust 0
Router(config-rf-chan)#docsis-channel-id 1
Router(config-rf-chan)#qam-profile 1
```

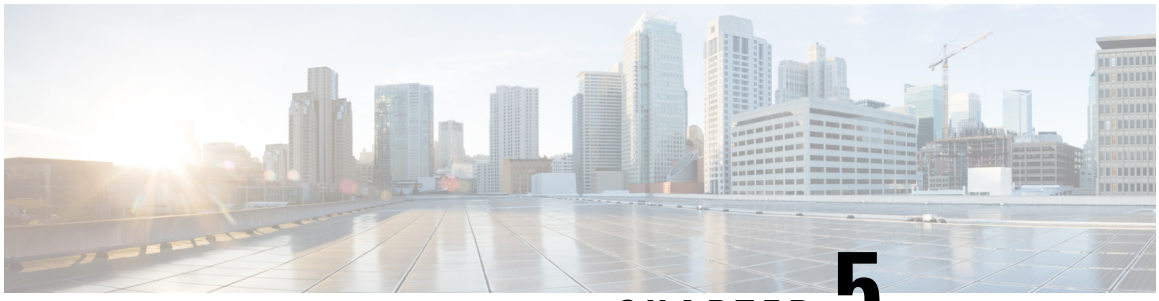
Feature Information for QAM Video Carriers

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 https://cfnng.cisco.com/ 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 7: Feature Information for QAM Video Carriers

Feature Name	Releases	Feature Information
QAM Video Carriers	Cisco IOS XE Everest 16.6.1	This feature was integrated on the Cisco cBR Series Converged Broadband Routers.
Annex A Variable Channel Witdh	Cisco IOS XE Everest 16.6.1	This feature was integrated on the Cisco cBR Series Converged Broadband Routers.



CHAPTER 5

PSIP and EAS Support for Broadcast QAM

This document provides information on the support for PSIP and EAS and how to configure Cisco cBR series routers to avail the support.

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.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

- Hardware Compatibility Matrix for the Cisco cBR Series Routers, on page 25
- Information About PSIP and EAS Support, on page 27
- How to Configure PSIP and EAS Sessions, on page 27
- Configuration Example, on page 30
- Troubleshooting Tips, on page 30
- Feature Information for PSIP and EAS Support, on page 31

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 8: 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	**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 • PID—CBR-CCAP-LC-G2-R • PID—CBR-SUP-8X10G-PIC • PID—CBR-2X100G-PIC Digital PICs: • PID—CBR-DPIC-8X10G • PID—CBR-DPIC-2X100G Cisco cBR-8 Downstream PHY Module: • PID—CBR-D31-DS-MOD Cisco cBR-8 Upstream PHY Modules: • PID—CBR-D31-US-MOD

Note Do not use DPICs (8X10G and 2x100G) to forward IP traffic, as it may cause buffer exhaustion, leading to line card reload.

The only allowed traffic on a DPIC interface is DEPI, UEPI, and GCP traffic from the Cisco cBR-8 router to Remote PHY devices. Other traffic such as DHCP, SSH, and UTSC should flow via another router, since DPICs cannot be used for normal routing.

Information About PSIP and EAS Support

The Cisco cBR Series Router provides support for merging of Program and System Information Protocol (PSIP) and Emergency Alert Signaling (EAS) streams. This support allows to merge the PSIP and EAS information for digital terminal adapter (DTA) boxes. Merging these two streams helps in avoiding Continuity Counter (CC) errors and packet drops.

An operator can configure a session as PSIP and EAS when creating a session in a broadcast QAM. Operators can configure Passthru session as psip and data-piping session as eas.

Prerequisites for PSIP and EAS Support

PSIP and EAS are applicable to table based sessions on broadcast QAMs. The following prerequisites are applicable to configuring the PSIP and EAS sessions:

- Service Distribution Group (SDG)
- Virtual Carrier Group (VCG)
- Bind VCG to SDG
- Logical Edge Device (LED)
- Protocol of LED specified as table-based.
- Associate VCG to LED

How to Configure PSIP and EAS Sessions

You should create a Passthru session with PSIP and data session with EAS.

This section contains the following:

Configuring PSIP and EAS Sessions

The following sample commands show how to configure the sessions with PSIP and EAS.

```
cable video
  service-distribution-group service distribution group name id <ID>
    rf-port integrated-cable slot/bay/port
  virtual-carrier-group name [id number]
    service-type narrowcast
    rf-channel start_channel-end_channel tsid start_tsid-end_tsid output-port-number
start_number-end_number
  bind-vcg
    vcg vcg-name sdg <sdg name>
  logical-edge-device name [id] number
    protocol table-based
      virtual-edge-input-ip ip-address [vrf vrf-name] input-port-number port-number
      vcg <vcg name>
      active
  table-based
    vcg <vcg name>
      rf-channel <channel number>
```

```
        session SESS_PSIP input-port <id> start-udp-port udp port number processing-type
passthru psip
        session SESS_EAS input-port <id> start-udp-port udp port number processing-type
data eas
```

Verifying the PSIP and EAS Configurations

The following example shows how to verify the configured PSIP and EAS sessions.

```
show cable video session logical-edge-device id 1
Total Sessions = 2

Session  Output Frequency  Streaming  Sess Session Source  UDP  Input   Output  Input Output
  Input   Output  Encrypt  Encrypt  Low PMV  Session
Id       Port   Hz         Type       Type Ucast Dest IP/  Port Program Program State State
   Bitrate Bitrate Type     Status   Lat NUM  Name
                                          Mcast IP (S,G)
-------------------------------------------------------------------------------------------
1048576  101    93000000   Passthru   UDP  174.102.1.1     49652  -       -       ACTIVE-PSI
 ON 895556  904871   CLEAR    -  N - SESS_PSIP.1.0.1.0.49652
1048577  101    93000000   Data-Piping UDP 174.102.1.1     49653 -       -       ACTIVE
 ON 908578  904857   CLEAR    - N  - SESS_EAS.1.0.1.0.49653
```

Verifying the PSIP Session Configuration

```
show cable video session logical-edge-device id 1 session-id 1048576
1048576
Session Name        : SESS_PSIP.1.0.1.0.49652
Session Id          : 1048576
Creation Time       : Fri Feb  2 07:30:06 2018

Output Port         : 101
TSID                : 100
ONID                : 0
Number of Sources   : 1
  Destination IP    : 174.102.1.1
  UDP Port          : 49652
Config Bitrate      : not specified
Jitter              : 100 ms
Processing Type     : Passthru
Stream Rate         : VBR
Program Number      : -
Idle Timeout        : 2000 msec
Init Timeout        : 2000 msec
Off Timeout         : 60 sec
Encryption Type     : CLEAR
Encryption Status   : -

Input Session Stats:
====================
  State: ACTIVE-PSI, Uptime: 0 days 00:00:25
  IP Packets: In 5005, RTP 0, Drop 0
  TP Packets: In 28092, PCR 1003, PSI 107, Null 1938
              Unreference 0, Discontinuity 0
  Errors: Sync loss 0, CC error 0, PCR Jump 0,
          Underflow 0, Overflow 0, Block 0
  Bitrate: Measured 1647418 bps, PCR 1836378 bps

Output Session Stats:
=====================
  State: ON, Uptime: 0 days 00:00:25
```

```
  TP Packets: In 28074, PCR 1000, PSI 106,
              Drop 0, Forward 27968, Insert 0
  Errors: Info Overrun 0, Info Error 0, Block 0, Overdue 0,
          Invalid Rate 0, Underflow 0, Overflow 0
  Bitrate: Measured 1643931 bps

PSIP Stats:
===========
  Total Packets: in 1905, out 31
  MGT: in 1, out 1, version 8, length 1458, carousel 7160
  RRT: in 1, out 1, version 0, length 901, carousel 5
  STT: in 28, out 28, version 0, length 20, carousel 1
  VCT: in 1, out 1, version 4, length 244, carousel 670

PAT Info:
=========
  Version 1, TSID 1, len 16, section 0/0
  Program 1: PMT 8020

Input PMT Info:
===============
  Program 1, Version 1, PCR 8000, Info len 0
  PID 8000: Type 2, Info len 5, (desc 2 len 3)
  PID 8001: Type 129, Info len 17, (lang eng), (desc 5 len 4), (desc 129 len 3)

Output PMT Info:
================
  Program 1, Version 1, PCR 8000, Info len 0
  PID 8000: Type 2, Info len 5, (desc 2 len 3)
  PID 8001: Type 129, Info len 17, (lang eng), (desc 5 len 4), (desc 129 len 3)
```

Verifying EAS Session Configuration

```
show cable video session logical-edge-device id 1 session-id 1048577
Session Name        : SESS_EAS.1.0.1.0.49653
Session Id          : 1048577
Creation Time       : Fri Feb  2 07:30:06 2018

Output Port         : 101
TSID                : 100
ONID                : 0
Number of Sources   : 1
  Destination IP    : 174.102.1.1
  UDP Port          : 49653
Config Bitrate      : not specified
Jitter              : 100 ms
Processing Type     : Data-Piping
Stream Rate         : VBR
Program Number      : -
Idle Timeout        : 2000 msec
Init Timeout        : 2000 msec
Off Timeout         : 60 sec
Encryption Type     : CLEAR
Encryption Status   : -

Input Session Stats:
====================
  State: ACTIVE, Uptime: 0 days 00:00:30
  IP Packets: In 6006, RTP 0, Drop 0
  TP Packets: In 33804, PCR 1204, PSI 0, Null 2232
              Unreference 0, Discontinuity 0
  Errors: Sync loss 0, CC error 0, PCR Jump 0,
          Underflow 0, Overflow 0, Block 0
```

```
  Bitrate: Measured 1682436 bps, PCR 1816387 bps

Output Session Stats:
=====================
  State: ON, Uptime: 0 days 00:00:30
  TP Packets: In 33669, PCR 1201, PSI 0,
              Drop 0, Forward 33669, Insert 0
  Errors: Info Overrun 0, Info Error 0, Block 0, Overdue 0,
          Invalid Rate 0, Underflow 0, Overflow 0
  Bitrate: Measured 1678854 bps

EAS Stats:
==========
  Total Packets: in 4, out 1
  EAS: in 1, out 1, version 19, length 238, carousel 32
```

Configuration Example

This section provides example of PSIP and EAS configuration.

Example: PSIP and EAS Configuration

```
cable video
  service-distribution-group sdg1 id 1
    rf-port integrated-cable 7/0/0
  virtual-carrier-group vcg1 id 1
    service-type narrowcast
    rf-channel 0 tsid 100 output-port-number 101
  bind-vcg
    vcg vcg1 sdg sdg1
  logical-edge-device led1 id 1
    protocol table-based
      virtual-edge-input-ip 192.168.1.1 input-port-number 1
      vcg vcg1
      active
  table-based
    vcg vcg1
    rf-channel 0
      session SESS_PSIP input-port 1 start-udp-port 49652 processing-type passthru psip
      session SESS_EAS input-port 1 start-udp-port 49653 processing-type data eas
```

Troubleshooting Tips

The following tips help in troubleshooting issues:

- Make sure that PSIP session is configured as processing-type passthru and psip
- Make sure that EAS session is configured as processing-type data and eas
- When the PSIP session becomes ACTIVE-PSI, verify the PSIP Stats under the session details command.

  Similarly, when the EAS session becomes ACTIVE, verify the EAS Stats under the session details command.

The out-count and carousel-count should increment.

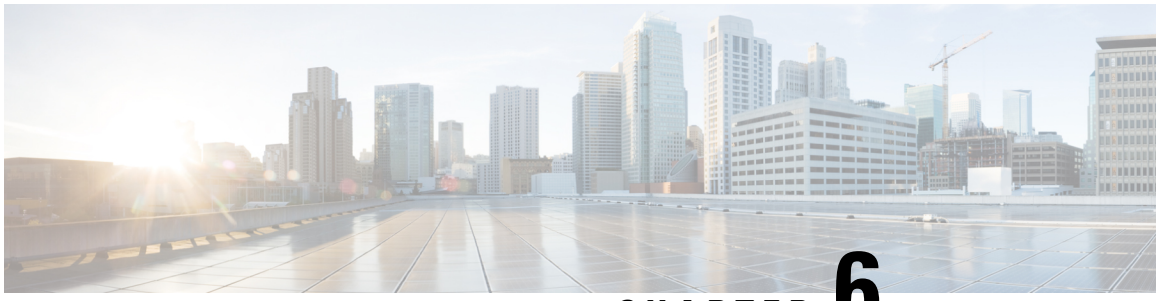
Feature Information for PSIP and EAS Support

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 https://cfnng.cisco.com/ 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 9: Feature Information for PSIP and EAS Support

Feature Name	Releases	Feature Information
PSIP and EAS Support	Cisco IOS XE Fuji 16.7.1	This feature was integrated on the Cisco cBR Series Converged Broadband Routers.



CHAPTER 6

NIT Reference Support for Broadcast QAM

This document provides information on the support for NIT reference and how to configure Cisco cBR series routers to avail the support.

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.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

- Hardware Compatibility Matrix for the Cisco cBR Series Routers, on page 33
- Information About NIT Reference Support, on page 35
- How to Configure NIT Reference, on page 35
- Configuration Example , on page 36
- Troubleshooting Tips, on page 36
- Feature Information for NIT Reference Support, on page 37

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 10: 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	**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 • PID—CBR-CCAP-LC-G2-R • PID—CBR-SUP-8X10G-PIC • PID—CBR-2X100G-PIC Digital PICs: • PID—CBR-DPIC-8X10G • PID—CBR-DPIC-2X100G Cisco cBR-8 Downstream PHY Module: • PID—CBR-D31-DS-MOD Cisco cBR-8 Upstream PHY Modules: • PID—CBR-D31-US-MOD

Note Do not use DPICs (8X10G and 2x100G) to forward IP traffic, as it may cause buffer exhaustion, leading to line card reload.

The only allowed traffic on a DPIC interface is DEPI, UEPI, and GCP traffic from the Cisco cBR-8 router to Remote PHY devices. Other traffic such as DHCP, SSH, and UTSC should flow via another router, since DPICs cannot be used for normal routing.

Information About NIT Reference Support

The Cisco cBR Series Router provides support for Network Information Table (NIT) reference. This feature enables the operator to configure NIT PID from the IOS CLI. The NIT helps in conveying information about the physical organization of the multiplexes and transport streams (TS) carried through a specific network and also the characteristics of the network.

When the NIT PID is not configured, it falls back to the input stream's NIT PID. In this case, the NIT PID may be none or NIT PID based on the input stream.

Table 11: Test 1

Col 1	Col2 Col3	Col3
2	3	4
2	2	38
7	8	7

Table 12: Test 2

Col1	Col 2	Col3
1	3	2
4	42	3
3	3	1

Table 13: Test 3

Test col1	Test col2	Test col3
1	3	4
8	6	7
6	7	r5

How to Configure NIT Reference

This section contains the following topics:

Configuring NIT Reference

The following sample commands show how to configure NIT reference.

```
configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

```
  cable video
   default-nit-reference ?
     <1-8190>  1-8190

   default-nit-reference 100
%%All existing sessions will be updated with default-nit-reference.
Re-configure Default NIT reference? [Yes/No][confirm]
```

Verifying the NIT Reference Configuration

The following example shows how to verify the NIT reference configuration.

```
video-LWR-S-A4#sh run | s cable vid
cable video
  multicast-uplink Port-channel23 access-list all-multicasts rp 2.23.1.1
  default-nit-reference 100
  mgmt-intf VirtualPortGroup 0
  encryption
```

Removing the NIT Reference

To remove the configured NIT PID, use the **no default-nit-reference <NIT PID>** command.

```
no default-nit-reference
%%All existing sessions will be updated with default-nit-reference.
Re-configure Default NIT reference? [Yes/No][confirm]
```

Configuration Example

This section provides example of Cisco cBR-8 Converged Broadband Router NIT reference configuration.

Example: NIT Reference Configuration

```
video-LWR-S-A4#conf term
Enter configuration commands, one per line.  End with CNTL/Z.
video-LWR-S-A4(config)#cable video
video-LWR-S-A4(config-video)#default-nit-reference ?
  <1-8190>  1-8190

video-LWR-S-A4(config-video)#default-nit-reference 100
%%All existing sessions will be updated with default-nit-reference.
Re-configure Default NIT reference? [Yes/No][confirm]
video-LWR-S-A4(config-video)#
```

Troubleshooting Tips

The following tips help in troubleshooting issues:

- After configuring NIT PID, check whether the streams are in ACTIVE-PSI for the QAM

- Verify that the configured NIT PID is present in the PAT’s program 0
- After removing the NIT reference configuration (NIT PID), verify the following,
  - If the input stream has NIT PID, the PAT's program 0 contains the input stream's NIT PID
  - If the NIT PID is not present in the input stream, the program 0 should not be present in the PAT

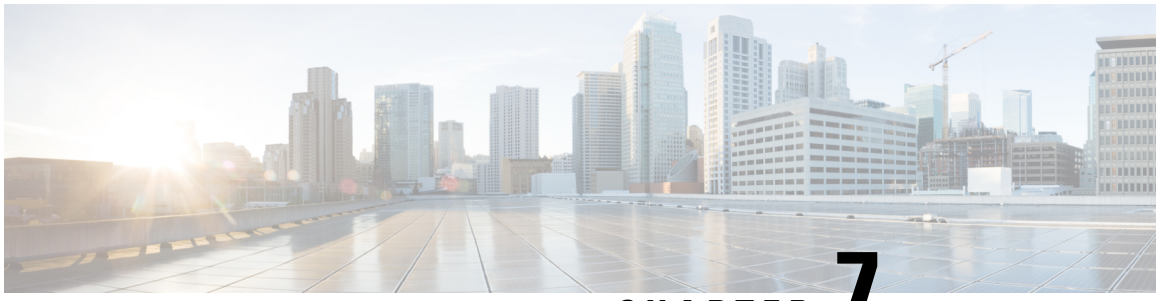
Feature Information for NIT Reference Support

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 https://cfnng.cisco.com/ 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 14: Feature Information for NIT Reference Support

Feature Name	Releases	Feature Information
NIT Reference Support	Cisco IOS XE Fuji 16.7.1	This feature was integrated on the Cisco cBR Series Converged Broadband Routers.



CHAPTER 7

Logical Edge Devices

A Logical Edge Device (LED) is a virtual edge device within the cBR-8 and can be provisioned for static or dynamic sessions.

Contents

- Information about Logical Edge Devices, on page 39
- How to Configure the Logical Edge Devices, on page 39
- Configuration Examples, on page 46
- Feature Information for Logical Edge Devices, on page 47

Information about Logical Edge Devices

An LED interfaces remotely to a head end video Session Resource Manager (SRM) using the GQI protocol. It also represents a group of locally managed table-based video sessions.

In Cisco cBR-8, you can create up to 32 LEDs to simultaneously manage the video QAM carriers. Each LED manages a set of virtual QAM carriers independently. Due to the limitation of the GQI protocol, a GQI LED can only manage a set of QAM carriers in a single line card, unlike the table-based LED, which can manage more than a single line card.

In addition, an LED can be optionally configured to support the D6 discovery protocol to report a QAM resource to the SRM.

How to Configure the Logical Edge Devices

This section describes how to configure LEDs for the video session on Cisco cBR-8.

Configuring Session-Based (Dynamic) Logical Edge Devices

GQI is a protocol for the GQI LED to interface with the remote SRM.

For system using discovery protocol, the D6 discovery protocol should be enabled to report the QAM resources of the LED to the remote SRM.

An active flag should be enabled on the LED to indicate that it is active. This flag indicates that the connectivity with the SRM can be setup and the LED can start handling GQI message exchange from the SRM.

You cannot edit or remove the LED data when it is in the active mode. To do so, you must first move the LED to inactive mode and then disconnect it from the SRM.

Due to the limitations of the GQI protocol, GQI LED cannot have Virtual Carrier Groups that span across multiple cable line cards (CLC).

Note In Cisco IOS-XE Release 16.5.1, only GQI version 2 is supported for all GQI LEDs.

Before You Begin

The following data is necessary to define a GQI LED:

- The Management IP address that the SRM uses to setup connectivity with the LED. The IP address must be in the same subnet as configured in the VirtualPortGoup.
- A unique MAC address per LED. Using the chassis MAC address as a basis, increment the least significant number to give a unique identifier (MAC address) for each LED. This number should be unique with respect to the GQI server and does not really relate to a true MAC address. Thus, the number is irrelevant, but needs to be unique.

Tip Use the **show diag all eeprom detail | include MAC** command to get the chassis MAC address.

- The primary and secondary IP addresses of the remote SRM.
- Virtual Carrier Group (VCG). For more information, see Video Virtual Carrier Group and Virtual Edge Input.
- Connection-orientated controls such as, keep alive, reset interval, and timeout value.
- Virtual Edge Input (VEI) configured with a routable IP address from within the network. For more information, see Video Virtual Carrier Group and Virtual Edge Input.

To configure the session-based LEDs, complete the following procedure:

```
configure terminal
cable video
logical-edge-device name [id  number]
protocol gqi
mgmt-ip ip address
server ip address
virtual-edge-input ip address input-port-number port number
vcg vcg name
vcg vcg name
mac-address mac address
keepalive retry retry count interval seconds
reset interval seconds
active
```

Verifying the Session-Based (Dynamic) Logical Edge Devices Configuration

To verify a GQI LED configuration, use the **show cable video logical-edge-device** command as shown in the example below:

```
show cable video logical-edge-device id 1
Logical Edge Device: led
Id: 1
Protocol: GQI
Service State: Active
Discovery State: Disable
Management IP: 1.33.2.10
MAC Address: c414.3c17.6000
Number of Servers: 2
   Server 1: 1.200.1.193
   Server 2: 1.200.1.183
Reset Interval: 5
Keepalive Interval: 5    Retry Count:3
Number of Virtual Carrier Groups: 2
Number of Share Virtual Edge Input: 1
Number of Physical Qams: 94
Number of Sessions: 240
No Reserve PID Range

Virtual Edge Input:
Input Port   VEI                 Slot/Bay     Bundle       Gateway
ID           IP                                ID           IP
-----------------------------------------------------------------
1            174.102.1.1         7/0          -            -

Virtual Carrier Group:
ID    Name                              Total      Total      Service-Distribution-Group
    Service-Distribution-Group
                                        VEI        RF-channel Name
    ID
-------------------------------------------------------------------------------------------
1     vcg                               0          28         sdg
    1
2     vcg-2                             0          19         sdg
    1

Integrated      Physical   Admin      Operational  TSID         ONID         Output
VCG          SDG          Encryption
Cable           QAM ID     State      State                                 Port
ID           ID           Capable
-------------------------------------------------------------------------------------------
7/0/0:20        20          ON         UP           1            1000         1
1            1            powerkey
7/0/0:21        21          ON         UP           2            1000         2
1            1            powerkey
7/0/0:22        22          ON         UP           3            1000         3
1            1            powerkey
7/0/0:23        23          ON         UP           4            1000         4
1            1            powerkey
7/0/0:24        24          ON         UP           5            1000         5
1            1            powerkey
7/0/0:25        25          ON         UP           6            1000         6
1            1            powerkey
7/0/0:26        26          ON         UP           7            1000         7
1            1            powerkey
7/0/0:27        27          ON         UP           8            1000         8
1            1            powerkey
7/0/0:28        28          ON         UP           9            1000         9
1            1            powerkey
```

```
7/0/0:29        29          ON          UP            10            1000          10
1            1           powerkey
7/0/0:30        30          ON          UP            11            1000          11
1            1           powerkey
7/0/0:31        31          ON          UP            12            1000          12
1            1           powerkey
7/0/0:32        32          ON          UP            13            1000          13
1            1           powerkey
7/0/0:33        33          ON          UP            14            1000          14
1            1           powerkey
7/0/0:34        34          ON          UP            15            1000          15
1            1           powerkey
7/0/0:35        35          ON          UP            16            1000          16
1            1           powerkey
7/0/0:36        36          ON          UP            17            1000          17
1            1           powerkey
7/0/0:37        37          ON          UP            18            1000          18
1            1           powerkey
7/0/0:38        38          ON          UP            19            1000          19
1            1           powerkey
7/0/0:39        39          ON          UP            20            1000          20
1            1           powerkey
7/0/0:40        40          ON          UP            21            1000          21
1            1           powerkey
7/0/0:41        41          ON          UP            22            1000          22
1            1           powerkey
7/0/0:42        42          ON          UP            23            1000          23
1            1           powerkey
7/0/0:43        43          ON          UP            24            1000          24
1            1           powerkey
7/0/0:44        44          ON          UP            25            1000          25
1            1           powerkey
7/0/0:45        45          ON          UP            26            1000          26
1            1           powerkey
7/0/0:46        46          ON          UP            27            1000          27
1            1           powerkey
7/0/0:47        47          ON          UP            28            1000          28
1            1           powerkey
7/0/7:20        20          ON          UP            1             1000          1
1            1           powerkey
7/0/7:21        21          ON          UP            2             1000          2
1            1           powerkey
7/0/7:22        22          ON          UP            3             1000          3
1            1           powerkey
7/0/7:23        23          ON          UP            4             1000          4
1            1           powerkey
7/0/7:24        24          ON          UP            5             1000          5
1            1           powerkey
7/0/7:25        25          ON          UP            6             1000          6
1            1           powerkey
7/0/7:26        26          ON          UP            7             1000          7
1            1           powerkey
7/0/7:27        27          ON          UP            8             1000          8
1            1           powerkey
7/0/7:28        28          ON          UP            9             1000          9
1            1           powerkey
7/0/7:29        29          ON          UP            10            1000          10
1            1           powerkey
7/0/7:30        30          ON          UP            11            1000          11
1            1           powerkey
7/0/7:31        31          ON          UP            12            1000          12
1            1           powerkey
7/0/7:32        32          ON          UP            13            1000          13
1            1           powerkey
```

```
7/0/7:33        33          ON          UP          14          1000          14
1           1           powerkey
7/0/7:34        34          ON          UP          15          1000          15
1           1           powerkey
7/0/7:35        35          ON          UP          16          1000          16
1           1           powerkey
7/0/7:36        36          ON          UP          17          1000          17
1           1           powerkey
7/0/7:37        37          ON          UP          18          1000          18
1           1           powerkey
7/0/7:38        38          ON          UP          19          1000          19
1           1           powerkey
7/0/7:39        39          ON          UP          20          1000          20
1           1           powerkey
7/0/7:40        40          ON          UP          21          1000          21
1           1           powerkey
7/0/7:41        41          ON          UP          22          1000          22
1           1           powerkey
7/0/7:42        42          ON          UP          23          1000          23
1           1           powerkey
7/0/7:43        43          ON          UP          24          1000          24
1           1           powerkey
7/0/7:44        44          ON          UP          25          1000          25
1           1           powerkey
7/0/7:45        45          ON          UP          26          1000          26
1           1           powerkey
7/0/7:46        46          ON          UP          27          1000          27
1           1           powerkey
7/0/7:47        47          ON          UP          28          1000          28
1           1           powerkey
7/0/0:1         1           ON          UP          29          1000          29
2           1           powerkey
7/0/0:2         2           ON          UP          30          1000          30
2           1           powerkey
7/0/0:3         3           ON          UP          31          1000          31
2           1           powerkey
7/0/0:4         4           ON          UP          32          1000          32
2           1           powerkey
7/0/0:5         5           ON          UP          33          1000          33
2           1           powerkey
7/0/0:6         6           ON          UP          34          1000          34
2           1           powerkey
7/0/0:7         7           ON          UP          35          1000          35
2           1           powerkey
7/0/0:8         8           ON          UP          36          1000          36
2           1           powerkey
7/0/0:9         9           ON          UP          37          1000          37
2           1           powerkey
7/0/0:10        10          ON          UP          38          1000          38
2           1           powerkey
7/0/0:11        11          ON          UP          39          1000          39
2           1           powerkey
7/0/0:12        12          ON          UP          40          1000          40
2           1           powerkey
7/0/0:13        13          ON          UP          41          1000          41
2           1           powerkey
7/0/0:14        14          ON          UP          42          1000          42
2           1           powerkey
7/0/0:15        15          ON          UP          43          1000          43
2           1           powerkey
7/0/0:16        16          ON          UP          44          1000          44
2           1           powerkey
7/0/0:17        17          ON          UP          45          1000          45
2           1           powerkey
```

```
7/0/0:18        18          ON          UP          46          1000          46
2           1           powerkey
7/0/0:19        19          ON          UP          47          1000          47
2           1           powerkey
7/0/7:1         1           ON          UP          29          1000          29
2           1           powerkey
7/0/7:2         2           ON          UP          30          1000          30
2           1           powerkey
7/0/7:3         3           ON          UP          31          1000          31
2           1           powerkey
7/0/7:4         4           ON          UP          32          1000          32
2           1           powerkey
7/0/7:5         5           ON          UP          33          1000          33
2           1           powerkey
7/0/7:6         6           ON          UP          34          1000          34
2           1           powerkey
7/0/7:7         7           ON          UP          35          1000          35
2           1           powerkey
7/0/7:8         8           ON          UP          36          1000          36
2           1           powerkey
7/0/7:9         9           ON          UP          37          1000          37
2           1           powerkey
7/0/7:10        10          ON          UP          38          1000          38
2           1           powerkey
7/0/7:11        11          ON          UP          39          1000          39
2           1           powerkey
7/0/7:12        12          ON          UP          40          1000          40
2           1           powerkey
7/0/7:13        13          ON          UP          41          1000          41
2           1           powerkey
7/0/7:14        14          ON          UP          42          1000          42
2           1           powerkey
7/0/7:15        15          ON          UP          43          1000          43
2           1           powerkey
7/0/7:16        16          ON          UP          44          1000          44
2           1           powerkey
7/0/7:17        17          ON          UP          45          1000          45
2           1           powerkey
7/0/7:18        18          ON          UP          46          1000          46
2           1           powerkey
7/0/7:19        19          ON          UP          47          1000          47
2           1           powerkey
```

-

Configuring the D6 Discovery Protocol

D6 discovery protocol is the discovery portion of the Comcast Next Generation on Demand (NGOD) specification. D6 discovery protocol sends out carrier information such as frequency, annex, modulation mode, interleave, and edge input information such as IP address and maximum bandwidth to an Edge Resource Manager (ERM). D6 discovery protocol also sends unique structured names (topological location information) for each edge input or carrier output. From these structured names, and input and RF port numbers, the ERM can infer the topological network location of both the QAM streaming input port (IP) and RF output port (MPEG).

The D6 discovery protocol configuration can be performed only when the LED protocol is either table-based or GQI. The LED must be in inactive mode to edit or create a D6 discovery protocol configuration. The D6 discovery protocol configuration parameters are:

- Management IP—The source IP address used to establish a connection with the external D6 discovery protocol server (ERM). The IP address must be in the same subnet as configured in a virtual port group.

For GQI LED, this configuration is not needed under D6 discovery protocol as it is automatically fetched from the LED configuration.

- D6 discovery protocol server IP address and port—Identifies the remote D6 discovery protocol server (ERM) IP address and listening port used by the D6 discovery protocol client in LED to setup a connection with the peer. You can configure only one server address and port per LED.
- FQDN (Fully Qualified Domain Name)—This can be given instead of IP address for D6 discovery protocol server.
- Streaming zone—Streaming zone as configured in the D6 discovery protocol server (ERM). The name should match with the configured D6 discovery protocol server in the ERM for the connection to be established.
- Component name—The name of the Edge QAM device. Each LED is considered by the D6 discovery protocol server as a separate Edge QAM component. This name is used by the D6 discovery protocol server to represent the LED.
- Timeout value—(Optional) Time to wait for connection in socket call.
- Hold time value—(Optional) Time interval that decides the interval of the keepalive message exchange between the client and the server.
- Input group—(Optional) Each virtual edge input IP address under the LED can be assigned an input group name and the maximum bandwidth that is used to send traffic to it. This information is used in D6 discovery protocol messages when advertising the edge inputs to the D6 discovery protocol server. If these parameters are not configured then for group name, the LED or the VCG name, and the default bandwidth of 20 Gbps are used. You must repeat this command for each VEI and VCG under the LED. For GQI LED, there is no option to set VEI IP under the VCG, so, this input group CLI is not available for the VCGs for GQI LEDs.

To configure the D6 discovery protocol, complete the following procedure:

```
configure terminal
cable video
logical-edge-device device name [id number]
protocol gqi | table-based
mgmt-ip ip address
server ip address
virtual-edge-input ip address input-port-number port number
vcg vcg name
vcg vcg name
mac-address mac address
keepalive retry retry count interval seconds
reset interval seconds
discovery d6
streaming-zone name
component-name name
d6-server ip address [port]
d6-server fqdn domain-name
timeout seconds
holdtime seconds
input-group led vei-ip led vei ip address group-name group name [bandwidth mbps]
```

```
exit
active
```

Verifying the D6 Configuration

To verify the D6 discovery protocol configuration, use the **show cable video logical-edge-device** command as shown in the example below.

This CLI command shows the status and statistics of the D6 client associated to the LED. In the example below, it shows the duration and number of open, updated, keepalive and notification messages exchanged between the D6 client and the server in that duration. It also indicates how many unknown or unrecognized messages are received from the server. When the open message count is more than 1, it indicates that the connection is terminated and reconnected.

```
show cable video logical-edge-device id 1 d6
Logical Edge Device: led1
Id: 1
D6 Summary:
-------------------------------------------------
Enabled              : Yes
VREP Version         : 2
D6 State             : Established
Management IP        : 1.21.2.11
Source Port          : 6069
D6 Server IP         : 172.25.20.144
D6 Server Port       : 6069
Hold Time(negotiated): 30
Timeout              : 90
Keep Alive Interval  : 10
Streaming Zone       : Sanjose.ciscolab
failure Reason       : No Failure
-------------------------------------------------

D6 Statistics:
-----------------------------------------------------------------
Duration  Dir  Open    Update   KeepAlive Notification Unknown
-----------------------------------------------------------------
1          RX     1         0           9            0       0
1          TX     1        13          11            0       0
-----------------------------------------------------------------
```

Configuration Examples

This section provides configuration examples for the LED configuration.

Example: GQI LED Configuration

Example: Example: GQI LED Configuration

```
cable video
  mgmt-intf VirtualPortGroup 0
  encryption
    linecard 7/0 ca-system powerkey scrambler des
  service-distribution-group sdg id 1
    onid 1000
    rf-port integrated-cable 7/0/0
```

```
  rf-port integrated-cable 7/0/7
virtual-carrier-group vcg id 1
  encrypt
  rf-channel 20-47 tsid 1-28 output-port-number 1-28
virtual-carrier-group vcg-2 id 2
  encrypt
  rf-channel 1-19 tsid 29-47 output-port-number 29-47
bind-vcg
  vcg vcg sdg sdg
  vcg vcg-2 sdg sdg
logical-edge-device led id 1
  protocol gqi
    mgmt-ip 1.33.2.10
    mac-address c414.3c17.6000
    server 1.200.1.193
    server 1.200.1.183
    virtual-edge-input-ip 174.102.1.1 input-port-number 1
    vcg vcg
    vcg vcg-2
    active
```

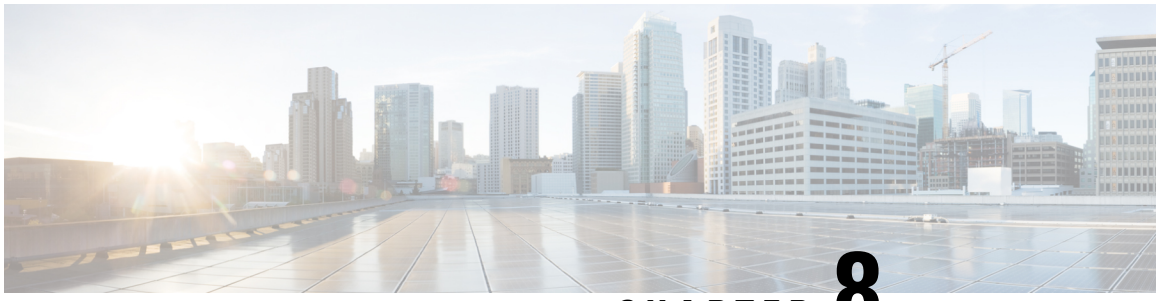
Feature Information for Logical Edge Devices

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 https://cfnng.cisco.com/ 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 Logical Edge Devices

Feature Name	Releases	Feature Information
Logical Edge Devices	Cisco IOS XE Everest 16.6.1	This feature was integrated on the Cisco cBR Series Converged Broadband Routers.



CHAPTER 8

Cisco Smart Licensing for Video

The Cisco Smart Licensing for Video on the Cisco cBR router leverages existing Cisco cBR Smart Licensing framework that includes Call Home and SLA capabilities.

- Video Smart Licensing , on page 49
- Information About Video Smart Licensing, on page 49
- How to Verify Video Smart Licensing, on page 50
- Configuration Examples, on page 51
- Use Cases or Deployment Scenarios, on page 52
- Feature Information for Video Smart Licensing, on page 54

Video Smart Licensing

The Cisco Smart Licensing feature uses a pooled license model. All FRUs in the chassis and multiple such chassis share the entitlements for Upstream (US), Downstream (DS), WAN, Narrowcast (NC), Broadcast (BC), encrypted licenses (PME, PKY, DVB), and Replicate (RPL) as long as they do not exceed the entitlement count for that pool.

For information on entitlement usage, see the Cisco Smart Licensing.

Information About Video Smart Licensing

Benefits of Smart Licensing

Cisco Smart Licensing is intended to overcome the limitations and issues of the enforced licensing method. For more information, see the Cisco Smart Licensing document .

Prerequisites for Video Smart Licensing

See the Cisco Smart Licensing document.

Restrictions for Video Smart Licensing

For video services, the VCG service type determines the number of licenses consumed for bound VCGs. The QAM channel **shut**/**no shut** state has no relevance for video (unlike DOCSIS services). When the service type is not defined, the NC license entitlements are consumed per QAM channel.

How to Verify Video Smart Licensing

Verifying Video Smart Licensing Using Show Commands

Use the **show cable license** command to verify video smart licensing configuration.

To verify all license information, use the **show cable license all** command:

```
Router# show cable license all

-----------------------------------------
Entitlement:  Downstream License
Consumed count: 768
Consumed count reported to SmartAgent: 0 Forced-Shut count: 0 Enforced state: No Enforcement

-----------------------------------------
Entitlement:  Upstream License
Consumed count: 64
Consumed count reported to SmartAgent: 64 Forced-Shut count: 0 Enforced state: No Enforcement

-----------------------------------------
Entitlement:  WAN License
Consumed count: 2
Consumed count reported to SmartAgent: 2 Forced-Shut count: 0 Enforced state: No Enforcement

-----------------------------------------
Entitlement:  LCHA License
Consumed count: 0
Consumed count reported to SmartAgent: 0 Forced-Shut count: 0 Enforced state: No Enforcement

-----------------------------------------
Entitlement:  Video Narrowcast License
Consumed count: 0
Consumed count reported to SmartAgent: 0 Forced-Shut count: 0 Enforced state: No Enforcement

-----------------------------------------
Entitlement:  Video Narrowcast Replicate License Consumed count: 0 Consumed count reported
 to SmartAgent: 0 Forced-Shut count: 0 Enforced state: No Enforcement

-----------------------------------------
Entitlement:  Video Narrowcast PKEY License Consumed count: 0 Consumed count reported to
SmartAgent: 0 Forced-Shut count: 0 Enforced state: No Enforcement

-----------------------------------------
Entitlement:  Video Narrowcast PME License Consumed count: 0 Consumed count reported to
SmartAgent: 0 Forced-Shut count: 0 Enforced state: No Enforcement

-----------------------------------------
Entitlement:  Video Narrowcast DVB License Consumed count: 0 Consumed count reported to
SmartAgent: 0 Forced-Shut count: 0 Enforced state: No Enforcement
```

To view specific video license configuration, use the appropriate keyword with the **show cable license** command:

```
Router# show cable license ?
  all     Show all license information
  ds      DOCSIS downstreams
  lcha    LCHA groups
  nc      Narrowcast video
  nc_dvb  Narrowcast video DVB
  nc_pky  Narrowcast video PowerKEY
  nc_pme  Narrowcast video PME
  nc_rpl  Narrowcast video replicate
  us      DOCSIS upstreams
  wan     WAN ports
```

For example, to verify Narrowcast video configuration, use the **show cable license nc** command:

```
Router # show cable license nc
-----------------------------------------
Entitlement:  Video Narrowcast License
Consumed count: 128
Consumed count reported to SmartAgent: 128 Forced-Shut count: 0 Enforced state: No Enforcement
```

Configuration Examples

Example 1: Show Running Output for Basic Configuration

```
cable video
 service-distribution-group sdg-lic id 64
   rf-port integrated-cable 7/0/0
 service-distribution-group sdg-lic1 id 63
  rf-port integrated-cable 7/0/1
 virtual-carrier-group vcg-lic1 id 158
  rf-channel 0 tsid 65535 output-port-number 1
 virtual-carrier-group vcg-lic2 id 157
  rf-channel 1-3 tsid 65532-65534 output-port-number 2-4
 virtual-carrier-group vcg-lic3 id 156
  rf-channel 4-7 tsid 65528-65531 output-port-number 5-8
 virtual-carrier-group vcg-lic4 id 155
  rf-channel 8-15 tsid 65520-65527 output-port-number 9-16
 virtual-carrier-group vcg-lic5 id 154
  rf-channel 16-31 tsid 65504-65519 output-port-number 17-32
 virtual-carrier-group vcg-lic6 id 153
  rf-channel 32-63 tsid 65472-65503 output-port-number 33-64
 virtual-carrier-group vcg-lic7 id 152
  rf-channel 64-127 tsid 65408-65471 output-port-number 65-128
 virtual-carrier-group vcg-lic8 id 151
  rf-channel 0-127 tsid 65280-65407 output-port-number 129-256
 bind-vcg
  vcg vcg-lic1 sdg sdg-lic
  vcg vcg-lic2 sdg sdg-lic
  vcg vcg-lic3 sdg sdg-lic
  vcg vcg-lic4 sdg sdg-lic
  vcg vcg-lic5 sdg sdg-lic
  vcg vcg-lic6 sdg sdg-lic
```

```
  vcg vcg-lic7 sdg sdg-lic
  vcg vcg-lic8 sdg sdg-lic1
exit
```

Example 2: Show Running Output for QRG and NC License Configuration

```
cable video
  service-distribution-group sdg-lic id 64
    rf-port integrated-cable 7/0/0
    rf-port integrated-cable 7/0/2
  service-distribution-group sdg-lic1 id 63
    rf-port integrated-cable 7/0/1
    rf-port integrated-cable 7/0/3
    rf-port integrated-cable 7/0/4
    rf-port integrated-cable 7/0/5
    rf-port integrated-cable 7/0/6
    rf-port integrated-cable 7/0/7
  virtual-carrier-group vcg-lic1 id 158
    rf-channel 0-55 tsid 65480-65535 output-port-number 1-56
   virtual-carrier-group vcg-lic2 id 157
    rf-channel 0-55 tsid 65424-65479 output-port-number 57-112
  bind-vcg
    vcg vcg-lic1 sdg sdg-lic
    vcg vcg-lic2 sdg sdg-lic1
exit
```

Use Cases or Deployment Scenarios

Case 1: Narrowcast Video Services with PowerKEY Encryption

```
cable video
 encrypt
 linecard 7/0 ca-system powerkey scrambler des
 service-distribution-group sdg-lic id 64
  rf-port integrated-cable 7/0/0
  rf-port integrated-cable 7/0/2
  rf-port integrated-cable 7/0/3
 service-distribution-group sdg-lic1 id 63
  rf-port integrated-cable 7/0/1
  rf-port integrated-cable 7/0/4
  rf-port integrated-cable 7/0/5
  rf-port integrated-cable 7/0/6
  rf-port integrated-cable 7/0/7
 virtual-carrier-group vcg-lic1 id 158
 encrypt
  rf-channel 0 tsid 65535 output-port-number 1
 virtual-carrier-group vcg-lic2 id 157
  rf-channel 1-3 tsid 65532-65534 utput-port-number 2-4
 virtual-carrier-group vcg-lic3 id 156
 encrypt
  rf-channel 4-7 tsid 65528-65531 output-port-number 5-8
 virtual-carrier-group vcg-lic4 id 155
  rf-channel 8-15 tsid 65520-65527 output-port-number 9-16
 virtual-carrier-group vcg-lic5 id 154
 encrypt
  rf-channel 16-31 tsid 65504-65519 output-port-number 17-32
```

```
 virtual-carrier-group vcg-lic6 id 153
  rf-channel 32-63 tsid 65472-65503 output-port-number 33-64
 virtual-carrier-group vcg-lic7 id 152
 encrypt
  rf-channel 64-127 tsid 65408-65471 output-port-number 65-128
 virtual-carrier-group vcg-lic8 id 151
 encrypt
  rf-channel 0-127 tsid 65280-65407 output-port-number 129-256
 bind-vcg
  vcg vcg-lic1 sdg sdg-lic
  vcg vcg-lic2 sdg sdg-lic
  vcg vcg-lic3 sdg sdg-lic
  vcg vcg-lic4 sdg sdg-lic
  vcg vcg-lic5 sdg sdg-lic
  vcg vcg-lic6 sdg sdg-lic
  vcg vcg-lic7 sdg sdg-lic
  vcg vcg-lic8 sdg sdg-lic1
exit
```

Case 2: Narrowcast Video Services with PME Encryption

```
cable video
 encrypt
 linecard 7/0 ca-system pme scrambler dvs042
 service-distribution-group sdg-lic id 64
  rf-port integrated-cable 7/0/0
  rf-port integrated-cable 7/0/2
  rf-port integrated-cable 7/0/3
 service-distribution-group sdg-lic1 id 63
  rf-port integrated-cable 7/0/1
  rf-port integrated-cable 7/0/4
  rf-port integrated-cable 7/0/5
  rf-port integrated-cable 7/0/6
  rf-port integrated-cable 7/0/7
 virtual-carrier-group vcg-lic1 id 158
  rf-channel 0 tsid 65535 output-port-number 1
 virtual-carrier-group vcg-lic2 id 157
 encrypt
  rf-channel 1-3 tsid 65532-65534 output-port-number 2-4
 virtual-carrier-group vcg-lic3 id 156
  rf-channel 4-7 tsid 65528-65531 output-port-number 5-8
 virtual-carrier-group vcg-lic4 id 155
 encrypt
  rf-channel 8-15 tsid 65520-65527 output-port-number 9-16
 virtual-carrier-group vcg-lic5 id 154
  rf-channel 16-31 tsid 65504-65519 output-port-number 17-32
 virtual-carrier-group vcg-lic6 id 153
 encrypt
  rf-channel 32-63 tsid 65472-65503 output-port-number 33-64
 virtual-carrier-group vcg-lic7 id 152
  rf-channel 64-127 tsid 65408-65471 output-port-number 65-128
 virtual-carrier-group vcg-lic8 id 151
 encrypt
  rf-channel 0-127 tsid 65280-65407 output-port-number 129-256
 bind-vcg
  vcg vcg-lic1 sdg sdg-lic
  vcg vcg-lic2 sdg sdg-lic
  vcg vcg-lic3 sdg sdg-lic
  vcg vcg-lic4 sdg sdg-lic
  vcg vcg-lic5 sdg sdg-lic
  vcg vcg-lic6 sdg sdg-lic
  vcg vcg-lic7 sdg sdg-lic
```

```
  vcg vcg-lic8 sdg sdg-lic1
exit
```

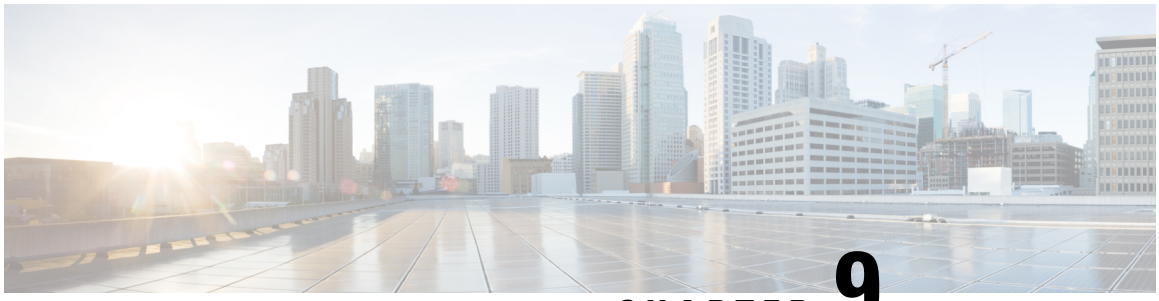
Feature Information for Video Smart Licensing

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 https://cfnng.cisco.com/ 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 16: Feature Information for Video Smart Licensing

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



CHAPTER 9

Physical to Virtual Binding

The Virtual Carrier Group (VCG) is bound to a Service Distribution Group (SDG) using a bind command (bind-vcg). This connects the virtual carriers to the physical ports listed in the SDG. After binding, a path from the Virtual Edge Input (VEI) is mapped to the RF ports.

- Information About Physical to Virtual Binding, on page 55
- How to Configure VPME Encryption, on page 55
- Configuration Examples, on page 56
- Feature Information for Physical to Virtual Binding, on page 57

Information About Physical to Virtual Binding

In general, more than one VCG can be bound to the same SDG, only if the RF-channels in the VCG are not overlapping each other. However, one VCG cannot be bound to multiple SDGs.

If you want to configure one VCG to multiple SDGs, you should configure QAM replication instead. For more information, see Configuring QAM Replication section.

How to Configure VPME Encryption

This section describes how to configure physical to virtual binding and QAM replication on Cisco cBR-8.

- Configuring Physical to Virtual Binding, on page 55
- Configuring QAM Replication, on page 56

Configuring Physical to Virtual Binding

To bind a set of virtual RF-channels defined in the VCG to the physical port in the SDG, perform the following:

```
enable
configure terminal
cable video
bind-vcg
vcg vcg-name sdg sdg-name
exit
```

Configuring QAM Replication

To configure QAM replication to one or more ports, add the ports to an SDG configuration as following:

```
enable
configure terminal
cable video
service-distribution-group name
rf-port integrated-cable slot/bay/port
rf-port integrated-cable slot/bay/port
exit
```

Configuration Examples

This section provides configuration examples for the physical to virtual binding configuration.

Example 1: Physical to Virtual Binding Configuration

The following is a sample in which the port 7/0/2 of SDG *west-region* binds with 0 to 10 RF-channels of VCG *movie-channels* to physically identify the 7/0/2:0 to 7/0/2:10 QAM carriers.

Example 1 :

```
Router#config t
Router(config)#cable video
Router(config-video)#service-distribution-group  west-region
Router(config-video-sdg)#rf-port  integrated-cable  7/0/2
Router(config-video-sdg)#exit
Router(config-video)#virtual-carrier-group movie-channels
Router(config-video-vcg)#rf-channel 0-10 tsid 1-11 output-port-num 1-11
Router(config-video-vcg)#exit
Router(config-video)#bind-vcg
Router(config-video-bd)# vcg movie-channels sdg west-regions
```

Example 2: Physical to Virtual Binding Configuration

The following is a sample in which the *movie-channels* VCG and *news-channels* VCG bind with *west-regions* SDG.

Example 2 :

```
Router#config t
Router(config)#cable video
Router(config-video)#service-distribution-group  west-region
Router(config-video-sdg)#rf-port  integrated-cable  7/0/2
Router(config-video-sdg)#exit
Router(config-video)#virtual-carrier-group movie-channels
Router(config-video-vcg)#rf-channel 0-10 tsid 1-11 output-port-num 1-11
Router(config-video-vcg)#exit
Router(config-video)#virtual-carrier-group news-channels
Router(config-video-vcg)#rf-channel 11-15 tsid 12-16 output-port-num 12-16
Router(config-video-vcg)#exit
Router(config-video)#bind-vcg
Router(config-video-bd)# vcg movie-channels sdg west-regions
Router(config-video-bd)# vcg news-channels sdg west-regions
```

Example 3: QAM Replication Configuration

The following is a sample in which video replication is set across 7/0/0 and 7/0/1 ports:

Example 3 :

```
Router#config t
Router(config)#cable video
Router(config-video)# service-distribution-group  qrg-example
Router(config-video-sdg)# rf-port  integrated-cable  7/0/0
Router(config-video-sdg)# rf-port  integrated-cable  7/0/1
```

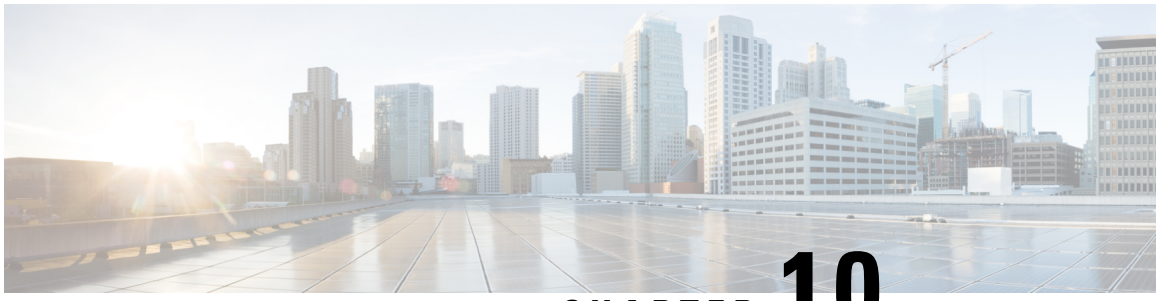
Feature Information for Physical to Virtual Binding

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 https://cfnng.cisco.com/ 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 Physical to Virtual Binding

Feature Name	Releases	Feature Information
Physical to Virtual Binding	Cisco IOS XE Everest 16.6.1	This feature was integrated on the Cisco cBR Series Converged Broadband Routers.



CHAPTER 10

Table Based Configuration

The table-based video is a local session management that provisions using CLI. The statically allocated local video sessions can be either unicast or multicast video stream.

- Information About Table Based Configuration, on page 59
- Configuring Table Based Session, on page 59
- Virtual Edge Input Bundling, on page 60
- 10-6 UDP Port Mapping, on page 62
- Feature Information for Table Based Configuration, on page 64

Information About Table Based Configuration

Table-based video session configuration can be performed for a range or an individual session under each Quadrature Amplitude Modulation (QAM) carrier that is being assigned to a table-based Logical Edge Device (LED). In cBR-8, you can create multiple LEDs for table-based video sessions; each LED manages one set of QAM carriers for table-based sessions. Table-based sessions can be configured as a pass-through, remap, or a data piping session.

Configuring Table Based Session

To configure the encryption type for a VOD session, perform the following steps:

```
enable
configure terminal
cable video
table-based
vcg vcg-name
rf-channel n-m
session sess-name input-port id start-udp-port udp port number
num-sessions-per-qam 1-80 processing-type remap start-program n jitter
10-200 msec [cbr | vbr]
exit
```

Configuration Example

The following is a sample in which two sessions are created per RF channel, HBO-1 and HBO-2 are for channel 0, HBO-3 and HBO-4 are for channel 1. The destination IP address is obtained from VCG (if any), otherwise from the LED broadcast.

```
Router(config)#cable video
Router(config-video)#table-based
Router(config-video-tb)#vcg bcast
Router(config-video-tb-vcg)#rf-channel 0-1
Router(config-video-tb-vcg-sess)# session HBO input-port 10 start-udp-port 1
num-sessions-per-qam 2 processing-type remap start-program 1 jitter 100 cbr
Router(config-video-tb-vcg-sess)# session HBO bundle-id 1 start-udp-port 49152
num-sessions-per-qam 2 processing-type program start-program 1 jitter 100 cbr
```

Virtual Edge Input Bundling

Virtual Edge Input Bundling assists with load balancing from the Head End. This allows multiple VEIs to be accessed via a gateway, since it is unknown at the time of configuration which VEI the stream will come in on. Thus, when the Head End sends a stream to the gateway, it enters the cBR-8 in on any VEI in the bundle. VEI bundling can be performed only if table based protocol is used for a particular LED.

To bundle the VEIs, perform the following steps:

Before You Begin

- All video sessions must have unique UDP ports for the Head End.
- Create two or more Virtual Edge Inputs using the following command:

```
virtual-edge-input-ip ipaddr vrf vrfname input-port-number #
```

Note Same IP address cannot be used in more than one bundle.

```
enable
configure terminal
cable video
logical-edge-device
protocol table-based
vei-bundle id input-port-number #
exit
```

Verifying Virtual Edge Input Data

To verify the VEI data, use the following command:

```
Router# show cable video logical-edge-device [all | id | name]
```

Example:

```
Router# show cable video logical-edge-device id 1
Logical Edge Device: led-vei
Id: 1
Protocol: Table-based
Service State: Active
```

```
Discovery State: Disable
Number of Virtual Carrier Groups: 1
Number of Share Virtual Edge Input: 5
Number of Physical Qams: 5
Number of Sessions: 0
No Reserve PID Range

Virtual Edge Input:
Input Port   VEI                  Slot/Bay     Bundle       Gateway
ID           IP                                ID           IP
-----------------------------------------------------------------
11           11.11.11.11          7/0          -            -
22           22.22.22.22          7/0          -            -
66           66.66.66.66          7/0          40000        177.0.10.3
77           77.77.77.77          7/0          40000        177.0.10.3
222          222.222.222.222      7/0          40000        177.0.10.3

Virtual Carrier Group:
ID  Name      Total    Total       Service-Distribution-Group   Service-Distribution-Group
              VEI      RF-channel  Name                         ID
-------------------------------------------------------------------------------------------
1   vcg-vei   5        5           sdg-vei                      1

Integrated   Physical  Admin  Operational  TSID  ONID   Output   VCG   SDG    Encryption
Cable        QAM ID    State  State                     Port     ID    ID     Capable
-------------------------------------------------------------------------------------------
7/0/3:0      208       ON     UP           0     0      1        1     1      clear
7/0/3:1      209       ON     UP           1     0      2        1     1      clear
7/0/3:2      210       ON     UP           2     0      3        1     1      clear
7/0/3:3      211       ON     UP           3     0      4        1     1      clear
7/0/3:4      212       ON     UP           4     0      5        1     1      clear
```

Verifying VEI Bundles

To view the VEI bundles, use the following command:

```
Router# show cable video vei-bundle all
```

Example:

This is a sample output of the show command that displays the VEI bundle details.

```
Router# show cable video vei-bundle all
Total VEI Bundles: 1
Bundle       LED          Input Port   VEI              Slot/Bay     Gateway
ID           ID           ID           IP                            IP
-------------------------------------------------------------------------------
40000        1            33           33.33.33.33      7/0          177.0.10.3
40000        1            44           44.44.44.44      7/0          177.0.10.3
40000        1            66           66.66.66.66      7/0          177.0.10.3
40000        1            77           77.77.77.77      7/0          177.0.10.3
40000        1            222          222.222.222.222  7/0          177.0.10.3
```

Configuration Example

The following is a sample in which five VEIs are created on VCG and bundled:

```
cable video
  service-distribution-group sdg-vei id 1
```

```
    rf-port integrated-cable 7/0/3
  virtual-carrier-group vcg-vei id 1
    virtual-edge-input-ip 111.111.111.111 input-port-number 111
    virtual-edge-input-ip 222.222.222.222 input-port-number 222
    virtual-edge-input-ip 33.33.33.33 input-port-number 33
    virtual-edge-input-ip 44.44.44.44 input-port-number 44
    virtual-edge-input-ip 55.55.55.55 vrf Video-VOD-Vrf input-port-number 55
    rf-channel 0-4 tsid 0-4 output-port-number 1-5
 virtual-carrier-group vcg-vei1 id 2
    virtual-edge-input-ip 111.111.111.111 input-port-number 111
    virtual-edge-input-ip 222.222.222.222 input-port-number 222
    virtual-edge-input-ip 33.33.33.33 input-port-number 33
    virtual-edge-input-ip 44.44.44.44 input-port-number 44
    rf-channel 5-10 tsid 5-10 output-port-number 5-10
bind-vcg
  vcg vcg-vei sdg sdg-vei
  vcg vcg-vei1sdg sdg-vei
logical-edge-device led-vei id 1
  protocol table-based
    virtual-edge-input-ip 11.11.11.11 input-port-number 11
    virtual-edge-input-ip 22.22.22.22 input-port-number 22
    virtual-edge-input-ip 66.66.66.66 input-port-number 66
    virtual-edge-input-ip 77.77.77.77 input-port-number 77
    virtual-edge-input-ip 222.222.222.222 vrf Mgmt-MPEG-video-intf-vrf input-port-number
222
 vcg vcg-vei
 vei-bundle 40000 input-port-number 33,44,66,77,222
active
```

10-6 UDP Port Mapping

Starting from Cisco IOS XE Fuji 16.9.1, 10-6 UDP port mapping feature is supported in the table-based configuration for VOD.

To be consistent and compatible with the existing configuration, this feature adds a 10-6 UDP port mapping method to identify that this LED supports the feature, and change UDP port number to an optional parameter in the table-based session configuration.

If table-based session is not configured and 10-6 UPD port mapping is enabled for the LED, then the system generates remap sessions configuration only. If table-based session is configured, user has the option to skip providing UDP port number if he/she wants the udp port number to be automatically generated by the system.

Restrictions for 10-6 UDP Port Mapping

In order to fit the output port number and program number in a 16-bit value to represent an UDP port number per VOD session, output port number must be configured in the range of 1 to 1024, and program number must be configured in the range of 1 to 63 per QAM channel. Due to this limitation, the configuration must follow this guideline, otherwise the UDP port mapping for table-based configuration will be rejected.

UDP port mapping feature supports remap sessions configuration for table-based protocol LED only.

Configuring 10-6 UDP Port Mapping

To configure the 10-6 UDP port mapping, perform the following steps:

```
cable video
logical-edge-device name[id id ]
protocol table-based
udp-port-mapping-method 10-6
```

If 10-6 mapping is used and no unicast remap session is configured for the VCG, table-based unicast remap sessions will be automatically created for each VCG with default setting and using the first input port configured on the VCG if any, otherwise it will use the input port from the LED. User doesn't need to explicitly provision the sessions.

Verifying 10-6 UDP Port Mapping Configuration

To verify if the 10-6 UDP port mapping is enabled, use **show cable video logical-edge-device** command as shown in the following example:

```
Router# show cable video logical-edge-device id 1
Logical Edge Device: LED_DVB
Id: 1
Protocol: Table-based
Service State: Active
Discovery State: Disable
10-6 UDP Port Mapping Enabled: Yes
Number of Virtual Carrier Groups: 3
Number of Share Virtual Edge Input: 3
Number of Physical Qams: 384
Number of Sessions: 0
No Reserve PID Range

Virtual Edge Input:
Input Port   VEI                  Slot/Bay     Bundle       Gateway
ID           IP                                ID           IP
-----------------------------------------------------------------
```

10-6 UDP Port Mapping Configuration Example

Below is an example of generated session CLI commands when LED detects a UDP port mapping method is 10-6 mapping, and no table-based session is configured for the VCG.

```
Router(config)# cable video
Router(config-video)# service-distribution-group SDG_DVB id 1
Router(config-video-sdg)# rf-port integrated-cable 8/0/0
Router(config-video)# service-distribution-group sg-1 id 2
Router(config-video-sdg)# rf-port integrated-cable 9/0/0
Router(config-video)# service-distribution-group sg-2 id 3
Router(config-video-sdg)# rf-port integrated-cable 7/0/0
Router(config-video)# virtual-carrier-group VCG_DVB id 1
Router(config-video-vcg)# virtual-edge-input-ip 174.103.1.1 input-port-number 2
Router(config-video-vcg)# encrypt
Router(config-video-vcg)# service-type narrowcast
Router(config-video-vcg)# rf-channel 0-4 tsid 100-104 output-port-number 10-14
Router(config-video)# virtual-carrier-group VCG_CLR id 2
Router(config-video-vcg)# virtual-edge-input-ip 174.104.1.1 input-port-number 3
Router(config-video-vcg)# service-type narrowcast
Router(config-video-vcg)# rf-channel 5-9 tsid 105-109 output-port-number 15-19
Router(config-video)# virtual-carrier-group vcg-1 id 3
```

```
Router(config-video-vcg)# virtual-edge-input-ip 174.101.1.1 input-port-number 1
Router(config-video-vcg)# service-type narrowcast
Router(config-video-vcg)# rf-channel 0-4 tsid 1-5 output-port-number 1-5
Router(config-video)# bind-vcg
Router(config-video-bd)# vcg VCG_DVB sdg SDG_DVB
Router(config-video-bd)# vcg vcg-1 sdg sg-1
Router(config-video-bd)# vcg VCG_CLR sdg sg-2
Router(config-video)# logical-edge-device LED_DVB id 1
Router(config-video-led)# protocol table-based
Router(config-video-led-protocol)# vcg VCG_DVB
Router(config-video-led-protocol)# vcg vcg-1
Router(config-video-led-protocol)# vcg VCG_CLR
Router(config-video-led-protocol)# virtual-edge-input-ip 10.1.1.1 input-port 4
Router(config-video-led-protocol)# virtual-edge-input-ip 10.2.2.2 input-port 5
Router(config-video-led-protocol)# virtual-edge-input-ip 10.3.3.3 input-port 6
Router(config-video-led-protocol)# vei-bundle 1 input-port 4, 5
Router(config-video-led-protocol)# vei-bundle 2 input-port 1, 3
Router(config-video-led-protocol)# udp-port-mapping-method 10-6
Router(config-video-led-protocol)# active
Router(config-video)# table-based
Router(config-video-tb)# vcg VCG_DVB
Router(config-video-tb-vcg)#rf-channel 0-4
Router(config-video-tb-vcg-sess)# session VCG_DVB input-port 2 num-sessions-per-qam 63
processing-type remap start-program 21 repeat
Router(config-video-tb)# vcg vcg-1
Router(config-video-tb-vcg)#rf-channel 0-4
Router(config-video-tb-vcg-sess)# session vcg-1 input-port 1 num-sessions-per-qam 63
processing-type remap start-program 21 repeat
Router(config-video-tb)# vcg VCG_CLR
Router(config-video-tb-vcg)#rf-channel 5-9
Router(config-video-tb-vcg-sess)#session VCG_CLR input-port 3 num-sessions-per-qam 63
processing-type remap start-program 21 repeat
Router(config-video-tb-vcg-sess)#session abc input-port 4 udp-port 1000 processing-type
passthru
```

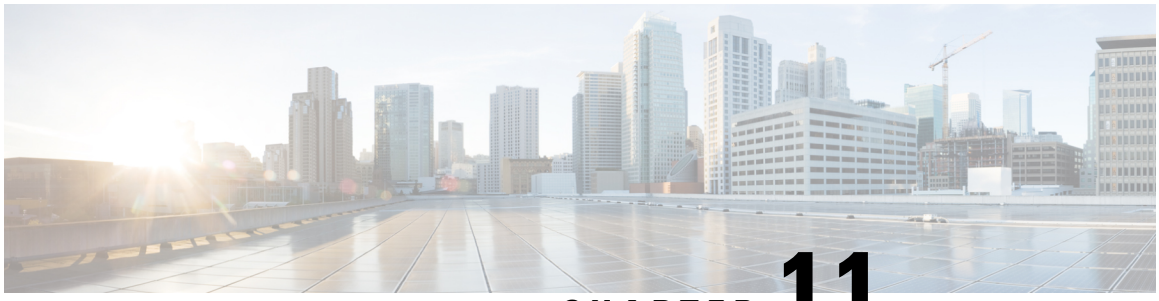
Feature Information for Table Based Configuration

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 https://cfnng.cisco.com/ 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 18: Feature Information for Table Based Configuration

Feature Name	Releases	Feature Information
Table based configuration	Cisco IOS XE Everest 16.6.1	This feature was integrated on the Cisco cBR Series Converged Broadband Routers.



CHAPTER 11

Management IP Interface

The management interface is used for the video control plane messages, such as session creation and deletion, between the Logical Edge Devices (LED) and the external Edge Resource Manager (ERM) server.

Contents

- Information About Management IP Interface , on page 65
- How to Configure the Management IP Interface, on page 65
- Configuration Examples, on page 68
- Feature Information for Management IP Interface, on page 68

Information About Management IP Interface

Video Logical Edge Device (LED) communicates with an external Edge Resource Manager (ERM) and a D6 server via the management interface. The physical interface for the connection is a front panel WAN port.

The following are the characteristics of the management interface:

- The management interface configuration is applied on both active and standby supervisor. However, only the active supervisor's management interface is connected to the external server.
- VirtualPortGroup interface must be configured prior to configuring the cable video management interface.
- Cable video management interface must be configured prior to configuring an LED that uses the management interface.

How to Configure the Management IP Interface

This section describes how to configure the management IP interface for the video session on Cisco cBR-8.

Configuring the Management IP Interface consists of the following three steps:

- Configuring the VirtualPortGroup Interface, on page 66
- Configuring the Cable Video Management Interface, on page 67
- Configuring the LED Management Interface, on page 67

Configuring the VirtualPortGroup Interface

First step towards configuring the Management IP Interface is to configure a VirtualPortGroup interface. You can also configure secondary IP addresses on the VirutalPortGroup interface, similar to a gigabit Ethernet interface IP address configuration.

To configure the VirtualPortGroup interface, complete the following procedure:

```
configure terminal
interface VirtualPortGroup virtual port group number
ip address ip address subnet-mask
ip address ip address subnet-mask secondary
end
```

Verifying the VirtualPortGroup Interface Configuration

To verify the VirtualPortGroup interface configuration, use the **show run interface VirtualPortGroup** command as shown in the example below:

```
show run interface VirtualPortGroup 0
Building configuration...

Current configuration : 145 bytes
!
interface VirtualPortGroup0
 ip address 1.22.3.1 255.255.255.0 secondary
 ip address 1.22.2.1 255.255.255.0
 no mop enabled
 no mop sysid
end
```

The VirtualPortGroup interface is in a down state. The interface comes up after the cable video management interface is configured.

Verifying the VirtualPortGroup Interface State

To verify the VirtualPortGroup interface state, use the **show interfaces VirtualPortGroup** command as shown in the example below:

```
show interfaces VirtualPortGroup 0
VirtualPortGroup0 is up, line protocol is up
  Hardware is Virtual Port Group, address is badb.ad09.7077 (bia badb.ad09.7077)
  Internet address is 1.22.2.1/24
  MTU 1500 bytes, BW 2500000 Kbit/sec, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not supported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output 00:24:14, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicasts)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
```

```
 0 packets output, 0 bytes, 0 underruns
 0 output errors, 0 collisions, 0 interface resets
 0 unknown protocol drops
 0 babbles, 0 late collision, 0 deferred
 0 lost carrier, 0 no carrier
 0 output buffer failures, 0 output buffers swapped out
```

Troubleshooting Tips

- To check if the management interface IP route is up, use the following command:

```
show ip interface brief | include VirtualPortGroup 0
VirtualPortGroup0 1.22.2.1 YES NVRAM up up
```

- To ping the VirtualPortGroup interface, use the following command:

```
ping 1.22.2.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.22.2.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Configuring the Cable Video Management Interface

Before You Begin

VirtualPortGroup interface must be configured before configuring the cable video management.

To configure the cable video management interface, complete the following procedure:

```
configure terminal
cable video
mgmt-interface VirtualPortGroup virtual port group number
end
```

Verifying the Cable Video Management Interface Configuration

To verify the VirtualPortGroup interface configuration, use the **show run | include mgmt-intf** command as shown in the example below:

```
show run | include mgmt-intf
  mgmt-intf VirtualPortGroup 0
```

Configuring the LED Management Interface

Before You Begin

- Cable video management interface must be configured before configuring an LED that uses the management interface.
- Management IP address and the VirtualPortGroup IP address must be in the same subnet. It is recommended that the management IP addresses (for LED with Protocol GQI, DVB, PME and D6) are configured starting at the VirtualPortGroup IP address plus 2 and incrementing or Broadcast address minus 3 and decrementing. Typically, the VirtualPortGroup IP address is network address plus 1. Then, network address plus 2 is used internally by cBR-8. If the VirtualPortGroup IP is the Broadcast address minus 1, then the Broadcast address minus 2 is used internally by cBR-8.

To configure the LED management interface, complete the following procedure:

```
configure terminal
cable video
logical-edge-device device name
protocol gqi
mgmt-ip management ip address
exit
```

Verifying the LED Management Interface Configuration

To verify the VirtualPortGroup interface state, use the **show run | begin logical-edge-device test** command as shown in the example below:

```
sh run | begin logical-edge-device test
logical-edge-device test id 2
protocol gqi
mgmt-ip 1.22.2.10
```

Troubleshooting Tips

To ping the management interface, use the following command:

```
video-LWR-S-C2# ping 1.22.2.10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.22.2.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Configuration Examples

This section provides configuration examples for the management IP interface.

Management IP Interface

The following example shows how to create a management IP interface:

```
configure terminal
interface VirtualPortGroup 0
ip address 1.23.2.1 255.255.255.0
cable video
mgmt-interface VirtualPortGroup 0
logical-edge-device test id 2
protocol gqi
mgmt-ip 1.23.2.10
exit
exit
```

Feature Information for Management IP Interface

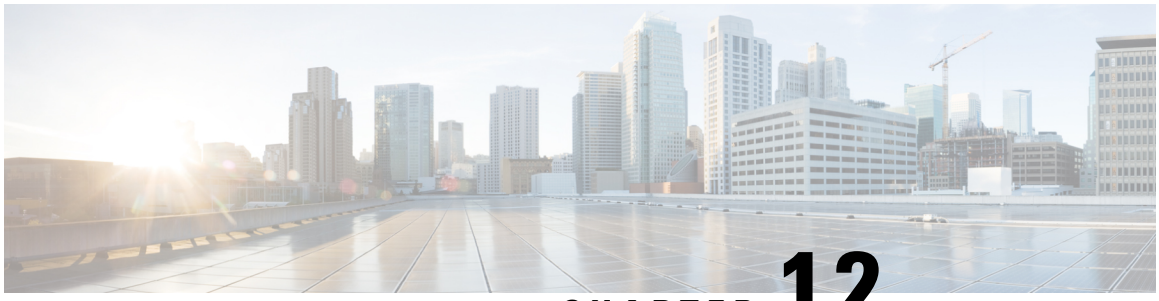
Use Cisco Feature Navigator to find information about the platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release,

feature set, or platform. To access Cisco Feature Navigator, go to the https://cfnng.cisco.com/ 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 19: Feature Information for Management IP Interface

Feature Name	Releases	Feature Information
Management IP Interface	Cisco IOS XE Everest 16.6.1	This feature was integrated on the Cisco cBR Series Converged Broadband Routers.



CHAPTER 12

Video Encryption

The Cisco cBR-8 supports PowerKey and Privacy Mode Encryption (PME) encryption CA systems for Video On Demand (VOD) sessions to address security concerns. However, only one encryption type can be installed on the line card. There are two levels to the CA system. The lower level encrypts the actual data streams. The upper level specifies the control words that are used to encrypt the data streams.

- Information About Encryption, on page 71
- How to Configure Encryption for the Data Stream, on page 72
- Configuration Examples for Encryption, on page 73
- Configuring Privacy Mode Encryption, on page 73
- Troubleshooting Video Encryption Issues, on page 76
- Feature Information for Encryption, on page 80

Information About Encryption

The encrypted sessions can be created on any QAM carriers on a line card. Only the Single Program Transport Stream (SPTS) VOD session can be encrypted. Encryption is not supported on the Pass-through, and Data-piping sessions.

The VOD session can be encrypted in any of the following types of encryption:

- PowerKey for video session management protocol GQI
- Privacy Mode Encryption (PME) for Table-based session
- Digital Video Broadcasting (DVB)

The scrambler mode varies based on the type of encryption, as given in the following table:

Table 20: Supported Encryption Types and Scrambler Modes

Encryption Type	Scrambler Mode
PowerKey	DES, 3DES
PME	DVS-042
DVB	DVB-CSA

Prerequisites for Encryption

You should configure the Virtual Carrier Group (VCG) to setup an encrypted session. For more details, see the Configuring Virtual Carrier Group, on page 72.

How to Configure Encryption for the Data Stream

This section describes how to configure encryption for the video session on Cisco cBR-8.

- Enforcing Data Stream Encryption Type, on page 72
- Configuring Virtual Carrier Group, on page 72
- Verifying Encryption Configuration, on page 73

Enforcing Data Stream Encryption Type

Note Once the line card and VCG are configured for PowerKey encryption, further configuration of the Cisco cBR-8 is not required.

To configure the encryption type for a VOD session, perform the following steps:

Before You Begin

Configure the Virtual Carrier Group (VCG) to setup an encrypted session. For more details, see .

```
enable
configure terminal
cable video
encryption
linecard slot/bay ca-system [dvb | pme | powerkey] scrambler scrambler-type
exit
```

Configuring Virtual Carrier Group

To configure the Virtual Carrier Group (VCG) for setting up an encrypted session, perform the following steps:

```
enable
configure terminal
cable video
virtual-carrier-group name [id #]
rf-channel start-channel#-end-channel# tsid start-tsid-end-tsid output-port-number
 start-number-end-num
virtual-edge-input ipaddr input-port-number #
encrypt
exit
```

Verifying Encryption Configuration

To verify the encryption configurations, use the following command:

show cable video encryption linecard [*all | slot number*]

Example 1:

```
Router#show cable video encryption linecard 7/0 Line card: 7/0
CA System Scrambler
==============================================
powerkey des
```

Example 2:

```
Router#show cable video encryption linecard all Line card: 7/0
CA System Scrambler
==============================================
powerkey des
```

Configuration Examples for Encryption

This section provides configuration examples for the Encryption feature.

Example: Enforcing Data Stream Encryption Type

The following is a sample in which the line card in slot 7 is configured for powerkey encryption.

```
Router(config)#cable video Router(config-video)#encryption
Router(config-video-encrypt)#linecard 7/0 ca-system powerkey scrambler des
```

Example: Configuring Virtual Carrier Group

The following is a sample in which the QAM channel from 64 to 158 are encryption capable if the virtual channels are successfully bound to a Service Distribution Group. The sessions created on those QAM carriers are encrypted using the scrambler installed on the line card.

```
Router(config)#cable video
Router(config-video)#virtual-carrier-group sdv-grp
Router(config-video-vcg)#rf-channel 64-158 tsid 64-158 output-port-number 64-158
Router(config-video-vcg)virtual-edge-input 14.1.1.1 input-port-number 1
Router(config-video-vcg)encrypt
Router(config-video-vcg)#exit
```

Configuring Privacy Mode Encryption

Only one device from the MSO site can communicate with the Encryption Renewal System (ERS) and obtain the latest ECM templates. The CEM communicates with the ERS and sends the ECM templates to the Cisco Edge QAM devices in the MSO site.

You can configure the following:

- VODS-ID—IDs assigned by CCAD or ARRIS to the MSO site. The configured VODS-ID on the Cisco cBR-8 and the CEM must be same.
- CEM IP—Interface IP of the Windows/Linux system through which the CEM can be reached by Cisco cBR-8.

- CEM Port—Port number on which the CEM listens for connections from the Cisco cBR-8.
- Management Interface—Source IP address of the Cisco cBR-8 virtual interface through which the connection must be established with the CEM server.

Note There can be only one entry for VODS-ID, CEM IP, CEM Port, and Management Interface IP. If you configure any new values for these parameters, the previous configuration is cleared. You can clear the configurations using the 'no' form of the command.

Configuring VODS-ID

To configure the VODS-ID of the CEM, perform the following steps:

```
enable
configure terminal
cable video
encryption
pme vodsid id
exit
```

Configuring CEM IP and Port

To configure the CEM IP and port of the CEM, perform the following steps:

```
enable
configure terminal
cable video
encryption
pme cem ip-address tcp_port
exit
```

Configuring Management IP

To configure the PME management IP address to establish CEM connection, perform the following steps:

Before You Begin

The virtual port group must be configured before configuring the management IP. For more information, see the *Configuring a VirtualPortGroup iIterface* section.

```
enable
configure terminal
cable video
encryption
pme mgmt-ip ip-address
exit
```

Verifying PME Connection Status

To verify the connection status between the Cisco Converged EdgeQAMManager (CEM) application and the Cisco cBR-8,use the following command:

show cable video encryption linecard [*all | slot number*]

This command displays the following information:

- VODS-ID—Specifies the configured VODS-ID on the CEM and Cisco cBR-8.
- CEM IP—Specifies the IP through which CEM can be reached by Cisco cBR-8.
- CEM Port—Specifies the port on which the CEM obtain connections from Cisco cBR-8.
- Local Mgmt IP—Specifies the Cisco cBR-8 interface through which the connection is established with the CEM.
- Local Port—Specifies the Local Port number assigned for the connection with the CEM.
- CEM Connection State—Specifies the status of the connection with the CEM (Connected (or) Not Connected).
- Count of ECMs recd—Specifies the count of ECMs received from the CEM.

Example:

This is a sample output of the show command that displays the connection status of PME.

```
Router#show cable video encryption pme status
PME Connection Status:
VODS-ID : 111
CEM IP : 1.200.1.163
CEM Port : 5000
Local Mgmt IP : 1.24.2.6
Local Port : 50394
CEM Connection State : Connected Count of ECMs recd : 2
```

Verifying PME Version

To verify the version information of the PME module loaded in the chassis, use the following command:

show cablevideo encryption pme version

The version information is read from the IOS PME subsystem. The version information displays in MAJOR.MINOR version format.

Example:

This is a sample output of the show command that displays the version details of PME.

```
Router#show cable video encryption pme version
PME Version: 1.0
```

Verifying PME Sessions on a Line Card

To verify the sessions that use the PME modules that are loaded on a specific line card, use the following command:

show cable video encryption pme linecard [*slot | bay*] **session** {*1-65535 | all | summary*}

Example 1:

This is a sample output of the show command that displays the session details that use PME modules.

```
Router#show cable video encryption pme linecard 7/0 session all Count of ECMG Streams: 4
==================== ECMG Stream DATA ========================
Stream
ID num EcmId CP# CwE CPDur NomCPD EcmRqst EcmRsp
---------- ---------- ---- --- ----- ------ ---------- ----------

0020(0032) 0020(0032) 0002 0 0 40000 7 2
0021(0033) 0021(0033) 0002 0 0 40000 7 2
0040(0064) 0040(0064) 0002 0 0 40000 7 2
0041(0065) 0041(0065) 0002 0 0 40000 7 2
video-LWR-B-A7B#show cable video encryption pme linecard 7/0 session 32 Stream 32, session
 7681 is active

Stream number = 32 Session number = 7681
ECM requests = 8 ECM replies = 2
ECM ID = 32 CryptoPeriod num = 2
CP duration = 0 Nominal duration = 40000
CA transfer mode = 1 Stream status = No Error Blob details

video-LWR-B-A7B#show cable video encryption pme linecard 7/0 session summary Currently
active streams:
Active = 4 ECM req/resp mismatch = 4
ECM req, all streams = 32 ECM resp, all streams = 8

Since last reset:
Sessions created = 4 Sessions deleted = 0
ECMs received = 2 ECMs discarded = 0
```

Troubleshooting Video Encryption Issues

A Video On Demand (VOD) session might fail at the subscriber site due to multiple factors. One of the factors is scrambling.

If scrambling fails during the VOD purchase, the Program Map Table is held back which in turn results in a VOD failure. Though there are alarms already available in the software that indicates the scrambling failure, it gives a high level error and does not provide information about the reason for the failure. These alarms are logged in syslog.

New Events and Alarms for Video Encryption Debugging

Cisco IOS-XE Release 16.12.1y supports New Events and Alarms for Video Scrambling Debugging Log Enhancement. The following new logs provide better debugging of VOD failures. All the new logs are written in btrace log of respective line card.

- Whenever a session under an encrypted VCG gets input to ACTIVE-PSI, the log will be written along with session id, on-id, ts-id and program number.
- Whenever the scrambling starts, the log will be written along with on-id, ts-id and program number.
- After the VoD ends and input goes to off state, a log will be written along with session id, on-id, ts-id and program number.
- If the scrambling fails for any session, then details about the failure will be logged along with the existing alarm in supervisor console.

You can use the **show platform software trace message lc-veman <LC slot number>/0** command to view the logs. See the following example:

```
Router# show platform software trace message lc-veman 8/0
This command is being deprecated. Please use 'show logging process' command.
executing cmd on chassis local ...


2020/02/03 03:34:05.046653 {veman_8-0}{1}: [scs] [7197]:  (warn):  02/03 20:34:04.477 [scs]:
 [7197]: (warning): PERFORMANCE: entering ScsTask too late (65 ms since last tick)

2020/02/03 03:34:05.046624 {veman_8-0}{1}: [scs] [7197]:  (warn):  02/03 20:34:04.179 [scs]:
 [7197]: (warning): PERFORMANCE: entering ScsTask too late (67 ms since last tick)

2020/02/03 03:34:05.046558 {veman_8-0}{1}: [scs] [7197]:  (warn):  02/03 20:34:04.073 [scs]:
 [7197]: (warning): PERFORMANCE: entering ScsTask too late (61 ms since last tick)
```

The following table shows all the new logs and alarms logged in the btrace log.

Table 21: New logs and alarms logged in the btrace log

Alarm/Event	Log Type	Log Message
Input ON	Event	I/p on Ses <session id> qam <on-id>/<ts-id> Sid <program number> qid <qam-id>
Input OFF	Event	I/p off Ses <session id> qam <on-id>/<ts-id> Sid <program number> qid <qam-id>
Scrambling started	Event	Scrambling started. Qam <on-id>/<ts-id> Sid <program number> SCG <SCG id>
Scrambling not started (no Input)	Alarm **Set/Clear**	(117) No i/p=Qam: <on-id>/<ts-id> Sid: <program number>
Scrambling not started (no ECMs)	Alarm **Set/Clear**	(19) No ECMs=CAS:<CAS-id> Qam: <on-id>/<ts-id> Sid: <program number>; SCG=<SCG id>
Scrambling not started (no ECMG)	Alarm **Set/Clear**	(19) Missing Ecmg/Timings; SuperCAS Id=<CAS Id>; ECM Id=1

- **Input ON**

  When a subscriber purchases a VOD session, the VOD asset stream is expected to be hitting the cBR8 input. Once the input stream is detected and the session gets to ACTIVE-PSI state, this information is logged along with the following information:

  - Session ID
  - QAM ID

- Original network ID
- Transport stream ID
- Program number

- **Input OFF**

  When the VoD ends, the input stream stops. The session will move to IDLE state after few milliseconds of input unavailability. After the Off timer, the session will move to OFF state during which this information is logged along with the following.

  - Session ID
  - QAM ID
  - Original network ID
  - Transport stream ID
  - Program number

- **Scrambling started**

  On VOD purchase, after all the required conditions are met for scrambling (Input stream availability, ECM availability, etc.,), the session will get scrambled. That event is logged with following information.

  - Original network ID
  - Transport stream ID
  - Program number
  - SCG ID

- **Scrambling not started (no input)**

  On VoD purchase, if the input VoD asset stream is not hitting the cBR8 for more than 10 seconds, then this alarm is set and logged in the btrace log. After this log is set, if the input starts hitting the cBR8 or if the VoD session is torn down, this alarm will be cleared and also be logged in the btrace log. This log has the following information.

  - Original network ID
  - Transport stream ID
  - Program number

Note This alarm is applicable only for Powerkey and DVB session-based scrambling.

- **Scrambling not started (no ECMs)**

  If the scrambling is not started due to unavailability of ECMs, then this alarm is set and logged in the btrace log. After this log is set, if the ECM is received or if the VoD session is torn down, this alarm will be cleared and also be logged in the btrace log. This log has the following information.

  - Original network ID

- Transport stream ID
- Program number
- CAS ID
- SCG ID

- **Scrambling not started (no ECMG)**

  If the scrambling is not started due to unavailability of ECMG server, then this alarm is set and logged in the btrace log. After this log is set, if the ECMG is connected or if the VoD session is torn down, this alarm will be cleared and also be logged in the btrace log. This log has the following information.

  - CAS ID
  - ECM ID

Note This alarm should never happen for Powerkey and PME scrambling.

Example Logs

Following are the example logs for the new events and alarms:

- **Input ON**

```
I/p on Ses 1048578 qam 65535/65041 Sid 65002 qid 9
```

- **Input OFF**

```
I/p off Ses 1048578 qam 65535/65041 Sid 65002 qid 9
```

- **Scrambling started**

```
Scrambling started. Qam 65535/65002 Sid 65041 SCG 1057576
```

- **Scrambling not started (no ECMs) Alarm set**

```
Set: (19) No ECMs=CAS:0x09520000 Qam:65535/65041 Sid:65002,=;SCG=1057576=;
```

- **Scrambling not started (no ECMs) Alarm clear**

```
Clear: (19) No ECMs=CAS:0x09520000 Qam:65535/65041 Sid:65002,=;SCG=1057576=;
```

- **Scrambling not started (no input) Alarm set**

```
Set: (117) No i/p=Qam:65535/65041 Sid:65002,=;
```

- **Scrambling not started (no input) Alarm clear**

```
Clear: (117) No i/p=Qam:65535/65041 Sid:65002,=;
```

- **Scrambling not started (no ECMG) Alarm set**

```
Set: (19) =Missing Ecmg/Timings=;SuperCAS Id=0x01230000=;ECM Id=1=;
```

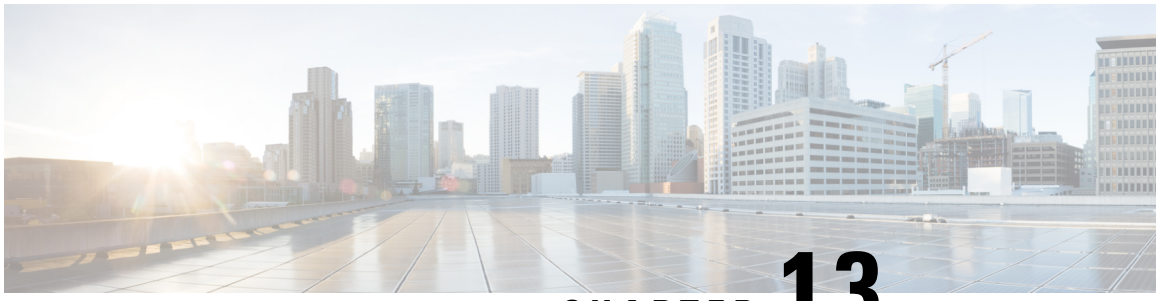
Feature Information for Encryption

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 https://cfnng.cisco.com/ 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 22: Feature Information for Encryption

Feature Name	Release	Feature Information
Encryption	Cisco IOS XE Everest 16.6.1	This feature was integrated on the Cisco cBR Series Converged Broadband Routers.
Video Encryption Debugging Log Enhancement	16.12.1y	This feature was integrated on the Cisco cBR Series Converged Broadband Routers.



CHAPTER 13

Global Video Configuration

You can perform some global configurations for provisioning the video services. These configurations have some default values. If you do not choose to change those values, the default values are used. The following sections describe the procedures for global configurations.

Contents

- Configuring the Default ONID, on page 81
- Configuring the Default PSI interval, on page 81
- Configuring Video Session Timeouts, on page 82
- Configure Video Interface IP, on page 82
- Configure Virtual Routing and Forwarding, on page 83
- Configuration Examples, on page 83
- Feature Information for Global Video Configuration, on page 84

Configuring the Default ONID

By default, the system ONID is 0, which is commonly used in North America. If the default value of the ONID is used, the TSID must be unique. You can change the default ONID. If you change the ONID, the TSID-ONID pair must be unique. The ONID must be in the range of 0 to 65535.

```
configure terminal
cable video
default-onid default onid number
```

Configuring the Default PSI interval

By default, the Program Specific Information (PSI) interval is 100 msec. You can change the default PSI interval. The PSI interval must be in the range of 40 to 1000.

```
configure terminal
cable video
default-psi-intervaldefault-psi-interval msec
```

Configuring Video Session Timeouts

The default video session init timeout is 1000 msec, the idle session timeout is 250 msec, and the off session timeout is 60 seconds. You can change these default values. The following are the permissible ranges for the timeouts:

- Init session timeout—100 to 60000
- Idle session timeout —100 to 5000
- Off session timeout —1 to 1800

```
configure terminal
cable video
timeout init-session timeout msec
timeout idle-session timeout msec
timeout off-session timeout sec
```

Configure Video Interface IP

The Cisco cBR-8 can automatically configure IP addresses of line card video interfaces. The Cisco cBR-8 uses IP addresses from a pool of IP addresses that you provide.

Use the **routing-interface-ip** command to set the video interface IP address for each CLC in the Cisco cBR-8. If the subnet size is 2, the Cisco cBR-8 sets the video interface IP address starting at Slot 0 to the IP address you provide. For subnet sizes greater than 2, the Cisco cBR-8 adds 1 to the IP address you provide and sets it as the video interface IP address. Do not use subnet 255.255.255.255. The Cisco cBR-8 sets the IP address of each subsequent video interface by incrementing IP address by the subnet size.

For example, executing the command **routing-interface-ip** *192.0.2.0 255.255.255.252* **secondary***198.51.100.0 255.255.255.252*, configures the video interfaces as follows:

Video Interface	Primary IP Address	Secondary IP Address	Subnet Mask	Subnet Size
Video 0/0/0	192.0.2.1	198.51.100.1	255.255.255.252	4
Video 0/0/1	192.0.2.5	198.51.100.5	255.255.255.252	4
Video 1/0/0	192.0.2.9	198.51.100.9	255.255.255.252	4
Video 1/0/1	192.0.2.13	198.51.100.13	255.255.255.252	4
Video 2/0/0	192.0.2.17	198.51.100.17	255.255.255.252	4
Video 2/0/1	192.0.2.21	198.51.100.21	255.255.255.252	4
Video 3/0/0	192.0.2.25	198.51.100.25	255.255.255.252	4
Video 6/0/0	192.0.2.33	198.51.100.33	255.255.255.252	4
Video 7/0/0	192.0.2.41	198.51.100.41	255.255.255.252	4
Video 7/0/1	192.0.2.45	198.51.100.45	255.255.255.252	4

Video 8/0/0	192.0.2.49	198.51.100.49	255.255.255.252	4
Video 8/0/1	192.0.2.53	198.51.100.53	255.255.255.252	4
Video 9/0/0	192.0.2.57	198.51.100.57	255.255.255.252	4
Video 9/0/1	192.0.2.61	198.51.100.61	255.255.255.252	4

Note

- Video interface IP configuration is optional. By default, the Cisco cBR-8 uses 10.100.x.x subnets for primary IP addresses and 10.101.x.x subnets for secondary IP addresses of video interfaces. Use the **routing-interface-ip** command only when the default configuration conflicts with the existing network.
- Configure the video interface IP before configuring any other video-specific configurations like logical edge device and virtual service group configurations.

Configure Virtual Routing and Forwarding

From Cisco IOS XE Amsterdam 17.3.1x, you can configure user-specific VRF to line card video interfaces. This configuration is to support video interfaces to participate in NX-GEN VPN.

Use the **routing-interface-vrf** command to configure user-specific VRF to line card video interfaces.

```
configure terminal
cable video
routing-interface-vrf slot slot vrf-name vrf-name
```

Note

- Virtual routing and forwarding configuration is optional. This configuration is not required in non-VPN deployments. By default the Cisco cBR-8 places all video interfaces in the VRF Mgmt-MPEG-video-intf.
- Configure VRF separately for each line card.
- Configure virtual routing and forwarding before configuring any other video-specific configurations like logical edge device and virtual service group configurations.

Configuration Examples

This section provides examples for the global video configuration.

Example: Global Video Configuration

```
configure terminal
cable video
default-onid 10
```

```
default- psi-interval 50
timeout init-session 200 msec
timeout idle-session 250 msec
timeout off-session 500 sec
```

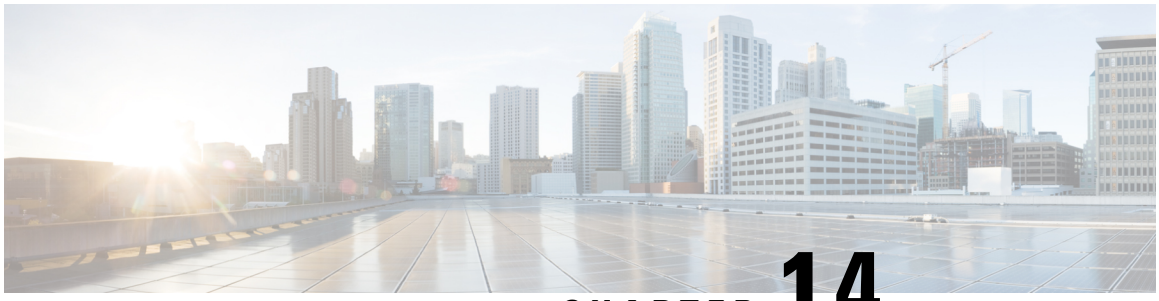
Feature Information for Global Video Configuration

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 https://cfnng.cisco.com/ 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 23: Feature Information for Global Video Configuration

Feature Name	Releases	Feature Information
Global Video Configuration	Cisco IOS XE Everest 16.6.1	This feature was integrated on the Cisco cBR Series Converged Broadband Routers.



CHAPTER 14

Advanced Video MPEG Features

Cisco cBR Series Converged Broadband Router supports the following video features.

- Information about Advanced Video MPEG Features, on page 85
- How to Configure Advanced Video MPEG Features, on page 85
- Configuration Examples for Advanced Video MPEG Features, on page 86
- Feature Information for Advanced Video MPEG Features, on page 86

Information about Advanced Video MPEG Features

Reserved Output PID Range

The reserved output PID range allows the user to specify a range of PIDs that will not be used as output for remapped sessions. A range of up to 4000 PIDs from 1-8190 can be reserved.

One continuous reserved PID range is supported for each chassis. Note that the protection is only good for future output remapped PIDs, so the reserved PID range is expected to be configured before any remapped sessions are created. Remapped PIDs within the reserved range that already exists will not be reallocated.

How to Configure Advanced Video MPEG Features

Configuring Reserved Output PID Range

To configure reserved output range, follow the steps below:

```
enable
configure terminal
cable video
reserve-pid-range start-pid-end-pid
```

Verifying Reserved Output PID Range Configuration

To verify the reserved output PID range configuration, use the **show cable video logical-edge-device id** *id* **reserve-pid-range** command as shown in the example below.

```
Router# show cable video logical-edge-device id 1 reserve-pid-range
Logical Edge Device: led1
Id: 1
Reserve PID Range: 1-4000
```

Configuration Examples for Advanced Video MPEG Features

This section provides configuration examples for the advanced video MPEG features:

Example: Configuring Reserved Output PID Range

The following example shows how to configure reserved output PID range.

```
enable
configure terminal
cable video
reserve-pid-range 4000-4100
```

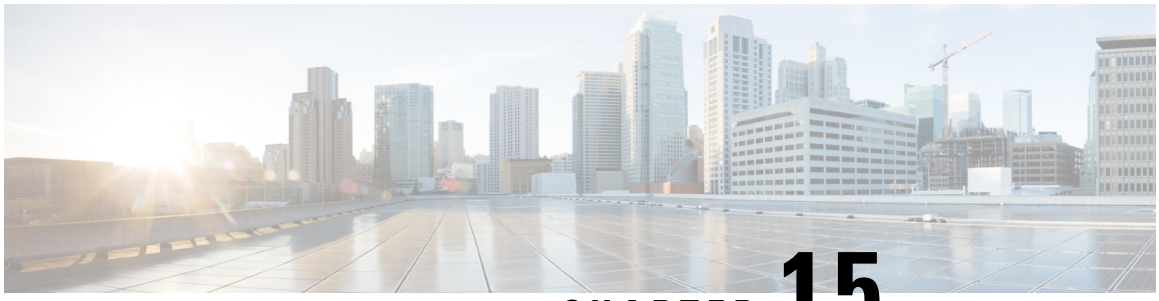
Feature Information for Advanced Video MPEG Features

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 https://cfnng.cisco.com/ 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 24: Feature Information for Advanced Video MPEG Features

Feature Name	Releases	Feature Information
Advanced Video MPEG Features	Cisco IOS XE Everest 16.6.1	This feature was integrated on the Cisco cBR Series Converged Broadband Routers.



CHAPTER 15

Important Notes

The following are some important notes for Management IP Interface and Virtual Routing Interface.

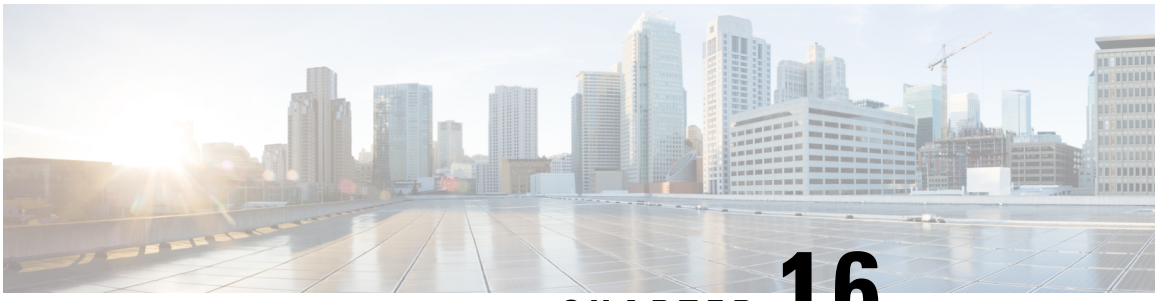
- Video Packet Routing Requirements, on page 87

Video Packet Routing Requirements

A routing protocol, such as OSPF or IS-IS, must be enabled on the cBR-8 in order for video data packets from the head end to reach the virtual QAMs. On the cBR-8, enable a routing protocol as described in the routing configuration guide.

Once the routing protocol is set up correctly, the cBR-8 will advertise the internal static routes for the video data path to the head end.

The user needs to configure the Virtual Edge Input (VEI) with a routable IP address from within the customer's network. More information, see Configuring Virtual Edge Input under Logical Edge Device.



CHAPTER 16

Cisco cBR-8 as Auxiliary Video Core

The Cisco cBR-8 Converged Broadband Router can act as the video core, the DOCSIS core, and the principal core in a cable network. This chapter describes the use of a Cisco cBR-8 Converged Broadband Router as an auxiliary video core.

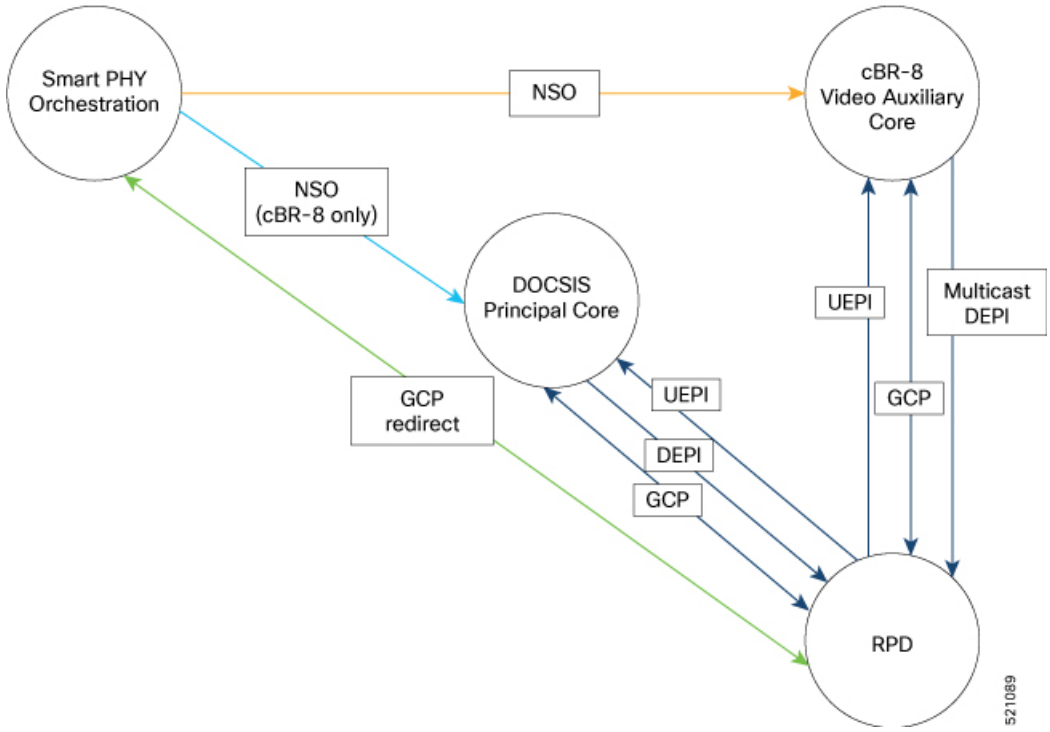
- Information About cBR-8 as Auxiliary Video Core, on page 89
- How to Configure cBR-8 as Auxiliary Video Core, on page 90
- Configuration Examples for cBR-8 as Auxiliary Video Core, on page 91
- Feature Information for cBR-8 as Auxiliary Video Core, on page 92

Information About cBR-8 as Auxiliary Video Core

The Cisco cBR-8 supports both Generic Control Protocol (GCP) and Downstream External PHY Interface (DEPI) control and data planes. From Cisco IOS XE Amsterdam 17.3.1w release, you can configure a Cisco cBR-8 as an Remote PHY Auxiliary Video Core. Use the Cisco cBR-8 as an Auxiliary Video Core to support video and OOB with a Cisco cnBR or to support video on a separate Cisco cBR-8 other than the DOCSIS core.

This feature allows configuring a Cisco cBR-8 as an auxiliary video core without having DOCSIS configuration on the same Cisco cBR-8. The auxiliary video core, the DOCSIS core, and the principal core interface separately with RPDs.

Figure 1: Remote PHY Architecture with a Cisco cBR-8 as Auxiliary Video Core



Limitations

When you configure separate Cisco cBR-8s as DOCSIS and video cores, you must avoid RF channel reuse. A combined cBR-8 DOCSIS and Video Core ensures that RF channel reuse does not occur. Error detection occurs only when an RPD receives the configuration.

How to Configure cBR-8 as Auxiliary Video Core

When you configure a Cisco cBR-8 as an auxiliary video core, downstream RPDs receive video configuration from the auxiliary video core. The RPDs receive DOCSIS configuration and other management configuration from the DOCSIS core and the principal core respectively. The DOCSIS core can also be the principal core.

You can configure the auxiliary core such that RPDs receive video, OOB, and NDF-NDR configurations. Alternately, you can configure these features on the principal core.

Note

- The Viavi system allows Narrowband Digital Forward (NDF) and Narrowband Digital Return (NDR) configuration only from the principal core as it relies on MIBs from the principal core.
- If the Auxiliary Video Core and RPD are in separate PTP domains, you have to configure the downstream controller-profile channel type as Video Async.

Configure DOCSIS Principal Core

To configure the DOCSIS principal core, run the following commands.

```
cable rpd <RPD name>
 identifier <RPD ID>
 rpd-ds <port-ID> downstream-pilot-tone profile <ID>
 core-interface <slot/subslot/port>
  principal
  rpd-ds <port-ID> downstream-cable <slot/subslot/port> profile <ID>
  rpd-us <port-ID> upstream-cable <slot/subslot/port> profile <ID>
 r-dti <ID>
 rpd-event profile <ID>
 rpd-55d1-us-event profile <ID>
```

Configure cBR-8 as Auxiliary Video Core

To configure a Cisco cBR-8 as an auxiliary video core, run the following commands.

```
cable rpd <RPD name>
 identifier <RPD ID>
 core-interface <slot/subslot/port>
  rpd-ds <ID> downstream-cable <slot/subslot/port> profile <ID>
 core-interface <slot/subslot/port>
  rpd-ds <ID> downstream-cable <slot/subslot/port> profile <ID>
  rpd-ds <ID> downstream-cable <slot/subslot/port> profile <ID>
 rpd-event profile <ID>
 rpd-55d1-us-event profile <ID>
```

Configuration Examples for cBR-8 as Auxiliary Video Core

Example: Configuring cBR-8 as Auxiliary Video Core

The following example shows how to configure a Cisco cBR-8 as an auxiliary video core.

```
cable rpd RPD-A
 identifier 0053.0014.be8e
 core-interface Te9/1/0
  rpd-ds 0 downstream-cable 9/0/1 profile 2
 core-interface Te9/1/6
  rpd-ds 0 downstream-cable 9/0/31 profile 31
  rpd-ds 0 downstream-cable 9/0/30 profile 32
 rpd-event profile 0
 rpd-55d1-us-event profile 0
```

Example: Configuring cBR-8 as Auxiliary Video and OOB Core

The following example shows how to configure a Cisco cBR-8 as auxiliary video and OOB core.

```
cable rpd RPD-A
 identifier 0053.0014.be8e
 core-interface Te9/1/0
  rpd-ds 0 downstream-cable 9/0/1 profile 2
  rpd-ds 0 downstream-oob-vom 1 profile 1
  rpd-us 0 upstream-oob-varpd 1 profile 1
 core-interface Te9/1/6
  rpd-ds 0 downstream-cable 9/0/31 profile 31
  rpd-ds 0 downstream-cable 9/0/30 profile 32
```

```
 rpd-event profile 0
 rpd-55d1-us-event profile 0
```

Example: Configuring DOCSIS Principal Core

The following example shows how to configure the DOCSIS principal core.

```
cable rpd RPD-RI01
 identifier 0053.0014.be8e
 rpd-ds 0 downstream-pilot-tone profile 1
 core-interface Te9/1/2
  principal
  rpd-ds 0 downstream-cable 9/0/8 profile 1
  rpd-us 0 upstream-cable 9/0/22 profile 1
 r-dti 2
 rpd-event profile 0
 rpd-55d1-us-event profile 0
```

Feature Information for cBR-8 as Auxiliary Video Core

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 https://cfnng.cisco.com/ 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.

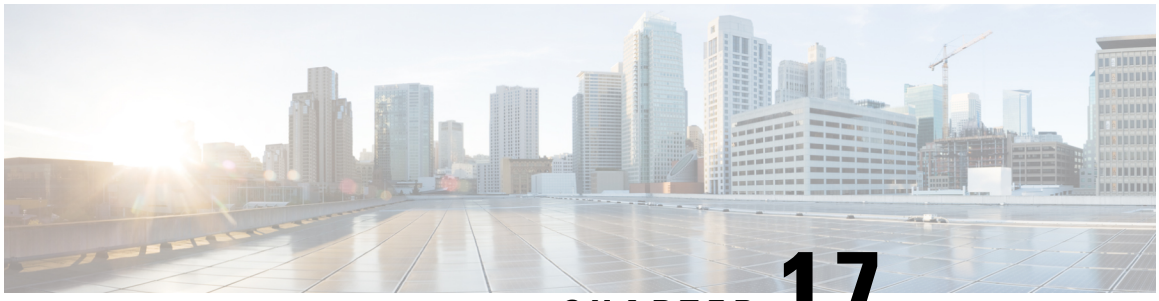
Table 25:

Feature Name	Release	Feature Information
cBR-8 as Auxiliary Video Core	Cisco IOS XE Amsterdam 17.3.1w	This feature was introduced on the Cisco cBR-8 Converged Broadband Router.

PART II

Cisco cBR Converged Broadband Routers Video Features

- PowerKEY VOD, on page 95
- DOCSIS Downstream Controllers, on page 105
- Simple Content Protection Video Session Support, on page 111
- Table-Based Video and VPME Encryption , on page 115
- PMV Support for Table-Based Videos, on page 131
- Video QAM Replication, on page 141
- D6 Discovery Protocol, on page 147
- Switched Digital Video, on page 157
- DVB Video on Demand, on page 169
- DualCrypt Encryption Mode Support, on page 179
- Low Latency VOD Support, on page 191
- Video MIBs, on page 197
- Expanded GQI Protocol Support, on page 201
- Advanced MPEG Features, on page 209
- Video Notifications, on page 221



CHAPTER 17

PowerKEY VOD

PowerKEY Video On Demand refers to video content that is chosen by the subscriber and streamed specifically to the subscriber. The content is encrypted using PowerKEY conditional access through a video session that is created on the Cisco cBR-8 specifically for each request.

Contents

- Information About PowerKEY VOD, on page 95
- How to Configure PowerKEY VOD, on page 95
- Configuration Examples, on page 101
- Feature Information for PowerKEY VOD, on page 102

Information About PowerKEY VOD

PowerKEY Video On Demand is used in a Cisco cable environment to provide edge-encrypted video-on-demand movies and other content to subscribers. The subscriber selects the content via an on-screen selection and the set-top box (STB) notifies the head-end of the request. The head-end equipment receives the request from the STB and triggers the Session Resource Manager (SRM) to create an encrypted video session on the Cisco cBR-8. At the same time, the video streamer is triggered to begin streaming the content in a UDP stream to the Cisco cBR-8. The Cisco cBR-8 receives an unscrambled video content, encrypts it using PowerKEY, combines the scrambled stream with other content destined for the RF carrier, and transmits the RF signal from the RF port.

PowerKEY VOD allows the operator to provide secure, encrypted video streams to a particular subscriber over the RF plant.

Overview of PowerKEY VOD

PowerKEY VOD allows the operator to provide secure, encrypted video streams to a particular subscriber over the RF plant.

How to Configure PowerKEY VOD

- Configuring the Encryption Type on the Line Card
- Configuring the Encrypted Virtual Carrier Groups

- Configuring the Service Distribution Groups and Binding
- Configuring the Logical Edge Device and GQI Protocol
- Verifying the PowerKEY VOD Configuration

Configuring the Encryption Type on the Line Card

The Cisco IOS-XE Release 16.5.1 supports PowerKey and PME encryption CA systems, but allows only one encryption type to be installed on the line card. There are two levels in the CA system. The lower level scrambler, which encrypts the actual data streams and the upper level conditional access system, which handles how the control words are transferred from the encrypting device to the decrypting device.

To specify the type of encryption used to scramble the data streams, complete the following procedure:

```
configure terminal
cable video
encryption
linecard slot/bay ca-system [pme | powerkey] scrambler scrambler-type
exit
```

PowerKey currently supports DES and Privacy Mode Encryption (PME) supports DVS-042 type of encryption, as given in the following table:

Table 26: Supported Encryption Types and Scrambler Modes

Encryption Type	Scrambler Mode
PME	DVS-042
PKEY	DES

Verifying the Encryption Configuration

To verify the encryption type of a line card, use the **show cable video encryption linecard** command as shown in the example below:

```
show cable video encryption linecard 7/0
Line card: 7/0
CA System       Scrambler
================================
powerkey        des
```

Configuring the Encrypted Virtual Carrier Groups

For the sessions to be encrypted on the Cisco cBR-8, the Virtual Carrier Groups (VCGs) must be specified as **encrypt** and the line card must be configured as encrypted. In this way, the operator can choose the carriers on the line card that support encryption and other carriers that support only clear or pre-encrypted sessions. Each encrypted carrier consumes an encrypted carrier license.

For the VCG to be used in a Logical Edge Device (LED) that is configured with the GQI protocol, each RF carrier must be assigned with an output port number. The LED must be configured with the Generic QAM Interface (GQI) protocol in order to support session-based operation.

Note For PowerKEY VOD, you have to specify the session-based operation.

To configure the VCG, complete the following procedure:

```
configure terminal
cable video
virtual-carrier-group vcg-name
rf-channel channel range tsid tsid range output-port-number port num range
virtual-edge-input ip-address [vrf] vrf name input-port-number number
encrypt
exit
```

Verifying the Encrypted Virtual Carrier Groups Configuration

To verify the encrypted VCGs configuration, use the **show cable video virtual-carrier-group name** command as shown in the example below:

```
show cable video virtual-carrier-group name vod-grp
```

Configuring the Service Distribution Groups and Binding

The Service Distribution Group (SDG) is a collection of one or more RF ports and defines the physical slot/bay/port to be used in a video service. After you configure an SDG, you can bind a VCG to an SDG. The binding connects the carriers defined in the VCG to the physical port listed in the SDG. After binding, a path from the Virtual Edge Input (VEI) is mapped to the RF ports.

To configure the SDGs and binding, complete the following procedure:

```
configure terminal
cable video
service-distribution-group sdg name id sdg number
onid onid for port
rf-port integrated-cable slot/bay/port
exit
bind-vcg
vcg vcg-name sdg sdg-name
end
```

Configuring the Logical Edge Device and GQI Protocol

The PowerKEY VOD feature on the Cisco cBR-8 is directed by an external Session Resource Manager (SRM) that creates video sessions in response to a subscriber selecting VOD content to watch on the set top box. You must configure a Logical Edge Device (LED) supporting the GQI protocol on the Cisco cBR-8 to support the PowerKEY VOD.

The LED is configured with the GQI protocol as the LED communicates with an external SRM using the GQI protocol. The GQI protocol supports the creation and deletion of sessions on the carriers owned by this LED.

Tip Use the following command to get the chassis MAC address:

```
Router#show diag all eeprom detail | include MAC
Chassis MAC Address : 54a2.740e.2000
MAC Address block size : 1024
```

Using the Chassis MAC as a basis, increment the least significant number to give a unique identifier (mac-address) for each LED. This number needs to be unique with respect to the GQI server and does not really relate to a true MAC address. Thus, the number is irrelevant, but needs to be unique.

To configure the Logical Edge Device and GQI Protocol, complete the following procedure:

```
configure terminal
cable video
logical-edge-device led name id led number
protocol gqi
mgmt-ip management ip address
mac-address mac address from this chassis range
server ip address of srm
virtual-edge-input-ip ip addr for content [vrf] vrf name input-port-number num
vcg virtual edge qam name (may be multiple vcgs in an LED)
active n
end
```

Verifying the PowerKEY VOD Configuration

The PowerKEY encrypted VOD LED is active and communicates with the external SRM device after configuring the encryption type on the line card, VCGs, binding of SDGs, and LED with GQI protocol are completed.

To verify the Logical Edge Device configuration, use the **show cable video logical-edge-device name** *led name* command (or) **show cable video logical-edge-device id** *led number* command as shown in the example below:

```
show cable video logical-edge-device name pkvodled
Logical Edge Device: pkvodled
Id: 1
Protocol: GQI
Service State: Active
Discovery State: Disable
Management IP: 1.23.2.10
MAC Address: 54a2.740d.dc99
Number of Servers: 1
Server 1: 1.200.3.75
Reset Interval: 8
Keepalive Interval: 10    Retry Count:3
Number of Virtual Carrier Groups: 1
Number of Share Virtual Edge Input: 1
Number of Physical Qams: 20
Number of Sessions: 0
No Reserve PID Range

Virtual Edge Input:
Input Port   VEI              Slot/Bay     Bundle       Gateway
ID           IP                            ID           IP
```

```
-----------------------------------------------------------------
1            174.10.2.1          7/0          -            -
```

Verify the following:

- The service state of the LED should be active and the other fields must be same as the configured values.
- The connection to the remote SRM should be displayed to ensure that there is a valid network connection to the SRM.
- Execute the **show cable video gqi connections** command. The following is the sample output when the connection is not established to the SRM :

```
LED Management Server     Connection    Version Event   Reset      Encryption
ID  IP         IP         Status                Pending Indication Discovery
-------------------------------------------------------------------------------
1   1.23.2.10  1.200.3.75 Not Connected  0      0       Not Sent   Not Sent
```

The following is the sample output when the connection is established to the SRM:

```
LED Management Server     Connection    Version Event   Reset      Encryption
ID  IP         IP         Status                Pending Indication Discovery
-------------------------------------------------------------------------------
1   1.23.2.10  1.200.3.75 Not Connected 2       0       ACKED      ACKED
```

Once the connection is established, the SRM may create encrypted sessions on the carriers of the LED.

- To view the encrypted sessions, use the **show cable video session logical-edge-device id** *led name* **summary** command as shown in the example below:

```
show cable video session logical-edge-device id  1summary
Video Session Summary:

Active    : 1        Init      : 0         Idle      : 0
Off       : 0        Blocked   : 0         PSI-Ready : 1
UDP       : 1        ASM       : 0         SSM       : 0
Remap     : 1        Data      : 0         Passthru  : 0
Total Sessions: 1
```

- The individual session information can be displayed for the entire LED, for a particular port or line card. The details of a single session may be displayed by specifying a session-id or session-name. To display all the sessions on the LED, use the **show cable video session logical-edge-device name** *led name* command as shown in the example below:

```
show cable video session logical-edge-device name pkvodled
Total Sessions = 1

Session Output Streaming Session Destination UDP   Output  Input      Output Input
Id      Port   Type      Type               Port  Program State      State  Bitrate
-------------------------------------------------------------------------------------
1048576 1      Remap     UDP    174.101.1.1  4915  1       ACTIVE-PSI ON     732788

Output  Encrypt  Encrypt    Session
Bitrate Type     Status     Name
---------------------------------
1715446 PowerKey Encrypted  0x0000000000001
```

If the session is encrypted and transmitted properly, the session is displayed as shown in the above example. The input state is "ACTIVE-PSI". The output state is "ON". For PowerKEY encrypted sessions, the Encrypt Type will be "PowerKey" and the Encrypt Status will be "Encrypted".

If the session is created as a clear session, then the Encrypt Type will be "CLEAR" and the Encrypt Status will be "-".

If the GQI connection is not in connected state or if the sessions are not in the proper states then, troubleshoot the connection. For more information, see Troubleshooting Tips, on page 100.

Troubleshooting Tips

GQI Connection

GQI connection problems can be the result of a problem in the network, such as a problem in the external SRM device, or in the Cisco cBR-8 configuration. The first problem is beyond the scope of this document, however to verify the Cisco cBR-8 configuration, the management interface port must be configured properly and be active (not shutdown).

Session Input State

- If a session's input state is "OFF" or another state that is not "ACTIVE_PSI" then the problem is related to content receiving on the Cisco cBR-8. This could be a problem elsewhere in the head-end network or with the video streaming device. The Virtual Edge Input address specified in the LED should match the destination IP address used by the streaming device.

  To display the LED, use the following command:

  show cable video logical-edge-device id *led number*

- The Virtual Edge Inputs are listed in the output. Check the streaming device to ensure the destination IP address matches the appropriate VEI. Additionally, verify whether the UDP port of the video content from the streamer matches the UDP port shown in the session display on the Cisco cBR-8, using the following command:

  show cable video session logical-edge-device id *led number*

- The TenGigabitEthernet port where the VEI address is routed must not be in the shutdown state. To check the appropriate interface, use the following command:

  show interface TenGigabitEthernet *slot/bay/port*

Session Output State

- If a session's input state is "Active-PSI" and the output state is not "OFF", then the problem is related to the physical port channel configuration. The output of the **show logical edge device** command also shows all the carriers and their Admin and Operation state.

  To display the carriers and their state, use the following command:

  show cable video scg logical-edge-device id *number*

```
show cable video logical-edge-device id number
Integrated Physical Admin Operational TSID ONID Output VCG   SDG  Encryption
Cable      QAM ID   State State                Port   ID    ID   Capable
-------------------------------------------------------------------------
8/0/0:0    0        ON    UP           1   100   1     1    1     powerkey
```

```
8/0/0:1    1        ON    UP          2   100   2     1    1     powerkey
8/0/0:2    2        ON    UP          3   100   3     1    1     powerkey
8/0/0:3    3        ON    UP          4   100   4     1    1     powerkey
```

- If the output port corresponding to the session does not show "ON" for Admin State and an Operational State as "UP", then there is a problem with the configuration.To display the output port details, use the following command:

  show cable video output-port *output port number*

Session Encrypt Status

- If an encrypted GQI session has an Output State or Encrypt Status of "Pending", it means there is a problem with the PowerKEY encryption of the session, or it is possible the encryption on the session is just getting ready to start. First the session command should be executed over a few seconds to ensure that the session was not transitioning from Pending to Active. If the state is Pending, then there is a problem with the encryption.

  To troubleshoot this problem the operator can check the Scrambling Control Group (SCG) that corresponds to this session. Using the session id from the session display, the SCG ID can be found using the following command:

  show cable video scg logical-edge-device id*led number*

```
LED 1 has 8137 SCGs on 128 carriers

SCG ID     Session ID  LED   TSID  ONID
----------------------------------------
68157683   1048819     1     1     100
68157684   1048820     1     1     100
```

  To verify the SCG ID of the session, use the following command:

  show cable video scg logical-edge-device id *led number* | **inc** *session id*

```
68157684   1048820     1     1     100
```

  To verfiy the SCG session information, use the following command:

  show cable video scg id *SCG id*

```
SCGid: 68157684
Status: SUCCESS
TSID:    1
ONID:  100
Nominal CP: 550
```

  If the Status does not show SUCCESS, then there must be a problem with the Encrypted Key exchange between the Cisco cBR-8 and SRM.

Configuration Examples

This section provides configuration examples for the PowerKEY VOD feature:

Example: Configuring Encryption Type on the Line Card

The following example shows how to create a management IP interface:

```
configure terminal
cable video
encryption
linecard 7/0 ca-system powerkey  scrambler des
exit
```

Example: Configuring Encrypted Virtual Carrier Groups

The following example shows how to configure the QAM channels from 64 to 158. These channels are encryption capable once the VCG is successfully bound to a Service Distribution Group. The sessions created on these QAM carriers are encrypted using the scrambler installed on the line card.

```
configure terminal
cable video
virtual-carrier-group vod-group
rf-channel 64-158 tsid 64-158 output-port-number 64-158
virtual-edge-input-ip14.1.1.1 input-port-number 1
virtual-edge-input-ip14.2.1.1 vrf Video-VOD-Vrfinput-port-number 2
encrypt
exit
```

Example: Configuring Service Distribution Groups and Binding

The following example shows how to configure the service distribution groups and binding:

```
configure terminal
cable video
logical-edge-device pkvodled id 1
protocol gqi
mgmt-ip 1.20.2.10
mac-address 54ab.6409.dc99
server 1.200.3.75
virtual-edge-input-ip 174.10.2.1 input-port-number 1
virtual-edge-input-ip 174.11.2.1 vrf Video-VOD-Vrfinput-port-number 2
vcg vod-grp
active n
end
```

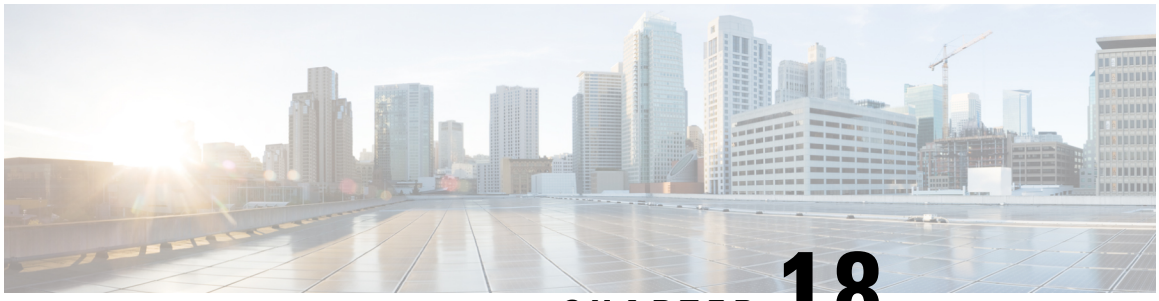
Feature Information for PowerKEY VOD

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 https://cfnng.cisco.com/ 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 27: Feature Information for PowerKEY VOD

Feature Name	Releases	Feature Information
PowerKEY VOD	Cisco IOS XE Everest 16.6.1	This feature was integrated on the Cisco cBR Series Converged Broadband Routers.



CHAPTER 18

DOCSIS Downstream Controllers

The table lists the features, the Cisco cBR version in which it was introduced, and also gives a short description of the feature.

Table 28: Feature History

Feature Name	Release Information	Feature Description
DOCSIS Downstream Controllers	Cisco IOS XE Bengaluru 17.6.1a	This release supports 32 DOCSIS controllers and 32 video controllers on the CBR-CCAP-LC-G2-R line card.

Cisco cBR-8 routers support DOCSIS with 32 DOCSIS controllers and 32 video controllers on the CBR-CCAP-LC-G2-R line card. The CBR-CCAP-LC-40G-R line card supports 32 downstream controllers. The 32 video SGs (downstream-video) are supported in addition to the existing 32 SGs (downstream-cable).

Downstream-cable supports both DOCSIS and video channels. If you want to increase the number of DOCSIS channels, move the video channels from downstream-cable to downstream-video so that you can avail all 32 downstream-cable controllers for DOCSIS.

Configure the DOCSIS channel in the legacy downstream-cable and the video channel in the new downstream-video.

You can choose downstream-video controllers option in the following two ways:

- The Service Distribution Group (SDG) configuration under cable video contains the option
- The Core configuration in the cable RPD configuration

  The controller profile with the new video option helps to bind to the downstream-video controllers.

- Configure Video Controllers, on page 105
- Verify Video Controller-Profile, on page 106
- Examples of Video Configuration, on page 109

Configure Video Controllers

For Remote PHY line cards, SDG specifies the line card, bay, and downstream cable-controller where the video is destined. Use RPD `downstream-cable slot/bay/controller` command instead of `rf-port`

`integrated-cable slot/bay/port` command. You can specify only one downstream cable controller for an SDG. Hence, cBR-8 routers do not support.

So there are two types of controllers in RPHY:

downstream-cable: `rpd downstream-cable slot/bay/controller`

downstream-video: `rpd downstream-video slot/bay/controller`

Cisco RPD 1x2 can join up to 30 multicast streams simultaneously for video. The Cisco HA Shelf can join up to 30 multicast streams simultaneously for each RPD for video.

Configure Video Controller-Profile

Use the following sample command to configure the video controller profile.

Use different profile IDs for the cable downstream controller-profile video and cable downstream controller-profile.

```
Router(config)#cable downstream controller-profile 10 ?
  I-CMTS  Configure I-CMTS controller profile
  RPHY    Configure RPHY controller profile (default)
  Video   Configure Video controller profile
  copy    Copy configuration from exist controller profile
  <cr>    <cr>

Router(config)#cable downstream controller-profile 10 video
Router(config-controller-profile)#
```

Note Add the keyword `video` to the controller profile. Otherwise, you cannot associate the profile to the downstream-video controller.

Configure RF Channel Type

You can configure only the video RF channels under the video controller-profile.

Use the following command to configure RF channel type:

```
Router(config-controller-profile)#rf 0 7
Router(config-prof-rf-chan)#type ?
  video  VIDEO (Asynchronous Mode)
```

Bind Video Controller to RPD DS Port

Use the following command to bind the video controller to an RPD DS port:

```
Router(config-rpd-core)#rpd-ds 0 downstream-video 1/0/?
  <0-31>  Controller port number
```

Verify Video Controller-Profile

Use the following command to verify the video controller-profile:

```
Router#show cable downstream controller-profile configured
Configured downstream controller-profiles:
I-CMTS
0   1

RPHY
99  101 134 195 197 199 200 221 223 225
227 249

VIDEO
2   10
```

Verify a Single Video Controller-Profile

Use the following command to verify a specific video controller-profile:

```
Router#show cable downstream controller-profile 2
Downstream controller-profile 2, type Video
Description:
Video controller-profile is being used by controller Downstream-Video:
  1/0/0, 1/0/3,
  Admin:  UP
  MaxOfdmSpectrum: 0
  MaxCarrier: 158
  Mode: normal
  Free freq block list has 2 blocks:
    45000000  - 264999999
    271000000 - 1217999999
  DS Splitting: No
  OFDM frequency exclusion bands: None
Configured RF Channels:
Chan Admin Frequency  Type        Annex Mod  srate Qam-profile  dcid  output
 0    UP   268000000  VIDEO-ASYNC  B    64    5057  0           -     NORMAL
```

Verify Video Controller-Profile Association

Use the following command to verify the video controller-profile association:

```
Router#show cable downstream controller-profile association
I-CMTS
Controller Integrated-Cable   Downstream controller-profile id
None

RPHY
Controller Downstream-Cable   Downstream controller-profile id
9/0/11                        223

Video
Controller Downstream-Video   Downstream controller-profile id
1/0/0                         2
1/0/3                         2
```

Debug Video Controller-Profile

Use the following sample command to debug the video controller-profile.

```
Router#debug cable controller-profile ?
  ds     Enable DS controller profile debug
  us     Enable US controller profile debug
  video  Enable Video controller profile debug

Router#debug cable controller-profile video
Video Controller Profile debugging is on
```

Show Details of All Video Controller Configurations

```
Router#show cable video downstream-video all

QAM           Port       TSID  ONID  Output  Physical     Admin      Operational
Virtual-Carrier-Group            Service-Distribution-Group       Logical-Edge-Device
         Encryption Total
Controller    Type                   Port    QAM ID       State      State        Name
                         Name                             Name
 Capable    Sessions
-----------------------------------------------------------------------------------------------
9/0/3:4       RPHY       -     -     0       160          ON         UP           -
                         -                                -
 clear      0
9/0/3:5       RPHY       -     -     0       161          ON         UP           -
                         -                                -
 clear      0
9/0/3:6       RPHY       -     -     0       162          ON         UP           -
                         -                                -
 clear      0
9/0/3:7       RPHY       -     -     0       163          ON         UP           -
                         -                                -
 clear      0
9/0/3:8       RPHY       -     -     0       164          ON         UP           -
                         -                                -
 clear      0
 --More--

Router#show cable video downstream-video 9/0/3 rf-channel 20

Downstream-Cable: 9/0/35
RF Channel: 20
TSID: 20
ONID: 0
Physical QAM ID: 176
Admin State: ON
Operational State: UP
Virtual Carrier Group Name: vcg_R
Virtual Carrier Group ID: 8
Service Distribution Group Name: sdg-R
Service Distribution Group ID: 9
Logical Edge Device Name: led-R
Logical Edge Device ID: 2
Total Bandwidth: 38810700 bps
Available Bandwidth: 38810700 bps
Oversubscribed Bandwidth: 0 bps
Total Sessions: 1

show cable video session logical-edge-device id 2 downstream-video 9/0/3 summary
CHN3-RACK3-RPHY#$l-edge-device id 2 downstream-video 9/0/3 summary
Video Session Summary For Chassis:

Active    : 0               Init      : 0                Idle       : 0
Off       : 1               Blocked   : 0                PSI-Ready  : 0
UDP       : 1               ASM       : 0                SSM        : 0
Remap     : 1               Data      : 0                Passthru   : 0
Remux     : 0               Pending   : 0                Encrypted  : 0
Low Latency: 0

Total Sessions       : 1
Total Input Bitrate  : 0 BPS
Total Output Bitrate : 0 BPS

Router#$show cable video session logical-edge-device id 2 downstream-video 9/0/3
Total Sessions = 1
```

```
Session    Output Frequency  Streaming   Sess Session Source                 UDP   Input
  Output  Input      Output  Input    Output   Encrypt        Encrypt        Low PMV
Session
Id         Port   Hz         Type        Type Ucast Dest IP/Mcast IP (S,G)    Port  Program
 Program State      State   Bitrate  Bitrate  Type           Status         Lat NUM   Name
-------------------------------------------------------------------------------------------
2097152    20     221000000  Remap       UDP  171.113.2.21                    49520 -
  1       OFF        ON      0        0        CLEAR          -              N   -
test_video.9.0.2.20.49520
```

```
show cable video session logical-edge-device id 2 downstream-video 9/0/3 debug
Router#$ion logical-edge-device id 2 downstream-video 9/0/3 debug
Total Sessions = 1

Session    Output Output
|<------------------Input------------------>|<------------------Output------------------>|
Id         Port   Prog    Sync-Loss CC-Err    PCR-Jump  UnderFlow OverFlow  Block     Dropped
   Overrun   Error     Block     Overdue   Inv-Rate  UnderFlow OverFlow  Dropped
-------------------------------------------------------------------------------------------
2097152    20     1       0         0         0         0         0         0         0
      0         0         0         0         0         0         0         0
```

Examples of Video Configuration

This section provides examples of the configuration.

```
Router(config)#cable downstream controller-profile 99 ?
  I-CMTS  Configure I-CMTS controller profile
  RPHY    Configure RPHY controller profile (default)
  Video   Configure Video controller profile
  copy    Copy configuration from exist controller profile
  <cr>    <cr>

Router(config)#cable downstream controller-profile 99 video
Router(config-controller-profile)#
```

Video Service Group Configuration

Manually, create video service groups (VSG) in the Cisco cBR-8 router, before you configure video service for each RPD. Provide a logical name for the VSG.

```
cable virtual-service-group 18584 downstream-cable 1/0/8 profile 101
cable virtual-service-group 18585 downstream-cable 1/0/9 profile 101
cable virtual-service-group 18586 downstream-cable 1/0/10 profile 101
cable virtual-service-group 18587 downstream-cable 1/0/11 profile 101
cable virtual-service-group 18588 downstream-cable 1/0/24 profile 101
cable virtual-service-group 18589 downstream-cable 1/0/25 profile 101
cable virtual-service-group 18590 downstream-cable 1/0/26 profile 101
```

Video Profile

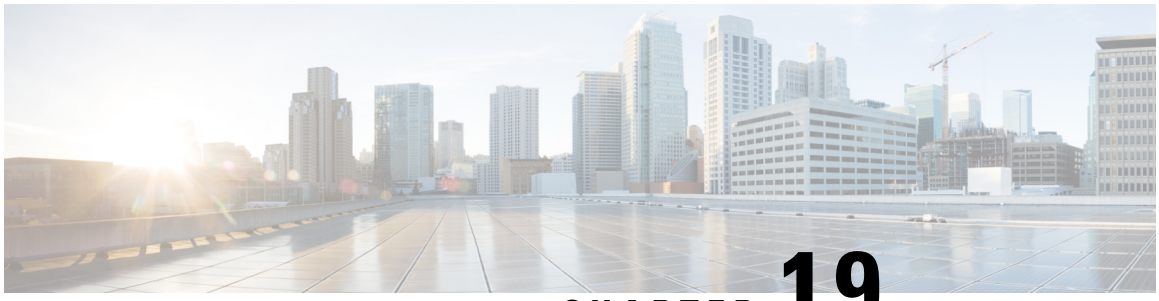
```
cable downstream controller-profile 99 Video
 description Test_Downstream_Video_Controller
 max-carrier 158
 rf-chan 4 35
  type VIDEO SYNC
  qam-profile 1
  frequency 125000000
  rf-output NORMAL
```

SDG Configuration

```
cable video
service-distribution-group sdg-video id 9
    rpd downstream-video 9/0/3
```

RPD Configuration

```
cable rpd LC9_RPD0_RACK5_6x12_SHF2
 description RPD0_RACK5_6x12_SHF2
 identifier f86b.d9ff.fafc
 core-interface Te9/1/0
  principal
  rpd-ds 0 downstream-cable 9/0/4 profile 10
  rpd-ds 0 downstream-video 9/0/3 profile 99
  rpd-us 0 upstream-cable 9/0/1 profile 1
 core-interface Te9/1/2
  rpd-ds 0 downstream-cable 9/0/13 profile 32
 r-dti 1
 rpd-event profile 0
 rpd-55d1-us-event profile
```



CHAPTER 19

Simple Content Protection Video Session Support

Cisco cBR Converged Broadband routers provide support for Simple Content Protection (SCP) video encryption licensing, which enables third-party products, such as Digital Transport Adapters (DTA), avail the capability of encrypting video streams compatible with Cisco's SCP conditional access (CA) system.

- Support for SCP Conditional Access System, on page 111
- Configure Cisco cBR Routers for SCP, on page 112
- Feature Information for SCP Video Session Support, on page 113

Support for SCP Conditional Access System

Cisco cBR Converged Broadband Router supports uDTA-SCP for broadcast (linear) services and thus removes the need for a bulk encryptor.

SCP is a conditional access system. When a Cisco controller system is combined with an Entitlement Control Message (ECM) generator, along with the licensed encryption device, it enables the Cisco conditional access systems to provide protection for various services. These are services such as linear broadcast (Basic, Expanded Basic, Digital Basic, Premium, PPV, and IPPV), switched digital video (SDV), and on-demand content (VoD).

The Cisco Conditional Access technologies that are enabled by this license include PowerKEY and Simple Content Protection. The technologies are enabled in modes compliant with the existing deployed CPE devices that employ those CA technologies.

Prerequisites

The following are the prerequisites for configuring SCP on Cisco cBR routers:

- SCP services are configured in DTACS/EC and sessions are configured on SCP-PCG.
- These multicast session configurations on SCP QAM must be manually configured on the Cisco cBR-8 routers as static table-based sessions.
- The DCM is configured for SCP scrambling along with the ROSA SI server (AC Manager, SCS configurator, and Scrambling control task).

Configure Cisco cBR Routers for SCP

To configure and enable SCP on Cisco cBR Converged Broadband routers, do the following tasks:

- Create a Virtual Carrier Group (VCG) with the QAM channel, which carries the SCP content.
- Create Service Distribution Group (SDG) for SCP.
- Create VCG-SDG bind.

Create SDG and VCG

To create SDG and VCG, use the following commands:

```
service-distribution-group service distribution group name ID
rf-port integrated-cable slot/bay/port
virtual-carrier-group name [id number]
service-type narrowcast
rf-channel start_channel-end_channel tsid start_tsid-end_tsid output-port-number
start_number-end_number
bind-vcg
vcg vcg-name sdg sdg-name
```

Example: Creating SDG and VCG

The following example shows how to create the SDG and the VCG:

```
service-distribution-group sdg1 id 1
rf-port integrated-cable 1/0/0
virtual-carrier-group vcg1 id 1
service-type narrowcast
rf-channel 20-24 tsid 120-124 output-port-number 120-124
bind-vcg
vcg vcg1 sdg sdg1
```

Create a Table-based LED for SCP

To create a table-based LED for SCP, use the following commands:

```
logical-edge-device name id ID
protocol table-based
virtual-edge-input-ip ip-address input-port-number port-number
vcg vcg-name
active
```

Example: Creating a Table-based LED for SCP

The following example shows how to create a table-based LED:

```
logical-edge-device led1 id 1
protocol table-based
virtual-edge-input-ip 198.51.100.1 input-port-number 1
vcg vcg1
active
```

Configure Table-based and PSIP Sessions

Configure table-based sessions with the same output service ID as the one configured in DTACS (service ID) or DCM output service ID (for example, 209). You should also configure PSIP session that carries SI data required for the uDTA box.

```
cable video
table-based
vcg vcg-name
rf-channel ID
session sess-name group <IP address> processing-type remap start-program n
session SESS_PSIP group <IP address> processing-type passthru psip
```

Example: Configuring Table-based and PSIP Sessions

The following example shows how to configure table-based session and PSIP session:

```
cable video
table-based
vcg vcg1
rf-channel 21
session SESS_SCP group 203.0.113.1 processing-type remap start-program 209
session SESS_PSIP group 203.0.113.32 processing-type passthru psip
```

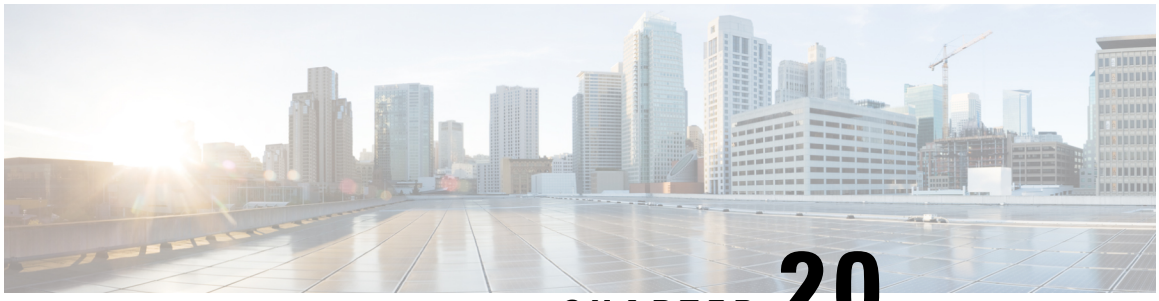
Feature Information for SCP Video Session Support

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 https://cfnng.cisco.com/ 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 29: Feature Information for PMV Support for Table-Based Videos

Feature Name	Releases	Feature Information
SCP Video Session Support	Cisco IOS XE Fuji 16.9.1a	This feature was introduced on the Cisco cBR Series Converged Broadband Router.



CHAPTER 20

Table-Based Video and VPME Encryption

Table-based video is a configuration mode for video sessions. This feature statically maps UDP flows into appropriate RF QAM channels. Each UDP flow is identified by the destination IP address of the MPEG traffic and UDP port number. The configuration contains the input port number, which is resolved into a unique destination IP address, the UDP port, and an output program number.

The Video on Demand (VOD) Privacy Mode Encryption (PME) enables the Cisco Edge QAM Manager (CEM) to encrypt the VOD content streamed through Motorola/Arris VOD systems. PME encryption is applicable for table-based sessions.

- Overview of VPME, on page 115
- How to Configure Table-Based Video Session, on page 116
- How to Configure VPME Encryption, on page 126
- Configuration Examples For VPME Encryption, on page 129
- Feature Information for Table-Based Video and VPME Encryption, on page 130

Overview of VPME

The PME Video On Demand system integrates the encrypted VOD content within an Arris digital cable headend. A VOD system provides the clear content while the Cisco cBR-8 and CEM are added to provide encryption. The details on the usage of the CEM are described in this chapter. Every MSO site should have the CEM application, which is the single entity connecting to the Arris Encryption Renewal System (ERS). All the Cisco cBR-8s on this MSO site should connect to this CEM.

Prerequisites for VPME

To enable VPME encryption, the connection to the CEM should be configured. VPME is a licensed feature and requires appropriate license on the chassis. The following connection should be configured:

- The video traffic flow on the Ten Gigabit interface.
- Table-based video sessions.
- QAM PHY parameters for the physical QAM channel.

Restrictions for VPME

You can configure the line card in only one mode as the table-based session configuration and dynamic GQI-based sessions are mutually exclusive. Hence, PME and PowerKey encryption are also mutually exclusive modes at the line card level. For more details, see *Configuring the Encryption Type on the Line Card* section.

How to Configure Table-Based Video Session

Configuring Table-Based Video

Before You Begin

Before configuring table-based sessions, you must configure the physical and virtual constructs for Cisco cBR-8. You must also configure the Logical Edge Device (LED), Service Distribution Group (SDG), binding and Virtual Carrier Group (VCG).

The following is an example for LED configuration. In this example, assumes that the video traffic is routed via the input ports of Virtual Edge Input (VEI).

```
logical-edge-device pme_tbv id 1
protocol table-based
virtual-edge-input-ip 172.16.0.1 input-port-number 1
vcg pme_tbv
active
```

In the above example, protocol table-based indicates that this LED supports table-based sessions.

For more information, see the *How to Configure the Logical Edge Devices* section. For details related to D6 protocol, see the *How to Configure the D6 Discovery Protocol* section.

Configuring Table-Based Session : VEI Input Port-Based

To configure the table-based session based on Virtual Edge Input (VEI), complete the following procedure:

```
configure terminal
cable video
table-based
vcg vcg-name
rf-channel n-m
session name {input-port number | bundle-id number}
start-udp-port number num-sessions-per-qam number processing-type
 {program | data } start-program number [repeat] jitter
ms [cbr | vbr ]
exit
```

The **table-based** keyword is the root keyword. The entire table-based configuration should be under this keyword. Within this, the configuration is separated based on the VCG. Within each VCG, the configuration can be created for each QAM channel.

- Processing-type
  - Remap—Configures VoD sessions as remap.
  - Data—Configure video streams that are not dejittered, and remapped. For example, Beacons, carousel, and so on.

- Repeat—Repeats the program number across QAM channels.

Example:

The following is an example in which two sessions are created on all QAM channels from 20 to 22.

```
configure terminal
cable video
table-based
vcg pme_tbv
rf-channel 20-22
session bago_tbv input-port 1 start-udp-port 49152 num-sessions-per-qam 2 processing-type
remap start-program 32 jitter 150 cbr
exit
```

The following is an example in which one session is created on each QAM channel.

```
configure terminal
cable video
table-based
vcg pme_tbv2
rf-channel 23
session pme_tbv input-port 1 start-udp-port 50152 num-sessions-per-qam 1 processing-type
remap start-program 5 jitter 150 cbr
rf-channel 24
session pme_tbv input-port 1 start-udp-port 50153 num-sessions-per-qam 1 processing-type
remap start-program 5 jitter 150 cbr
exit
```

Configuring Table-Based Session :VEI Bundle-Based

Before You Begin

- Create two or more VEIs.
- Bundle the VEIs.

For more details, see *Virtual Edge Input Bundling* section.

To configure the VEI bundled table-based session, complete the following procedure:

configure terminal
cable video
table-based
vcg *vcg-name*
rf-channel *n-m*
session *name* **bundle-id** *number* **start-udp-port**
number **num-sessions-per-qam** *number* **processing-type**
{*program* | *passthru* | *data* } **start-program** *number*
[**repeat**] **jitter** *ms* [**cbr** | **vbr**]
exit

Example:

The following is an example in which a session is created for VEI bundle (10) .

```
configure terminal
cable video
table-based
vcg pme_vcg
rf-channel 20-21
session tbv bundle-id 10 start-udp-port 49152 num-sessions-per-qam 2 processing-type remap
```

```
 start-program 1 repeat jitter 100 vbr
exit
```

Virtual Edge Input Bundling

To create and bundle the VEIs, complete the following procedure:

configure terminal
cable video
logical-edge-device *name*
protocol table-based
virtual-edge-input-ip *ip address* **input-port-number** *number*
vcg*vcg-name*
vei-bundle *id* **input-port-number** *number*
active
exit

Example:

The following is an example in which a bundle (10) is created with two input ports (1 and 2) each with distinct IP address.

```
configure terminal
cable video
logical-edge-device pme_led id 1
protocol table-based
virtual-edge-input-ip 172.16.0.1 input-port-number 1
virtual-edge-input-ip 172.16.0.1 input-port-number 2
vcg pme_vcg
vei-bundle 10 input-port-number 1,2
active
exit
```

Verifying Table-Based Video Configuration

Verify All Sessions Configured on an LED

To verify all the sessions configured on a particular LED, use the **show cable video session logical-edge-device id** *number* command as shown in the example below:

```
show cable video session logical-edge-device id 1
Total Sessions = 6

Session Output Streaming Session Destination UDP   Output  Input      Output Input   Output
  Encrypt Encrypt Session
Id      Port   Type      Type               Port  Program State      State  Bitrate Bitrate
 Type    Status  Name
-------------------------------------------------------------------------------------------
1048576  1      Remap    UDP     174.21.1.1  49152 32      ACTIVE-PSI ON     1718234 1702594
 CLEAR    -      bago_tbv.1.0.1.20.49152
1048577  1      Remap    UDP     174.21.1.1  49153 33      ACTIVE-PSI ON     1718631 1702594
 CLEAR    -      bago_tbv.1.0.1.20.49153
1048578  2      Remap    UDP     174.21.1.1  49154 34      ACTIVE-PSI ON     1717832 1702977
 CLEAR    -      bago_tbv.1.0.1.21.49154
1048579  2      Remap    UDP     174.21.1.1  49155 35      ACTIVE-PSI ON     1717322 1702977
 CLEAR    -      bago_tbv.1.0.1.21.49155
1048580  3      Remap    UDP     174.21.1.1  49156 36      ACTIVE-PSI ON     1718697 1702959
 CLEAR    -      bago_tbv.1.0.1.22.49156
1048581  3      Remap    UDP     174.21.1.1  49157 37      ACTIVE-PSI ON     1717542 1702959
```

```
 CLEAR    -      bago_tbv.1.0.1.22.49157
```

verify the summary of the session details

To verify the summary of the session details at a LED level, use the **show cable video session logical-edge-device id** *number* **summary** command as shown in the example below:

```
show cable video session logical-edge-device id 1 summary
Video Session Summary:

Active    : 6        Init      : 0        Idle      : 0
Off       : 0        Blocked   : 0        PSI-Ready : 6
UDP       : 6        ASM       : 0        SSM       : 0
Remap     : 6        Data      : 0        Passthru  : 0
Total Sessions: 6
```

Verify QAM PHY Parameters of RF-channel

To verify the QAM PHY parameters of RF-channel that are configured on the RF port, which is controller Integrated-Cable 7/0/0, use the **show controllers integrated-Cable** *slot/bay/port***rf-channel** *n-m* command as shown in the example below:

```
show controllers integrated-Cable 7/0/0 rf-channel 0-95
Chan State Admin Frequency  Type   Annex Mod  srate Interleaver  dcid  power  output
 0     UP   UP   93000000   VIDEO   B    256   5361  I32-J4       -    34     NORMAL
 1     UP   UP   99000000   VIDEO   B    256   5361  I32-J4       -    34     NORMAL
 2     UP   UP   105000000  VIDEO   B    256   5361  I32-J4       -    34     NORMAL
 3     UP   UP   111000000  VIDEO   B    256   5361  I32-J4       -    34     NORMAL
 4     UP   UP   117000000  VIDEO   B    256   5361  I32-J4       -    34     NORMAL
 5     UP   UP   123000000  VIDEO   B    256   5361  I32-J4       -    34     NORMAL
 6     UP   UP   129000000  VIDEO   B    256   5361  I32-J4       -    34     NORMAL
 7     UP   UP   135000000  VIDEO   B    256   5361  I32-J4       -    34     NORMAL
 8     UP   UP   141000000  VIDEO   B    256   5361  I32-J4       -    34     NORMAL
 9     UP   UP   147000000  VIDEO   B    256   5361  I32-J4       -    34     NORMAL
 10    UP   UP   153000000  VIDEO   B    256   5361  I32-J4       -    34     NORMAL
```

Output State is OFF

Procedure

Step 1 Verify the video traffic using the **show cable video session logical-edge-device id 1** command. In the below example, the output state is OFF. This value confirm that there is no output traffic.

```
Session Output Streaming Session Destination UDP   Output  Input Output Input   Output
Encrypt Encrypt Session
Id      Port   Type      Type               Port  Program State State  Bitrate Bitrate
Type    Status  Name
-------------------------------------------------------------------------------------
1048582    1   Remap     UDP     172.16.0.1  49152 32      OFF   OFF    0       0       PME
     Pending bago_tbv.1.0.1.20.49152
1048583    1   Remap     UDP     172.16.0.1  49153 33      OFF   OFF    0       0       PME
     Pending bago_tbv.1.0.1.20.49153
1048584    2   Remap     UDP     172.16.0.1  49154 34      OFF   OFF    0       0       PME
     Pending bago_tbv.1.0.1.21.49154
1048585    2   Remap     UDP     172.16.0.1  49155 35      OFF   OFF    0       0       PME
```

```
     Pending bago_tbv.1.0.1.21.49155
1048586    3   Remap     UDP     172.16.0.1  49156 36      OFF   OFF    0       0       PME
     Pending bago_tbv.1.0.1.22.49156
1048587    3   Remap     UDP     172.16.0.1  49157 37      OFF   OFF    0       0       PME
     Pending bago_tbv.1.0.1.22.49157
```

Step 2 Verify if the RF output of the controller is shut using the **show cable video integrated-cable** command.

```
Router#show cable video integrated-cable 8/0/0

Integrated TSID ONID Output Physical    Admin Operational Virtual-Carrier Service-Distribution
 Logical-Edge Encryption Total
Cable                Port   QAM ID      State State       -Group Name     -Group Name
     -Device Name Capable    Sessions
------------------------------------------------------------------------------------------
8/0/0:20   1     0    1    unavailable  OFF   DOWN        pme_tbv        pme_tbv
     pme_tbv      pme        2
8/0/0:21   2     0    2    unavailable  OFF   DOWN        pme_tbv        pme_tbv
     pme_tbv      pme        2
8/0/0:22   3     0    3    unavailable  OFF   DOWN        pme_tbv        pme_tbv
     pme_tbv      pme        2
8/0/0:23   4     0    4    unavailable  OFF   DOWN        pme_tbv        pme_tbv
     pme_tbv      pme        2
8/0/0:24   5     0    5    unavailable  OFF   DOWN        pme_tbv        pme_tbv
     pme_tbv      pme        0
```

a) If the RF output of the controller is shut, you must unshut the port. This action changes the status as ON for the corresponding QAMs. You can verify the state using the **show cable video integrated-cable** command.

```
Router#show cable video integrated-cable 8/0/0

Integrated TSID ONID Output Physical Admin Operational Virtual-Carrier
Service-Distribution Logical-Edge Encryption Total
Cable                Port   QAM ID   State State       -Group Name     -Group Name
     -Device Name Capable    Sessions
------------------------------------------------------------------------------------------
8/0/0:20   1     0    1     48       ON    UP          pme_tbv        pme_tbv
    pme_tbv       pme        2
8/0/0:21   2     0    2     49       ON    UP          pme_tbv        pme_tbv
    pme_tbv       pme        2
8/0/0:22   3     0    3     50       ON    UP          pme_tbv        pme_tbv
    pme_tbv       pme        2
8/0/0:23   4     0    4     51       ON    UP          pme_tbv        pme_tbv
    pme_tbv       pme        2
8/0/0:24   5     0    5     24       ON    UP          pme_tbv        pme_tbv
    pme_tbv       pme        2
```

Step 3 Verify the JIB channel number for a specific QAM channel using the **show cable video integrated-cable** command.

```
Router#show controllers integrated-Cable 7/0/0 rf-channel 21 verbose

Chan State Admin Frequency  Type   Annex Mod  srate Interleaver  dcid  power  output
 21    UP   UP   219000000  VIDEO   B    256   5361  I32-J4       -    34     NORMAL
 Qam profile: 1
 Spectrum Inversion: Off
 Frequency Lane: 1  Block: 3  index: 6
 Resource status:   OK
 License: granted <01:07:01 EDT Feb 19 2016>
 QAM Replication:
    Group ID: 57344 (Pilot)
    Slot group ID: 0
```

```
    Members: 7/0/0:21 (P) 7/0/1:21  7/0/2:21  7/0/3:21

   Channel Replication Status: Up
 JIB channel number: 21
Chan Pr EnqQ  Pipe  RAF   SyncTmr Vid Mac            Video Primary DqQ  TM Mpts Sniff
  21 --    21     0  6880       0   1 0000.0000.0000     1       0   21  0    5 NO 86
Grp  Prio P  Prate Phy0-ctl Phy1-ctl Enable Tun-Id  L2TPv3_Ses_id
   2    0  0     1        1        0   TRUE       0      2
Chan   Qos-Hi   Qos-Lo    Med-Hi   Med-Lo    Low-Hi   Low-Lo
  21    32774    16384     32768    16384     65536    32768
Chan  Med Low TB-neg Qos_Exc  Med_Xof  Low_Xof    Qdrops(H-M-L)  Pos Qlen(Hi-Med-lo) Fl
   21   0   0      0       0        0        0    0    0    0  N 23808     0 11656  0
  DSPHY Register Local Copy: QPRHI = c0005564, QPRLO = 216ab0
  DSPHY Register Local Copy Vaddr = 800002e4, qam2max_mapping = 80000015
  DSPHY Register Local Copy: SPR ID = 15, SPR Mapping= c200000b
  Last read from HW: Fri Feb 19 01:07:57 2016
   QPRHI = c0005564, QPRLO = 216ab0, SPR = c200000b SPRMAPING c0000205 Q2Max 80000015
  Last time read spr rate info from HW: Fri Feb 19 03:06:43 2016
    SPR ID 21, rate value in kbps 3463, overflow count 0, underflow count 0
```

Output Status is Idle or Pending

Procedure

Step 1 Verify the video traffic. In the below example, the input bitrate is zero, and the input state is IDLE / OFF. These values confirm that there is no input traffic.

```
Router#sh cable video session logical-edge-device id 1
Total Sessions = 6

Session Output Streaming Session Destination UDP   Output  Input Output Input   Output
Encrypt Encrypt Session
Id      Port   Type      Type                Port  Program State State  Bitrate Bitrate
Type    Status  Name
-------------------------------------------------------------------------------------------
1048588    1   Remap     UDP     172.16.0.1  49152 32      IDLE  PENDING 0       0       PME
     Pending bago_tbv.1.0.1.20.49152
1048589    1   Remap     UDP     172.16.0.1  49153 33      IDLE  PENDING 0       0       PME
     Pending bago_tbv.1.0.1.20.49153
1048590    2   Remap     UDP     172.16.0.1  49154 34      IDLE  PENDING 0       0       PME
     Pending bago_tbv.1.0.1.21.49154
1048591    2   Remap     UDP     172.16.0.1  49155 35      IDLE  PENDING 0       0       PME
     Pending bago_tbv.1.0.1.21.49155
1048592    3   Remap     UDP     172.16.0.1  49156 36      IDLE  PENDING 0       0       PME
     Pending bago_tbv.1.0.1.22.49156
1048593    3   Remap     UDP     172.16.0.1  49157 37      IDLE  PENDING 0       0       PME
     Pending bago_tbv.1.0.1.22.49157
```

Step 2 Verify details of the video traffic over the mid plane interface through which traffic is routed to the video data plane on the line card. The mid plane is specific to the line-card slot. On subsequent trials, the output packet count should keep increasing. You can verify the output packet count using the **show interfaces video** command.

```
Router#show interfaces video 7/0/0 accounting

Video7/0/0
```

```
                Protocol    Pkts In   Chars In   Pkts Out   Chars Out
                      IP          0          0   2211315936 2653579123200
                 DEC MOP          0          0         12        756
                     ARP          0          0          4        112

Video7/0/0
                Protocol    Pkts In   Chars In   Pkts Out   Chars Out
                      IP          0          0   2220252160 2664302592000
                 DEC MOP          0          0         12        756
                     ARP          0          0          4        112
```

Step 3 If the packet count is not increasing, verify the 10 GigE physical interface through which the video traffic is fed to the chassis using the **show interfaces** command. In the below example, the video traffic is fed through the 10GigE interface 4/1/0 and the counter for packets keeps incrementing.

```
Router#show interfaces tenGigabitEthernet 4/1/0 accounting
TenGigabitEthernet4/1/0
                Protocol    Pkts In   Chars In   Pkts Out  Chars Out
                   Other         15       1155       1814     109078
                      IP 8038262210 9404766785700          0          0
                 DEC MOP         15       1155         14       1078
                     ARP          0          0          1         60
Router#show interfaces tenGigabitEthernet 4/1/0 accounting
TenGigabitEthernet4/1/0
                Protocol    Pkts In   Chars In   Pkts Out  Chars Out
                   Other         15       1155       1816     109198
                      IP 8047199112 9415222959870          0          0
                 DEC MOP         15       1155         14       1078
                     ARP          0          0          1         60
```

Input State is Active and not Active PSI

If the input state is Active and the input PSI information is not detected, verify the input PMT information section for this particular session.

Procedure

Verify the details of a particular video session, using the **show cable video session logical-edge-device id** *led-id* **session-id** *id* command.

```
Router#show cable video session logical-edge-device id 1 session-id 1048599
Session Name        : bago_tbv.1.0.1.22.49157
Session Id:         : 1048599
Creation Time:      : Thu Feb 18 18:21:25 2016

Output Port         : 3
TSID                : 3
ONID                : 0
Number of Sources   : 1
  Destination IP    : 172.16.0.1
  UDP Port          : 49157
Config Bitrate      : 2000000
Jitter              : 150 ms
Processing Type     : Remap
Stream Rate         : CBR
Program Number      : 37
```

```
Idle Timeout        : 250 msec
Init Timeout        : 1000 msec
Off Timeout         : 60 sec
Encryption Type     : PME
Encryption Status   : Encrypted

Input Session Stats:
====================
  State: ACTIVE-PSI, Uptime: 0 days 00:01:01
  IP Packets: In 12202, RTP 0, Drop 0
  TP Packets: In 69979, PCR 2447, PSI 1323, Null 3233, Unreference 153
  Errors: Discontinuity 8, Sync loss 0, CC error 0, PCR Jump 17,
          Underflow 0, Overflow 0, Block 0
  Bitrate: Measured 1716626 bps, PCR 1800140 bps

Output Session Stats:
=====================
  State: ON, Uptime: 0 days 00:01:01
  TP Packets: In 70535, PCR 2440, PSI 1320,
              Drop 910, Forward 68305, Insert 1752
  Errors: Info Overrun 0, Info Error 0, Block 0, Overdue 0,
          Invalid Rate 0, Underflow 0, Overflow 0
  Bitrate: Measured 1723591 bps

PAT Info:
=========
  Version 0, TSID 1, len 20, section 0/0
  Program 0: NIT 16
  Program 1: PMT 8020

Input PMT Info:
===============
  Program 1, Version 0, PCR 8000, Info len 0
  PID 8000: Type 2, Info len 5, (desc 2 len 3)
  PID 8001: Type 129, Info len 17, (lang eng), (desc 5 len 4), (desc 129 len 3)

Output PMT Info:
================
  Program 37, Version 1, PCR 273, Info len 6, (CA SYS-ID 18249, PID 303)
  PID 273: Type 2, Info len 5, (desc 2 len 3)
  PID 274: Type 129, Info len 17, (lang eng), (desc 5 len 4), (desc 129 len 3)

Output PID Map:
===============
  PID 8000 -> 273
  PID 8001 -> 274
  PID 8020 -> 272
```

Abnormalities on the Output

If there are any abnormalities in the output such as macro blocks, ans so on, verify if there are any issues such as CC errors or PCR errors in the MPEG packet.

Verify the session details, using the **show cable video session logical-edge-device id** *led-id* **session-id** *id* command. This command displays errors for both input session stats and output session stats.

Configuring CEM Connectivity for PME Encryption

This section explains how to configure the connectivity to the external CEM and enforce PME encryption on the line card.

Only one device from the MSO site can communicate with the Encryption Renewal System (ERS) and obtain the latest ECM templates. The CEM communicates with the ERS and sends the ECM templates to the Cisco Edge QAM devices in the MSO site.

You can configure the following:

- VODS-ID—IDs assigned by CCAD/ARRIS to the MSO site. The configured VODS-ID on the Cisco cBR-8 and the CEM must be same.
- CEM IP—Interface IP of the Windows/Linux system through which the CEM can be reached by Cisco cBR-8.
- CEM Port—Port number on which the CEM listens for connections from the Cisco cBR-8.
- Management Interface—Source IP address of the cBR-8 virtual interface through which the connection must be established with the CEM server.

Note There can be only one entry for VODS-ID, CEM IP, CEM Port, and Management Interface IP. If you configure any new values for these parameters, the previous configuration is cleared. You can clear the configurations using the 'no' form of the command.

Configuring VODS-ID

To configure the VODS-ID of the CEM, perform the following steps:

```
enable
configure terminal
cable video
encryption
pme vodsid id
exit
```

Configuring CEM IP and Port

To configure the CEM IP and port of the CEM, perform the following steps:

```
enable
configure terminal
cable video
encryption
pme cem ip-address tcp_port
exit
```

Configuring Management IP

To configure the PME management IP address to establish CEM connection, perform the following steps:

The virtual port group must be configured before configuring the management IP. For more information, see the Configuring the VirtualPortGroup Interface section.

```
enable
configure terminal
cable video
encryption
pme mgmt-ip ip-address
exit
```

Verifying CEM Connectivity

To verify the connection status of PME, use the **show cable video encryption pme status** command as shown in the following example:

```
Router#show cable video encryption pme status
PME Connection Status:
VODS-ID : 111
CEM IP : 1.200.1.163
CEM Port : 5000
Local Mgmt IP : 1.24.2.6
Local Port : 50394
CEM Connection State : Connected
Count of ECMs recd : 2
```

Connectivity with CEM is Lost

Procedure

Step 1 If the CEM connection status is Not Connected, verify the VODS-ID, CEM IP, CEM port and local Mgmt IP address parameters using the **show cable video encryption pme status** command.

```
Router#show cable video encryption pme status
PME Connection Status:
======================
VODS-ID              : 111
CEM IP               : 1.200.1.163
CEM Port             : 5000
Local Mgmt IP        : 1.35.2.5
Local Port           : 0
CEM Connection State : Not Connected
```

Step 2 If the PME connection parameters are valid, ensure there is route from the Cisco cBR-8's Virtual management iinterface to the CEM by using the **ping** command. Ping the CEM IP address from the virtualPortGroup 0 on which the management IP is created.

```
Router#ping 1.200.1.163 source virtualPortGroup 0
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 1.200.1.163, timeout is 2 seconds:
Packet sent with a source address of 1.35.2.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

Step 3 Verify the alarms in the logs for any connectivity loss.

```
Feb 18 18:28:12.053 IST: %VEMAN-3-CEM_CONNECTION_LOST: CLC4: sup_veman:  Alarm Set: CEM
Connection Lost: Connection closed by peer-1.200.1.163:5000
```

How to Configure VPME Encryption

Enforcing Data Stream Encryption Type

Before You Begin

Configure the Virtual Carrier Group (VCG) to setup an encrypted session. For more details, see *Configuring Virtual Carrier Group* section.

To configure the encryption type for a VOD session, perform the following steps:

```
enable
configure terminal
cable video
encryption
linecard slot/bay ca-system [dvb | pme | powerkey] scrambler scrambler-type
 [dvb-csa | des | dvs042]
exit
```

Configuring Virtual Carrier Group

To configure the Virtual Carrier Group (VCG) for setting up an encrypted session, perform the following steps:

```
enable
configure terminal
cable video
encryption
virtual-carrier-group name[idnumber]
rf-channel start-channel number-end-channel number tsid start-tsid-end-tsid
output-port-number start-num-end-num
virtual-edge-input ipaddr input-port-number port-number
encrypt
exit
```

Verifying VPME Encryption Configuration

- To verify the encryption configurations, use the **show cable video encryption linecard** [*all* | *slot number*] command as shown in the following example:

```
Router#show cable video encryption linecard 7/0
Line card: 7/0
CA System Scrambler
```

```
====================================
PME dvs-042
```

- To verify the encryption status of all sessions on an LED, use the **show cable video session logical-edge-device id** *id* command as shown in the following example:

```
Router#show cable video session logical-edge-device id 1
Total Sessions = 6

Session Output Streaming Session Destination UDP   Output  Input      Output Input
Output  Encrypt Encrypt   Session
Id      Port   Type      Type                Port  Program State      State  Bitrate
Bitrate Type    Status    Name
-------------------------------------------------------------------------------------
1048582 1      Remap     UDP     172.16.0.1  49152 32      ACTIVE-PSI ON     996413
981109  PME     Encrypted bago_tbv.1.0.1.20.49152
1048583 1      Remap     UDP     172.16.0.1  49153 33      ACTIVE-PSI ON     1004787
981246  PME     Encrypted bago_tbv.1.0.1.20.49153
1048584 2      Remap     UDP     172.16.0.1  49154 34      ACTIVE-PSI ON     995088
984011  PME     Encrypted bago_tbv.1.0.1.21.49154
1048585 2      Remap     UDP     172.16.0.1  49155 35      ACTIVE-PSI ON     993061
984051  PME     Encrypted bago_tbv.1.0.1.21.49155
1048586 3      Remap     UDP     172.16.0.1  49156 36      ACTIVE-PSI ON     994238
988617  PME     Encrypted bago_tbv.1.0.1.22.49156
1048587 3      Remap     UDP     172.16.0.1  49157 37      ACTIVE-PSI ON     1004658
988602  PME     Encrypted bago_tbv.1.0.1.22.49157
```

- To verify the various sessions, which use the PME modules that are loaded on a specific line-card, use the **show cable video encryption pme linecard** *slot/bay* **session** *1-65535* | **all** | **summary** command as shown in the example below:

```
Router#show cable video encryption pme linecard 7/0 session all
Count of ECMG Streams: 4
==================== ECMG Stream DATA ========================
Stream
ID num EcmId CP# CwE CPDur NomCPD EcmRqst EcmRsp
---------- ---------- ---- --- ----- ------ ---------- ----------
0020(0032) 0020(0032) 0002 0 0 40000 7 2
0021(0033) 0021(0033) 0002 0 0 40000 7 2
0040(0064) 0040(0064) 0002 0 0 40000 7 2
0041(0065) 0041(0065) 0002 0 0 40000 7 2

Router#show cable video encryption pme linecard 7/0 session 32
Stream 32, session 7681 is active
Stream number = 32 Session number = 7681
ECM requests = 8 ECM replies = 2
ECM ID = 32 CryptoPeriod num = 2
CP duration = 0 Nominal duration = 40000
CA transfer mode = 1 Stream status = No
Error Blob details

Router#show cable video encryption pme linecard 7/0 session summary
Currently active streams:
Active = 4
ECM req/resp mismatch = 4
ECM req, all streams = 32
ECM resp, all streams = 8
Since last reset:
Sessions created = 4
```

```
Sessions deleted = 0
ECMs received =2
ECMs discarded = 0
```

No PMT at the Output

Procedure

Step 1 Verify the encryption status using the **show cable video session logical-edge-device id** command. If the encrypt status is shown as ca-waiting, then PMT is withheld.

```
Router#show cable video session logical-edge-device id 1
Total Sessions = 6

Session Output Streaming Session Destination UDP   Output  Input      Output Input   Output
  Encrypt Encrypt    Session
Id      Port   Type      Type               Port  Program State      State  Bitrate Bitrate
 Type    Status     Name
-------------------------------------------------------------------------------------------
1048582 1      Remap     UDP     172.16.0.1  49152 32      ACTIVE-PSI PENDING 996413 981109
  PME     ca-waiting bago_tbv.1.0.1.20.49152
```

Step 2 Verify if the ECM count is zero using the **show cable video encryption pme status** command.

```
Router#show cable video encryption pme status
PME Connection Status:
VODS-ID : 111
CEM IP : 1.200.1.163
CEM Port : 5000
Local Mgmt IP : 1.24.2.6
Local Port : 50394
CEM Connection State : Connected
Count of ECMs recd : 0
```

Step 3 Verify if the ECM request or response count is 0 using the **show cable video encryption pme linecard** *slot/bay* **session summary** command.

```
Router#show cable video encryption pme linecard 7/0 session summary
Currently active streams:
Active = 4
ECM req/resp mismatch = 4
ECM req, all streams = 32
ECM resp, all streams = 8
Since last reset:
Sessions created = 4
Sessions deleted = 0
ECMs received =2
ECMs discarded = 0
```

Configuration Examples For VPME Encryption

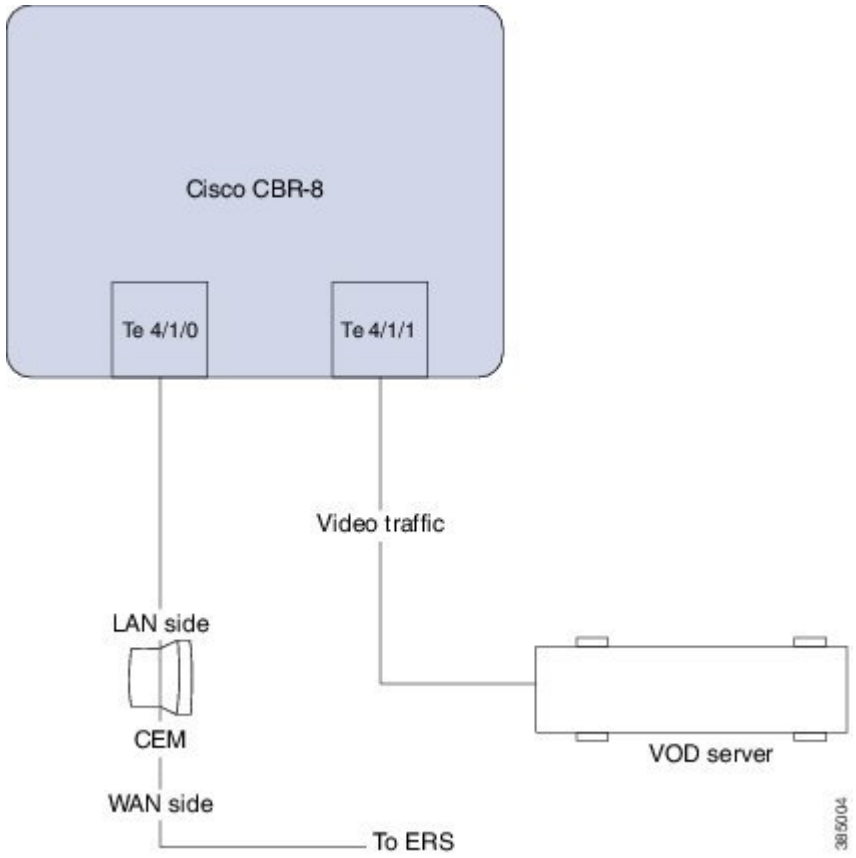
The following example shows running output for a PME configuration:

```
cable video

mgmt-intf virtualPortGroup 0

virtual-carrier-group pme_tbv
encrypt
service-type narrowcast
rf-channel 20-24 tsid 1-5 out 1-5

service-distribution-group pme_tbv
rf-port integrated-cable 7/0/0

bind-vcg
vcg pme_tbv sdg pme_tbv

encryption
linecard 7/0 ca-system pme scrambler dvs
pme vodsid 111
pme cem 1.200.1.163 5000
pme mgmt-ip 1.25.2.6

logical-edge-device pme_tbv
protocol table-based
virtual-edge-input-ip 174.101.1.1 input 1
vcg pme_tbv
active

table-based
vcg vcg_replication
rf-channel 21-31
session pme_tbv1 in 1 start-udp-port 49152 num-sessions-per-qam 2 processing-type remap
start-program 32 jitter 150 cbr
session pme_tbv2 in 1 start-udp-port 50001 num-sessions-per-qam 2 processing-type remap
start-program 64 jitter 150 cbr
```

Use Cases or Deployment Scenarios

Topology

A typical topology for CEM connectivity is shown below:



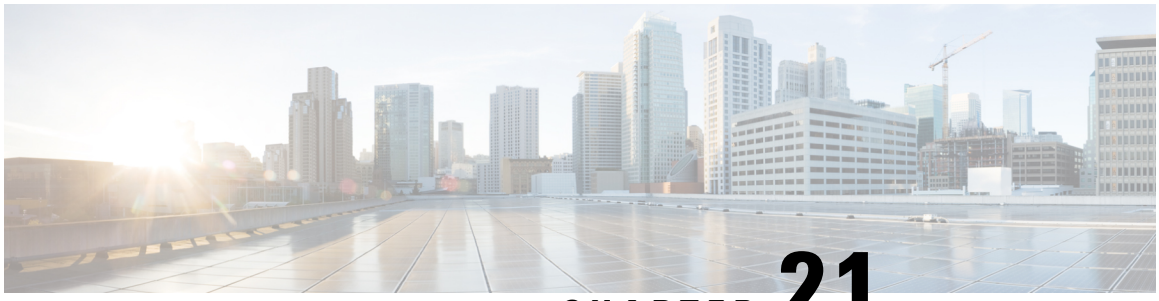
Feature Information for Table-Based Video and VPME Encryption

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 https://cfnng.cisco.com/ 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 30: Feature Information for Table-Based Video and VPME Encryption

Feature Name	Releases	Feature Information
Table-Based Video and VPME Encryption	Cisco IOS XE Everest 16.6.1	This feature was integrated on the Cisco cBR Series Converged Broadband Routers.



CHAPTER 21

PMV Support for Table-Based Videos

The PMV support for table-based videos enables the operators to specify a range of PIDs that can be used for a specific UDP flow. Operators require this feature when they want to know in advance which PIDs are selected for a specific UDP flow. .

Contents

- Information About the PMV Support for Table-Based Videos, on page 131
- How to Configure PMV, on page 133
- Disabling PMV Allocation Scheme for LED, on page 135
- Configuration Examples, on page 136
- Feature Information for PMV Support, on page 139

Information About the PMV Support for Table-Based Videos

This feature is used in deployments, where PID allocations are required and allows the operator to configure fixed PID groups for a specific UDP flow. To avail this feature, the operator can choose a specific group of PIDs using a PID map value. The operators can enable this feature at the LEDs that are configured for table-based video sessions.

Overview of PMV

This feature uses the following PID group allocation scheme for allocating PIDs for table-based session.

```
Start PID = PID offset + (PID Map Value x 32)
```

The attributes in this scheme are explained in the following table:

Attribute	Description
Start PID	Value of the first PID in this specific PID group.
PID offset	PID value to factor is standard PIDs. The hardcoded value is 48.
PID Map value	Configurable value for selecting a specific PID group. This attribute can take values from 0 to 251.

To enable this feature for a table-based QAM, the operator should specify the following details:

- Whether the operator wants to use this static allocation scheme that is mentioned in this section
- The actual PID group to pick for a session (PMV)

The PMV is assigned per UDP flow. When a configuration entry with a UDP range is created, the PMV value automatically increments by 1 from the PMV entry corresponding to the first UDP port.

When PMV = 0, PMT PID = 48 + (0 x 32) = 48, the elementary stream PIDs take the values from 49 to 79.

When PMV = 1, PMT PID = 48 + (1 x 32) = 80, the elementary stream PIDs take the values from 81 to 111.

The following table provides an overview of how PMVs are related to the selected PIDs.

PMV	**0**	**1**	**...**	**251**
PMT	48	80	...	8080
ES PID 1	49	81	...	8081
ES PID 2	50	82	...	8082
...	...	...	...	...
ES PID 31	79	111	...	8111

Prerequisites for Configuring PMV

PMV is applicable only for table-based video sessions. The following prerequisites are applicable for configuring PMV for the sessions.

- Service Distribution Group (SDG)
- Virtual Carrier Group (VCG)
- Bind VCG to SDG
- Logical Edge Device (LED)
- Protocol of LED specified as table-based
- Associate VCG to LED

Restrictions for Configuring PMV

The following restrictions are applicable for configuring PMV for the sessions:

- This feature is applicable only to the table-based sessions.
- The PMV feature applies only to SPTS remap sessions, because the MPTS sessions always use pass-through mode.

- After you configure PMV, it affects only the PID group allocation scheme and does not affect the PID allocation scheme inside a PID group.
- This allocation scheme is specified at the LED level and is optional. If not specified, the system uses the default LRU-based scheme.
- If the operator reserves a PID range after the PMV allocates a PID group, it will be handled similarly to that of the existing Least Recently Used (LRU) allocation scheme.

How to Configure PMV

To configure PMV, do the following tasks:

- Enable the PMV allocation scheme in the LED protocol configuration
- Configure the PMV for a session in the RF channel

Enabling PMV Allocation Scheme for LED

Before You Begin

- Identify the LED for which you want to enable the PMV
- Make sure that the LED protocol is set to table-based

Note If table-based video sessions are already present on VCGs that are bound to the LEDs, enabling PMV removes these sessions. Later, you must reconfigure them with the specified PMV values.

Procedure

To enable the PMV allocation scheme for LED, follow this procedure:

```
Router>enable
Router#configure terminal
Router(config)#cable video
Router(config-video)#logical-edge-device led_tbv id 1
Router(config-video-led)#protocol table-based
Router(config-video-led-protocol)#pmv
%%All sessions configured for this LED will be removed.
Enable PMV? [Yes/No] [confirm] Y
Router(config-video-led-protocol)#
```

Verifying the PMV Configuration on LED

To verify that you have enabled the PMV for an LED, run the **show running-config** command as provided in the following example:

```
Router# show running-config | s cable video
cable video
  mgmt-intf VirtualPortGroup 0
```

```
service-distribution-group sdg_tbv id 1
  rf-port integrated-cable 7/0/0
service-distribution-group sdg_tbv1 id 2
  rf-port integrated-cable 7/0/1
virtual-carrier-group vcg_tbv id 1
  service-type narrowcast
  rf-channel 0-95 tsid 1-96 output-port-number 1-96
virtual-carrier-group vcg_tbv1 id 2
  service-type narrowcast
  rf-channel 0-95 tsid 97-192 output-port-number 97-192
bind-vcg
  vcg vcg_tbv sdg sdg_tbv
  vcg vcg_tbv1 sdg sdg_tbv1
logical-edge-device led_tbv id 1
  protocol table-based
    virtual-edge-input-ip 174.101.1.1 input-port-number 1
    vcg vcg_tbv
    vcg vcg_tbv1
    pmv
    active
```

How to Configure Sessions with PMV Value

Each session in an RF channel can have a PMV value in the range of 0 to 251.

Before You Begin

- Identify the VCG and RF channel for which you want to create sessions

  Make sure that the LED that VCG is part has PMV enabled

Procedure

To configure an RF channel session with the PMV value, follow this procedure:

```
Router>enable
Router#configure terminal
Router(config)#cable video
Router(config-video)#logical-edge-device led_tbv id 1
Router(config-video-led)#protocol table-based
Router(config-video-led-protocol)#virtual-edge-input-ip 174.101.1.1 input-port-number 1
Router(config-video-led-protocol)#vcg vcg_tbv
Router(config-video-led-protocol)#vcg vcg_tbv1
Router(config-video-led-protocol)#pmv
Router(config-video-led-protocol)#active
Router(config-video-led-protocol)#table-based
Router(config-video-tb)#vcg vcg_tbv
Router(config-video-tb-vcg)#rf-channel 0
Router(config-video-tb-vcg-sess)#session session1 input-port 1 start-udp-port 30000
processing-type remap start-program 20 start-pmv 0 cbr

Router(config-video-tb-vcg-sess)#rf-channel 1
Router(config-video-tb-vcg-sess)#session session_group1 input-port 1 start-udp-port 6000
num-sessions-per-qam 15 processing-type remap start-program 40 start-pmv 0 cbr

Router(config-video-tb-vcg-sess)#session session_group2 input-port 1 start-udp-port 8000
num-sessions-per-qam 10 processing-type remap start-program 80 start-pmv 30 cbr
Router(config-video-tb-vcg-sess)#
```

Verifying the PMV on RF Channel Sessions

To verify the PMV configuration on an RF channel session, run the **show cable video session** command as provided in the following example:

```
Router# show cable video session logical-edge-device id 1
```

Troubleshooting Tips

When configuring RF channel sessions, if you configure the same PMV value for two or more sessions of the same RF channel, an error appears and the CLI command is rejected.

If you have to configure a reserved PID range, configure it before assigning the PMV values to the sessions. This process enables Cisco cBR-8 Series Router to reject the session configuration. It also shows a warning message to the operator when configuring those sessions with the PMV value that can allocate PIDs in the reserve PID range.

If PMV is enabled for an LED, when configuring sessions for RF channels that are part of the LED, without the *start-pmv* value, Cisco cBR-8 Series Router uses the default PMV value of 0.

Disabling PMV Allocation Scheme for LED

Before You Begin

- Identify the LED for which you want to disable the PMV
- If table-based sessions are already present on VCGs that are bound to the LEDs, disabling the PMV removes these sessions. Later, reconfigure them without the PMV values.

Procedure

To disable the PMV allocation scheme for LED, follow this procedure:

```
Router>enable
Router#configure terminal
Router(config)#cable video
Router(config-video)#logical-edge-device led_tbv id 1
Router(config-video-led)#protocol table-based
Router(config-video-led-protocol)#no pmv
%%All sessions configured for this LED will be removed.
Disable PMV? [Yes/No] [confirm] Y
Router(config-video-led-protocol)#
```

Verifying the Disabled PMV Configuration

To verify whether the PMV configuration is disabled on an LED, run the **show running-config | s cable video** command as provided in the following example:

```
Router# show running-config | s cable video

cable video
  mgmt-intf VirtualPortGroup 0
  service-distribution-group sdg_tbv id 1
    rf-port integrated-cable 7/0/0
```

```
service-distribution-group sdg_tbv1 id 2
  rf-port integrated-cable 7/0/1
virtual-carrier-group vcg_tbv id 1
  service-type narrowcast
  rf-channel 0-95 tsid 1-96 output-port-number 1-96
virtual-carrier-group vcg_tbv1 id 2
  service-type narrowcast
  rf-channel 0-95 tsid 97-192 output-port-number 97-192
bind-vcg
  vcg vcg_tbv sdg sdg_tbv
  vcg vcg_tbv1 sdg sdg_tbv1
logical-edge-device led_tbv id 1
  protocol table-based
    virtual-edge-input-ip 174.101.1.1 input-port-number 1
    vcg vcg_tbv
    vcg vcg_tbv1
    active
```

Configuration Examples

This section provides examples for configuring PMV on table-based video.

Example 1: Assigning PMV to a Session on a Single RF Channel

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#cable video
Router(config-video)#mgmt-intf VirtualPortGroup 0
Router(config-video)#service-distribution-group sdg-1 id 1
Router(config-video-sdg)#rf-port integrated-cable 8/0/0
Router(config-video-sdg)#service-distribution-group sdg-2 id 2
Router(config-video-sdg)#rf-port integrated-cable 8/0/1
Router(config-video-sdg)#virtual-carrier-group vcg-1 id 1
Router(config-video-vcg)#encrypt
Router(config-video-vcg)#service-type narrowcast
Router(config-video-vcg)#rf-channel 20 tsid 1-21 output-port-number 1-21
Router(config-video-vcg)#virtual-carrier-group vcg-2 id 2
Router(config-video-vcg)#encrypt
Router(config-video-vcg)#service-type narrowcast
Router(config-video-vcg)#rf-channel 20 tsid 22-42 output-port-number 22-42
Router(config-video-vcg)#bind-vcg
Router(config-video-bd)#vcg vcg-1 sdg sdg-1
Router(config-video-bd)#vcg vcg-2 sdg sdg-2
Router(config-video-bd)#logical-edge-device led1 id 1
Router(config-video-led)#protocol table-based
Router(config-video-led-protocol)#virtual-edge-input-ip 174.101.1.1 input-port-number 1
Router(config-video-led-protocol)#vcg vcg-1
Router(config-video-led-protocol)#vcg vcg-2
Router(config-video-led-protocol)#pmv
%%All sessions configured for this LED will be removed.
Enable PMV? [Yes/No] [confirm]Y
Router(config-video-led-protocol)#active
Router(config-video-led-protocol)#table-based
Router(config-video-tb)#vcg vcg-1
Router(config-video-tb-vcg)#rf-channel 20
Router(config-video-tb-vcg-sess)#session TBV70 input-port 1 start-udp-port 49153
processing-type remap start-program 7001 start-pmv 230 bit-rate 2000000
Router(config-video-tb-vcg)#vcg vcg-2
Router(config-video-tb-vcg)#rf-channel 20
Router(config-video-tb-vcg-sess)#session TBV_VCG2 input-port 1 start-udp-port 50153
num-sessions-per-qam 15 processing-type remap start-program 7001 start-pmv 230 bit-rate
```

```
2000000
Router(config-video-tb-vcg)#
```

Example 2: Assigning PMV to Sessions for Multiple RF Channels in a VCG

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#cable video
Router(config-video)#mgmt-intf VirtualPortGroup 0
Router(config-video)#encryption
Router(config-video-encrypt)#linecard 8/0 ca-system powerkey scrambler des
%WARNING: Linecard has to be reloaded for scrambling to work.

%WARNING: Standby linecard 7 has to be reloaded for video redundancy to work properly.

Router(config-video-encrypt-dvb-conf)#service-distribution-group sdg1 id 1
Router(config-video-sdg)#onid 100
Router(config-video-sdg)#rf-port integrated-cable 8/0/0
Router(config-video-sdg)#service-distribution-group sdg2 id 2
Router(config-video-sdg)#onid 200
Router(config-video-sdg)#rf-port integrated-cable 8/0/1
Router(config-video-sdg)#service-distribution-group sdg3 id 3
Router(config-video-sdg)#onid 300
Router(config-video-sdg)#rf-port integrated-cable 8/0/2
Router(config-video-sdg)#service-distribution-group sdg4 id 4
Router(config-video-sdg)#onid 400
Router(config-video-sdg)#rf-port integrated-cable 8/0/3
Router(config-video-sdg)#service-distribution-group sdg5 id 5
Router(config-video-sdg)#onid 500
Router(config-video-sdg)#rf-port integrated-cable 8/0/4
Router(config-video-sdg)#service-distribution-group sdg6 id 6
Router(config-video-sdg)#onid 600
Router(config-video-sdg)#rf-port integrated-cable 8/0/5
Router(config-video-sdg)#service-distribution-group sdg7 id 7
Router(config-video-sdg)#onid 700
Router(config-video-sdg)#rf-port integrated-cable 8/0/6
Router(config-video-sdg)#service-distribution-group sdg8 id 8
Router(config-video-sdg)#onid 800
Router(config-video-sdg)#rf-port integrated-cable 8/0/7
Router(config-video-sdg)#service-distribution-group sdg1dup id 9
Router(config-video-sdg)#onid 900
Router(config-video-sdg)#rf-port integrated-cable 8/0/0
Router(config-video-sdg)#virtual-carrier-group vcg1 id 1
Router(config-video-vcg)#encrypt
Router(config-video-vcg)#service-type narrowcast
Router(config-video-vcg)#rf-channel 0-55 tsid 1-56 output-port-number 1-56
Router(config-video-vcg)#virtual-carrier-group vcg2 id 2
Router(config-video-vcg)#encrypt
Router(config-video-vcg)#service-type narrowcast
Router(config-video-vcg)#rf-channel 0-55 tsid 57-112 output-port-number 57-112
Router(config-video-vcg)#virtual-carrier-group vcg3 id 3
Router(config-video-vcg)#encrypt
Router(config-video-vcg)#service-type narrowcast
Router(config-video-vcg)#rf-channel 0-55 tsid 113-168 output-port-number 113-168
Router(config-video-vcg)#virtual-carrier-group vcg4 id 4
Router(config-video-vcg)#encrypt
Router(config-video-vcg)#service-type narrowcast
Router(config-video-vcg)#rf-channel 0-55 tsid 169-224 output-port-number 169-224
Router(config-video-vcg)#virtual-carrier-group vcg5 id 5
Router(config-video-vcg)#encrypt
Router(config-video-vcg)#service-type narrowcast
Router(config-video-vcg)#rf-channel 0-55 tsid 1-56 output-port-number 225-280
Router(config-video-vcg)#virtual-carrier-group vcg6 id 6
```

```
Router(config-video-vcg)#encrypt
Router(config-video-vcg)#service-type narrowcast
Router(config-video-vcg)#rf-channel 0-55 tsid 57-112 output-port-number 281-336
Router(config-video-vcg)#virtual-carrier-group vcg7 id 7
Router(config-video-vcg)#encrypt
Router(config-video-vcg)#service-type narrowcast
Router(config-video-vcg)#rf-channel 0-55 tsid 113-168 output-port-number 337-392
Router(config-video-vcg)#virtual-carrier-group vcg8 id 8
Router(config-video-vcg)#encrypt
Router(config-video-vcg)#service-type narrowcast
Router(config-video-vcg)#rf-channel 0-55 tsid 169-224 output-port-number 393-448
Router(config-video-vcg)#bind-vcg
Router(config-video-bd)#vcg vcg1 sdg sdg1
Router(config-video-bd)#vcg vcg2 sdg sdg2
Router(config-video-bd)#vcg vcg3 sdg sdg3
Router(config-video-bd)#vcg vcg4 sdg sdg4
Router(config-video-bd)#vcg vcg5 sdg sdg5
Router(config-video-bd)#vcg vcg6 sdg sdg6
Router(config-video-bd)#vcg vcg7 sdg sdg7
Router(config-video-bd)#vcg vcg8 sdg sdg8
Router(config-video-bd)#logical-edge-device led1 id 1
Router(config-video-led)#protocol table-based
Router(config-video-led-protocol)#virtual-edge-input-ip 174.102.1.1 input-port-number 2
Router(config-video-led-protocol)#vcg vcg1
Router(config-video-led-protocol)#vcg vcg2
Router(config-video-led-protocol)#active
Router(config-video-led-protocol)#logical-edge-device led2 id 2
Router(config-video-led)#protocol table-based
Router(config-video-led-protocol)#virtual-edge-input-ip 174.101.1.1 input-port-number 1
Router(config-video-led-protocol)#vcg vcg5
Router(config-video-led-protocol)#vcg vcg6
Router(config-video-led-protocol)#vcg vcg7
Router(config-video-led-protocol)#vcg vcg8
Router(config-video-led-protocol)#pmv
%%All sessions configured for this LED will be removed.
Enable PMV? [Yes/No] [confirm]Y
Router(config-video-led-protocol)#active
Router(config-video-led-protocol)#logical-edge-device led3 id 3
Router(config-video-led)#protocol table-based
Router(config-video-led-protocol)#virtual-edge-input-ip 174.103.1.1 input-port-number 3
Router(config-video-led-protocol)#vcg vcg3
Router(config-video-led-protocol)#vcg vcg4
Router(config-video-led-protocol)#active
Router(config-video-tb)#table-based
Router(config-video-tb)#vcg vcg5
Router(config-video-tb-vcg)#rf-channel 0-55
Router(config-video-tb-vcg-sess)#session SESS_TB input-port 1 start-udp-port 50000
num-sessions-per-qam 20 processing-type remap start-program 1 start-pmv 0 bit-rate 1800000
Router(config-video-tb-vcg-sess)#vcg vcg6
Router(config-video-tb-vcg)#rf-channel 0-55
Router(config-video-tb-vcg-sess)#session SESS_TB input-port 1 start-udp-port 52000
num-sessions-per-qam 20 processing-type remap start-program 1 start-pmv 0 bit-rate 1800000
Router(config-video-tb-vcg-sess)#vcg vcg7
Router(config-video-tb-vcg)#rf-channel 0-55
Router(config-video-tb-vcg-sess)#session SESS_TB input-port 1 start-udp-port 54000
num-sessions-per-qam 20 processing-type remap start-program 1 start-pmv 0 bit-rate 1800000
Router(config-video-tb-vcg-sess)#vcg vcg8
Router(config-video-tb-vcg)#rf-channel 0-23
Router(config-video-tb-vcg-sess)#session SESS_TB input-port 1 start-udp-port 56000
num-sessions-per-qam 20 processing-type remap start-program 1 start-pmv 0 bit-rate 1800000
Router(config-video-tb-vcg-sess)#
```

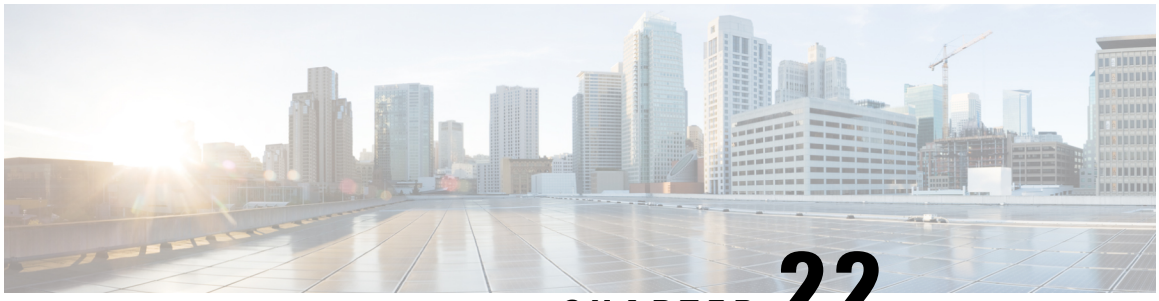
Feature Information for PMV Support

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 https://cfnng.cisco.com/ 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 31: Feature Information for PMV Support for Table-Based Videos

Feature Name	Releases	Feature Information
PMV Support for Table-Based Videos	Cisco IOS XE Everest 16.6.1	This feature was integrated on the Cisco cBR Series Converged Broadband Routers.



CHAPTER 22

Video QAM Replication

The Video QAM replication feature allows video carriers to be replicated to support service group alignment between DOCSIS and Video service groups.

Contents

- QAM Replication, on page 141
- Information About Replication, on page 141
- Configuring Replication for Table-Based or Session-Based Video, on page 143
- Configuration Examples, on page 144
- Feature Information for Replication, on page 145

QAM Replication

The QAM replication feature allows duplication of content on multiple QAM carriers. This feature is internal to the cBR-8 and replaces the need for external splitters, allowing content to be replicated across multiple ports on a line card.

Information About Replication

- **Multiple Ports**: Multiple ports in a Service Distribution Group (SDG) replicate all QAMs from the Virtual Carrier Group (VCG) to output port listed in the same SDG.
- **Unicast**: Unicast (Video on Demand) services cannot be replicated across line cards.

Overview of QAM Replication

Video on Demand (VoD) or unicast services cannot be replicated across line cards. You can accomplish replication by adding more than one RF port to an SDG. This feature works for the SDG regardless of whether the video sessions are table-based or session-based.

Replication also applies to the QAM PHY parameters. Hence, the QAM PHY parameters like frequency, annex, and symbol rate of the replicated QAM carrier are the same as the QAM PHY parameters on the pilot QAM carrier.

QAM replication is achieved in two ways: software and hardware. The line card performs the hardware QAM replication. Each line card has the capability to replicate an output QAM (Pilot QAM) from one port to another output QAM (Replicate QAM) on another port.

Note QAM replication in the same port is not supported.

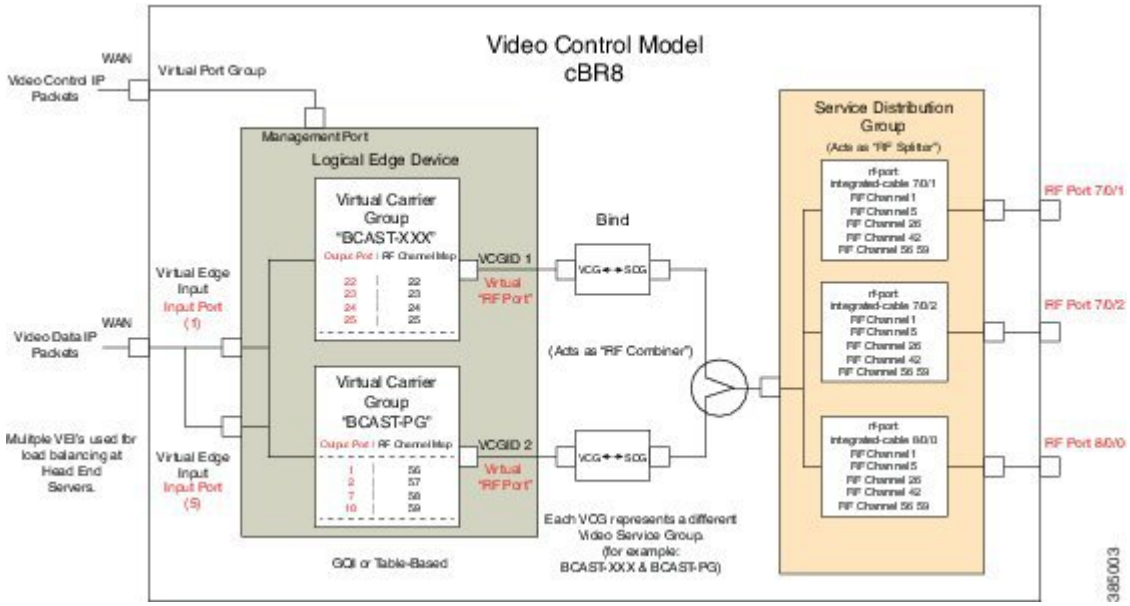
The **service-distribution-group** construct is used to perform replication. Hardware replication is supported when the replication of individual QAM Carriers is limited to the same line card.

The **bind-vcg** construct, which is used to determine the physical QAMs to be replicated, is analogous to combiner and splitter combination. The RF ports combine all the QAMs routed to them. Then, one or more inputs are split to one or more RF output ports.

Benefits of QAM Replication

QAM replication reduces the need for external HFC components like splitters and combiners in the RF plant.

The figure below illustrates the bind operation that replaces a combiner and a splitter and performs replication on multiple ports that are assigned to an SDG.



Prerequisites for Replication

The controller type for the slot/bay/port used for the SDG should be set as 'VIDEO'. The errors corresponding to the incorrect controller type used in the SDG appear during the bind operation.

Perform the following steps to set the controller type:

```
configure terminal
controller Integrated-Cable slot/bay/port
rf-channel start-channel - end-channel
type VIDEO
```

```
start-frequency frequency
rf-output normal
power-adjust number
qam-profile qam-profile number
```

Restrictions for QAM Replication

- Hardware can support QAM replication only within the same line card.
- The output of a source QAM in any port can be replicated to only one QAM in another port. Replication within the same port is not supported.
- The current line card has a maximum of eight ports. Hence, for each line card a pilot QAM can have up to seven replicates (one on each port).
- Standard routing protocols prohibit routing of unicast traffic (VOD) to multiple destinations (across line cards).

Configuring Replication for Table-Based or Session-Based Video

Replication is configured within the SDG by adding a set of RF ports to the same SDG. To configure replication you must choose the Pilot QAM carriers, a set of QAM carriers belonging to a RF port. The Pilot QAM carriers are denoted by the first RF port added under SDG. The rest of RF ports, which carry the replicated content, are specified within this SDG.

Choose the QAM carriers, which carry the content to be replicated, by configuring Virtual Carrier Group (VCG) and specifying the number of QAM channels that are replicated in each RF port. When the pilot QAM carrier is removed, one of the remaining replicated QAM carriers is automatically chosen as pilot QAM carrier.

To configure the replication, complete the following procedure:

```
configure terminal
cable video
service-distribution-group service distribution group name
rf-port integrated-cable slot/bay/port
rf-port integrated-cable slot/bay/port
virtual-carrier-group vcg_replication id number
virtual-edge-input-ip ip-address vrf vrf-name input-port-number number
rf-channel n-m tsid n-m output-port-number n-m
bind-vcg
vcg vcg_replication sdg sdg_replication
```

Verifying Replication of Table Based Video Sessions

To verify the replication information including the replication group ID, pilot or replicant, and the associated status, use the **show cable card** *slot/bay***qam-repl group** command as shown in the example below:

```
Router#show cable card 7/0 qam-repl group
-----------------------------------------------------------------
Grp Slot Chan QAM Grp   Chan
ID Grp cnt type State List
ID  [port:chan state role]
```

```
U:Up   P:Pilot
D:Down R:Replicant

------------------------------------------------------------------
57344 0    4  VID   U   0:21  UP   1:21  UR   2:21  UR   3:21  UR

57345 1    4  VID   U   0:22  UP   1:22  UR   2:22  UR   3:22  UR

57346 2    4  VID   U   0:23  UP   1:23  UR   2:23  UR   3:23  UR

57347 3    4  VID   U   0:24  UP   1:24  UR   2:24  UR   3:24  UR

57348 4    4  VID   U   0:25  UP   1:25  UR   2:25  UR   3:25  UR

57349 5    4  VID   U   0:26  UP   1:26  UR   2:26  UR   3:26  UR

57350 6    4  VID   U   0:27  UP   1:27  UR   2:27  UR   3:27  UR

57351 7    4  VID   U   0:28  UP   1:28  UR   2:28  UR   3:28  UR

57352 8    4  VID   U   0:29  UP   1:29  UR   2:29  UR   3:29  UR

57353 9    4  VID   U   0:30  UP   1:30  UR   2:30  UR   3:30  UR

57354 10   4  VID   U   0:31  UP   1:31  UR   2:31  UR   3:31  UR


------------------------------------------------------------------
Total number of Replication groups on slot 7/0: 11
```

To verify the sessions on the pilot QAM carrier, use the **show cable video session logical-edge-device id** *number* command as shown in the example below:

```
Router#show cable video session logical-edge-device id 1
Total Sessions = 22


Session    Output     Streaming   Session  Destination     UDP        Output      Input
Output    Input    Output   Encrypt  Encrypt   Session
Id         Port       Type        Type      Port           Program    State       State
Bitrate   Bitrate  Type     Status     Name
-------------------------------------------------------------------------------------------
1048598    21         Remap       UDP      172.16.0.1     49152 32    ACTIVE-PSI  ON
1104548  1088424    CLEAR    -         bago_tbv.1.21.49152
1048599    21         Remap       UDP      172.16.0.1     49153 33    ACTIVE-PSI  ON
1104482  1088424    CLEAR    -         bago_tbv.1.21.49153
1048600    22         Remap       UDP      172.16.0.1     49154 34    ACTIVE-PSI  ON
1104922  1090656    CLEAR    -         bago_tbv.1.22.49154
1048601    22         Remap       UDP      172.16.0.1     49155 35    ACTIVE-PSI  ON
1105033  1090534    CLEAR    -         bago_tbv.1.22.49155
1048602    23         Remap       UDP      172.16.0.1     49156 36    ACTIVE-PSI  ON
1114332  1092488    CLEAR    -         bago_tbv.1.23.49156
1048603    23         Remap       UDP      172.16.0.1     49157 37    ACTIVE-PSI  ON
1104353  1092488    CLEAR    -
```

Configuration Examples

The following example configures replication across four RF ports on line card 7/0:

```
configure terminal
cable video
```

```
service-distribution-group sdg replication id 1
rf-port integrated-cable 7/0/0
rf-port integrated-cable 7/0/1
rf-port integrated-cable 7/0/2
rf-port integrated-cable 7/0/3
virtual-carrier-group vcg_replication id  1
virtual-edge-input-ip 172.31.1.1 vrf vrf-name input-port-number 1
rf-channel 21-31 tsid 21-31 output-port-number 21-31
bind-vcg
vcg vcg_replication sdg sdg_replication
```

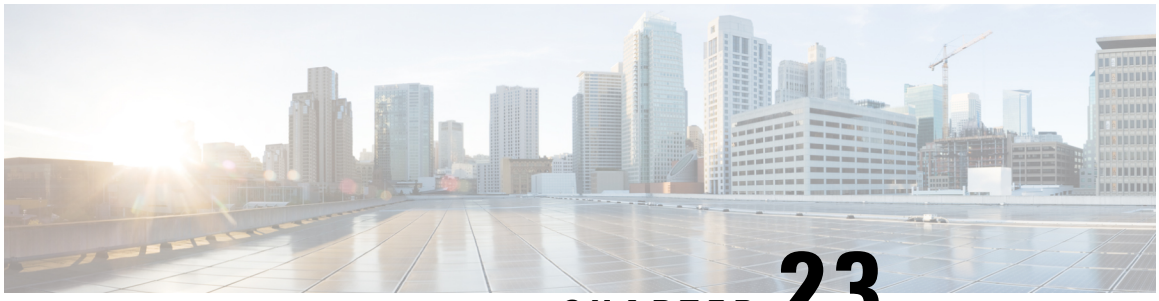
Feature Information for Replication

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 https://cfnng.cisco.com/ 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 32: Feature Information for Replication

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



CHAPTER 23

D6 Discovery Protocol

The D6 discovery protocol is part of the Comcast Next Generation on Demand (NGOD) specification. This protocol helps in advertising the video QAM carrier information like frequency, modulation mode, annex, and edge input for the video traffic such as IP address, group name, maximum bandwidth, and so on, to an Edge Resource Manager (ERM). The D6 discovery protocol also sends unique structured names (topological location information) for each edge input or carrier output. From these structured names, and input and RF port numbers, the ERM can infer the topological network location of both the QAM streaming input port (IP) and RF output port (MPEG).

Contents

- Information About D6 Discovery Protocol, on page 147
- How to Configure the D6 Discovery Protocol, on page 149
- Example: D6 Discovery Protocol Configuration, on page 153
- Deployment Scenario for the D6 Discovery Protocol, on page 154
- Feature Information for D6 Discovery Protocol, on page 155

Information About D6 Discovery Protocol

The following sections provide more information about the D6 discovery protocol.

Overview of the D6 Discovery Protocol

You should configure the D6 discovery protocol for each Logical Edge Device (LED). When the LED is set to active, the D6 discovery protocol establishes a connection with the ERM and sends out the below information to the ERM:

- Streaming Zone—The streaming zone within which the LED operates. You must configure a streaming zone.
- Component Name—The name of the LED for the ERM to associate the subsequent update messages. You must configure a component name.
- Vendor Specific String—Contains the vendor and mode names. When using PME encryption, the D6 vendor-string must be changed to something other than “Cisco”, for example, vendor-string “CBR8”. For PowerKEY encryption, the vendor-string is an optional configuration and the default value is “Cisco CBR8k”.

Edge inputs are configured under the LED or the Virtual Carrier Groups (VCG) associated to the LEDs. For each edge input, the following information is sent to the ERM:

- IP Address—As configured under LED or VCG associated to the LED.
- Port—As configured for each input port.
- Max Bandwidth—As configured under the input group of D6 configuration. The defaults value is 20 Gbps.
- Group name—As configured under the input group of D6 configuration. The default value is the LED name if the input port is configured under LED or the VCG name if the input port is configured under VCG

For every QAM (RF channel) configured under the LED through VCG, the following information is sent to the ERM:

- Route—Route state as Reachable, if a QAM is added, Withdrawn, if a QAM is removed.
- QAM Group Name—As configured for the VCG name.
- QAM Name—Streaming zone.tsid (for example, 1234.100). Streaming zone is configured under D6 and TSID is configured under VCG for every QAM.
- Total Bandwidth— Total bandwidth of the QAM.
- QAM Parameters:
  - Frequency—Center frequency of this carrier
  - Interleaver
  - Modulation Mode
  - TSID
  - Annex—A/B
  - Channel Width - 6 MHz/8 MHz
- UDP Map—This is sent only for the table-based session configurations. A table of the UDP port for each MPEG program number is sent out through this.
- Output Port—The configured VCG ID is sent out as the Output Port ID.

The configuration updates are sent to the ERM through different update messages. D6 also exchanges the keep alive messages periodically to retain the TCP connection with the ERM.

Prerequisites for D6 Discovery Protocol

- As the D6 configuration is placed under the LED protocol configuration, you must complete the following configurations before configuring the D6 discovery protocol:
  - Service Distribution Group (SDG)
  - Virtual Carrier Group (VCG)
  - Bind VCG to SDG

- Logical Edge Device (LED)
- Associate VCG to LED

- Since the D6 discovery protocol requires a management IP for communicating with the external server, ensure that the virtual port group interface is configured and the same is set for the management interface under cable video. Follow the procedure below to configure a virtual port group:

```
configure terminal
cable video
mgmt-intf VirtualPortGroup virtual port group id
```

- If you must configure a Fully Qualified Domain Name (FQDN) for the D6 server configuration instead of the IP address, then ensure that you configure the name server before configuring the D6 discovery protocol. Use the **show ip dns view** command to see if the DNS name server is configured. Follow the procedure below to configure the name server:

```
ip name-server ip address
ip domain name domain name
ip domain lookup
```

How to Configure the D6 Discovery Protocol

You can perform the D6 configuration only when the LED protocol is either table-based or GQI.

Configuring the Mandatory D6 Discovery Protocol Parameters

The mandatory D6 configuration parameters are:

- Management IP—The source IP address used to establish connection with the external D6 server (ERM). The IP address must be in the same subnet as configured in a virtual port group. For GQI LED, this configuration is not needed under the D6 discovery protocol as it is automatically fetched from the GQI LED configuration.
- D6 discovery protocol server IP address and port—This is to identify the remote D6 server (ERM) IP address and listening port used by the D6 client in LED to setup connection with the peer. You can configure only one server address and port per LED. There are two ways to setup the IP address, either by directly providing the IP address or by configuring the FQDN. Either one is sufficient for establishing a connection with the server. If you configure both, then the IP address is preferred over the FQDN. Both IP address and FQDN configurations must point to the same server and port.
- Streaming zone—Streaming zone as configured in the D6 server (ERM). The name should match with the one configured in the ERM for the connection to be established.
- Component name—The name of the Edge QAM device. Each LED is considered by the D6 server as a separate Edge QAM component. This name is used by the D6 server to represent the LED.

Before You Begin

Ensure the following:

- Virtual port group interface is configured and a management IP for the D6 discovery protocol is identified (in case of table-based LED).

- Management interface is set to this virtual port group interface under the cable video configuration.
- You have the D6 server IP address or the FQDN, the port value, and the streaming zone name readily available.
- If FQDN is to be used, ensure that the name server is configured and the FQDN is resolving to the IP address by verifying using the **ping <fqdn>** command.
- The LED is configured with either table-based or GQI protocol.
- The LED turns to active without any issue. If errors occur, resolve them first.
- The LED is set to “no active” state.

To configure the D6 discovery protocol for table-based LEDs, complete the following procedure:

```
 configure terminal
cable video
logical-edge-device device name [id number]
protocol  table-based
no active
discovery-protocol d6
mgmt-ip ip address
streaming-zone name
component-name name
d6-server ip address [port]
d6-server fqdn domain-name [port]
exit
active
```

To configure the D6 discovery protocol for GQI LEDs, complete the following procedure:

```
configure terminal
cable video
logical-edge-device device name [id number]
protocol gqi
no active
discovery-protocol d6
streaming-zone name
component-name name
d6-server ip address [port]
d6-server fqdn domain-name [port]
exit
active
```

Verifying the D6 Discovery Protocol Configurations

To verify the D6 discovery protocol configuration, use the **show cable video logical-edge-device** command as shown in the example below.

This CLI command shows the status and statistics of the D6 client associated to the LED. You can view all the configuration and operation status of the D6 client. In the example below, it shows the duration and the number of open, updated, keepalive and notification messages exchanged between the D6 client and the server, in that duration. It also indicates how many unknown or unrecognized messages are received from the server. When the open message count is more than 1, it indicates that the connection is terminated and reconnected.

```
show cable video logical-edge-device id 1 d6

Logical Edge Device: LED_PME
Id: 1
Protocol: Table-based

D6 Summary:
-------------------------------------------------
Enabled              : Yes
VREP Version         : 2



D6 State             : Established
Management IP        : 1.21.2.250
Source Port          : 6069
D6 server FQDN       : New_host1.test1
D6 Server IP         : 1.200.1.86
D6 Server Port       : 6069
Hold Time(negotiated): 240
Timeout              : 20
Keep Alive Interval  : 80
Streaming Zone       : 3409
Failure Reason       : No Failure
-------------------------------------------------

D6 Statistics:
-----------------------------------------------------------------
Duration  Dir  Open    Update   KeepAlive Notification Unknown
-----------------------------------------------------------------
0          RX     1         0          19            0       0
0          TX     1        17           2            0       0
-----------------------------------------------------------------
```

In the above example, the D6 State as “Established” and the Failure Reason as “No Failure” indicates that the D6 configurations are adequate and it is able to establish the connection with the D6 server or the ERM.

The D6 Statistics section of the output describes various messages exchanged between the D6 client and the D6 server in both the directions (Rx means received and Tx means transmitted). There is no update message from the D6 server to the D6 client, so the Update message count in the RX row should always be 0. The notification message is sent in case of error. When the notification is received, the connection is reset. Unknown message count should be 0, any number greater than 0 indicates a packet corruption. Update message is sent for every update. All the edge input IPs are sent in one update message, but there is a separate update message for every QAM in the LED. So, the update message count increases based on the number of QAMs in the LED. KeepAlive messages are exchanged periodically with the interval defined by the "Keep Alive Interval". This Keep Alive Interval is a function of the Hold time configuration, which is one third of the hold time

Troubleshooting the D6 Mandatory Parameters Configuration

- Troubleshooting tips for possible configuration errors:
  - The management IP should be unique and should be in the subnet of the virtual port group.
  - If both, D6 server IP address and FQDN are configured, ensure that the same port value is used for both.
  - Ensure that the proper D6 server IP address or FQDN name is used.
  - If FQDN is used, verify that the name server is configured and the FQDN gets resolved to the correct IP address by issuing the **ping <fqdn>** command.

- Troubleshooting tips when the D6 state remains Idle:
  - The failure reason indicates the type of failure. For most of the failures, the D6 client retries the connection periodically. Check if it recovers after some time.
  - Verify if the streaming zone configuration is matching with the D6 server setting.
  - Verify if the TCP port number configured for the D6 server in Cisco cBR-8 is matching with the listening port of the D6 server or the ERM.
  - Check if you can ping the D6 server IP address from both the sides, that is, from the Cisco cBR-8 to the D6 server and from the D6 server to the Cisco cBR-8. Try to ping the virtual port group IP and the management IP assigned to the LED from the D6 server. If the ping fails, check the routing between the Cisco cBR-8 and the D6 server.
    - Verify if the D6 server is up and running and ready to accept the connection.
    - Verify if the virtual port group interface is up.
    - Verify if the 10 Gb interface through which the management traffic is passing in to the Cisco cBR-8, is up.

Configuring the D6 Discovery Protocol Optional Parameters

The optional D6 discovery protocol configuration parameters are:

- Vendor string—Vendor specific string for the ERM to identify the vendor. Contains the vendor and the model name. The default value is "Cisco CBR8k"
- Timeout value—Time to wait for the connection in socket call. The default value is 10 seconds.
- Hold time value —This value decides the interval of the keepalive message exchange between the client and the server. The default value is 30 seconds.
- Input group—Each virtual edge input (VEI) IP address under the LED can be assigned an input group name and the maximum bandwidth that is used to send traffic to it. Also, each VCG associated to LED can have a group name and bandwidth. D6 protocol uses this name for all the VEI IP addresses under the VCG. This information is used in the D6 messages when advertising the edge inputs to the D6 server. If these parameters are not configured for the group name, then the LED name for VEI IP addresses under the LED or the VCG name for the VEI IP addresses under the VCG is used. For bandwidth, the default value is 20 Gbps.

Repeat this command for each VEI IP address and VCG under the LED.

Before You Begin

- Ensure that the VEI IP addresses are configured under the LED.
- Ensure that the VCGs are associated to the LED.

To configure the D6 discovery protocol optional parameters, complete the following procedure:

```
configure terminal
cable video
logical-edge-device device name [id number]
protocol  table-based
```

```
no active
discovery-protocol d6
vendor-string <string>
timeout seconds
holdtime seconds
input-group vcg id <id> group-name <name>[ bandwidth <mbps>]
input-group led vei-ip <ip> group-name <name>[ bandwidth <mbps>]
exit
active
```

Verifying the Hold Time and Timeout Settings

To verify the hold time and timeout settings, use the **show cable video logical-edge-device** command. The output is the same as shown in the Verifying the D6 Discovery Protocol Configurations, on page 150 section. The hold time affects the keepalive interval, so the new value for the keepalive interval should be one third of the hold time. Also, in the D6 statistics section, the keepalive count increases (in the TX row) based on the keepalive interval.

Troubleshooting the D6 Optional Parameters Configuration

These are optional parameters and do not affect the basic functionalities of D6 discovery protocol. Any change in the D6 discovery protocol configuration will result in a reset of the D6 connection and a reconnection with the new values. So, the D6 state will momentarily move to Idle and then back to Established state.

Example: D6 Discovery Protocol Configuration

The following example shows a complete D6 configuration:

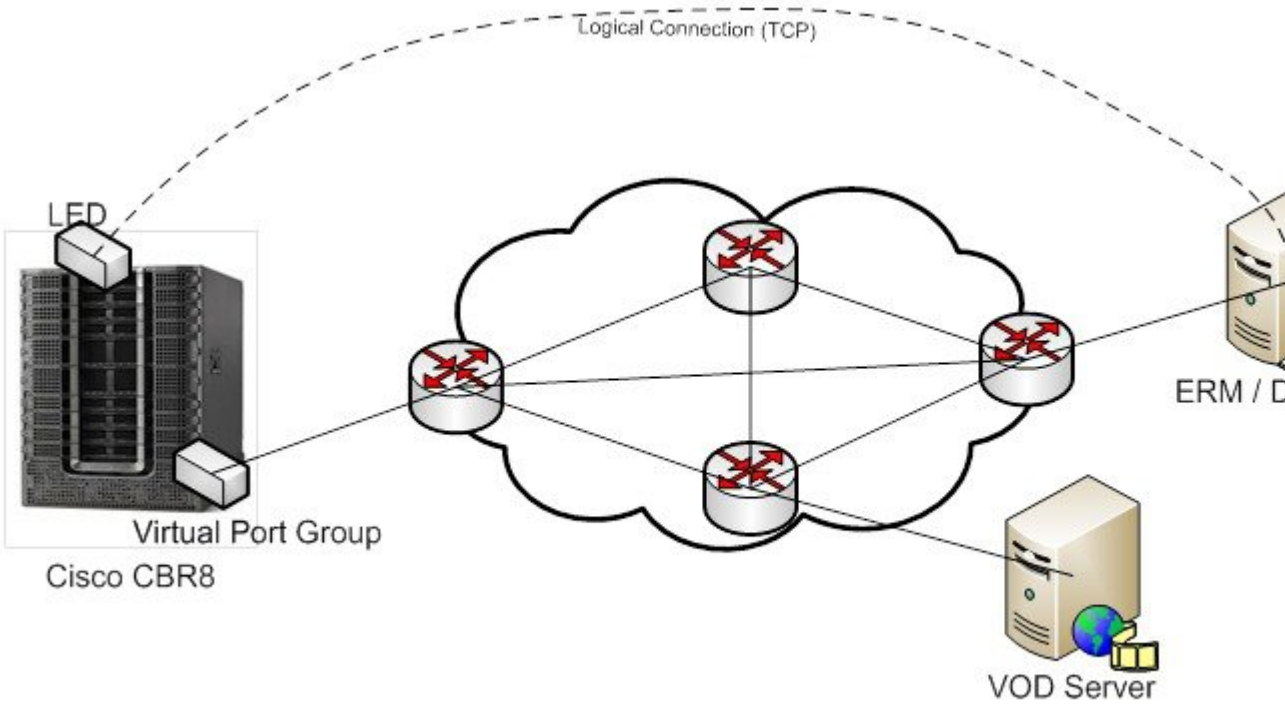
```
cable video
  mgmt-intf VirtualPortGroup 0
  encryption
    linecard 7/0 ca-system pme scrambler dvs042
    pme vodsid 111
    pme cem 1.200.1.163 5000
    pme mgmt-ip 1.25.2.6
  service-distribution-group sdg-pme id 1
    rf-port integrated-cable 7/0/7
  virtual-carrier-group vcg-pme id 1
    encrypt
    service-type narrowcast
    rf-channel 18 tsid 18 output-port-number 23
  bind-vcg
    vcg vcg-pme sdg sdg-pme
  logical-edge-device led-pme id 1
    protocol table-based
      virtual-edge-input-ip 174.101.1.1 vrf Video-VOD-Vrf input-port-number 1
      vcg vcg-pme
      discovery-protocol d6
        mgmt-ip 1.25.2.7
        vendor-string cBR8
        streaming-zone 3509
        component-name led56100
        d6-server 1.200.1.99 17654
 timeout 20
        holdtime 60
      active
```

```
 table-based
   vcg vcg-pme
     rf-channel 18
      session sess1 input-port 1 start-udp-port 49152 num-sessions-per-qam 2 processing-type
remap start-program 1 jitter 100 cbr
```

Deployment Scenario for the D6 Discovery Protocol

The diagram below depicts a typical topology for the D6 feature:

Figure 2: D6 Deployment



- The advertised edge input IPs over D6 protocol to ERM makes the ERM aware of the edge input options for the QAMs. When multiple VEI IP features are used, the D6 advertises all of the available VEI IPs to the ERM. This enables the ERM to identify the most feasible edge input IP for sending the video traffic to the QAMs, based on the physical topology.
- As D6 advertises the QAMs available in the LED, and updates the ERM whenever new QAMs are added or the existing QAMs are removed, the ERM is always updated about the resources that it owns.
- D6 advertises the UDP port used for each MPEG program number of the table-based sessions. This enables the ERM to identify the proper use of UDP ranges for each TSIDs or QAMs.

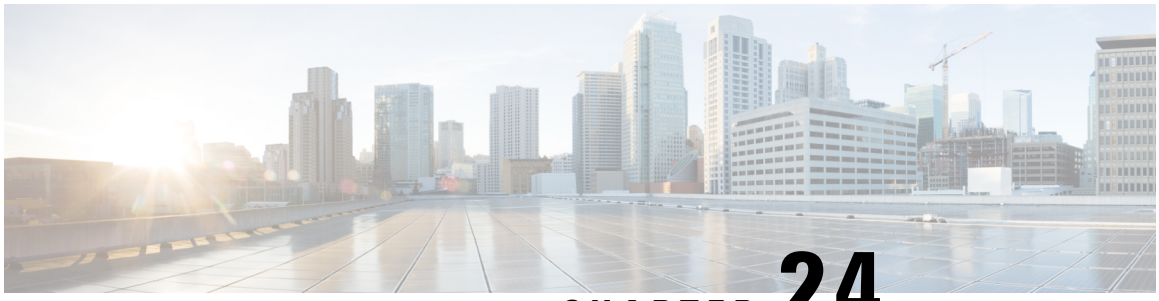
Feature Information for D6 Discovery Protocol

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 https://cfnng.cisco.com/ 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 33: Feature Information for D6 Discovery Protocol

Feature Name	Releases	Feature Information
D6 Discovery Protocol	Cisco IOS XE Everest 16.6.1	This feature was integrated on the Cisco cBR Series Converged Broadband Routers.



CHAPTER 24

Switched Digital Video

- Switched Digital Video Services, on page 157
- QAM Sharing, on page 159
- QAM Replication, on page 159
- MPTS Pass-through Session, on page 160
- Configuring Multicast Routing, on page 160
- Configuring Multicast Label, on page 161
- Configuring Multicast Table-based Sessions, on page 161
- Configuring Source Switching, on page 162
- Verifying Switched Digital Video Configuration, on page 162
- Configuration Examples for Switched Digital Video, on page 163
- Troubleshooting Switched Digital Video Configuration, on page 167
- Feature Information for Switched Digital Video, on page 167

Switched Digital Video Services

The Switched Digital Video (SDV) services are supported for the MPEG video subsystem on the Cisco cBR-8 router. It consists of Multicast IP Packet based video streams that are managed as "Video Sessions".The Cisco cBR-8 router supports both Any Source Multicast (ASM) and Source Specific Multicast (SSM) sessions.

- For ASM, the input is identified by the group IP address.
- For SSM, the input is identified by the source and group IP address pair.

In both cases, the UDP ports are ignored. Both ASM and SSM can co-exist but cannot overlap in a group IP address. Hence, for a group IP address, either a single ASM, or one or more SSM can be used.

Session Cloning

Session cloning refers to the ability of forwarding an input to multiple output QAM channels. Only multicast sessions can be cloned. The output QAM channels are located on the same or different line cards. However, an input cannot be cloned on the same QAM channel. Cloning is available on session-based GQIv2 or Table-based sessions. It is applicable to re-mapped, pass-through, and data piping sessions. All cloned sessions must have the same processing type, bitrate and jitter value. For re-mapped sessions, each output copy will have a different output program number.

Redundant Multicast Sources

The redundant multicast sources feature supports up to four SSM/ASM multicast address pairs per video session. However, only multicast traffic from one source is forwarded to the output QAMs. When the active source fails, another source is chosen automatically. Multicast sources must be unique within a redundant group and cannot overlap across redundant groups.

The order of the sources is critical when multicast sessions are configured via GQI or VSRM. For a given group IP address, the source IP addresses must be specified in the same order.

For example: The group IP address 232.1.2.3 used with two sessions must have the source IP addresses specified in the same order.

Session A configured with group IP 232.1.2.3 source 174.2.3.4 source2 174.4.5.6 source3 174.7.8.9 and session B or any session created after session A configured using group IP 232.1.2.3, must have the source IP addresses in this same order as specified for session A. That is, source 174.2.3.4 source2 174.4.5.6 source3 174.7.8.9.

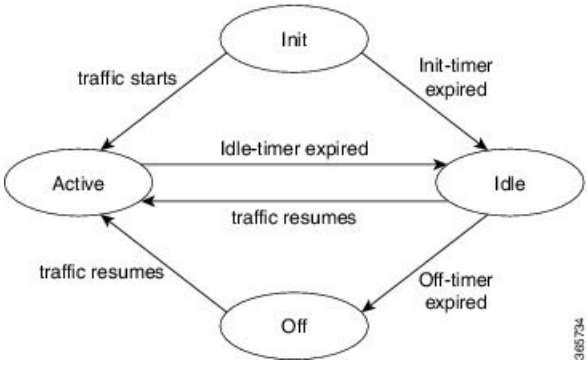
This ensures that all sessions switch to the same source IP address when a source switch occurs. Additionally, sessions configured via GQI have up to three sources available for redundancy, whereas multicast labels configured for table-based sessions have up to four sources available for redundancy.

Multicast labels must use unique groups and S/G pairs. These pairs cannot be used by other multicast labels or by multicast sessions that use S/G pairs. For example, when one multicast session uses {[S1, G], [S2, G] and [S3, G]}, another session cannot use {[S1, G], [S4, G]}.

Multicast source change is based on the session state; INIT, IDLE, ACTIVE or OFF. A session configured for the first time is in INIT state and stays in this state for a brief time. If traffic starts before the INIT timer expires, it moves to the ACTIVE state, otherwise to the IDLE state.

When traffic starts, the session remains in ACTIVE state as long as traffic continues to flow. When traffic stops for a time longer than the IDLE timer, the session moves to IDLE state. During IDLE state, PAT and PMT of the session is retained as the output. If traffic resumes in this state, the session moves to ACTIVE state again with all its previous PSI and remapping information unaltered.

In IDLE state, if traffic does not start or resume before the OFF timer expires, the session transitions to OFF state. When traffic resumes for a session in OFF state, it is treated as a new session.



Sessions that transition from ACTIVE to IDLE have higher priority and will be moved to the backup source than those that were newly created and have changed from INIT to IDLE.

Benefits of Switched Digital Video

Switched Digital Video provides the following benefits:

- Saves space, maintenance and cost.
- Allows customers to oversubscribe bandwidth.

Prerequisites for Switched Digital Video

- To access multicast capability, configure multicast routing.
- To switch sources for table-based sessions, configure at least two sources for a multicast label and then associate with the desired session.

Restrictions for Switched Digital Video

- While creating a multicast label, up to four sources can be associated with one group IP address.
- Labels are used with table-based video sessions only.
- Sessions created with GQI Tools do not use labels. However, they can have up to three sources associated with one group IP address.

QAM Sharing

Unicast and multicast video sessions can co-exist on the same QAM channel for VOD, SDV or Gaming sessions. QAM sharing requires a common Edge Resource Manager to avoid oversubscription of QAM resources between services.

Note QAM sharing with MPTS pass-thru sessions is not supported.

QAM Replication

Multicast sessions can be replicated from one port to other ports on the same line card and/or across line cards.

The difference between a cloned session and replicated sessions is:

- Cloned sessions are initiated by a user on session creation. Each session has a unique session id and may have different output configuration.
- Replicated sessions have the same output configuration attributes. For sessions that are replicated across line cards, session on each line card will have its own unique session id.

MPTS Pass-through Session

Switched digital video (SDV) sessions are typically multicast SPTS remap type. The Cisco cBR-8 router also supports multicast MPTS pass-through and data-piping session types.

The MPTS session is assumed to have no collision in the PID space and program number space with other sessions that already exist within a QAM. Hence, SPTS remap and MPTS pass-through sessions cannot co-exist on the same QAM. Otherwise, there might be conflict when the PID and program numbers in the MPTS and SPTS remuxing are not unique on the output QAM channel.

For a pass-through session:

- The PAT is snooped and regenerated with the correct TSID.
- The PMT and other program data are not changed.
- PID remapping is not performed.
- Input NULL packets are dropped.
- Oversubscription results in random TP dropping, and all ghost PIDs are preserved in the output.

Configuring Multicast Routing

You can enable IP Multicast Distributed Switching (MDS) to provide distributed switching of multicast packets received at the line cards.

```
enable
configure terminal
 ip multicast-routing distributed
 ip pim ssm range all-multicasts
 ip pim rp-address ip-address
 interface type number
  ip pim sparse-dense-mode
  ip igmp version 3
 cable video
  multicast-uplink interface-name access-list access-list-name
```

When more than one physical or logical interfaces are used for reverse path forwarding (RPF) lookup, use loopback interface in **multicast-uplink** command and make sure that the loopback interface is routable/reachable on your network. Loopback interface of the cBR-8 can be enabled with **ip pim spare-mode** command and it is reachable to multicast source or reverse path.

Below is an example of configuration:

```
Router> enable
Router# configure terminal
Router(config)# cable video
Router(config-video)# multicast-uplink 'Loopback0' access-list "acl_name1" access-list-global
 "acl_name2" rp "rp-address"

Router(config)# interface Loopback0
Router(config-if)# ip address <ipaddress> <mask>
```

```
Router(config-if)# ip pim sparse-mode
Router(config-if)# end

Router(config)# ip access-list standard acl_name2
Router(config-std-nacl)# 10 permit 232.0.0.0 0.255.255.255
Router(config-std-nacl)#20 permit 227.0.0.0 0.255.255.255
Router(config-std-nacl)#30 permit 228.0.0.0 0.255.255.255
Router(config-std-nacl)#40 permit 231.0.0.0 0.255.255.255
Router(config-std-nacl)#50 permit 230.0.0.0 0.255.255.255

Router(config)# ip access-list standard acl_name1
Router(config-std-nacl)#10 permit 232.0.0.0 0.255.255.255
Router(config-std-nacl)#20 permit 231.0.0.0 0.255.255.255
```

`acl_name1` is a named-access-list to provisioned by user which provides multicast prefix belong to SSM range. Default is 232.*.*.*

`acl_name2` is a named-access-list to provisioned by user which provides multicast prefix belong to both SSM/ASM range.

`rp-address` is the actual IP address of the RP if ASM used.

Configuring Multicast Label

The Cisco cBR-8 router supports up to four multicast address pairs per multicast session for backup purpose. To specify additional sources for a multicast session for table-based, a label needs to be configured and attached to the session configuration. A maximum of 2000 multicast labels can be created but only 2048 multicast addresses can be active at a time.

Multicast label is used for table-based session configuration when more than one multicast source [S, G] is used as backup for the sessions. A mullticast label can only be created or deleted; it cannot be modified. The multicast label cannot be deleted before the sessions using it are removed.

Groups used by multicast labels must be unique like the multicast S/G pairs. However, sources may be used by more than one label as long as the group is unique. A maximum of 4 multicast sources is allowed in one label. If the label is used in multiple sessions, the sessions are considered as cloned sessions.

```
enable
configure terminal
 cable video
  table-based
   multicast-label label group group-ip source source-ip source2 source-ip source3
 source-ip source4 source-ip
```

Configuring Multicast Table-based Sessions

Similar to table-based unicast session configuration, sessions can be configured as individual sessions under each QAM carrier that is assigned to a table-based LED.

A multicast session can be configured with a single input multicast input source or multiple input sources for backup purpose. For multiple backup sources, a label is required to be associated with the session configuration. Same label can be applied to multiple sessions on different QAM channel. These sessions are considered as cloned sessions.

For session cloning on multiple QAMs within the same line card, only one copy of the traffic is forwarded to the line card. The line card replicates the input packets and forwards them to multiple QAMs. Each cloned copy of a remapped session will have the same or different output program number.

```
enable
configure terminal
 cable video
  table-based
   vcg vcg-name
    rf-channel channel
     session session-name group group-ip source source-ip processing-type {remap
 | passthru | data} start-program program-num [bit-rate bit-rate-number] [jitter
 jitter-number] [cbr | vbr]
```

Configuring Source Switching

Source switching happens automatically when the current source goes down. If more than one source IP is configured, the software will automatically switch to the next valid source IP, if it is available. However, to force switch from one valid source to another valid source, use the following commands:

```
Router(config)# cable video source-switch from-group group-ip from-source
source-ip

or

Router(config)# cable video source-switch to-group group-ip to-source source-ip
```

Verifying Switched Digital Video Configuration

```
Router#show cable video session logical-edge-device id 2
Total Sessions = 4

Session    Output     Streaming   Session Session Source                  UDP   Output
Input      Output Input    Output   Encrypt  Encrypt        Session
Id         Port       Type        Type    Ucast Dest IP/Mcast IP (S,G)    Port  Program
State      State  Bitrate  Bitrate  Type     Status         Name
-------------------------------------------------------------------------------------
2097152    142        Remap       SSM     175.2.5.6,232.5.6.7             0     1       OFF
        ON     0        0        CLEAR    -              SESS_PME2.1.7.338
2097153    163        Remap       SSM     175.6.1.13,232.2.1.6            0     2
INIT       ON     0        0        CLEAR    -              SESS_PME3.1.7.497
2097154    184        Passthru    SSM     175.2.6.7,232.5.6.15            0     -       OFF
        ON     0        0        CLEAR    -              SESS_PME4.1.7.656
2097155    230        Data-Piping SSM     175.7.2.2,232.2.6.7             0     -       OFF
        ON     0        0        CLEAR    -              SESS_PME6.1.7.978

Router#show cable video session logical-edge-device id 2 session-id 2097152
Session Name        : SESS_PME2.1.7.338
Session Id:         : 2097152
Creation Time:      : Fri Jun 24 16:30:45 2016
```

```
Output Port         : 142
TSID                : 142
ONID                : 0
Number of Sources   : 1
  Source IP         : 175.2.5.6
  Group IP          : 232.5.6.7
  UDP Port          : 0
Config Bitrate      : not specified
Jitter              : 100 ms
Processing Type     : Remap
Stream Rate         : VBR
Program Number      : 1
Idle Timeout        : 2000 msec
Init Timeout        : 2000 msec
Off Timeout         : 60 sec
Encryption Type     : CLEAR
Encryption Status   : -

Input Session Stats:
====================
  State: OFF, Uptime: 0 days 00:26:35
  IP Packets: In 0, RTP 0, Drop 0
  TP Packets: In 0, PCR 0, PSI 0, Null 0
              Unreference 0, Discontinuity 0
  Errors: Sync loss 0, CC error 0, PCR Jump 0,
          Underflow 0, Overflow 0, Block 0
  Bitrate: Measured 0 bps, PCR 0 bps

Output Session Stats:
=====================
  State: ON, Uptime: 0 days 00:26:35
  TP Packets: In 0, PCR 0, PSI 0,
              Drop 0, Forward 0, Insert 0
  Errors: Info Overrun 0, Info Error 0, Block 0, Overdue 0,
          Invalid Rate 0, Underflow 0, Overflow 0
  Bitrate: Measured 0 bps
```

Configuration Examples for Switched Digital Video

Example 1: Table-based Multicast Session Configuration

```
enable
configure terminal
ip pim rp-address 9.1.1.1
ip pim ssm range all-multicasts
ip access-list standard all-multicasts
 permit 233.0.0.0 0.255.255.255
 permit 234.0.0.0 0.255.255.255
 permit 235.0.0.0 0.255.255.255
 permit 236.0.0.0 0.255.255.255
 permit 237.0.0.0 0.255.255.255
 permit 238.0.0.0 0.255.255.255
 permit 232.0.0.0 0.255.255.255
 permit 224.0.0.0 0.255.255.255
 permit 239.0.0.0 0.255.255.255
interface TenGigabitEthernet4/1/2
 ip address 2.33.1.1 255.255.255.252
 ip pim sparse-mode
 ip igmp version 3
```

```
 ip ospf 64512 area 9
 load-interval 30
cable video
  multicast-uplink TenGigabitEthernet4/1/2 access-list all-multicasts
  service-distribution-group sdg-1 id 1
    rf-port integrated-cable 7/0/0
  virtual-carrier-group vcg-1 id 1
    service-type narrowcast
    rf-channel 0-55 tsid 1-56 output-port-number 1-56
  bind-vcg
    vcg vcg-1 sdg sdg-1
  logical-edge-device led_multicast id 1
    protocol table-based
      virtual-edge-input-ip 174.102.1.1 input-port-number 1
      vcg vcg-1
      active
  table-based
   multicast-label label1 group 232.2.1.1 source 175.2.2.2
    vcg vcg-1
      rf-channel 0
        session mcast1 multicast-label label1 processing-type remap start-program 1 jitter
 100 vbr
        session mcast2 group 236.0.1.1 source 175.10.5.2 processing-type passthru jitter
100 cbr
```

Example 2: Table-based Configuration for Replicated Multicast Pass-through Sessions

Below is a table-based configuration for multicast pass-through sessions replicated to all QAM ports on the same line card.

```
enable
configure terminal
cable video
  multicast-uplink TenGigabitEthernet4/1/2 access-list all-multicasts
  service-distribution-group sdg1 id 1
    rf-port integrated-cable 7/0/0
    rf-port integrated-cable 7/0/1
    rf-port integrated-cable 7/0/2
    rf-port integrated-cable 7/0/3
    rf-port integrated-cable 7/0/4
    rf-port integrated-cable 7/0/5
    rf-port integrated-cable 7/0/6
    rf-port integrated-cable 7/0/7
  virtual-carrier-group vcg1 id 1
    rf-channel 0-95 tsid 0-95 output-port-number 1-96
  bind-vcg
    vcg vcg1 sdg sdg1
  logical-edge-device led1 id 1
    protocol table-based
      virtual-edge-input-ip 174.102.1.1 input-port-number 1
      vcg vcg1
      active
  table-based
    multicast-label mlabel1 group 236.0.1.1 source 175.10.5.2 source2 175.10.6.20 source3
175.10.7.2
    vcg vcg1
     rf-channel 0
      session mcast1 multicast-label mlabel1 processing-type passthru vbr
     rf-channel 5
      session mcast2 group 237.0.1.1 source 175.10.6.2 processing-type passthru vbr
```

Example 3: QAM Sharing Configuration

Below is an example of how to create a PMT encrypted table-based session for both VOD and SDV on the same QAM channel on 7/0/0 RF port.

```
cable video
  multicast-uplink TenGigabitEthernet4/1/2 access-list all-multicasts
  mgmt-intf VirtualPortGroup 0
  encryption
    linecard 7/0 ca-system pme scrambler dvs042
    pme vodsid 111
    pme cem 1.200.1.163 5000
    pme mgmt-ip 1.33.2.6
  service-distribution-group sdg1 id 1
    rf-port integrated-cable 7/0/0
  virtual-carrier-group vcg1 id 1
    virtual-edge-input-ip 174.102.1.1 input-port-number 1
    encrypt
    service-type narrowcast
    rf-channel 20-34 tsid 20-34 output-port-number 20-34
  bind-vcg
    vcg vcg1 sdg sdg1
  logical-edge-device led1 id 1
    protocol table-based
      vcg vcg1
      active
  table-based
    multicast-label mlabel1 group 236.0.1.1 source 175.10.5.2 source2 175.10.6.2 source3
175.10.7.2
    vcg vcg1
      rf-channel 20
        session VOD input-port 1 start-udp-port 49152 processing-type remap start-program
1 jitter 100 vbr
       session SDV multicast-label mlabel1 processing-type remap start-program 1000 jitter
 100 vbr
!
```

Example 4: QAM Replication Configuration

Below is an example of how to configure multicast sessions with four backup sources and replicated on multiple line cards and multiple RF ports within the same line card.

```
cable video
  multicast-uplink TenGigabitEthernet4/1/2 access-list all-multicasts
  service-distribution-group sdg-1 id 1
    rf-port integrated-cable 7/0/0
    rf-port integrated-cable 7/0/1
    rf-port integrated-cable 8/0/0
    rf-port integrated-cable 8/0/1
  virtual-carrier-group vcg-1 id 1
    service-type broadcast
    rf-channel 0-55 tsid 1-56 output-port-number 1-56
bind-vcg
    vcg vcg-1 sdg sdg-1
  logical-edge-device led_multicast id 1
    protocol table-based
      virtual-edge-input-ip 174.102.1.1 input-port-number 1
      vcg vcg-1
    active
  table-based
    multicast-label label1 group 232.2.1.1 source 175.2.2.2 source2 175.2.3.2 source3
175.2.4.2 source4 175.5.1.12
    vcg vcg-1
      rf-channel 0
```

```
        session mcast1 multicast-label label1 processing-type remap start-program 1 jitter
 100 vbr
```

Example 5: SSM Session Configuration

The following examples show how to configure SSM sessions on a range of QAM channels with three multicast sources.

```
table-based
    multicast-label label110_1 group 232.2.1.35 source 175.2.2.2 source2 175.6.1.12 source3
 175.2.9.2
    multicast-label label103_1 group 232.2.1.30 source 175.2.2.2 source2 175.6.1.12 source3
 175.2.9.2
    vcg vcg-uni-multi0
      rf-channel 0
        session mcast multicast-label label110_1 processing-type remap start-program 1
jitter 100 cbr
      rf-channel 6
        session mcast multicast-label label103_1 processing-type remap start-program 1
jitter 100 cbr
```

Example 6: Multicast Session with Virtual Carrier Group as Service Type Broadcast Configuration

```
virtual-carrier-group VCG_PME0 id 1
    service-type broadcast
    rf-channel 20-35 tsid 100-115 output-port-number 100-115

  table-based
    multicast-label a2 group 232.5.6.7 source 175.2.5.6
   multicast-label exampleLabel group 232.2.1.6 source 175.6.1.13 source2 175.6.1.12 source3
 180.1.1.1 source4 175.6.1.14
    vcg VCG_PME2
      rf-channel 22
        session SESS_PME2 multicast-label a2 processing-type remap start-program 1
    vcg VCG_PME3
      rf-channel 23
        session SESS_PME3 multicast-label exampleLabel processing-type remap start-program
 2
```

Example 7: Sessions with Passthru and Data Processing Type

```
table-based
    multicast-label a2 group 232.5.6.7 source 175.2.5.6
   multicast-label exampleLabel group 232.2.1.6 source 175.6.1.13 source2 175.6.1.12 source3
 180.1.1.1 source4 175.6.1.14
    vcg VCG_PME2
      rf-channel 22
        session SESS_PME2 multicast-label a2 processing-type remap start-program 1
    vcg VCG_PME3
      rf-channel 23
        session SESS_PME3 multicast-label exampleLabel processing-type remap start-program
 2
    vcg VCG_PME4
      rf-channel 24
        session SESS_PME4 group 232.5.6.15 source 175.2.6.7 processing-type passthru
    vcg VCG_PME6
      rf-channel 30
        session SESS_PME6 group 232.2.6.7 source 175.7.2.2 processing-type data
```

Troubleshooting Switched Digital Video Configuration

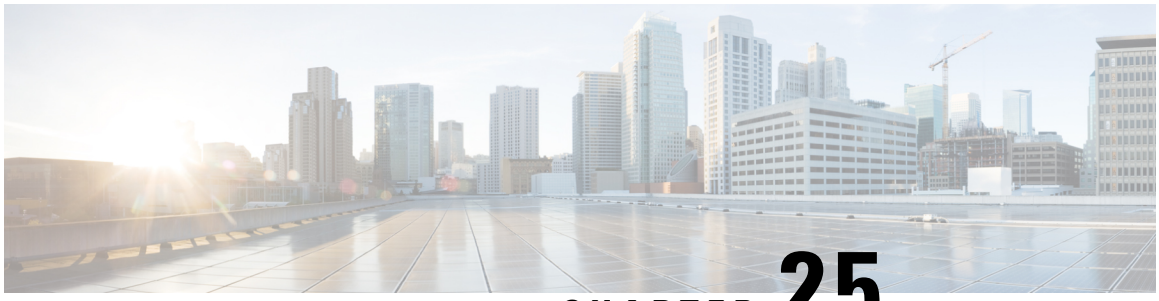
Problem	Possible Causes	Recommended Solution
%ERROR: Duplicate multicast source 175.2.5.6 group 232.5.6.7 not allowed for use in label groupDuplicate.	Group and Source are already used in an existing label.	Assign unique group and source IPs across multicast labels.
%ERROR: Duplicate multicast source 178.3.3.3 group 232.222.222.222 not allowed within label DuplicateSourceHere.	Source has been repeated within a label.	Assign unique source IP within a multicast label.
%ERROR: Duplicate multicast source 175.2.5.6 group 232.5.6.7 not allowed for use in this session.	Session has been created with a duplicate group IP. This group IP has been used in an existing multicast label.	Create the session with a unique group IP.
%ERROR Only one multicast session can be created per multicast session command; rf-channel range values, such as rf-channel 20-30, not allowed.	Session has been created on a range of RF channels.	RF channel range is not allowed. Create the session on an RF channel.

Feature Information for Switched Digital Video

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 https://cfnng.cisco.com/ 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.

Feature Name	Releases	Feature Information
Switched Digital Video	Cisco IOS XE Everest 16.6.1	This feature was integrated on the Cisco cBR Series Converged Broadband Routers.



CHAPTER 25

DVB Video on Demand

The Digital Video Broadcasting (DVB) protocol for encrypting the video services as defined in the ETSI TS 103 197 DVB Simulcrypt specification has been implemented in the cBR-8. This document contains an overview of the commands for configuring DVB on the cBR-8 chassis and the commands for viewing the status of the encryption of services.

Contents

- Information About DVB VOD, on page 169
- How to Configure DVB, on page 171
- Configuration Examples, on page 175
- Additional References, on page 177
- Feature Information for Low Latency VOD Support, on page 177

Information About DVB VOD

Overview of DVB VOD

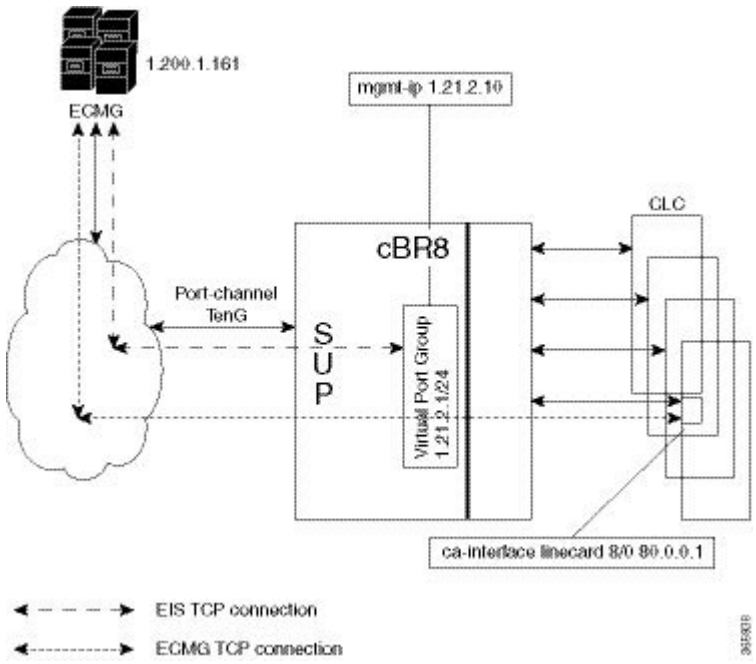
This feature enables the operator to scramble the video sessions on the chassis. It involves the configuration to establish a connection with the Entitlement Control Message Generator (ECMG) and the Event Information Scheduler (EIS).

The two primary modes of scrambling are: session based scrambling and tier-based scrambling. The basic difference between the two modes is that the manner in which the Entitlement Control Messages (ECM) are requested from the ECMG. For session based scrambling, a control word (CW) is generated once every Crypto Period (CP) and the ECM is requested for each session. For tier-based scrambling, the control word is generated once every CP and the ECM generated by the ECMG for the CW is used by all the sessions in the chassis.

Session based Scrambling Setup

The connection with the external EIS Server is established via the Virtual Port Group in the Supervisor. The connection with the external ECMG server is established via the linecard.

Figure 3: Session based Setup



Fail-to-Clear

The fail-to-clear-duration feature is supported on DVB sessions and DualCrypt encryption modes. Based on the session encryption, the following two features are supported on the Cisco cBR Series Converged Broadband Routers.

Fail-to-Clear Duration for DVB Session-based Encryption

This feature is used along with DVB or DualCrypt encryption with external Event Information Scheduler (EIS) configuration. When encryption for a session fails in the Cisco cBR-8, this feature enables the operator to control the configured DVB-encrypted sessions to function without encryption for a configured duration. If the encryption still fails, the DVB session is marked as `Fail-to-black` after the fail-to-clear duration timeout.

Fail-to-Clear for DVB Tier-based Encryption

This feature is used along with Tier-based configuration. When encryption for a session fails in Cisco cBR-8, this feature enables the operator to control the configured DVB-encrypted sessions to function without encryption.

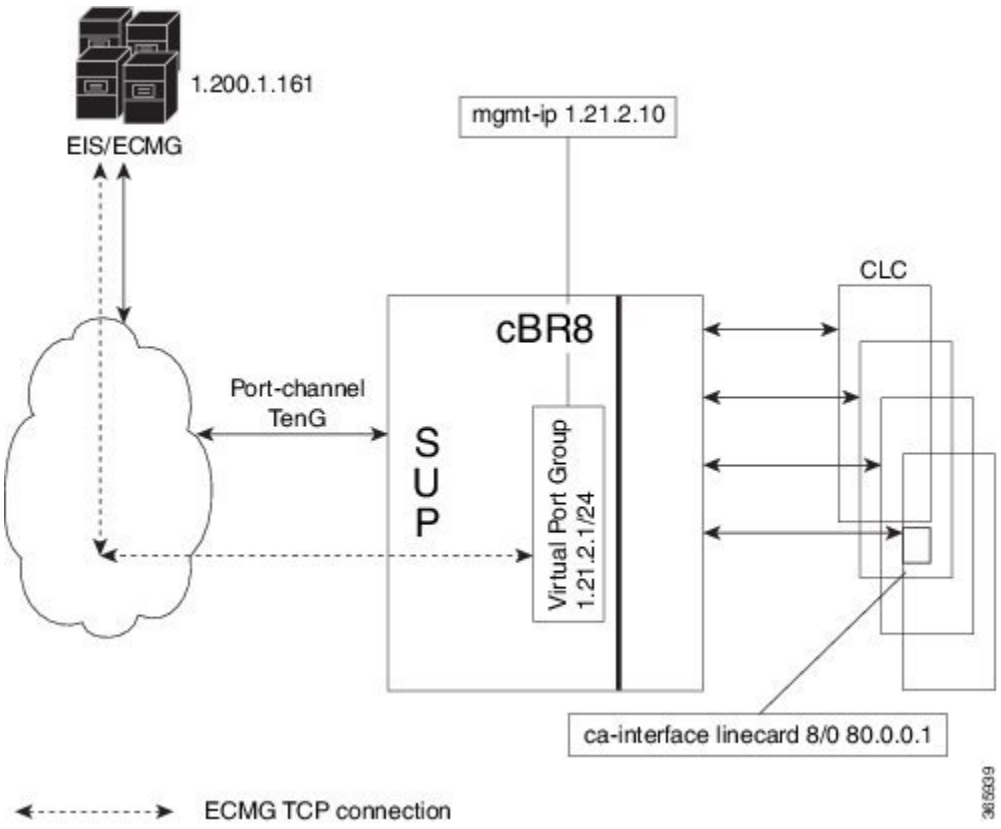
If fail-to-clear is configured, tier-based configuration is enabled, and then if the encryption fails, the DVB session's `Encrypt Status` is marked as `clear`. The status changes to `Encrypted` when the encryption starts.

This feature is not enabled by default.

Tier based Scrambling Setup

The connection with the external ECMG server is established via the Virtual Port Group in the Supervisor.

Figure 4: Tier based Setup



Restrictions for DVB

- This feature is applicable only for remapped table based sessions.
- Fail-to-clear-duration feature is applicable only to session-based scrambling for DVB CAS encryption.
- Fail-to-clear feature is applicable only to DVB tier-based scrambling sessions.

How to Configure DVB

Configuring DVB

Before You Begin

- Virtual Port Group interface must be configured and the management IP for DVB must be identified.
- Management interface is set to this Virtual Port Group interface under cable video configuration.
- Logical Edge Device is configured with the table based protocol.
- The encryption algorithm of the linecard is set to DVB-CSA.

- For session based scrambling, the CA interface on the linecard and the route for reaching the ECMG server must be specified.

To configure session based scrambling, follow the steps below:

```
enable
configure terminal
cable video
mgmt-intf VirtualPortGroup group_id
encryption
linecardslot/bay ca-system dvb scrambler dvb-csa
dvb
route-ecmg ECMG_Server_IP_Address Netmask Interface Forwarding_Router_IP_Address
mgmt-ip ip-address
eis EIS_Name id EIS_ID
listening-port port_number
fail-to-clear-duration < duration in seconds>
ca-interface linecardslot/bay IP_Address
ecmg ECMG_Name id ECMG_ID
mode vod linecardslot/bay
type [standard | hitachi | irdeto | nagra| pkey]
ca-system-id CA_System_ID CA_Subsystem_ID
ecm-pid-source [sid | auto | ecm-id | min-ecm-pid | max-ecm-pid]
connection id id priority connection_priority IP_Address Port
```

The fail-to-clear-duration is measured in seconds. The valid values are in the range from 0 to 10800 seconds. The default value is 0.

To configure tier based scrambling, follow the steps below:

```
enable
configure terminal
cable video
mgmt-intf VirtualPortGroup group_id
encryption
linecardslot/bay ca-system dvb scrambler dvb-csa
dvb
mgmt-ip ip-address
ecmg ECMG_Name id ECMG_ID
mode tier-based
type [standard | hitachi | irdeto | nagra| pkey]
ca-system-id CA_System_ID CA_Subsystem_ID
ecm-pid-source [sid | auto | ecm-id]
connection id id priority connection_priority IP_Address Port
tier-based
ecmg id ECMG_ID access-criteriaaccess_criteria_in_hex
fail-to-clear
enable
```

Note If the tier-based configuration is already enabled, you must first disable the tier-based configuration using the **no enable**, before you configure fail-to-clear feature.

Verifying the DVB Configuration

To verify the configuration of the encryption algorithm on the linecard, use the **show cable video encryption linecard** command as shown in the example below:

```
Router# show cable video encryption linecard 7/0
Line card: 7/0
CA System       Scrambler       DVB-Conformance
================================================
dvb             dvb-csa         Enabled
```

To verify the ECMG connection, use the **show cable video encryption dvb ecmg id** *id* **connection** command as shown in the example below:

```
Router# show cable video encryption dvb ecmg id 1 connection
------------------------------------------------------------------------------------------------------
ECMG ECMG           ECMG     CA Sys CA Subsys PID    Lower Upper Streams/ Open Streams/
Auto Chan Slot ECMG        ECMG
ID   Name           Type     ID     ID        Source limit limit ECMG     ECMG          ID
             Connections Application
------------------------------------------------------------------------------------------------------
1    polaris_ecmg01 standard 0x4748 0x0       sid    0     0     1        1
Enabled   RP   1           Tier-Based

ECMG Connections for ECMG ID = 1

-----------------------------------------------------------
Conn Conn     IP          Port    Channel  Conn    Open
-ID  Priority Address     Number  ID       Status  Streams
-----------------------------------------------------------
1    1        10.10.1.1  8888    1        Open    1
```

The sample output of the session based scrambling configuration verification command is shown below:

```
Router# show cable video encryption dvb ecmg id 7 connection
------------------------------------------------------------------------------------------------------
ECMG ECMG           ECMG     CA Sys CA Subsys PID    Lower Upper Streams/ Open Streams/
Auto Chan Slot ECMG        ECMG
ID   Name           Type     ID     ID        Source limit limit ECMG     ECMG          ID
             Connections Application
------------------------------------------------------------------------------------------------------
7    ecmg-7         standard 0x950  0x1234    sid    0     0     1680     1680
Enabled   7    1           VOD

ECMG Connections for ECMG ID = 1

-----------------------------------------------------------
Conn Conn     IP          Port    Channel  Conn    Open
-ID  Priority Address     Number  ID       Status  Streams
-----------------------------------------------------------
1    1        10.10.1.10  8888    1        Open    1
```

The status of the connection with the ECMG Server is indicated by the Conn Status. The Open Streams field indicates the number of Active ECM Streams.

To verify the EIS connection, use the **show cable video encryption dvb eis id** *id* command as shown in the example below:

```
Router# show cable video encryption dvb eis id 1
-------------------------------------------------------------------------------------------
EIS EIS  Peer       Management TCP  CP       CP       Overwrite Fail-To-Clear Connection
ID  Name IP         IP         Port Overrule Duration SCG       Duration      Status
```

```
--------------------------------------------------------------------------------
1   test 10.10.1.11 10.10.1.1  9898 DISABLED 0        DISABLED  400           Connected
```

To verify the CA Interface configuration in the case of session based scrambling, use the **show cable video encryption dvb ca-interface brief** command as shown in the example below:

```
Router# show cable video encryption dvb ca-interface brief
CA Interface configuration

------------------------------
Linecard    IP Address    VRF
------------------------------
7           10.10.1.1     N/A

ECMG Route configuration

-----------------------------------------------------
IP Address    NetMast         Interface
-----------------------------------------------------
10.10.1.10    255.255.255.224   TenGigabitEthernet4/1/2
```

To verify the encryption status of the sessions, use the **show cable video session logical-edge-device id** command as shown in the example below:

```
Router# show cable video session logical-edge-device id 1
Total Sessions = 1

Session Output Streaming Session Session Source                UDP   Output  Input
Output Input   Output  Encrypt Encrypt   Low     Session
Id      Port   Type      Type    Ucast Dest IP/Mcast IP (S, G) Port  Program State
State  Bitrate Bitrate Type    Status    Latency Name
-------------------------------------------------------------------------------------------------------------------
1048576 1      Remap     UDP     10.10.1.1                   49167 20      ACTIVE-PSI
   1695161 1689747 DVB     Encrypted N       dvbsess.1.0.1.0.23167
```

To verify the ECM PID and whether the CA Descriptor is added to the PMT, use the **show cable video session logical-edge-device id session-id** command as shown in the example below:

```
Router# show cable video session logical-edge-device id 1 session-id 1048576
Output PMT Info:
==============================
  Program 20, Version 3, PCR 49, Info len 18,  (CA SYS-ID 4748, PID 79)
  PID 49: Type 2, Info len 0
  PID 50: Type 3, Info len 6, (lang eng)
```

Troubleshooting Tips

If some configuration errors occur, see the following troubleshooting tips:

- The Management IP must be unique and in the subnet of virtual port group.
- Ensure that the ECMG Server is pingable with source interface as the virtual port group from the Cisco cBR-8 console. This indicates that the ECMG Server is reachable and route is valid.
- Ensure that the TCP port number configured for the ECMG Server in the Cisco cBR-8 is the same as that of the ECMG Server listening port.
- Ensure that the management IP is pingable from the EIS Server. Otherwise, check the routing between the cBR-8 chassis and the EIS server.

- Ensure that the listening port that is configured for the EIS is used for establishing the connection from the EIS Server.
- Ensure that the Virtual Port Group interface is active.
- Ensure that the TenGigabitEthernet interface using which the management traffic reaches the Cisco cBR-8 and the interface through which the CA interface route is configured are active.

Configuration Examples

This section provides examples for the DVB configuration.

Example 1: Basic Session-based Scrambling Configuration

```
Router>enable
Router#config terminal
Router(config)#interface VirtualPortGroup0
Router(config-if)#vrf forwarding vrf_script_red_1
Router(config-if)#ip address 10.10.1.1 255.255.255.224
Router(config-if)#no mop enabled
Router(config-if)#no mop sysid
Router(config-if)#exit
Router(config)#cable video
Router(config-video)#mgmt-intf VirtualPortGroup 0
Router(config-video)#encryption
Router(config-video-encrypt)#linecard 7/0 ca-system dvb scrambler dvb-csa
Router(config-video-encrypt-dvb-conf)#exit
Router(config-video-encrypt)#dvb
Router(config-video-encrypt-dvb)#scramble-video-audio
Router(config-video-encrypt-dvb)#route-ecmg 10.10.1.1 255.255.255.224 TenGigabitEthernet4/1/2
 10.10.1.1
Router(config-video-encrypt-dvb)#mgmt-ip 10.10.1.1
Router(config-video-encrypt-dvb)#eis eis-1 id 1
Router(config-video-encrypt-dvb-eis)#listening-port 8890
Router(config-video-encrypt-dvb-eis)#fail-to-clear-duration 400
Router(config-video-encrypt-dvb-eis)#cp-overrule 60
Router(config-video-encrypt-dvb-eis)#overwrite-scg
Router(config-video-encrypt-dvb-eis)#exit
Router(config-video-encrypt-dvb)#ca-interface linecard 1/0 10.10.1.1 vrf vrf_script_red_1
Router(config-video-encrypt-dvb)#ecmg ecmg-7 id 7
Router(config-video-encrypt-dvb-ecmg)#mode vod linecard 7/0
Router(config-video-encrypt-dvb-ecmg)#type standard
Router(config-video-encrypt-dvb-ecmg)#ca-system-id 950 1234
Router(config-video-encrypt-dvb-ecmg)#auto-channel-id
Router(config-video-encrypt-dvb-ecmg)#ecm-pid-source sid
Router(config-video-encrypt-dvb-ecmg)#connection id 1 priority 1 10.10.1.1 8888
Router(config-video-encrypt-dvb-ecmg)#desc-rule desc_8_1 id 1
Router(config-video-encrypt-dvb-ecmg-desc)#add-priv-data at-es-level private-data 12345678
 ecm-ids 81,82,83,84,85
Router(config-video-encrypt-dvb-ecmg-desc)#exit
Router(config-video-encrypt-dvb-ecmg)#overrule
Router(config-video-encrypt-dvb-ecmg-overrule)#max-comp-time 10000
Router(config-video-encrypt-dvb-ecmg-overrule)#min-cp-duration 60000
Router(config-video-encrypt-dvb-ecmg-overrule)#start-delay -5000
Router(config-video-encrypt-dvb-ecmg-overrule)#rep-period 125
Router(config-video-encrypt-dvb-ecmg-overrule)#max-streams 1920
Router(config-video-encrypt-dvb-ecmg-overrule)#end
Router#config terminal
Router(config)#cable video
```

```
Router(config-video)#service-distribution-group sdg-1 id 1
Router(config-video-sdg)#onid 1
Router(config-video-sdg)#rf-port integrated-cable 7/0/0
Router(config-video-sdg)#end
Router(config-video)#virtual-carrier-group vcg-1 id 1
Router(config-video-vcg)#encrypt
Router(config-video-vcg)#service-type narrowcast
Router(config-video-vcg)#rf-channel 0 tsid 1 output-port-number 1
Router(config-video-vcg)#end
Router(config-video)#bind-vcg
Router(config-video-bd)#vcg vcg-1 sdg sdg-1
Router(config-video-bd)#end
Router(config-video)#logical-edge-device led-1 id 1
Router(config-video-led)#protocol table-based
Router(config-video-led-protocol)#virtual-edge-input-ip 10.10.1.1 input-port-number 1
Router(config-video-led-protocol)#vcg vcg-1
Router(config-video-led-protocol)#end
Router(config-video-led)#end
Router(config-video)#table-based
Router(config-video-tb)#vcg vcg-1
Router(config-video-tb-vcg)#rf-channel 0
Router(config-video-tb-vcg-sess)#session tier_vcg-1 input-port 1 start-udp-port 49152
processing-type remap start-program 1 cbr
```

Example 2: Basic Tier-based Scrambling Configuration

```
Router>enable
Router#config terminal
Router(config)#cable video
Router(config-video)#mgmt-intf VirtualPortGroup 0
Router(config-video)#encryption
Router(config-video-encrypt)#linecard 7/0 ca-system dvb scrambler dvb-csa
Router(config-video-encrypt-dvb-conf)#conformance-dvb
Router(config-video-encrypt-dvb-conf)#exit
Router(config-video-encrypt)#dvb
Router(config-video-encrypt-dvb)#scramble-video-audio
Router(config-video-encrypt-dvb)#strong-pairing-enforce
Router(config-video-encrypt-dvb)#mgmt-ip 10.10.1.1
Router(config-video-encrypt-dvb)#ecmg tier-ecmg-1 id 1
Router(config-video-encrypt-dvb-ecmg)#mode tier-based
Router(config-video-encrypt-dvb-ecmg)#type standard
Router(config-video-encrypt-dvb-ecmg)#ca-system-id 4748 0
Router(config-video-encrypt-dvb-ecmg)#auto-channel-id
Router(config-video-encrypt-dvb-ecmg)#ecm-pid-source sid
Router(config-video-encrypt-dvb-ecmg)#connection id 1 priority 1 10.10.1.1 8888
Router(config-video-encrypt-dvb-ecmg)#desc-rule desc_1 id 1
Router(config-video-encrypt-dvb-ecmg-desc)#add-priv-data at-es-level private-data 12345678
 all
Router(config-video-encrypt-dvb-ecmg-desc)#exit
Router(config-video-encrypt-dvb-ecmg)#overrule
Router(config-video-encrypt-dvb-ecmg-overrule)#max-comp-time 10000
Router(config-video-encrypt-dvb-ecmg-overrule)#min-cp-duration 60000
Router(config-video-encrypt-dvb-ecmg-overrule)#start-delay -5000
Router(config-video-encrypt-dvb-ecmg-overrule)#rep-period 125
Router(config-video-encrypt-dvb-ecmg-overrule)#max-streams 1920
Router(config-video-encrypt-dvb-ecmg-overrule)#exit
Router(config-video-encrypt-dvb-ecmg)#exit
Router(config-video-encrypt-dvb)#tier-based
Router(config-video-encrypt-dvb-tb)#ecmg id 1 access-criteria 1234512345
Router(config-video-encrypt-dvb-tb)#fail-to-clear
Router(config-video-encrypt-dvb-tb)#enable
Router#config terminal
Router(config)#cable video
```

```
Router(config-video)#service-distribution-group sdg-1 id 1
Router(config-video-sdg)#onid 1
Router(config-video-sdg)#rf-port integrated-cable 7/0/0
Router(config-video-sdg)#end
Router(config-video)#virtual-carrier-group vcg-1 id 1
Router(config-video-vcg)#encrypt
Router(config-video-vcg)#service-type narrowcast
Router(config-video-vcg)#rf-channel 0 tsid 1 output-port-number 1
Router(config-video-vcg)#end
Router(config-video)#bind-vcg
Router(config-video-bd)#vcg vcg-1 sdg sdg-1
Router(config-video-bd)#end
Router(config-video)#logical-edge-device led-1 id 1
Router(config-video-led)#protocol table-based
Router(config-video-led-protocol)#virtual-edge-input-ip 10.10.1.1 input-port-number 1
Router(config-video-led-protocol)#vcg vcg-1
Router(config-video-led-protocol)#end
Router(config-video-led)#end
Router(config-video)#table-based
Router(config-video-tb)#vcg vcg-1
Router(config-video-tb-vcg)#rf-channel 0
Router(config-video-tb-vcg-sess)#session tier_vcg-1 input-port 1 start-udp-port 49152
processing-type remap start-program 1 cbr
```

Additional References

Related Documents

Related Topic	Document Title
Configuring Tier-Based Scrambling	*Cisco RF Gateway 10 Software Configuration Guide*

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 Low Latency VOD Support

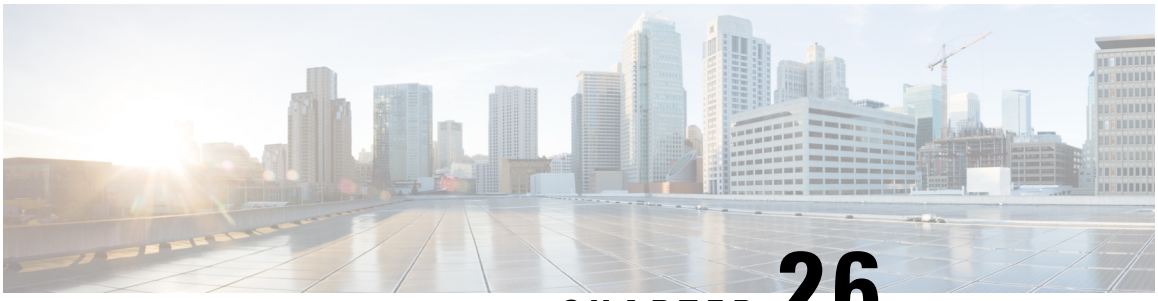
Use Cisco Feature Navigator to find information about the platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release,

feature set, or platform. To access Cisco Feature Navigator, go to the https://cfnng.cisco.com/ 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 34: Feature Information for Low Latency VOD Support

Feature Name	Releases	Feature Information
Low Latency VOD Support	Cisco IOS XE Everest 16.6.1	This feature was integrated on the Cisco cBR Series Converged Broadband Routers.



CHAPTER 26

DualCrypt Encryption Mode Support

The Dualcrypt Encryption feature enables the Session and Resource Manager (SRM) to configure the PowerKey and DVB CAS sessions on the same line card (LC) of the Cisco cBR-8 Converged Broadband Router.

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.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

- Hardware Compatibility Matrix for the Cisco cBR Series Routers, on page 179
- Information about DualCrypt Encryption Mode, on page 181
- How to Configure Dualcrypt Encryption Mode, on page 182
- Configuration Examples, on page 187
- Feature Information for DualCrypt Encryption Mode, on page 190

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 35: 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	**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 • PID—CBR-CCAP-LC-G2-R • PID—CBR-SUP-8X10G-PIC • PID—CBR-2X100G-PIC Digital PICs: • PID—CBR-DPIC-8X10G • PID—CBR-DPIC-2X100G Cisco cBR-8 Downstream PHY Module: • PID—CBR-D31-DS-MOD Cisco cBR-8 Upstream PHY Modules: • PID—CBR-D31-US-MOD

Note Do not use DPICs (8X10G and 2x100G) to forward IP traffic, as it may cause buffer exhaustion, leading to line card reload.

The only allowed traffic on a DPIC interface is DEPI, UEPI, and GCP traffic from the Cisco cBR-8 router to Remote PHY devices. Other traffic such as DHCP, SSH, and UTSC should flow via another router, since DPICs cannot be used for normal routing.

Information about DualCrypt Encryption Mode

You can use this feature when you want the PowerKey and DVB sessions on the same QAM channel. This feature is applicable only to GQI-based sessions, as it uses the Generic QAM Interface (GQI) protocol.

To configure the dualcrypt encryption mode, you should set up connections with Event Information Scheduler (EIS) and Entitlement Control Message Generator (ECMG).

Prerequisites for Dualcrypt Encryption Mode

- Ensure that the following components are available on your system before configuring dualcrypt encryption for sessions.
  - Service Distribution Group (SDG)
  - Virtual Carrier Group (VCG) with encrypt
  - Logical Edge Device (LED) with GQI protocol
  - Event Information Scheduler (EIS)
  - Entitlement Control Message Generator (ECMG)
- Ensure that the VCG is bound to SDG
- Ensure that the VCG is associated to LED
- Ensure that the Virtual Edge Input is configured only on LED
- Ensure that the following configurations are available on your system:
  - The encryption algorithm of the line card is set to DVB-CSA.

    You can set it using the following command:

    ```
    linecard <slot>/<bay> ca-system dualcrypt scrambler dvb-csa
    ```

  - The virtual port group interface is configured and the same is set for the management interface under cable video, because the DVB requires a management IP address for communicating with external servers.

    Use the following commands to set the virtual port group interface as management interface for cable video:

    ```
    configure terminal
    cable video
    mgmt-intf VirtualPortGroup <id>
    ```

  - The CA interface on the line card and the route for reaching the ECMG server are specified for session-based scrambling.

    Use the following commands to specify CA interface and the route:

    ```
    ca-interface linecard <slot>/<bay> <IP_Address>
    route-ecmg <ECMG_Server_IP_Address> <Netmask> <Interface>
    <Forwarding_Router_IP_Address>
    ```

- The **vrf <vrf_name>** keyword is configured for routes to populate on the respective VRFs, if you are using VRF for traffic or management seperately. Configure the CA interface with specific VRF name.

```
ca-interface linecard <slot>/<bay> <IP_Address> vrf <vrf_name>
```

- (Optional) The bind option is used to associate EIS with specific IP address or GQI-based LED

  To use a single IP address for GQI (create and delete sessions) and EIS (provision/de-provision SCGs), the operator should bind the EIS with GQI-based LED using the IP option and configure the required IP address. The IP address should be the subnet of the configured virtual port group. By default, the EIS uses the management IP address configured under DVB and the GQI uses the management IP address configured under LED for session control.

  The following sample commands show how to bind the EIS:

```
configure terminal
    cable video
    encryption
    dvb
    eis <name of eis>
    listening-port <1-65535> bind ip <ip address>
    or
    listening-port <1-65535> bind led <id | name> <led id | led name>
```

Note

- If all configured EIS are bound to a specific IP/LED using the bind option, the configuration of management IP address under DVB is optional.
- The bind option is not available in Cisco RF Gateway 10.

Restrictions for DualCrypt Encryption Mode

The following restrictions are applicable for configuring DualCrypt encryption mode:

- The DualCrypt Encryption feature is applicable only to GQI-based remapped sessions.
- Use this feature only for PowerKey, DVB, and Clear sessions.
- Do not use this feature along with tier-based scrambling mode.

How to Configure Dualcrypt Encryption Mode

Configuring DVB Session for DualCrypt Encryption

This section explains how to configure the session-based scrambling with DualCrypt encryption mode.

Procedure

To configure a DVB session for DualCrypt encryption, use the following commands:

```
enable
configure terminal
cable video
mgmt-intf VirtualPortGroup <group_id>
encryption
linecard <lcslot/subslot> ca-system dualcrypt scrambler dvb-csa
 dvb
  route-ecmg ECMG_Server_IP_Address Netmask Interface Forwarding_Router_IP_Address
  mgmt-ip IP_Address
  eis EIS_Name id EIS_ID
  listening-port port_number [bind {ip <ip address> | led < id <led id >| name <led name>>}]

  ca-interface linecard <slot>/<bay> IP_Address
  ecmg ECMG_Name id ECMG_ID
    mode vod linecard <slot>/<bay>
    type <standard/hitachi/irdeto/nagra/pkey>
    ca-system-id CA_System_ID CA_Subsystem_ID
    ecm-pid-source <sid/auto/ecm-id>
    connection id ID priority connection_priority IP_Address Port
```

Verifying DVB Session for DualCrypt Encryption

To verify the configuration of the encryption algorithm on the linecard, use the **show cable video encryption linecard <slot>/<bay>** command as shown in the efollowing xample:

```
Router#show cable video encryption linecard 8/0
Line card: 8/0
CA System       Scrambler       DVB-Conformance
================================================
dualcrypt       dvb-csa         Enabled
```

To verify the scrambler configuration, use the **show cable video encryption scrambler brief** command as shown in the following example:

```
Router#show cable video encryption scrambler brief
Scrambler information
Chassis wide scrambler: none
-------------------------------------------
Linecard    Current        Configured
            Scrambler      Scrambler
===========================================
1           Not Ready       None
2           Not Ready       None
3           Not Ready       None
4           Not Ready       None
5           Not Ready       None
6           Not Ready       None
7           dvb-csa         None
8           dvb-csa         dvb-csa
9           des/dvs042      None
```

To verify the ECMG connection, use the **show cable video encryption dvb ecmg id <id> connection** command as shown in the following example:

```
Router#show cable video encryption dvb ecmg id <ID> connection
-------------------------------------------------------------------------------------------------------------
ECMG ECMG ECMG     CA Sys CA Subsys  PID     Lower  Upper  Streams/ Open Streams/ Auto Chan
 Slot ECMG         ECMG
ID   Name Type     ID     ID         Source  limit  limit  ECMG     ECMG          ID
       Connections  Application
-------------------------------------------------------------------------------------------------------------
1    test standard 0x950  0x0        sid     0      0      1        1             Enabled
```

```
  7   1            VOD

ECMG Connections for ECMG ID = 1

------------------------------------------------------------------
Conn Conn     IP               Port    Channel Conn       Open
-ID  Priority Address          Number  ID      Status     Streams
------------------------------------------------------------------
1    1        10.10.1.1        9878    1       Open       1
------------------------------------------------------------------
```

The `Conn Status` field shows the status of the connection with the ECMG server and the `Open Streams` field indicates the number of active ECM streams.

To verify the EIS connection, use the **show cable video encryption dvb eis id <id>** command as shown in the following example:

```
Router#show cable video encryption dvb eis id <ID>
-------------------------------------------------------------------------------------------
EIS EIS  Peer       Management TCP  CP       CP       Overwrite Fail-To-Clear Connection
ID  Name IP         IP         Port Overrule Duration SCG       Duration      Status
-------------------------------------------------------------------------------------------
1   test 10.10.1.1 10.10.1.10  9898 DISABLED 0        DISABLED  0             Connected
```

Verifying the GQI Configuration

To verify the GQI connection, use the **show cable video gqi connection** command, as shown in the following example:

```
Router>show cable video gqi connection
LED Management Server      Connection Version Event   Reset      Encryption
ID  IP         IP          Status             Pending Indication Discovery
-------------------------------------------------------------------------
2   10.10.1.1   10.100.1.1 Connected  2       0       ACKED      Sent
```

To verify the statistics of GQI, use the **show cable video logical-edge-device id <ID> statistics** command, as shown in the following example:

```
Router>show cable video logical-edge-device id <ID> statistics

        Create  Delete  Insert Cancel Switch Reset      Encryption Event
        Session Session Packet Packet Source Indication Discovery  Notification
-------------------------------------------------------------------------------
Success 4       0       0      0      0      3          7          0
Error   0       0       0      0      0      0          0          0
Total   4       0       0      0      0      3          7          0
```

Verifying the GQI Sessions for Encryption

To verify whether the sessions are encrypted, use the `show cable video session logical-edge-device id <ID>` command, as shown in the following example, and check the `Encrypt Status` field.

```
Router>show cable video session logical-edge-device id <ID>
Total Sessions = 4

Session Output Streaming Session Session Source              UDP   Output  Input
Output Input    Output  Encrypt Encrypt   Low     Session
Id     Port   Type      Type    Ucast Dest IP/Mcast IP (S,G) Port  Program State      State
  Bitrate  Bitrate Type    Status    Latency Name
-------------------------------------------------------------------------------------------------------------------
```

```
1048580 20     Passthru  UDP     10.10.10.11                  49152 -       ACTIVE-PSI ON
    1713128  1698122 CLEAR   -         N        0x0000000000000000001
1048581 20     Remap     UDP     10.10.10.11                  49153 2       ACTIVE-PSI ON
    1711859  1707422 DVB     Encrypted N         0x0000000000000000002
1048582 23     Passthru  UDP     10.10.10.11                  49154 -       ACTIVE-PSI ON
    1711962  1699101 CLEAR   -         N         0x0000000000000000003
1048583 23     Remap     UDP     10.10.10.11                  49155 4       ACTIVE-PSI ON
    1712498  1707834 DVB     Encrypted N         0x0000000000000000004
```

The session's `Encrypt Status` should be `Encrypted`. The `Output State` should be `ON` to show the proper `Encrypt Status` for DVB sessions. If the `Output State` is `Pending`, the `Encrypt Status` will be shown as `Pending`.

To get a list of SCGs, use the `show cable video scg all` command as shown in the following example:

```
Router>show cable video scg allq
SCGs: 4    Carriers with SCGs: 3

-------------------------------------------------------------------
SCG        ON    TS  SCG Ref Activation CP Duration SCG    Sess LED/
ID         ID    ID  ID      Time       (msec)      Status Id   EIS
-------------------------------------------------------------------
900        1     20  65535   Immediate  10000       Active N/A  1
     Service IDs : 2
     ES PIDs : NA

9001       1     20  65535   Immediate  10000       Active N/A  1
     Service IDs : 1
     ES PIDs : NA

9006       1     22  65535   Immediate  10000       Active N/A  1
     Service IDs : 1
     ES PIDs : NA

9002       1     23  65535   Immediate  10000       Active N/A  1
     Service IDs : 4
     ES PIDs : NA

Number of SCGs = 4
```

Verifying ONID and TSID of the QAMs Configured for Specific LED

To get the details of ONID and TSID configured for QAMs configured under LED, use the **show cable video logical-edge-device id 1**, as shown in the following example, and verify the ONID and TSID details:

```
Logical Edge Device: led1
Id: 1
Protocol: GQI
Service State: Active
Discovery State: Disable
Management IP: 10.10.10.11
MAC Address:
Number of Servers: 1
   Server 1: 10.10.10.11
Reset Interval: 5
Keepalive Interval: 5    Retry Count:3
Number of Virtual Carrier Groups: 1
Number of Share Virtual Edge Input: 1
Number of Physical Qams: 39
Number of Sessions: 4
No Reserve PID Range

Virtual Edge Input:
```

```
Input Port   VEI                 Slot/Bay     Bundle       Gateway
ID           IP                                ID           IP
-------------------------------------------------------------
1            10.10.10.11         7/0          -            -


Virtual Carrier Group:
ID Name Total Total      Service-Distribution-Group Service-Distribution-Group
        VEI   RF-channel Name                       ID
-------------------------------------------------------------------------
1  vcg1 0     39         sdg1                       1


QAM        Port    Physical Admin Operational TSID ONID Output VCG SDG Encryption
Controller Type    QAM ID   State State                Port   ID  ID  Capable
-------------------------------------------------------------------------------
7/0/0:0    RF Port 0        ON    UP          1    1    1      1   1   dualcrypt
7/0/0:1    RF Port 1        ON    UP          2    1    2      1   1   dualcrypt
7/0/0:2    RF Port 2        ON    UP          3    1    3      1   1   dualcrypt
7/0/0:3    RF Port 3        ON    UP          4    1    4      1   1   dualcrypt
7/0/0:4    RF Port 4        ON    UP          5    1    5      1   1   dualcrypt
7/0/0:5    RF Port 5        ON    UP          6    1    6      1   1   dualcrypt
7/0/0:6    RF Port 6        ON    UP          7    1    7      1   1   dualcrypt
7/0/0:7    RF Port 7        ON    UP          8    1    8      1   1   dualcrypt
7/0/0:8    RF Port 8        ON    UP          9    1    9      1   1   dualcrypt
7/0/0:9    RF Port 9        ON    UP          10   1    10     1   1   dualcrypt
7/0/0:10   RF Port 10       ON    UP          11   1    11     1   1   dualcrypt
7/0/0:20   RF Port 20       ON    UP          20   1    20     1   1   dualcrypt
7/0/0:21   RF Port 21       ON    UP          21   1    21     1   1   dualcrypt
7/0/0:22   RF Port 22       ON    UP          22   1    22     1   1   dualcrypt
7/0/0:23   RF Port 23       ON    UP          23   1    23     1   1   dualcrypt
7/0/0:24   RF Port 24       ON    UP          24   1    24     1   1   dualcrypt
7/0/0:25   RF Port 25       ON    UP          25   1    25     1   1   dualcrypt
7/0/0:26   RF Port 26       ON    UP          26   1    26     1   1   dualcrypt
7/0/0:27   RF Port 27       ON    UP          27   1    27     1   1   dualcrypt
7/0/0:28   RF Port 28       ON    UP          28   1    28     1   1   dualcrypt
7/0/0:29   RF Port 29       ON    UP          29   1    29     1   1   dualcrypt
7/0/0:30   RF Port 30       ON    UP          30   1    30     1   1   dualcrypt
7/0/0:31   RF Port 31       ON    UP          31   1    31     1   1   dualcrypt
7/0/0:32   RF Port 32       ON    UP          32   1    32     1   1   dualcrypt
7/0/0:33   RF Port 33       ON    UP          33   1    33     1   1   dualcrypt
7/0/0:34   RF Port 34       ON    UP          34   1    34     1   1   dualcrypt
7/0/0:35   RF Port 35       ON    UP          35   1    35     1   1   dualcrypt
7/0/0:36   RF Port 36       ON    UP          36   1    36     1   1   dualcrypt
7/0/0:37   RF Port 37       ON    UP          37   1    37     1   1   dualcrypt
7/0/0:38   RF Port 38       ON    UP          38   1    38     1   1   dualcrypt
7/0/0:39   RF Port 39       ON    UP          39   1    39     1   1   dualcrypt
7/0/0:40   RF Port 40       ON    UP          40   1    40     1   1   dualcrypt
7/0/0:41   RF Port 41       ON    UP          41   1    41     1   1   dualcrypt
7/0/0:42   RF Port 42       ON    UP          42   1    42     1   1   dualcrypt
7/0/0:43   RF Port 43       ON    UP          43   1    43     1   1   dualcrypt
7/0/0:44   RF Port 44       ON    UP          44   1    44     1   1   dualcrypt
7/0/0:45   RF Port 45       ON    UP          45   1    45     1   1   dualcrypt
7/0/0:46   RF Port 46       ON    UP          46   1    46     1   1   dualcrypt
7/0/0:47   RF Port 47       ON    UP          47   1    47     1   1   dualcrypt
```

Troubleshooting Tips

If some configuration errors occur, see the following troubleshooting tips:

- The Management IP must be unique and in the subnet of virtual port group.

- Ensure that the ECMG Server is pingable with source interface as the virtual port group from the Cisco cBR-8 console. This indicates that the ECMG Server is reachable and route is valid.
- Ensure that the TCP port number configured for the ECMG Server in the Cisco cBR-8 is the same as that of the ECMG Server listening port.
- Ensure that the management IP is pingable from the EIS Server. Otherwise, check the routing between the cBR-8 chassis and the EIS server.
- Ensure that the listening port that is configured for the EIS is used for establishing the connection from the EIS Server.
- Ensure that the Virtual Port Group interface is active.
- Ensure that the TenGigabitEthernet interface using which the management traffic reaches the Cisco cBR-8 and the interface through which the CA interface route is configured are active.
- Ensure that the GQI connection is active and sessions are available to be set up.
- Ensure that the EIS connection is active and SCG is available in the Cisco cBR-8.
- Ensure that the CAS configured for ECMG matches the ECM group in SCG.
- Ensure that the ONID, TSID, and Program Number are synchronized with the configured sessions and SCG.

Configuration Examples

This section provides examples for configuring DualCrypt Encryption Mode:

Example: Basic Session-based Scrambling Configuration

```
cable video
mgmt-intf VirtualPortGroup 0
encryption
linecard 8/0 ca-system dualcrypt scrambler dvb-csa
dvb
route-ecmg 10.10.10.11 255.255.255.224 Port-channel26 2.26.1.2
mgmt-ip 10.10.10.11
eis test id 1
  listening-port 9898
ca-interface linecard 8/0 10.10.10.12
ecmg test id 1
mode vod linecard 8/0
type standard
ca-system-id 950 0
auto-channel-id
ecm-pid-source sid
connection id 1 priority 1 10.10.10.13 9878
service-distribution-group sdg1 id 1
  rf-port integrated-cable 8/0/0
virtual-carrier-group vcg1 id 1
encrypt
service-type narrowcast
rf-channel 20-47 tsid 20-47 output-port-number 20-47
bind-vcg
vcg vcg1 sdg sdg1
logical-edge-device led1 id 1
```

```
protocol gqi
mgmt-ip 10.10.10.10
server 10.100.10.11
virtual-edge-input-ip 10.10.10.11 input-port-number 1
vcg vcg1
active
```

Example: Session-based Configuration with EIS Binding to LED using LED ID

```
cable video
mgmt-intf VirtualPortGroup 0
encryption
linecard 8/0 ca-system dualcrypt scrambler dvb-csa
dvb
route-ecmg 10.10.10.11 255.255.255.224 Port-channel26 10.10.10.10
mgmt-ip 10.10.10.13
eis test id 1
  listening-port 9898 bind led id 1
ca-interface linecard 8/0 10.10.10.14
ecmg test id 1
mode vod linecard 8/0
type standard
ca-system-id 950 0
auto-channel-id
ecm-pid-source sid
connection id 1 priority 1 10.10.10.11 9878
service-distribution-group sdg1 id 1
onid 1
rf-port integrated-cable 8/0/0
virtual-carrier-group vcg1 id 1
encrypt
service-type narrowcast
rf-channel 20-47 tsid 20-47 output-port-number 20-47
bind-vcg
vcg vcg1 sdg sdg1
logical-edge-device led1 id 1
protocol gqi
mgmt-ip 10.10.10.11
server 10.10.10.112
virtual-edge-input-ip 10.10.10.11 input-port-number 1
vcg vcg1
active
```

Example: Configuration with EIS Binding to LED using LED Name

```
cable video
mgmt-intf VirtualPortGroup 0
encryption
linecard 8/0 ca-system dualcrypt scrambler dvb-csa
dvb
route-ecmg 10.10.10.11 255.255.255.224 Port-channel26 10.10.10.11
mgmt-ip 10.10.10.11
eis test id 1
  listening-port 9898 bind led name led1
ca-interface linecard 8/0 10.10.10.11
ecmg test id 1
mode vod linecard 8/0
type standard
ca-system-id 950 0
auto-channel-id
ecm-pid-source sid
connection id 1 priority 1 10.10.10.11 9878
service-distribution-group sdg1 id 1
```

```
onid 1
rf-port integrated-cable 8/0/0
virtual-carrier-group vcg1 id 1
encrypt
service-type narrowcast
rf-channel 20-47 tsid 20-47 output-port-number 20-47
bind-vcg
  vcg vcg1 sdg sdg1
logical-edge-device led1 id 1
protocol gqi
mgmt-ip 10.10.10.11
server 10.10.10.112
virtual-edge-input-ip 10.10.10.11 input-port-number 1
vcg vcg1
active
```

Example: EIS Binding to IP Address Other than Default DVB Management IP Address

```
cable video
mgmt-intf VirtualPortGroup 0
encryption
linecard 8/0 ca-system dualcrypt scrambler dvb-csa
dvb
route-ecmg 10.10.10.11 255.255.255.224 Port-channel26 10.10.10.11
mgmt-ip 10.10.10.11
eis test id 1
  listening-port 9898 bind ip 10.10.10.11
ca-interface linecard 8/0 10.10.10.11
ecmg test id 1
  mode vod linecard 8/0
  type standard
  ca-system-id 950 0
  auto-channel-id
  ecm-pid-source sid
  connection id 1 priority 1 10.10.10.11 9878
service-distribution-group sdg1 id 1
onid 1
rf-port integrated-cable 8/0/0
virtual-carrier-group vcg1 id 1
encrypt
service-type narrowcast
rf-channel 20-47 tsid 20-47 output-port-number 20-47
bind-vcg
  vcg vcg1 sdg sdg1
logical-edge-device led1 id 1
protocol gqi
mgmt-ip 10.10.10.11
server 10.10.10.11
virtual-edge-input-ip 10.10.10.11 input-port-number 1
vcg vcg1
active
```

Example: Session-based Configuration with VRF

```
cable video
  multicast-uplink Loopback410 access-list all-multicast vrf vrf_script_red_1 next-hop
10.10.10.11
  mgmt-intf VirtualPortGroup 0
  encryption
    linecard 1/0 ca-system dvb scrambler dvb-csa
    dvb
      route-ecmg 10.10.10.11 255.255.255.224 Port-channel21 10.10.10.1
      route-ecmg 10.10.10.16 255.255.255.224 Port-channel21 10.10.10.1
```

```
      mgmt-ip 10.10.10.10
      eis pytool1 id 1
        listening-port 2500
        cp-overrule 6
        overwrite-scg
      ca-interface linecard 1/0 10.10.10.0 vrf vrf_script_red_1
      ecmg emcg1 id 1
        mode vod linecard 1/0
        type standard
        ca-system-id 952 0
        auto-channel-id
        ecm-pid-source sid
        connection id 1 priority 1 10.10.10.11 5678
        connection id 2 priority 1 10.10.10.16 8765
      ecmg emcg2 id 2
        mode vod linecard 1/0
        type standard
        ca-system-id 951 0
        auto-channel-id
        ecm-pid-source sid
        connection id 1 priority 1 10.10.10.14 8765
      ecmg emcg3 id 3
        mode vod linecard 1/0
        type standard
        ca-system-id 950 0
        auto-channel-id
        ecm-pid-source sid
        connection id 1 priority 1 10.10.10.11 5678


interface VirtualPortGroup0
   vrf forwarding vrf_script_red_1
   ip address 10.10.10.11 255.255.224.0
   no mop enabled
   no mop sysid
```

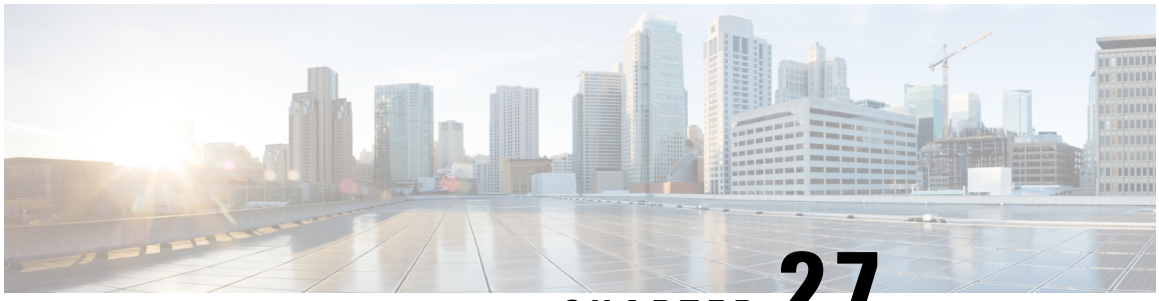
Feature Information for DualCrypt Encryption Mode

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 https://cfnng.cisco.com/ 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 36: Feature Information for DualCrypt Encryption Mode

Feature Name	Releases	Feature Information
DualCrypt Encryption Mode	Cisco IOS XE Everest 16.6.1	This feature was integrated on the Cisco cBR Series Converged Broadband Routers.



CHAPTER 27

Low Latency VOD Support

The Cisco cBR-8 router supports Low Latency Video on Demand (VOD) sessions for gaming.

Contents

- Information About Low Latency VOD Support, on page 191
- How to Configure Low Latency VOD Support, on page 192
- Feature Information for Low Latency VOD Support, on page 194

Information About Low Latency VOD Support

Overview of Low Latency VOD Support

Each Cisco cBR-8 RF linecard supports up to 1280 low latency VOD gaming sessions and up to 64 unique low latency QAMs. These numbers are applicable to both Annex A and B.

An output QAM is treated as low latency if it is associated with a virtual carrier group (VCG) that is configured as low-latency.

A table-based input session is treated as low latency if the session jitter <= 50 ms and output QAM is low latency.

A GQI input session is treated as low latency if the session type is gaming and output QAM is low latency.

Low latency VOD gaming, normal VOD, and Switched Digital Video (SDV) can share the same low latency QAM.

Each Cisco cBR-8 RF linecard supports up to 384 unique normal latency Annex B video QAMs (288 Annex A). Each QAM used for low latency reduces the number of remaining available QAMs by two. For example, the linecard can support up to 256 normal latency and 64 low latency Annex B QAMs.

The average latency of a low latency session is approximately 13 ms plus 50% of the jitter buffer size.

How to Configure Low Latency VOD Support

Configuring the Low Latency Virtual Carrier Group

To configure the low latency virtual carrier group, follow the steps below:

```
enable
configure terminal
cable video
virtual-carrier-group id
low-latency
```

If more than 64 low latency QAM channels are being configured, CLI will output the following error:

```
%ERROR: Number of low latency QAM channels configured has reached the linecard limit.
```

If a QAM is configured for low latency, it cannot be configured for broadcast and vice versa, CLI will output the following errors:

```
%ERROR: Failed to set low latency to virtual group.
Reason: Broadcast service type is set and cannot set low latency.

%ERROR: Failed to set_svctype to virtual group.
Reason: Low latency is set and cannot set service type to broadcast.
```

Verifying the Low Latency Virtual Carrier Group Configuration

To verify the configuration of the low latency virtual carrier group, use the **show cable video virtual-carrier-group** command as shown in the example below:

```
Router# show cable video virtual-carrier-group id 1
Name: vcg1
  ID: 1
  Service Distribution Group Name: sdg1
  Service Distribution Group ID: 1
  Logical Edge Device Name: led1
  Logical Edge Device ID: 1
  ServiceType: narrowcast
  Encrypted: N
  Low Latency: Y
  Number of VEIs: 0
  Virtual Edge Input:
  Input Port   VEI                 Bundle
  ID           IP                  ID
  ------------------------------------------------
  Number of RF-Channels: 8
  RF-Channel Range   TSID Range   Output Port Number Range
  ------------------------------------------------------
  0-7                100-107      100-107
```

Verifying the Low Latency in Linecard

To verify the low latency configuration in the linecard, use the **show cable video low-latency linecard** command as shown in the example below:

```
Router# show cable video low-latency linecard all
Line Card: 1
   Virtual-Carrier-Group: vcg1
   Service-Distribution-Group: sdg1
   Logical-Edge-Device: led1
   Number of RF-Channels: 8
   RF-Channel Range   TSID Range   Output Port Number Range
   ---------------------------------------------------------
   0-7                100-107             100-107

 Line Card: 2
   Virtual-Carrier-Group: vcg2
   Service-Distribution-Group: sdg2
   Logical-Edge-Device: led1
   Number of RF-Channels: 8
   RF-Channel Range   TSID Range   Output Port Number Range
   ---------------------------------------------------------
   0-7                200-207             200-207
```

Configuring the Jitter Buffer Size for Table Based Session

To configure the jitter buffer size for table-based session, follow the steps below:

```
enable
configure terminal
cable video
table-based
vcg vcg_name
rf-channel start_rf_channel-end_rf_channel
session session_name input-port input_port_number start-udp-port
unicast_udp_port_number num-sessions-per-qam max_sessions_per_qam_channel
processing-type [data|passthru|remap| remux] start-program program_number
jitter jitter_value
```

The default jitter buffer size for table-based video is 100 ms.

Configuring the Jitter Buffer Size for GQI

To configure the jitter buffer size for GQI session, follow the steps below:

```
enable
configure terminal
cable video
jitter session_type jitter_value
```

Verifying Jitter Buffer Size for GQI

To verify the jitter buffer size for GQI session, use the **show cable video jitter** command as shown in the example below:

```
Router# show cable video jitter
Session jitter:
  VOD: 200
  SDV: 200
  broadcast: 200
```

```
gaming: 5
table-based: 100
```

Verifying the Low Latency Sessions

To verify the configuration of the low latency session, use the **show cable video session logical-edge-device** command as shown in the example below:

```
Router# show cable video session logical-edge-device id 1
Total Sessions = 160

 Session  Output  Streaming   Session Session Source                UDP   Output  Input
   Output Input    Output   Encrypt  Encrypt  Low     Session
 Id       Port    Type        Type    Ucast Dest IP/Mcast IP (S,G)  Port  Program State
   State  Bitrate  Bitrate  Type     Status   Latency Name

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

 1048576  100     Remap       UDP     174.101.1.1                  49152 1       ACTIVE-PSI
 ON     1723787  1722987  CLEAR    -         Y       t1.1.0.1.0.49152
 1048577  100     Remap       UDP     174.101.1.1                  49153 2       ACTIVE-PSI
 ON     1724147  1722987  CLEAR    -         Y       t1.1.0.1.0.49153
 1048578  100     Remap       UDP     174.101.1.1                  49154 3       ACTIVE-PSI
 ON     1722807  1722987  CLEAR    -         Y       t1.1.0.1.0.49154
 1048579  100     Remap       UDP     174.101.1.1                  49155 4       ACTIVE-PSI
 ON     1723279  1722987  CLEAR    -         Y       t1.1.0.1.0.49155
 1048580  100     Remap       UDP     174.101.1.1                  49156 5       ACTIVE-PSI
 ON     1723665  1722987  CLEAR    -         Y       t1.1.0.1.0.49156
 1048581  100     Remap       UDP     174.101.1.1                  49157 6       ACTIVE-PSI
 ON     1724096  1722987  CLEAR    -         Y       t1.1.0.1.0.49157
 1048582  100     Remap       UDP     174.101.1.1                  49158 7       ACTIVE-PSI
 ON     1724475  1722987  CLEAR    -         Y       t1.1.0.1.0.49158
 1048583  100     Remap       UDP     174.101.1.1                  49159 8       ACTIVE-PSI
 ON     1723166  1722988  CLEAR    -         Y       t1.1.0.1.0.49159
 1048584  100     Remap       UDP     174.101.1.1                  49160 9       ACTIVE-PSI
 ON     1723595  1722988  CLEAR    -         Y       t1.1.0.1.0.49160
 1048585  100     Remap       UDP     174.101.1.1                  49161 10      ACTIVE-PSI
 ON     1724024  1722988  CLEAR    -         Y       t1.1.0.1.0.49161
 1048586  100     Remap       UDP     174.101.1.1                  49162 11      ACTIVE-PSI
 ON     1724425  1722988  CLEAR    -         Y       t1.1.0.1.0.49162
 1048587  100     Remap       UDP     174.101.1.1                  49163 12      ACTIVE-PSI
 ON     1723547  1722989  CLEAR    -         Y       t1.1.0.1.0.49163
 1048588  100     Remap       UDP     174.101.1.1                  49164 13      ACTIVE-PSI
 ON     1722215  1722988  CLEAR    -         Y       t1.1.0.1.0.49164
 1048589  100     Remap       UDP     174.101.1.1                  49165 14      ACTIVE-PSI
 ON     1722683  1722988  CLEAR    -         Y       t1.1.0.1.0.49165
 1048590  100     Remap       UDP     174.101.1.1                  49166 15      ACTIVE-PSI
 ON     1723060  1723001  CLEAR    -         Y       t1.1.0.1.0.49166
  --More--
```

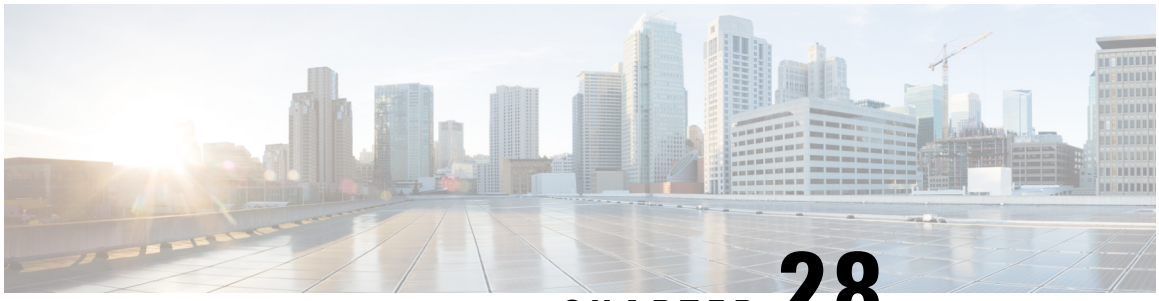
Feature Information for Low Latency VOD Support

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 https://cfnng.cisco.com/ 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 37: Feature Information for Low Latency VOD Support

Feature Name	Releases	Feature Information
Low Latency VOD Support	Cisco IOS XE Everest 16.6.1	This feature was integrated on the Cisco cBR Series Converged Broadband Routers.



CHAPTER 28

Video MIBs

The SCTE-HMS-MPEG-MIB and SCTE-HMS-QAM-MIB are supported under the video management framework of Cisco cBR-8 routers.

- SCTE-HMS-MPEG-MIB, on page 197
- SCTE-HMS-QAM-MIB, on page 198
- CISCO-ENTITY-ALARM-MIB, on page 199

SCTE-HMS-MPEG-MIB

SCTE-HMS-MPEG-MIB MIB module represents the MPEG equipment in the headend. It defines both the MPEG input and output MIB objects for managing MPEG input and output transport streams, programs and elementary streams. It provides both input and output related statistics, as well as program mapping and video session information. It includes the following tables:

mpegInputTSEntry

Provides the details of input transport stream to a video session.

mpegInputProgEntry

Describes the PSI of each incoming program.

mpegProgESEntry

Contains information about the elementary streams in a program.

mpegInputStatsEntry

Each entry in this table describes statistics for each input transport stream.

mpegInputUdpOriginationEntry

Specifies the UDP unicast or multicast flows of an input transport stream. For unicast streams, it represents the UDP port and optionally destination IP address of the input transport stream origination UDP IP flow. For multicast streams, it represents the set of SSM multicast groups of the input transport stream origination UDP IP flow.

mpegInsertPacketEntry

Describes packet insertion information. Typical packets that are inserted at the RF output of a device are PSI, PSIP, and CVCT MPEG packets. These packets have their own PID. This table may be empty if the video device does not support packet insertion or does not have any packet insertion configured.

mpegOutputStatsEntry

Specifies the diagnostic statistics objects for the output transport stream of an MPEG device.

mpegOutputTSEntry

Specifies the attributes of an outgoing transport stream SPTS or MPTS.

mpegOutputProgEntry

Describes the PSI of each outgoing program.

mpegOutputProgElemStatsEntry

Contains the statistical information associated with the elementary streams of an MPEG program.

mpegOutputUdpDestinationEntry

Specifies the UDP unicast or multicast of the output transport stream this entry references.

mpegProgramMappingEntry

Describes program mappings, i.e., ties the input destination to the output destination for every active program in the device.

mpegVideoSessionEntry

Stores video session information. The session type is VOD, SDV or DB. It captures logical information about a video stream, such as source and destination addresses, UDP port etc., and also ties this information with direct mapping of input and output programs.

mpegVideoSessionPtrEntry

Provides a quick reference of the program mapping and input/output transport stream connection information associated with a video session.

mpegInputTSOutputSessionEntry

Specifies the list of output session indexes that the input transport stream entry is feeding. For unicast sessions, it typically points to just one output session. For multicast sessions, it points to all the output sessions using this internally replicated input transport stream.

SCTE-HMS-QAM-MIB

SCTE-HMS-QAM-MIB represents edge QAM equipment present in the headend. It defines QAM channel related configuration MIB objects associated with physical and logical characteristics of the QAM channel. It includes the following tables:

qamChannelTable

Describes the configuration and attribution of each QAM channel designated by ifIndex.

qamChannelCommonTable

Describes QAM channel output bandwidth and utilization information designation by ifIndex.

qamConfigTable

Contains the following parameters for a range of QAM Channels:

- IP addresses configuration for the QAM channels (VEI IP Addresses)
- Program number range associated with QAM channels (constant in Cisco cBR-8 routers)
- UDP port range (constant in Cisco cBR-8 routers)

CISCO-ENTITY-ALARM-MIB

This MIB module defines the managed objects that support the monitoring of alarms generated by physical entities contained by the system, including chassis, slots, modules, ports, power supplies, and fans. It includes the following tables:

ceAlarmDescrMapTable

For each type of entity (represented entPhysicalVendorType OID), this table contains a mapping between a unique ceAlarmDescrIndex and entPhysicalvendorType OID.

ceAlarmDescrTable

This table contains a description for each alarm type defined by each vendor type employed by the system. Observe that this table is sparse in nature, as it is rarely the case that a physical entity type needs to define every alarm in its alarm space.

ceAlarmTable

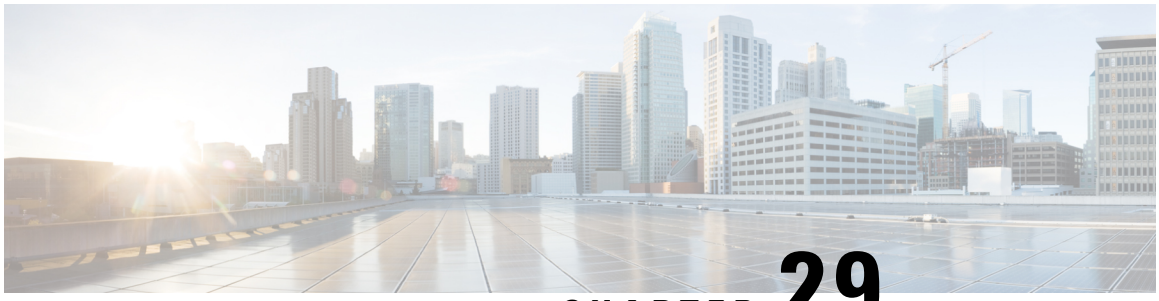
This table specifies alarm control and status information related to each physical entity contained by the system, including the alarms currently being asserted by each physical entity capable of generating alarms.

ceAlarmHistTable

This table contains a history of ceAlarmIndicate and ceAlarmClear traps generated by the agent.

ceAlarmFilterProfileTable

This table contains a list of alarm filter profiles.



CHAPTER 29

Expanded GQI Protocol Support

This document provides information on the GQI protocol support provided by the Cisco cBR-8 series routers. It also explains how to manage the Announce Event Messages generated as part of the GQI support.

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.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

- Hardware Compatibility Matrix for the Cisco cBR Series Routers, on page 201
- Information About GQI Protocol Support, on page 203
- How to Configure GQI Announce Events, on page 205
- Configuration Example for Announce Event, on page 208
- Feature Information for Expanded GQI Protocol Support, on page 208

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 38: 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	**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 • PID—CBR-CCAP-LC-G2-R • PID—CBR-SUP-8X10G-PIC • PID—CBR-2X100G-PIC Digital PICs: • PID—CBR-DPIC-8X10G • PID—CBR-DPIC-2X100G Cisco cBR-8 Downstream PHY Module: • PID—CBR-D31-DS-MOD Cisco cBR-8 Upstream PHY Modules: • PID—CBR-D31-US-MOD

Note Do not use DPICs (8X10G and 2x100G) to forward IP traffic, as it may cause buffer exhaustion, leading to line card reload.

The only allowed traffic on a DPIC interface is DEPI, UEPI, and GCP traffic from the Cisco cBR-8 router to Remote PHY devices. Other traffic such as DHCP, SSH, and UTSC should flow via another router, since DPICs cannot be used for normal routing.

Information About GQI Protocol Support

Cisco cBR-8 routers support the Generic QAM Interface (GQI) version 1, version 1 Extension, and version 2.

- GQIv1—This version does not support announce messages. However, the Cisco cBR-8 router generates GQIv1 extension announce event messages. To use GQIv1, you must block the announce messages on Cisco cBR-8.
- GQI v1 Extension—Provides a more neutral distribution path to non-cisco SRM products. This version supports type-2 commands, three announce messages, and offers a filtering mechanism to alleviate flooding the SRM with events. GQIv1 extension also supports more than 255 QAM carriers on each LED.
- GQI v2—Provides a generic QAM for the Explorer Controller (EC) and USRM.

On Cisco cBR-8, the eQAM is an embedded software process running on the Supervisor card. You can consider the eQAM as a Logical Edge Device (LED) and configure up to a maximum number of 32 LED instances running simultaneously. Each LED manages a set of QAM carriers for video session management. These LEDs interface remotely with SRMs using the GQI protocol.

If the remote SRM registers for both v1 and v2, the LED accepts the latest version. However, when the SRM sends a GQI request as v1, the Cisco cBR-8 router accepts v1, sends a response for v1, and also sends the announce event messages to the SRM in the GQIv1 Extension format.

The following table shows the features supported by GQIv1, GQIv1 Extension, and GQIv2.

Features	GQIv1	GQI v1 Extension	GQI v2
Announce Messages	None	2104, 5406, and 5200	All
Output Port (Number)	<= 255	> 255 Supported	> 255 Supported
Encryption	No	No	Yes

GQI Announce Event Messages

The LED sends Announce events that match the GQI version on the SRM. The GQI v1 Extension protocol uses Announce event messages for GQIv1 Extension and GQI v2 uses Announce event messages for v2.

Some SRMs may not handle the announce events or may only generate a log when it receives the announce event messages from the eQAM, without taking any action. To avoid flooding and minimize the number of Remote Procedure Call (RPC) messages sent to the server, the operator can disable the announce events on the LED through the Cisco cBR-8 CLI.

Cisco cBR does not provide announce event messages for GQIv1. However, with GQI v1 Extension, Cisco cBR provides three announce event messages. The GQIv2 protocol support provides all the supported GQI announce event messages.

Supported Announce Events

GQIv1 Extension supports the following announce events:

- Stream Active (2104)—The stream is successfully established and the session is active.
- Multicast Source Change (5406)—This event is triggered when the LED detects a loss of input of the source stream from the current multicast source and it fails over to a redundant multicast source.
- Stream Lost (5200)—The stream is lost and the video becomes idle or off.

GQIv2 supports the following announce event messages:

Code	Message	Description
2104	Stream Active and PSI built	The stream is successfully established, the PSI is built, and the session is active.
4400	Error Reading Content Data - PID Conflict	In some applications, the SRM can request not to remap the PID (no PID remapping). If this mode is used, the PID conflicts are not revealed to the eQAM until it sees the stream from the data plane. The eQAM sends an Announce request to the SRM when eQAM detects a PID conflict.
4401	Input TS invalid	When PAT and PMT are not found in the input stream.
5200	Stream Lost	The stream is lost and the video becomes idle or off.
5401	Downstream Failure	When QAM fails.
5404	Unable to Join	When LED attempts fails for all multicast transports.
5405	Input Failure	When eQAM fails to update the configuration for existing sessions.
5406	Multicast Source Change	This event is triggered when the LED detects a loss of input of the source stream from the current multicast source and it fails over to a redundant multicast source.
5502	Internal software error	When software error occurs or other codes do not apply.
5602	Bandwidth Exceed	When actual bandwidth exceeds the configured session bandwidth.

Blocking Announce Event Messages

To prevent flooding of too many announce events, you can specify how the announce event messages should be delivered to the SRM. If configured, the announce event is sent one at a time synchronously.

To use blocking mode for announce event messages, specify a timeout value range from 0 to 240 seconds. If the timeout value is greater than zero, after sending the announce event message to the server, LED sets up a timer with the timeout value, and waits for the announce event acknowledgement. If the timer expires before receiving the acknowledgement, the next announce event in the queue is sent and the timer is restarted. The failed announce event is discarded.

To disable blocking the announce event messages, you should set the timeout value to 0 which is the default value. If the value is zero, the LED does not wait for the announce acknowledgement before sending the next message. All announce events are sent to the SRM instantly.

GQI Announce Event Profile

The announce event profile allows the user to define how announce events are managed in the GQI protocol. The profile can include a timeout value for blocking the event messages and the list of events that the operator wants to filter.

The GQI Announce Event Profile provides the following functions and you can assign it to any GQI LED.

- Filtering out all announce events.

  This command disables and does not forward announce events to SRM.

- Timeout value for sending the announce event.
- In blocking mode, this timeout is triggered when the announce event acknowledgement is not received within a specified time.
- Filtering subset of unwanted events.

You can assign the announce event profile to an LED at any time, even when the LED is already active. If the server is already connected and in service, and an event profile is updated, which is already assigned to an LED, all existing announce events in the queue are discarded and restarted according to the new changes.

Prerequisites for Configuring GQI Announce Event Profile

To configuring GQI Announce Event Profile, the announce profile must be applied to the LED that supports the GQI protocol.

Restrictions for Configuring GQI Announce Event Profile

Announce event profile applies only to logical-edge-devices (LED) that support GQI protocol. The profile is not intended for table-based sessions.

How to Configure GQI Announce Events

This section contains the following:

Verifying the Logical Edge Device

To display the Announce Event profile that is assigned to the GQI LED, use the show cable video logical-edge-device command as given in the following example.

```
Router# show cable video logical-edge-device id 2
Logical Edge Device: led2
Id: 2
Protocol: GQI
Service State: Active
Discovery State: Disable
Management IP: 192.0.2.1
MAC Address: <MAC address>
Number of Servers: 2
   Server 1: 203.0.113.1
   Server 2: 203.0.113.1
Reset Interval: 5
Keepalive Interval: 5    Retry Count:3
Announce Event Profile: profile-2     Id: 3
Number of Virtual Carrier Groups: 1
Number of Share Virtual Edge Input: 1
Number of Physical Qams: 4
Number of Sessions: 0
No Reserve PID Range

Virtual Edge Input:
Input Port VEI      Slot/Bay  Bundle  Gateway
ID         IP                 ID      IP
-----------------------------------------------
1          x.x.1.1  7/0        -      -

Virtual Carrier Group:
ID   Name   Total      Total  Service-Distribution-Group  Service-Distribution-Group
VEI         RF-channel        Name                        ID
-------------------------------------------------------------------------------
2   vcg2      0          4    sdg2                         2
```

Verifying the GQI Connection

The following example shows the GQI connection details using the show cable video gqi connections command:

```
Router# show cable video gqi connections

LED  Management  Server   Connection  Protocol Event   Reset       Encryption
ID   IP          IP       Status      Version  Pending Indication  Discovery
-------------------------------------------------------------------------------
2    x.x.x.x     x.x.x.x  Connected     2       2       ACKED        Sent
```

Configuration Example for Announce Event

This section provides example for the GQI Announce Event Profile configuration.

Disabling Announce Event Profile

By default, all announce events are enabled. If all the events are filtered, the ack-timeout configured in the profile is no longer applicable, until you remove the filtering of all-events from the profile.

When you set the filtering to filter all-events, the individual event codes are removed from the CLI. The user is prompted before the changes take effect.

Use the following commands to disable announce events:

```
enable
configure terminal
cable video
  announce-event-profile disable-all id 1
      filter all-events

logical-edge-device led-1 id 1
   protocol gqi
    event-profile disable-all
    vcg vcg-1
    active
```

Filtering Announce Events

You can filter the events, and add or remove a filter, when the LED is in active mode. When the filtering is enabled, the events that are generated and still queued, are discarded, and are not sent to the SRM.

The following example shows how to filter a subset of events to the SRM, and uses synchronous send:

```
cable video
  announce-event-profile gqi-led-1 id 2
      ack-timeout 240
      filter 5502
      filter 5602

logical-edge-device led-1 id 1
   protocol gqi
    event-profile gqi-led-1
    vcg vcg-1
    active
```

Use the no command to revert it to the default value. If the ack-timeout is set to 0 or no ack-timeout, the LED resumes the non-blocking event and sends messages to the SRM. All pending events in the Cisco cBR router queue are forwarded to the SRM without waiting for the announce event acknowledgement. If you remove the filter command, the GQI resumes generating that specific event code and reports it to the SRM.

Verifying the Announce Event Profile Configuration

To display the configuration of announce event profile and a list of LEDs that use the profile, use the **show cable video announce-event-profile** *[name <profile-name> | id <#>]* command as given in the following example.

```
Router# show cable video announce-event-profile id 3
ID:3     Name: profile-2
  ACK timeout: 240 seconds
  Number of Event Filters: 10
    2104 4400 4401 5200 5401 5404 5405 5406 5502 5602

  Number of Logical-edge-device: 2
    ID    Name
    ----------------------------------------------------------------
    2     led2
    3     led3
```

Configuration Example for Announce Event

This section provides example for the GQI Announce Event Profile configuration.

Example: GQI Announce Event Profile Configuration

```
enable
configure terminal
cable video
  announce-event-profile gqi-led-1 id 2
      ack-timeout 240
      filter 5502
      filter 5602

logical-edge-device led-1 id 1
   protocol gqi
    event-profile gqi-led-1
    vcg vcg-1
    active
```

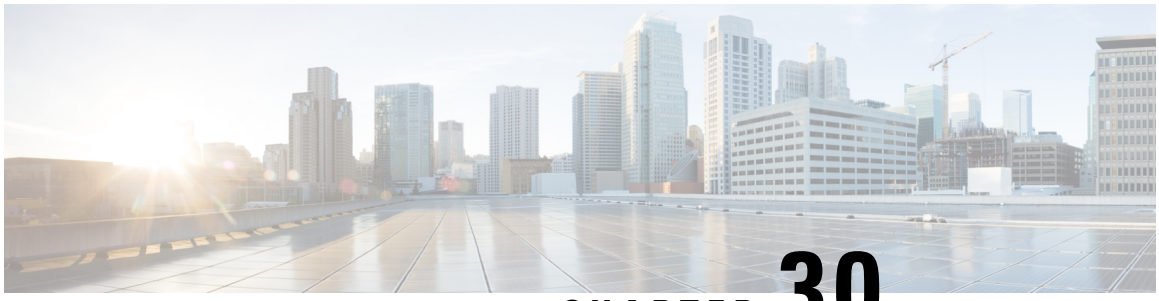
Feature Information for Expanded GQI Protocol Support

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 https://cfnng.cisco.com/ 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 Expanded GQI Protocol Support

Feature Name	Releases	Feature Information
Expanded GQI Protocol Support	Cisco IOS XE Everest 16.6.1	This feature was introduced on the Cisco cBR Series Converged Broadband Routers.



CHAPTER 30

Advanced MPEG Features

This document provides information on the support for advanced MPEG features and how to configure Cisco cBR series routers to avail the support.

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.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

- Advanced MPEG Features, on page 209
- Information About Advanced MPEG Features, on page 209
- How to Configure Advanced MPEG Features, on page 212
- Troubleshooting Tips for Possible Configuration Errors, on page 216
- Configuration Examples for Advanced MPEG Features, on page 217
- Feature Information for Advanced MPEG Features, on page 220

Advanced MPEG Features

Information About Advanced MPEG Features

The Cisco cBR-8 router supports the following advanced MPEG features:

- PID filtering
- Program filtering
- Custom PID remapping
- Multiprogram Transport Stream (MPTS) remuxing
- Enhanced input source switching

Overview of PID Filtering, Program Filtering, and PID Remapping

In a broadcast video environment, PID and program filtering allow you to filter PIDs and programs from a MPTS pass-through stream in the table-based video configuration mode. You can filter up to 32 PIDs and 16 programs for each input stream. PID filtering is supported for both unicast and multicast sessions.

Custom PID remapping allows you to specify remap rules for all four types of processing types—data piping, pass-through, remap, and remux sessions. You can remap both referenced PIDs (PIDs that are part of PMT) and unreferenced PIDs in an input stream.

When remapping referenced ES PIDs of a program on remap or remux session, the corresponding PMT is updated. In case of pass-through sessions, the output retains the pass-through PMT.

Rules for Configuring PID Filtering and PID Remapping

PID filter and remap rules are available in the cable video section of the **sh run | s cable video** command.

- You can specify filter rules for each video session. The key used to apply the remap rules is the combination of vcg, rf-channel, and input stream information.
- For unicast streams, the input stream information is the VEI IP address and the UDP port number.
- For ASM multicast streams, the input stream information is the group IP address.
- For SSM multicast streams, the input stream information is the source IP and the group IP address.
- You can configure up to 32 remap rules for each video session.

Benefits of Using PID Filtering and PID Remapping

Using PID filter and remap rules provide the following benefits:

- Specify PID remapping at the QAM channel level.
- Remap referenced and unreferenced PIDs from data, MPTS, or SPTS streams.
- Block all unreferenced PIDs from data stream or MPTS stream.
- Block specific unreferenced PIDs from data stream or MPTS stream.
- Block PMT PIDs in SPTS and MPTS streams.
- Remap PIDs from data streams as PMT PIDs for the services configured on the QAM channel.
- Insert PAT from an external data stream. *(also blocking the internally generated PAT by edge device being played out)*

Restrictions for PID Remapping

- Only 32 remap rules are allowed for each input stream on a rf-channel. This number of remap rules is inclusive of the specified filter rules.
- For a given RF channel there cannot be remap rules with the same output PIDs.

- For a given input stream on a rf-channel, there cannot be two rules with same input PID remapped to different output PIDs.
- The output PID value in a remap rule can be in a range between 0 to 8190.
- The PMT of remap and remux sessions cannot be remapped.
- When remapping referenced PID for a passthru session, the output PMT retains old value of the referenced PID. For remap session, the output PMT reflects the new value of the referenced PID.

Remapping PAT or SI from External Data Stream

Using remap rules, you can remap a PID that contains Program Allocation Table (PAT) or Service Information (SI) PIDs, on a rf-channel.

When an input stream on a rf-channel contains a rule to remap a data PID to PAT, the internally generated PAT playout is stopped. The PAT playout is dependent on the PID that carries the PAT.

SI PIDs and other data PIDs are remapped as usual.

Blocking Unreferenced PIDs

PIDs that are not part of any program are unreferenced PIDs. You can block unreferenced PIDs on a QAM channel. To block unreferenced PIDs, follow the steps as shown below:

```
Router(config)#cable video
Router(config-video)#filter pid vcg vcg1
Router(cable-video-filter)#rf-channel 20-21
Router(cable-video-filter-ch)#block-unref-pids
```

Overview of Enhanced Input Source Switching

Enhanced input source switching includes the following features:

- Manual switch—You can manually switch to a backup source.

Note The source from which you switch must be active.

- Program Clock Reference (PCR) based switch—You can choose automatic source switching, which is based on the bit rate of PCR PID. For example, when the PCR PID bit rate becomes 0 or the stream does not get PCR for three seconds, the source automatically switches to the backup or the next source.

Benefits of Using Enhanced Input Source Switching

Using enhanced input source switching provides the following benefits:

- In a multicast enviroment, monitor the bit rate of PCR PID. Initiate redundancy by switching to a backup source when the bitrate reaches 0. This is applicable for SPTS streams only.

Note Redundancy support for multicast ASM stream to switch to a backup port instead of a backup source is not supported.

- Support for manually switching to a backup source.

Overview of MPTS Remuxing

In table-based broadcast applications, MPTS remuxing allows you to choose specific programs from MPTS sessions using the program number. You can choose multiple programs from the same MPTS stream on a rf-channel. The programs that you do not choose are dropped. The program PIDs are automatically remapped at the output.

The input MPTS stream can be unicast or multicast stream. You can clone multicast sources across rf-channels. You cannot replicate unicast sources. You can map same input programs to different output programs on different rf-channels.

How to Configure Advanced MPEG Features

Configuring PID Filtering

To configure PID filtering for unicast stream, follow the steps below:

```
cable video
filter pid vcg vcg name
rf-channel range
vei-ip ip address udp-port udp port number
pid range
```

To configure PID filtering for ASM multicast stream, follow the steps below:

```
cable video
filter pid vcg vcg name
rf-channel range
asm-multicast group ip address
pid range
```

To configure PID filtering for SSM multicast stream, follow the steps below:

```
cable video
filter pid vcg vcg name
rf-channel range
ssm-multicast source ip address group ip address
pid range
```

Configuring Program Filtering

To configure program filtering for unicast stream, follow the steps below:

```
cable video
filter program vcg vcg name
rf-channel range
vei-ip ip address udp-port udp port number
program range
```

To configure PID filtering for ASM multicast stream, follow the steps below:

```
cable video
filter program vcg vcg name
rf-channel range
asm-multicast group ip address
program range
```

To configure PID filtering for SSM multicast stream, follow the steps below:

```
cable video
filter program vcg vcg name
rf-channel range
ssm-multicast source ip address group ip address
program range
```

Configuring PID Remapping

To configure custom PID remapping for unicast stream, follow the steps below:

```
cable video
remap pid vcg vcg name
rf-channel range
vei-ip ip address udp-port udp port number
program range range
```

To configure custom PID remapping for ASM multicast stream, follow the steps below:

```
cable video
remap pid vcg vcg name
rf-channel range
asm-multicast group ip address
program range range
```

To configure custom PID remapping for SSM multicast stream, follow the steps below:

```
cable video
remap pid vcg vcg name
rf-channel range
ssm-multicast source ip address group ip address
program range range
```

Configuring Remapping Data PID to PAT PID

To configure remapping data PID to PAT PID for unicast stream, follow the steps below:

```
Router(config)#cable video
Router(config-video)#remap pid vcg vcg1
Router(config-video-remap)#rf-channel 10
```

```
Router(config-video-remap-ch)#vei-ip 174.1.1.1 udp-port 49152
Router(config-video-remap-ch-ucast)#pid 6000 0
```

To configure remapping data PID to PAT PID for ASM multicast stream, follow the steps below:

```
Router(config)#cable video
Router(config-video)#remap pid vcg vcg1
Router(config-video-remap)#rf-channel 10-20
Router(config-video-remap-ch)#ssm-multicast 198.51.100.1 198.51.100.2
Router(config-video-remap-ch-mcast)# pid 6000 0
```

To configure remapping data PID to PAT PID for SSM multicast stream, follow the steps below:

```
Router(config)#cable video
Router(config-video)#remap pid vcg vcg1
Router(config-video-remap)#rf-channel 30
Router(config-video-remap-ch)#asm-multicast 198.51.100.1
Router(config-video-remap-ch-mcast)# pid 6000 0
```

Configuring Enhanced Input Source Switching

To manually switch to a backup source, follow the steps below:

```
Router# cable video source-switch from-group 203.0.113.1 from-source 203.0.113.3
Router# cable video source-switch to-group 203.0.113.1 to-source 203.0.113.2
```

To enable PCR PID based source switch, follow the steps below:

```
Router(config)#cable video
Router(config-video)#pcr-based-source-switch
```

To disable PCR PID based source switch, follow the steps below:

```
Router(config)#cable video
Router(config-video)#no pcr-based-source-switch
```

Configuring MPTS Remuxing

To configure MPTS remuxing for multicast sessions, follow the steps below:

```
Router(config)#cable video
Router(config-video)#table-based
Router(config-video-tb)#vcg <vcg-name>
Router(config-video-tb-vcg)#rf-channel <channel-num>
Router(config-video-tb-vcg-sess)# session <session-name> multicast-label <multicast_label>
 processing-type <remap | data | passthru|remux> input-program-num <num> output-program-num
 <num>
```

To configure MPTS remuxing for unicast sessions, follow the steps below:

```
Router(config)#cable video
Router(config-video)#table-based
Router(config-video-tb)#vcg <vcg-name>
Router(config-video-tb-vcg)#rf-channel <start-channel>-<end-channel>
Router(config-video-tb-vcg-sess)# session <session-name> input-port <vei-number>
start-udp-port <udp-port-number> processing-type <remap | data | passthru|remux>
input-program-num <num> output-program-num <num>
```

Verifying PID Filtering, Program Filtering, and PID Remapping

You can view the PID remaps, the PID filters, and the program filters using the session detail command as shown below:

```
Router(config-video-remap-ch-mcast)#$sion log id 1 session-id 1048583
Session Name         : ssml.1.2
Session Id           : 1048583
Creation Time        : Wed Dec 20 16:22:41 2017

Output Port          : 122
TSID                 : 122
ONID                 : 0
Number of Sources    : 1
    Source IP        : 192.0.2.254
    Group IP         : 192.0.2.255
    UDP Port         : 0
Config Bitrate       : Not specified
Jitter               : 100 ms
Processing Type      : Passthru
Stream Rate          : VBR
Program Number       : -
Idle Timeout         : 4500 msec
Init Timeout         : 5000 msec
Off Timeout          : 60 sec
Encryption Type      : CLEAR
Encryption Status    : -

PID Filter
1000 1002 1003 1004 1005 1006 1007 1008 1009 1010 1011 1012 1013 1014 1015 1016 1017 1018

Program Filter
10 11 12 13 14 15 16 17 18 19 20 21

PID Remap
20 → 30 34 → 134 35 → 135 36 → 136 37 → 137 38 → 138
```

Verifying MPTS Remuxing

To see the remux sessions along with input and output program numbers, use the **show cable video session** as shown below:

```
Router# show cable video session log id 1
Total Sessions = 4


Session    Output    Frequency    Streaming   Session Session Source                 UDP
  Input    Output   Input       Output  Input    Output   Encrypt  Encrypt  LOW  PMV  SESSION
Id         Port      Hz           Type        Type    Ucast Dest IP/Mcast IP (S,G)    Port
  Program  Program  State       State   Bitrate  Bitrate  Type     Status   LAT  NUM  NAME
-------------------------------------------------------------------------------------------
2097152    142       567000000    Remux       SSM     175.2.5.6,232.5.6.7            0
  1        100      ACTIVE-PSI  ON      78099327 17115419  CLEAR   -        N    -
SESS_PME2.1.7.338
2097153    163       567000000    Remux       SSM     175.6.1.13,232.2.1.6           0
  2        200      ACTIVE-PSI  ON      78099327 17115419  CLEAR   -        N    -
SESS_PME3.1.7.497
2097154    184       567000000    Remux       SSM     175.2.6.7,232.5.6.15           0
  3        300      ACTIVE-PSI  ON      78099327 17115419  CLEAR   -        N    -
SESS_PME4.1.7.656
2097155    230       567000000    Remux       SSM     175.7.2.2,232.2.6.7            0
  4        400      ACTIVE-PSI  ON      78099327 17115419  CLEAR   -        N    -
SESS_PME6.1.7.978
```

To see the remux processing type, follow the steps below:

```
Router# show cable video session log id 1 summary
Video Session Summary For Video
```

```
Active      : 6    Init      : 0      Idle       : 0
Off         : 6    Blocked   : 0      PSI-Ready  : 6
UDP         : 0    ASM       : 0      SSM        : 12
Remap       : 0    Data      : 0      Passthru   : 0
Remux       : 12   Pending   : 0      Encrypted  : 0
Low Latency : 0

Total Sessions: 12
Total Input Bitrate: 467067498 BPS
Total Output Bitrate: 99841084 BPS
```

Note The input and output bitrates shown for the remux ression is for the whole stream. The bitrates do not correspond to individual programs.

To see the list of input programs, remapped output programs, and the enabled output programs, follow the steps as shown below:

```
cable video
  multicast-uplink VirtualPortGroup0 access-list all-multicasts
  use-pcr-fo
  mgmt-intf VirtualPortGroup 0
  service-distribution-group sdg1 id 1
    rf-port integrated-cable 7/0/0
  virtual-carrier-group vcg1 id 1
    encrypt
    service-type narrowcast
    rf-channel 20-22 tsid 20-22 output-port-number 20-22
  bind-vcg
    vcg vcg1 sdg sdg1
  logical-edge-device led1 id 1
    protocol table-based
      virtual-edge-input-ip 203.0.113.1 input-port-number 1
      vcg vcg1
      active
  table-based
    vcg vcg1
      rf-channel 20
        session 20_pass group 203.0.113.1 source 203.0.113.2 processing-type passthru
  remap pid vcg vcg1
    rf-channel 20
      ssm-multicast 203.0.113.1 203.0.113.2
        pid 20 30
        pid 34-38 134-138
  filter pid vcg vcg1
    rf-channel 20
      ssm-multicast 203.0.113.1 203.0.113.2
        pid 1000-1020
  filter program vcg vcg1
    rf-channel 20
      ssm-multicast 203.0.113.1 203.0.113.2
        program 10-20
```

Troubleshooting Tips for Possible Configuration Errors

Troubleshooting tips for possible configuration errors:

- If a specific PID remap, PID filter or program filter rule is not applied, check the session detail command output if the PID rule is present as part of the session.
- If the PID remap, PID filter, or program filter rule is not present in the session detail command output, check if the VCG, the rf-channel, and the input information matches the session for which the remap rule should be applied.
- Make sure that the session is either a pass-through or a data-piping session.
- For multicast-based PID rules, check if the active source has the rule applied.

Configuration Examples for Advanced MPEG Features

Example 1: PID Filter—Table-based Unicast Session Configuration

Consider the below table-based unicast session on a input port number 1 with vei-ip 198.51.100.1

```
logical-edge-device led1 id 1
    protocol table-based
       virtual-edge-input-ip 198.51.100.1 input-port-number 1
       vcg vcg1
       active


table-based
    vcg vcg1
       rf-channel 2
           session unicast input-port 1 start-udp-port 49152 processing-type passthru
```

The corresponding filter rule is shown below:

```
filter pid vcg vcg1
     rf-channel 2
         vei-ip 198.51.100.1 udp-port 49152
            pid 120
            pid 20-30
```

Example 2: PID Filter—Table-based ASM Multicast Session Configuration

Consider a table-based ASM multicast session replicated on rf-channel 30-40.

```
table-based
    vcg vcg1
       rf-channel 2
           session asml group 198.51.100.2 processing-type passthru
```

You can specify PID rule for the session on each rf-channel a group of rf-channels as shown below:

```
filter pid vcg vcg1
    rf-channel 2
      asm-multicast 198.51.100.2
          pid 1000
          pid 1002-1020
```

Example 4: Program Filter—Table-based Unicast Session Configuration

Consider the below table-based unicast session on a input port number 1 with vei-ip 198.51.100.1

```
logical-edge-device led1 id 1
    protocol table-based
       virtual-edge-input-ip 198.51.100.1 input-port-number 1
       vcg vcg1
       active


table-based
    vcg vcg1
       rf-channel 2
           session unicast input-port 1 start-udp-port 49152 processing-type passthru
```

The corresponding filter rule is shown below:

```
filter program vcg vcg1
     rf-channel 2
         vei-ip 198.51.100.1 udp-port 49152
            program 10
            program 20
            program 30-40
```

Example 5: Program Filter—Table-based ASM Multicast Session Configuration

Consider a table-based ASM multicast session replicated on rf-channel 30-40.

```
table-based
    vcg vcg1
       rf-channel 2
           session asml group 198.51.100.2 processing-type passthru
```

You can specify PID rule for the session on each rf-channel a group of rf-channels as shown below:

```
filter program vcg vcg1
    rf-channel 2
      asm-multicast 198.51.100.2
          program 10-20
```

Example 6: Program Filter—Table-based SSM Multicast Session Configuration

Consider a SSM multicast stream as shown below:

```
table-based
    vcg vcg1
       rf-channel 2
          session ssml group 198.51.100.3 source 198.51.100.6 processing-type passthru
```

One of the remap rules is applied depending on the source and group match as shown below:

```
filter program vcg vcg1
    rf-channel 2
       ssm-multicast 198.51.100.200 198.51.100.254
          program 10-20
       ssm-multicast 198.51.100.201 198.51.100.254
          program 10-20
       ssm-multicast 198.51.100.203 198.51.100.254
          program 10-20
```

Example 7: PID Remap—Table-based Unicast Session Configuration

Consider the below table-based unicast session on a input port number 1 with vei-ip 198.51.100.1

```
table-based
    vcg vcg1
       rf-channel 20
           session unicast input-port 1 start-udp-port 49152 processing-type passthru
```

The corresponding remap assuming 32 input unreferenced PIDs is shown below:

```
remap pid vcg vcg1
     rf-channel 20
         vei-ip 198.51.100.1 udp-port 49152
            pid 100 200
            pid 101 201
            pid 102-130 202-230
            pid 131 240
```

Example 8: PID Remap—Table-based ASM Multicast Session Configuration

Consider a table-based ASM multicast session replicated on rf-channel 30-40.

```
table-based
    vcg vcg1
       rf-channel 2
           session asm_multi group 198.51.100.2 processing-type data
```

You can specify PID rule for the session on each rf-channel a group of rf-channels as shown below:

```
remap pid vcg vcg1
    rf-channel 30
      asm-multicast 198.51.100.2
          pid 1000 8189
    rf-channel 31-40
      asm-multicast 198.51.100.2
          pid 1000 8189
```

Example 9: PID Remap—Table-based SSM Multicast Session Configuration

Consider a SSM multicast stream as shown below:

```
table-based
    vcg vcg1
       rf-channel 30-40
          session ssm_multi group 198.51.100.3 source 198.51.100.6 processing-type data
```

One of the remap rules is applied depending on the source and group match as shown below:

```
remap pid vcg vcg1
    rf-channel 30-35
       ssm-multicast 198.51.100.200 198.51.100.254
          pid 1000 8190
       ssm-multicast 198.51.100.201 198.51.100.254
          pid 2000 8190
       ssm-multicast 198.51.100.203 198.51.100.254
          pid 1860 8190
```

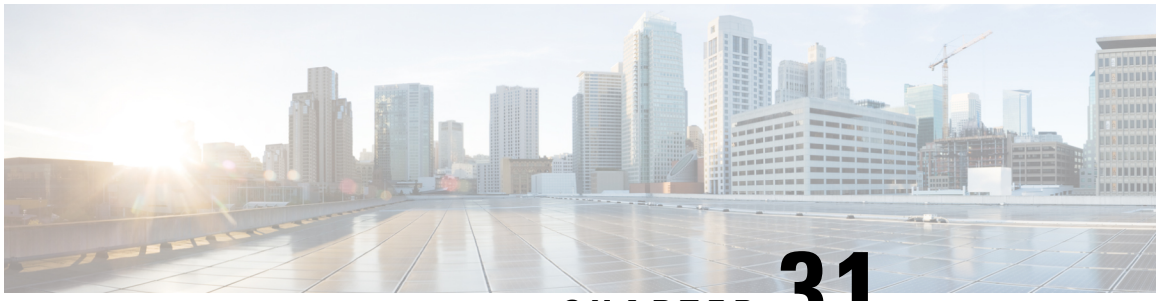
Feature Information for Advanced MPEG Features

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 https://cfnng.cisco.com/ 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 Advanced MPEG Features

Feature Name	Releases	Feature Information
Advanced MPEG Features	Cisco IOS-XE Release 16.8.1	This feature was introduced into Cisco IOS-XE Release 16.8.1 on the Cisco cBR Series Converged Broadband Routers.



CHAPTER 31

Video Notifications

This document provides information on the support for video notifications and how to configure Cisco cBR series routers to avail the support.

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.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

- Information About Video Notifications, on page 221
- How to Configure Video Notifications, on page 222
- Configuration Examples for Video Notifications, on page 224
- Configuring CC-ERROR Reporting, on page 225
- Feature Information for Video Notifications, on page 226

Information About Video Notifications

The Cisco cBR-8 router sends SNMP trap notifications about video related events.

Overview of Video Notifications

The Cisco cBR-8 router sends SNMP trap notifications for the following events:

- When connection is lost or when connection is re-established between Cisco Edge QAM Manager (CEM) application and Cisco cBR-8 router.
- When connection is lost or when connection is re-established between D6 Discovery Protocol servers and Cisco cBR-8 router.
- When connection is lost or when connection is re-established between Cisco cBR-8 router and the GQI Edge Resource Manager.
- When connection is established between CEM and Cisco cBR-8 router for 180 seconds, but Cisco cBR-8 router does not receive ECM templates from the CEM. Cisco cBR-8 router also sends a notification when it receives ECM templates from CEM.

- When QAM bandwidth exceeds the specified maximum bandwidth of the QAM channel. Cisco cBR-8 router also sends a notification when the QAM bandwidth returns to within the specified bandwidth.
- When two or more PIDs have the same number in a QAM channel.
- When two or more programs have the same number in a QAM channel.
- When connection is lost or when connection is re-established between the DVB ECMG server and Cisco cBR-8 router.
- Loss of connection or reconnection between the DVB EIS client and the Cisco cBR-8 router.
- When the input stream from the primary source for a video session is lost, and the backup source is now in the active state. If the ingress video stream packet has CC (Continuity Counter) errors as per the CC threshold and report-interval configuration.
- When no traffic is seen within the OFF-timeout period for a video session, and the session gets moved to an OFF state and stays OFF for 30sec. If the ingress video stream does not have the PMT table.

Note All cable video traps sent out are conform to the SCTE-HMS-ALAMRS-MIB standard (ANSI/SCTE 38-2 2011).

How to Configure Video Notifications

Note To know more about the commands referenced in this module, see the Cisco IOS Master Command List.

Configuring SNMP Notification Host

To configure remote SNMP notification host on the Cisco cBR-8, follow the steps below:

```
Router> enable
Router# configure terminal
Router(config)# snmp-server host ip-address [version {1 | 2c | 3 [auth | noauth | priv]}]
community-string [udp-port port-number]
```

UDP port 162 is the default port to receive SNMP notifications.

Configuring SNMP Notification Message Queue Length

To configure SNMP message queue length, follow the steps below:

```
Router> enable
Router# configure terminal
Router(config)# snmp-server queue-length <1-5000>
```

The recommended message queue length is 5000.

Configuring Video Notification

To enable all video notifications, follow the steps below:

```
Router> enable
Router# configure terminal
Router(config)# snmp-server enable traps video-cable
```

To enable one or more specific video notifications, follow the steps below:

```
Router> enable
Router# configure terminal
Router(config)# snmp-server enable traps video-cable [video_notification]
```

Table 41: Video Notification

Video Notification	Description
backup-source-active	Enable backup source active trap notification.
cc-err	Enable CC error trap notification.
cemconn	Enable CEM connection error trap notification.
d6conn	Enable D6 connection error trap notification.
ecmgconn	Enable ECMG connection error trap notification.
eisconn	Enable EIS connection error trap notification.
gqiconn	Enable GQI connection error trap notification.
input-stream-failure	Enable In Stream Failure error trap notification.
pidcflct	Enable PID conflict trap notification.
pmeecm	Enable PME ECM missing trap notification.
pmt-missing	Enable PMT Missing error trap notification.
progcflct	Enable program conflict trap notification.
qamovr	Enable QAM over-subscription trap notification.

Viewing Active Video Notifications

To view the list of active video notifications, perform the following steps:

```
Router# show cable video snmp-alarms

Displaying the Alarms MIB alarmslogtable
Alarm Log Index   Alarm ID   Instance   Severity   Slot     Alarm Message
-------------------------------------------------------------------------------------------------

 1                0          0          2          4        CEM_CONN:SET:0:0:
                                                             Connection closed with
                                                             CEM 1.200.1.163 - 5000
```

Disabling Video Notification

To disable video alarms, perform the following steps:

```
Router> enable
Router# configure terminal
Router(config)# no snmp-server enable traps video-cable
```

To disable one or more video alarms, perform the following steps:

```
Router> enable
Router# configure terminal
Router(config)# no snmp-server enable traps video-cable [video_notification]
```

Configuration Examples for Video Notifications

Example 1: Configuring Remote SNMP Notification Host

```
Router> enable
Router# configure terminal
Router(config)# snmp-server host 10.143.25.185 version 2c public udp-port 1602
```

Example 2: Configuring SNMP Notification Message Queue Length

```
Router> enable
Router# configure terminal
Router(config)# snmp-server queue-length 5000
```

Example 3: Enable Specific Video Notifications

```
Router> enable
Router# configure terminal
Router(config)# snmp-server enable traps video-cable cemconn pmeecm qamovr
```

Example 4: Disable Specific Video Notifications

```
Router> enable
Router# configure terminal
Router(config)# no snmp-server enable traps video-cable cemconn pmeecm qamovr
```

Example 5: Enable input-stream-failure error reporting with report-interval

```
Router> enable
Router# configure terminal
Router(config)# cable video
Router(config-video)# report-stream-error input-stream-failure report-interval 25
```

Example 6: Enable Continuity Counter error reporting on the chassis level with CC threshold and report-interval

```
Router> enable
Router# configure terminal
Router(config)# cable video
Router(config-video)# report-stream-error cc-error report-interval 15 threshold 10
```

Configuring CC-ERROR Reporting

Use the **report-stream-error cc-error** command under **cable video** to enable CC-ERROR reporting on the chassis level. The CC_ERROR monitor is disabled by default, you can enable the CC-ERROR monitor using the following commands.

- **report-stream-error cc-error report-interval** *interval* : Event report interval in minutes. The default value is 10 mins.
- **report-stream-error cc-error syslog enable**: Syslog notification for Error events.
- **report-stream-error cc-error threshold** *cc-error-count* : Threshold value to report the event. The default value is 5.

Enabling CC-ERROR Monitoring

The cc errors are only monitored if this command is configured:

```
Router(config)#cable video
 Router(config-video)#report-stream-error cc-error
```

Once this command is configured, cc-error set/clear messages are sent using the IPC message. If the command is not configured, it does not send any IPC message.

Enabling CC-ERROR Syslog

CC-ERROR messages are sent to syslog only if this command is configured:

```
Router(config)#cable video
Router(config-video)#report-stream-error cc-error syslog enable
```

- If the stream has a continuous cc-error, then only one message for the corresponding stream is sent. Here is a sample snippet of the message:

  ```
  ...
  Jun 19 18:05:11.776 IST: %VSESS-3-STREAM_ERROR: R0/0: led: 1 Slot: 3 CC_ERROR:SET:3:6:

  Reported on source 175.2.2.2:232.2.1.1:0
  ...
  ```

- The CC_ERROR CLEAR message is sent after the stream recovers from CC_ERROR. Here is a sample snippet of the message:

  ```
  ...
  Jun 19 18:05:16.765 IST: %VSESS-3-STREAM_ERROR: R0/0: led: 1 Slot: 3 CC_ERROR:CLEAR:3:0:

  Reported on source 192.2.2.2:232.2.1.1:0
  ...
  ```

Threshold Control

Configure the threshold value using the following command.

```
Router(config)#cable video
Router(config-video)#report-stream-error cc-error threshold cc-error-count
```

The default threshold value is 5. The valid range is 1 to 65535.

For example, when the threshold value is configured as 10, then if the CC_ERROR count value is greater than 10 then it sends the cc_error SET message.

Report-interval Control

Configure the report-interval value using the following command.

```
Router(config)#cable video
Router(config-video)#report-stream-error cc-error report-interval minutes
```

The default report interval value is 10. The valid range is 1 to 65535.

For example, when the report-interval value is configured as 45 and CC_ERROR is set and the clear message hits multiple times then

- all set/clear messages are not sent.
- only one set/clear is sent, and the number of set/clear messages are calculated. Here is a sample snippet of the message:

```
Jun 19 18:05:11.776 IST: %VSESS-3-STREAM_ERROR: R0/0: led: 1 Slot: 3 CC_ERROR:SET:3:6:

Reported on source 175.2.2.2:232.2.1.1:0

Jun 19 18:05:16.765 IST: %VSESS-3-STREAM_ERROR: R0/0: led: 1 Slot: 3 CC_ERROR:CLEAR:3:0:

Reported on source 175.2.2.2:232.2.1.1:0
```

- After 45 minutes, only one info message is sent, that shows how many times set/clear CC_ERROR has occurred during the 45-minutes interval. Here is a sample snippet of the message:

```
Jun 19 18:50:11.809 IST: %VSESS-3-STREAM_ERROR: R0/0: led: 1 Slot: 3 CC_ERROR:INFO:3:0:
 56
events occurred during last report interval(45 min) for source 175.2.2.2:232.2.1.1:0
```

Feature Information for Video Notifications

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 https://cfnng.cisco.com/ 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 42: Feature Information for Video Notifications

Feature Name	Releases	Feature Information
Video Notifications	Cisco IOS-XE Release 16.7.1	This feature was integrated into Cisco IOS-XE Release 16.7.1 on the Cisco cBR Series Converged Broadband Routers.

Feature Name	Releases	Feature Information
Video Notifications	Cisco IOS-XE Release 16.8.1	This feature was updated in Cisco IOS-XE Release 16.8.1d on the Cisco cBR Series Converged Broadband Routers.