Cisco cBR Converged Broadband Routers Video Features for Cisco IOS XE Everest 16.5.1

First Published: 2017-04-07

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

CONTENTS

CHAPTER 4

CHAPTER 5

CHAPTER 6

CHAPTER 1

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

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 1: Supported Encryption Types and Scrambler Modes

Encryption Type	Scrambler Mode
PME	DVS-042
PKEY	DES, 3DES

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 6.

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

Table 2: Feature Information for PowerKEY VOD

Feature Name	Releases	Feature Information
PowerKEY VOD	Cisco IOS XE Everest 16.5.1	This feature was integrated on the Cisco cBR Series Converged Broadband Routers.

CHAPTER 2

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

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
vcgvcg-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
```

Troubleshooting Video and VPME Encryption

Output State is OFF

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

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.

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
```

Troubleshooting Tips

Connectivity with CEM is Lost

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
```

Troubleshooting Tips

No PMT at the Output

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:

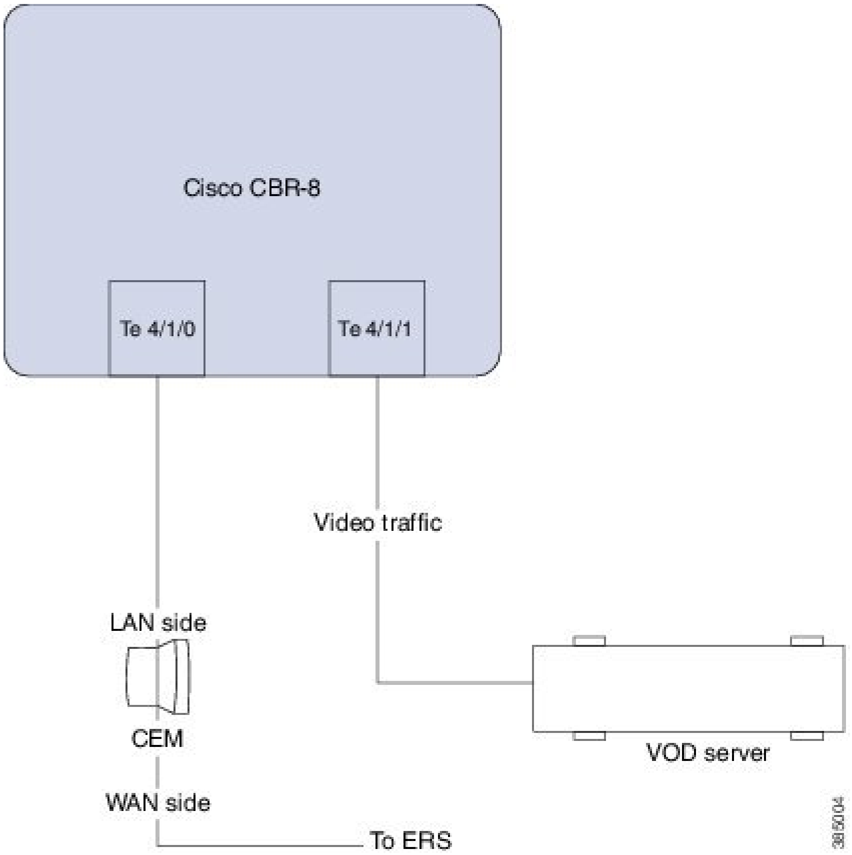
```
cable video
```

```
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

Table 3: Feature Information for Table-Based Video and VPME Encryption

Feature Name	Releases	Feature Information
Table-Based Video and VPME Encryption	Cisco IOS XE Everest 16.5.1	This feature was integrated on the Cisco cBR Series Converged Broadband Routers.

CHAPTER 3

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

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

Table 4: Feature Information for PMV Support for Table-Based Videos

Feature Name	Releases	Feature Information
PMV Support for Table-Based Videos	Cisco IOS XE Everest 16.5.1	This feature was integrated on the Cisco cBR Series Converged Broadband Routers.

CHAPTER 4

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

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.

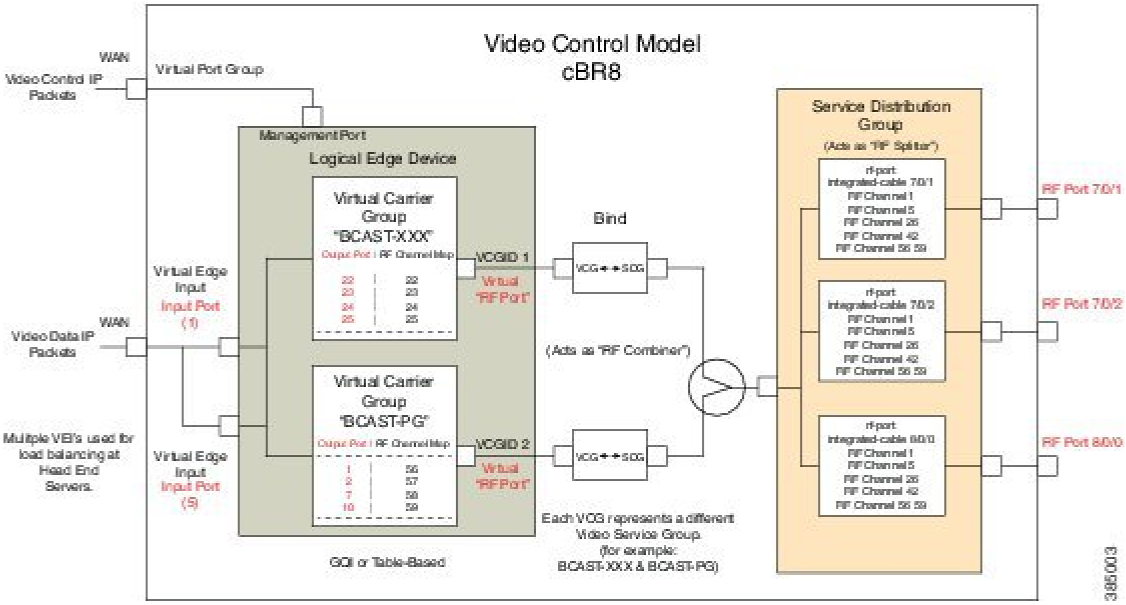
The **service-distribution-group** construct is used to perform replication. Hardware replication is supported when the replication of individual QAM Carriers is limited to the same line card.

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

Table 5: Feature Information for Replication

Feature Name	Releases	Feature Information
Replication	Cisco IOS XE Everest 16.5.1	This feature was integrated on the Cisco cBR Series Converged Broadband Routers.

CHAPTER 5

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

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 44 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

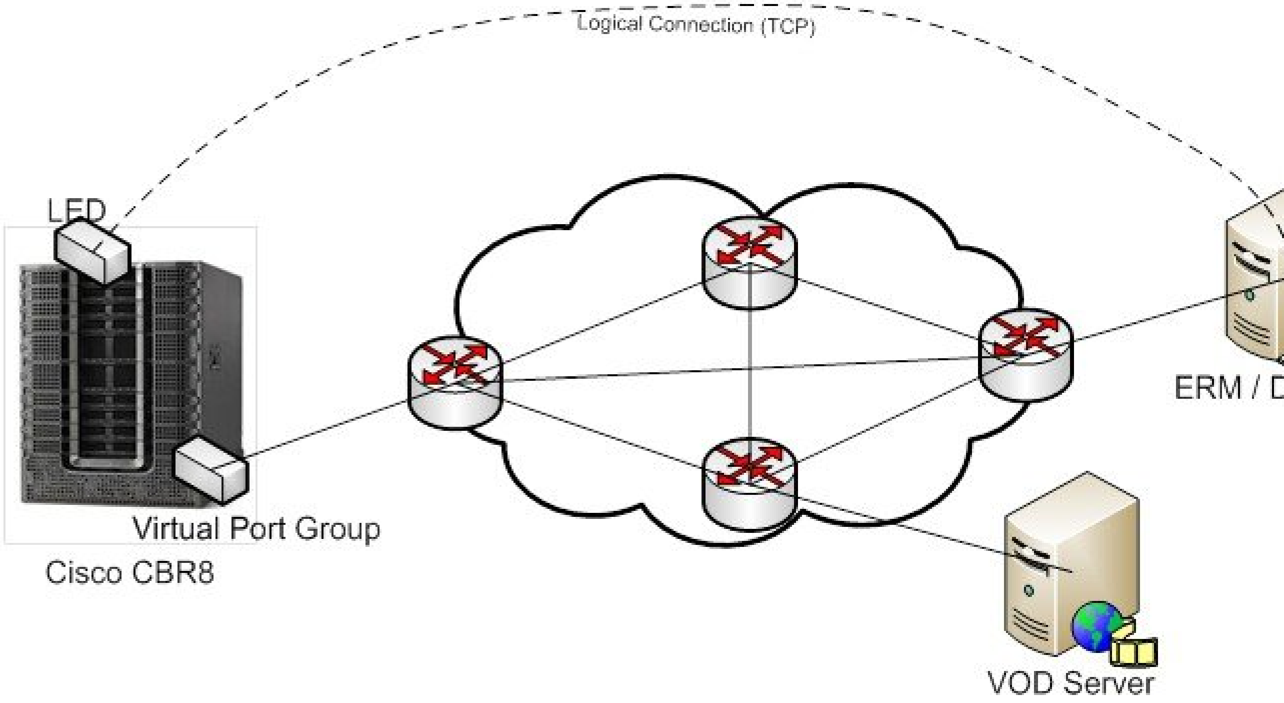
The following example shows a complete D6 configuration:

```
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 1: 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

Table 6: Feature Information for D6 Discovery Protocol

Feature Name	Releases	Feature Information
D6 Discovery Protocol	Cisco IOS XE Everest 16.5.1	This feature was integrated on the Cisco cBR Series Converged Broadband Routers.

CHAPTER 6

Switched Digital Video

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.

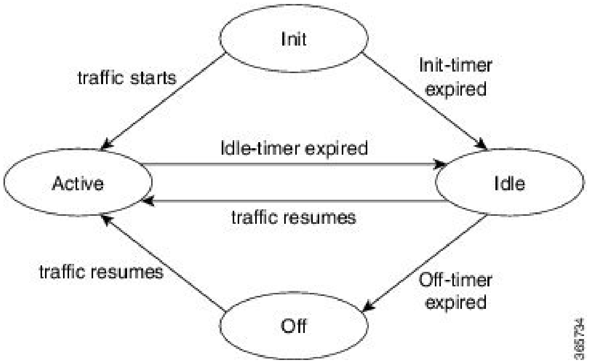
This ensures that all sessions switch to the same source IP address when a source switch occurs. Additionally, sessions configured via GQI have up to three sources available for redundancy, whereas multicast labels configured for table-based sessions have up to four sources available for redundancy.

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.

Information About Switched Digital Video

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.

How to Configure the Switched Digital Video Services

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
```

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.

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
```

Feature Information for Switched Digital Video

Feature Name	Releases	Feature Information
Switched Digital Video	Cisco IOS XE Everest 16.5.1	This feature was integrated on the Cisco cBR Series Converged Broadband Routers.

CHAPTER 7

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

Overview of DVB VOD

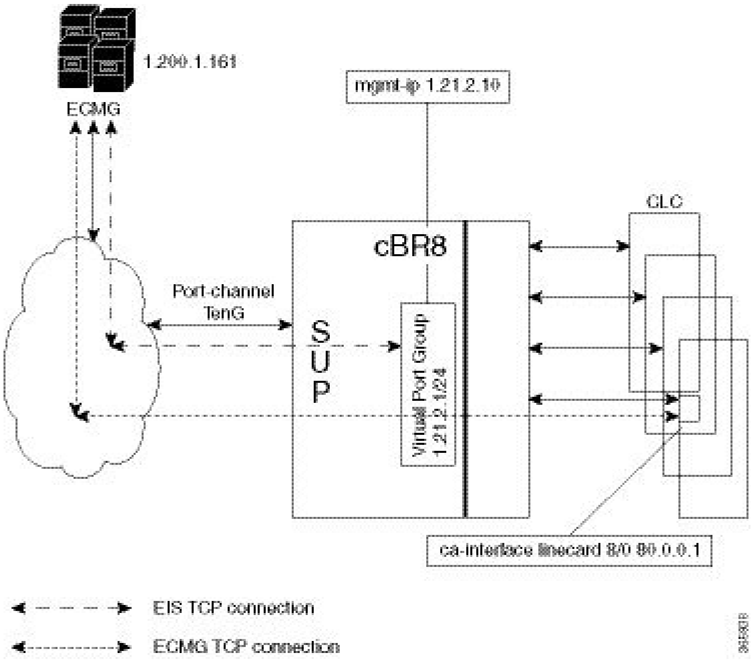
This feature enables the operator to scramble the video sessions on the chassis. It involves the configuration to establish a connection with the Entitlement Control Message Generator (ECMG) and the Event Information Scheduler (EIS).

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 linecard.

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 2: 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 Router s.

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 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.

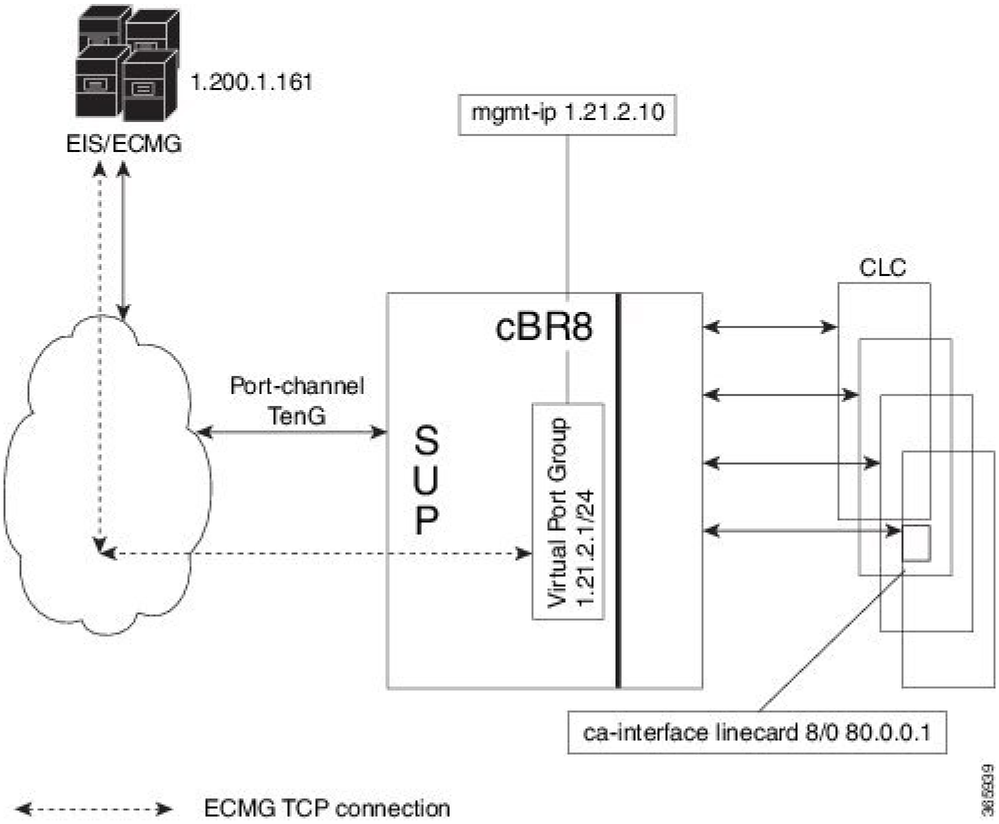
If fail-to-clear is configured, tier-based configuration is enabled, and then if the encryption fails, the DVB session's `Encrypt Status` is marked as `clear`. The status changes to `Encrypted` when the encryption starts.

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 3: 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 DVB Video on Demand

Table 7: Feature Information for DVB Video on Demand

Feature Name	Releases	Feature Information
DVB Video on Demand	Cisco IOS XE Everest 16.5.1	This feature was integrated on the Cisco cBR Series Converged Broadband Routers.
Fail-to-Clear	Cisco IOS XE Everest 16.5.1	This feature was integrated on the Cisco cBR Series Converged Broadband Routers.

CHAPTER 8

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.

Finding Feature Information

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

Hardware Compatibility Matrix for Cisco cBR Series Routers

Note The hardware components 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-CCAP-SUP-160G • PID—CBR-CCAP-SUP-60G • PID—CBR-SUP-8X10G-PIC	**Cisco IOS-XE Release 16.5.1 and Later Releases** Cisco cBR-8 CCAP Line Cards: • PID—CBR-LC-8D30-16U30 • PID—CBR-LC-8D31-16U30 • PID—CBR-RF-PIC • PID—CBR-RF-PROT-PIC • PID—CBR-CCAP-LC-40G-R Cisco cBR-8 Downstream PHY Modules: • PID—CBR-D30-DS-MOD • PID—CBR-D31-DS-MOD Cisco cBR-8 Upstream PHY Modules: • PID—CBR-D30-US-MOD

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        0x00000000000000000001
1048581 20     Remap     UDP     10.10.10.11                  49153 2       ACTIVE-PSI ON
    1711859  1707422 DVB     Encrypted N         0x00000000000000000002
1048582 23     Passthru  UDP     10.10.10.11                  49154 -       ACTIVE-PSI ON
    1711962  1699101 CLEAR   -         N         0x00000000000000000003
1048583 23     Remap     UDP     10.10.10.11                  49155 4       ACTIVE-PSI ON
    1712498  1707834 DVB     Encrypted N         0x00000000000000000004
```

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 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

Table 9: Feature Information for DualCrypt Encryption Mode

Feature Name	Releases	Feature Information
DualCrypt Encryption Mode	Cisco IOS XE Everest 16.5.1	This feature was integrated on the Cisco cBR Series Converged Broadband Routers.

CHAPTER 9

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

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

Table 10: Feature Information for Low Latency VOD Support

Feature Name	Releases	Feature Information
Low Latency VOD Support	Cisco IOS XE Everest 16.5.1	This feature was integrated on the Cisco cBR Series Converged Broadband Routers.

CHAPTER 10

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

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)