Cisco Converged Broadband Routers Software Configuration Guide For Video

First Published: 2015-03-26

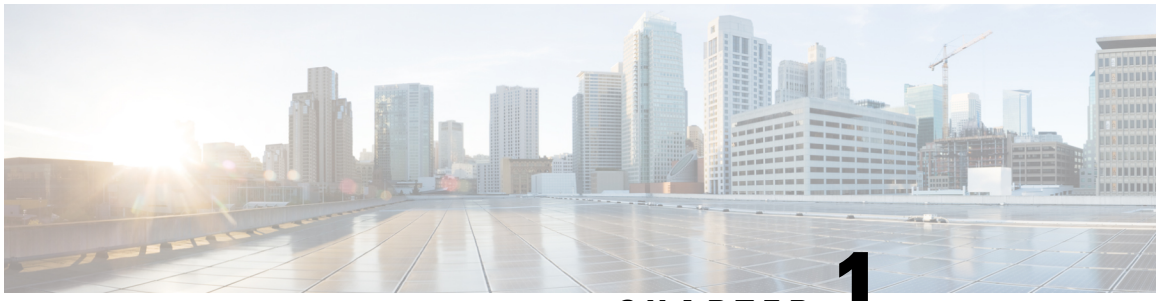
Last Modified: 2016-07-29

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

PART I

Basic Configuration and Provisioning Construct



CHAPTER 1

Video Services Provisioning Model

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

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

Information about Video Services Provisioning

Video Provisioning Constructs

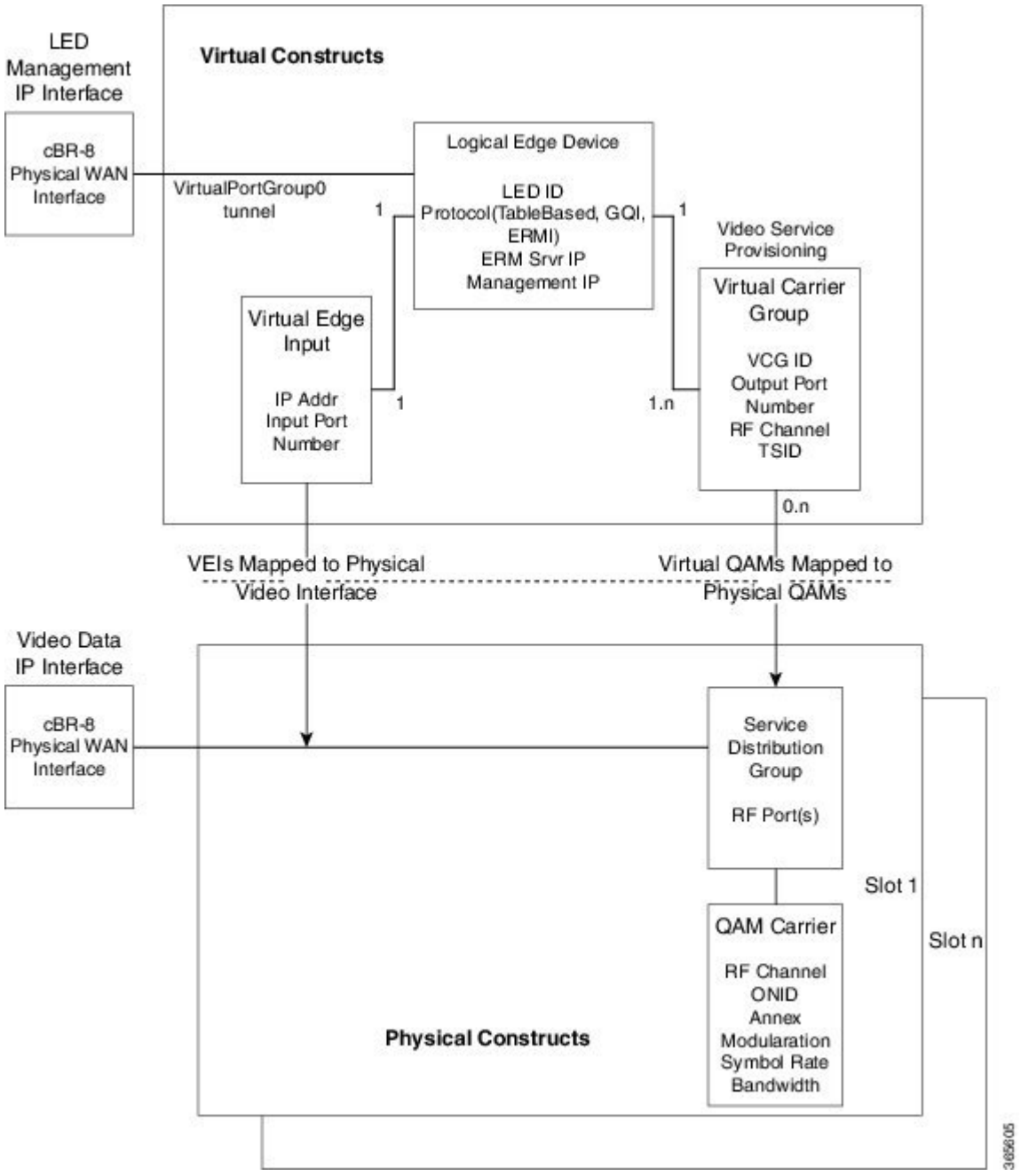
The Video Services Provisioning Model has the following elements:

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

Connection of Virtual and Physical Constructs

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

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



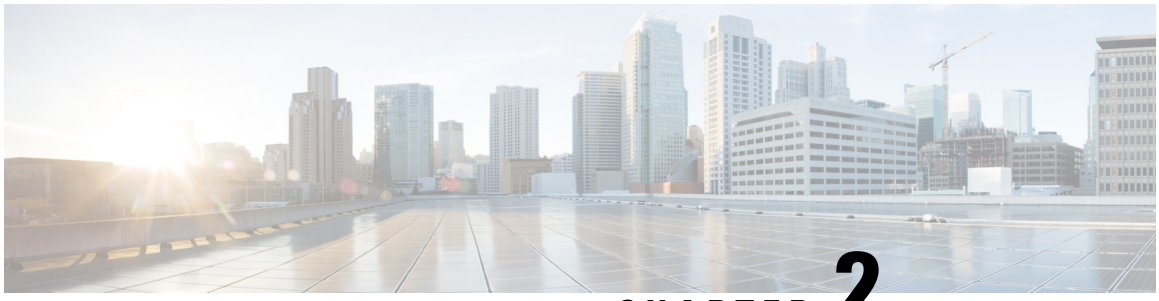
Feature Information for Video Services Provisioning

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

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

Table 1: Feature Information for Video Services Provisioning

Feature Name	Releases	Feature Information
Video Services Provisioning	IOS-XE 3.18.0S	The Cisco cBR-8 router has a redesigned video data model that creates virtual edge devices for simplifying provisioning and supporting virtual video service management.



CHAPTER 2

Video Virtual Carrier Group and Virtual Edge Input

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

Information about Virtual Carrier Group and Virtual Edge Input

Virtual Carrier Group

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

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

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

For more information on how the licenses are consumed, see the Cisco Smart Licensing for Video , on page 27.

Virtual Edge Input

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

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

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

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

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

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

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

How to Configure Virtual Carrier Group and Virtual Edge Input

Configuring Virtual Carrier Group

Before you begin

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

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

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

To configure virtual carrier group, follow the steps below:

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

Verifying Virtual Carrier Group Configuration

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

```
Router# show cable video virtual-carrier-group all
Number of Virtual Carrier Groups: 1
ID    Name   Input        Service-Distribution-Group   Logical-Edge-Device     Total
```

```
             IP Address   Name                          Name                    RF-Channel
-------------------------------------------------------------------------------------------
1     vcg-0    -            vcg                           vcgcast                  5
```

Configuring Virtual Edge Input under Logical Edge Device

Before you begin

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

To configure virtual edge input, follow the steps below:

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

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

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

Verifying Virtual Edge Input Configuration

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

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

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

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

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

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

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

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

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

Configuration Examples for Virtual Carrier Group and Virtual Edge Input

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

Example: Configuring Virtual Carrier Group

The following example shows how to configure virtual carrier group:

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

Example: Configuring Virtual Edge Input

The following example shows how to configure virtual edge input:

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

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

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

Under logical edge device, follow the steps below:

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

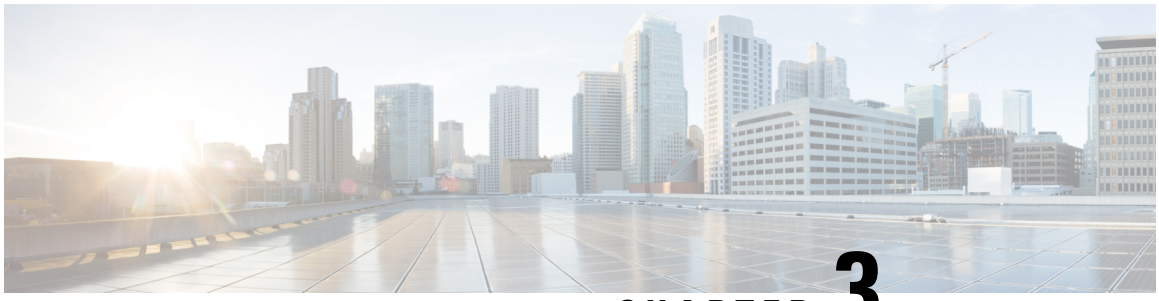
Feature Information for Virtual Carrier Group and Virtual Edge Input

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

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

Table 2: Feature Information for Virtual Carrier Group and Virtual Edge Input

Feature Name	Releases	Feature Information
Virtual Carrier Group and Virtual Edge Input	Cisco IOS-XE Release 3.18.0S	This feature was introduced on the Cisco cBR Series Converged Broadband Router s.
Using VRF for Video Session Traffic	Cisco IOS-XE Release 3.18.0Sa	An optional parameter **[vrf]** *vrf name* was added to **virtual-edge-input-ip** command.



CHAPTER 3

Service Distribution Group

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

Contents

Information About Service Distribution Group

The following are the required components for configuring an SDG:

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

The convention slot/bay/port represents the following:

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

How to Configure the Service Distribution Group

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

Defining the Physical Slot/Bay/Port

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

Before You Begin

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

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

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

Configuring QAM Replication

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

Before You Begin

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

To configure QAM replication, complete the following procedure:

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

Overriding the Default ONID

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

To override the default ONID, complete the following procedure:

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

Overriding the Default PSI Value

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

```
configure terminal
cable video
```

```
service-distribution-group  service distribution group name
psi-interval psi-interval  msec
```

Verifying Service Distribution Group Configuration

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

```
show cable video service-distribution-group all
Number of Service Distribution Groups: 1
ID  Name    Virtual-Carrier-Group   Logical-Edge-Device  RF-Port      ONID     PSI Interval

                     Name                    Name
-------------------------------------------------------------------------------------------------------
1   vod             vod                     LED             7/0/0        0         100
1   vod             vod                     LED             7/0/1        0         100
1   vod             vod                     LED             7/0/2        0         100
1   vod             vod                     LED             7/0/3        0         100
1   vod             vod                     LED             7/0/4        0         100
1   vod             vod                     LED             7/0/5        0         100
1   vod             vod                     LED             7/0/6        0         100
1   vod             vod                     LED             7/0/7        0         100
```

Troubleshooting Tips

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

Configuration Examples

This section provides example configurations for the service distribution group.

Configuring a Service Distribution Group

```
configure terminal
cable video
service-distribution-group vod id 1
 onid 100
 rf-port integrated-cable 7/0/0
 rf-port integrated-cable 7/0/1
 rf-port integrated-cable 7/0/2
 rf-port integrated-cable 7/0/3
```

Feature Information for Service Distribution Group

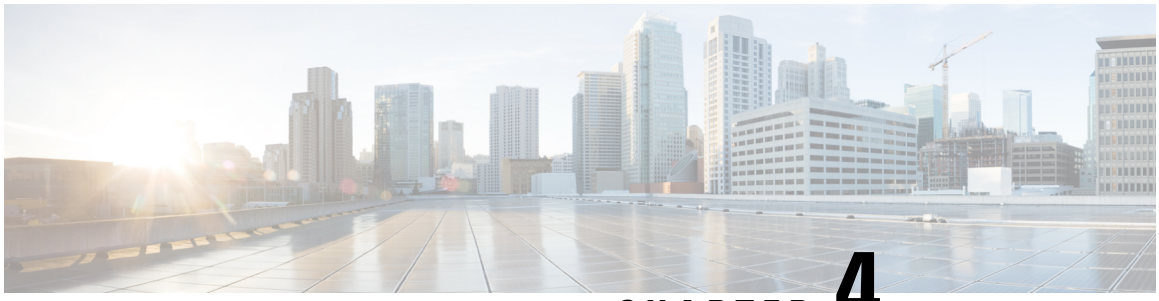
Use Cisco Feature Navigator to find information about the platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release,

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

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

Table 3: Feature Information for Service Distribution Group

Feature Name	Releases	Feature Information
Service Distribution Group	Cisco IOS-XE Release 3.18.0S	This feature was introduced on the Cisco cBR Series Converged Broadband Routers.



CHAPTER 4

Video QAM Carriers

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

Contents

Configuring the Video QAM Carriers

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

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

Configuration Examples

This section provides configuration examples for the QAM video carrier.

Video QAM Carriers

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

```
configure terminal
 controller integrated-cable 7/1/0
        rf-channel 1-3
            type video
            start-frequency 93000000
            rf-output normal
```

```
power-adjust 0
qam-profile 1
```

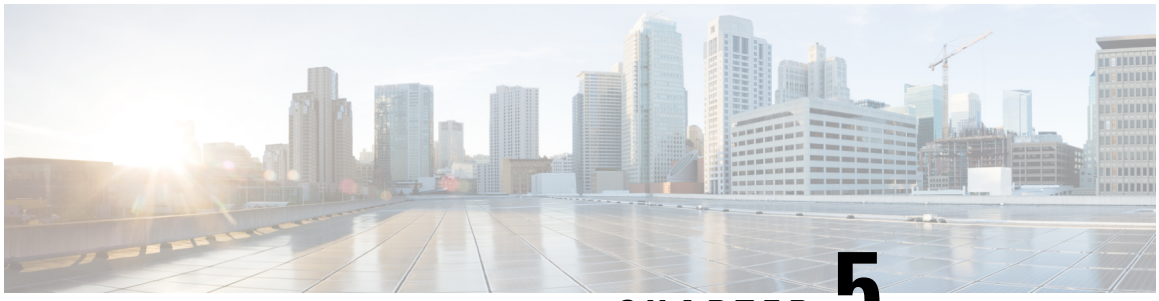
Feature Information for QAM Video Carriers

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

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

Table 4: Feature Information for QAM Video Carriers

Feature Name	Releases	Feature Information
QAM Video Carriers	Cisco IOS-XE Release 3.18.0S	This feature was introduced on the Cisco cBR Series Converged Broadband Routers.



CHAPTER 5

Logical Edge Devices

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

Contents

Information about Logical Edge Devices

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

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

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

How to Configure the Logical Edge Devices

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

Configuring Session-Based (Dynamic) Logical Edge Devices

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

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

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

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

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

Note In Cisco IOS-XE Release 3.18.0S, only GQI version 2 is supported for all GQI LEDs.

Before You Begin

The following data is necessary to define a GQI LED:

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

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

- The primary and secondary IP addresses of the remote SRM.
- Virtual Carrier Group (VCG). For more information, see Virtual Carrier Group, on page 5.
- Connection-orientated controls such as, keep alive, reset interval, and timeout value.
- Virtual Edge Input (VEI) configured with a routable IP address from within the network. For more information, see Video Virtual Carrier Group and Virtual Edge Input, on page 5.

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

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

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

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

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

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

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

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

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

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

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

-

Configuring the D6 Discovery Protocol

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

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

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

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

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

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

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

```
exit
active
```

Verifying the D6 Configuration

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

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

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

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

Configuration Examples

This section provides configuration examples for the LED configuration.

Example: GQI LED Configuration

Example: Example: GQI LED Configuration

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

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

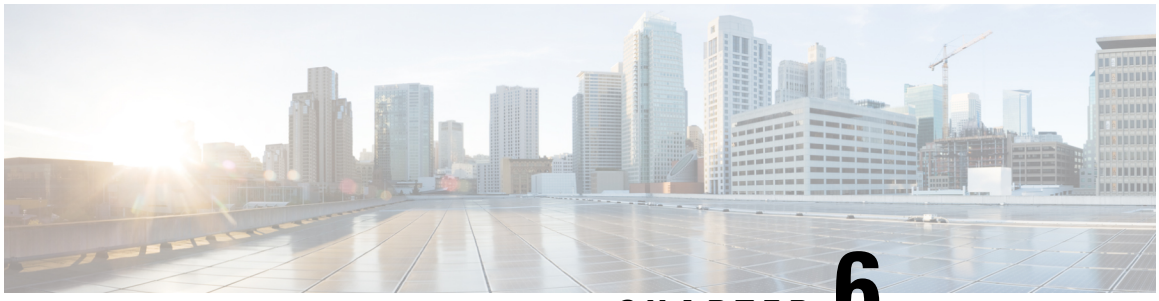
Feature Information for Logical Edge Devices

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 5: Feature Information for Logical Edge Devices

Feature Name	Releases	Feature Information
Logical Edge Devices	Cisco IOS-XE Release 3.18.0S	This feature was introduced on the Cisco cBR Series Converged Broadband Routers.



CHAPTER 6

Cisco Smart Licensing for Video

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

Video Smart Licensing

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

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

Information About Video Smart Licensing

Benefits of Smart Licensing

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

Prerequisites for Video Smart Licensing

See the Cisco Smart Licensing document.

Restrictions for Video Smart Licensing

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

How to Verify Video Smart Licensing

Verifying Video Smart Licensing Using Show Commands

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

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

```
Router# show cable license all

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

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

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

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

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

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

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

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

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

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

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

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

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

Configuration Examples

Example 1: Show Running Output for Basic Configuration

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

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

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

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

Use Cases or Deployment Scenarios

Case 1: Narrowcast Video Services with PowerKEY Encryption

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

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

Case 2: Narrowcast Video Services with PME Encryption

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

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

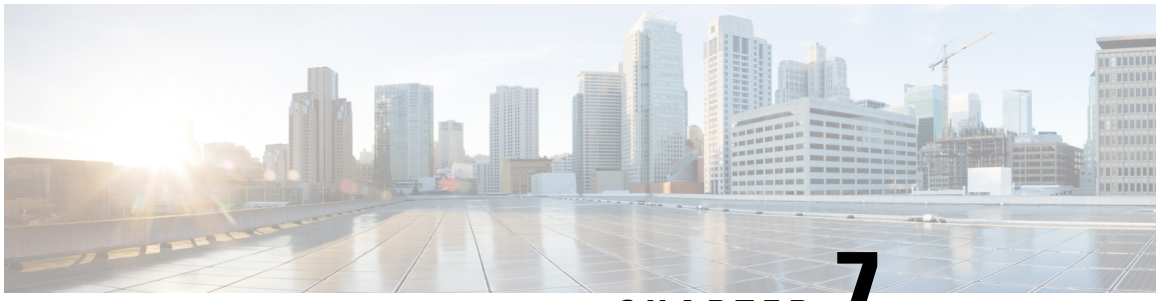
Feature Information for Video Smart Licensing

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

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

Table 6: Feature Information for Video Smart Licensing

Feature Name	Releases	Feature Information
Video Smart Licensing	Cisco IOS-XE Release 3.18.0S	This feature was introduced on the Cisco cBR Series Converged Broadband Router s.



CHAPTER 7

Physical to Virtual Binding

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

Information About Physical to Virtual Binding

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

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

How to Configure VPME Encryption

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

Configuring Physical to Virtual Binding

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

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

Configuring QAM Replication

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

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

Configuration Examples

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

Example 1: Physical to Virtual Binding Configuration

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

Example 1 :

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

Example 2: Physical to Virtual Binding Configuration

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

Example 2 :

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

Example 3: QAM Replication Configuration

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

Example 3 :

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

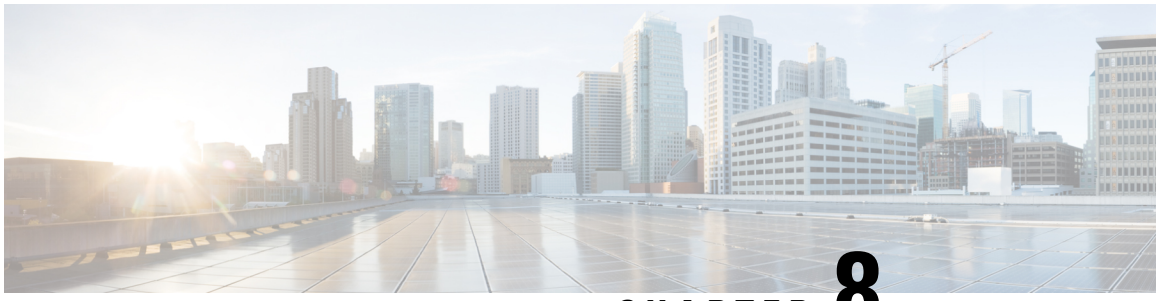
Feature Information for Physical to Virtual Binding

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

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

Table 7: Feature Information for Physical to Virtual Binding

Feature Name	Releases	Feature Information
Physical to Virtual Binding	Cisco IOS-XE Release3.18.0S	This feature was introduced on the Cisco cBR Series Converged Broadband Routers.



CHAPTER 8

Table Based Configuration

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

Information About Table Based Configuration

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

Configuring Table Based Session

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

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

Configuration Example

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

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

Virtual Edge Input Bundling

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

To bundle the VEIs, perform the following steps:

Before You Begin

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

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

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

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

Verifying Virtual Edge Input Data

To verify the VEI data, use the following command:

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

Example:

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

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

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

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

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

Verifying VEI Bundles

To view the VEI bundles, use the following command:

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

Example:

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

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

Configuration Example

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

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

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

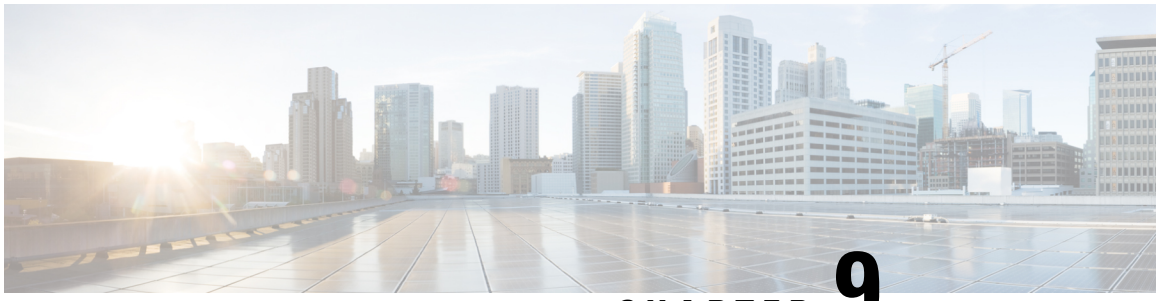
Feature Information for Table Based Configuration

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

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

Table 8: Feature Information for Table Based Configuration

Feature Name	Releases	Feature Information
Table based configuration	Cisco IOS-XE Release3.18.0S	This feature was introduced on the Cisco cBR Series Converged Broadband Routers.



CHAPTER 9

Management IP Interface

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

Contents

Information About Management IP Interface

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

The following are the characteristics of the management interface:

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

How to Configure the Management IP Interface

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

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

- Configuring the VirtualPortGroup Interface, on page 42
- Configuring the Cable Video Management Interface, on page 43
- Configuring the LED Management Interface, on page 43

Configuring the VirtualPortGroup Interface

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

To configure the VirtualPortGroup interface, complete the following procedure:

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

Verifying the VirtualPortGroup Interface Configuration

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

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

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

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

Verifying the VirtualPortGroup Interface State

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

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

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

Troubleshooting Tips

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

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

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

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

Configuring the Cable Video Management Interface

Before You Begin

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

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

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

Verifying the Cable Video Management Interface Configuration

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

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

Configuring the LED Management Interface

Before You Begin

- Cable video management interface must be configured before configuring an LED that uses the management interface.
- Management IP address and the VirtualPortGroup IP address must be in the same subnet.

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

```
configure terminal
cable video
logical-edge-device device name
```

```
protocol gqi
mgmt-ip management ip address
exit
```

Verifying the LED Management Interface Configuration

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

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

Troubleshooting Tips

To ping the management interface, use the following command:

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

Configuration Examples

This section provides configuration examples for the management IP interface.

Management IP Interface

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

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

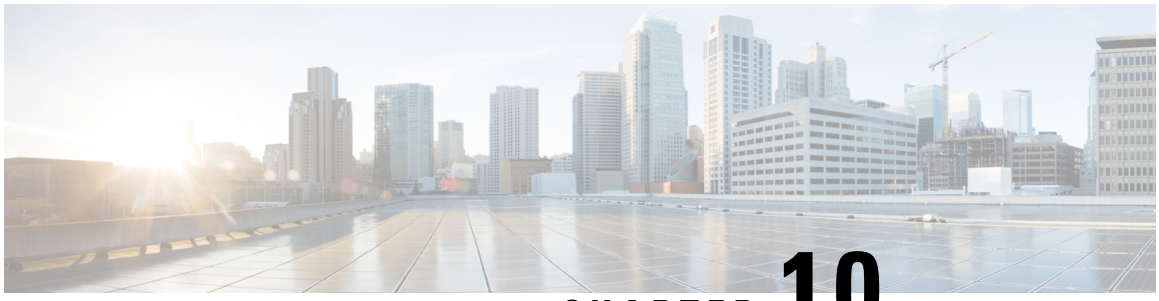
Feature Information for Management IP Interface

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

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

Table 9: Feature Information for Management IP Interface

Feature Name	Releases	Feature Information
Management IP Interface	Cisco IOS-XE Release 3.18.0S	This feature was introduced on the Cisco cBR Series Converged Broadband Routers.



CHAPTER 10

Video Encryption

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

Information About Encryption

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

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

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

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

Table 10: Supported Encryption Types and Scrambler Modes

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

Prerequisites for Encryption

You should configure the Virtual Carrier Group (VCG) to setup an encrypted session. For more details, see the Configuring Virtual Carrier Group, on page 48.

How to Configure Encryption for the Data Stream

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

Enforcing Data Stream Encryption Type

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

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

Before You Begin

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

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

Configuring Virtual Carrier Group

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

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

Verifying Encryption Configuration

To verify the encryption configurations, use the following command:

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

Example 1:

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

Example 2:

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

Configuration Examples for Encryption

This section provides configuration examples for the Encryption feature.

Example: Enforcing Data Stream Encryption Type

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

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

Example: Configuring Virtual Carrier Group

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

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

Configuring Privacy Mode Encryption

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

You can configure the following:

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

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

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

Configuring VODS-ID

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

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

Configuring CEM IP and Port

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

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

Configuring Management IP

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

Before You Begin

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

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

Verifying PME Connection Status

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

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

This command displays the following information:

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

Example:

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

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

Verifying PME Version

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

show cablevideo encryption pme version

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

Example:

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

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

Verifying PME Sessions on a Line Card

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

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

Example 1:

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

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

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

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

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

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

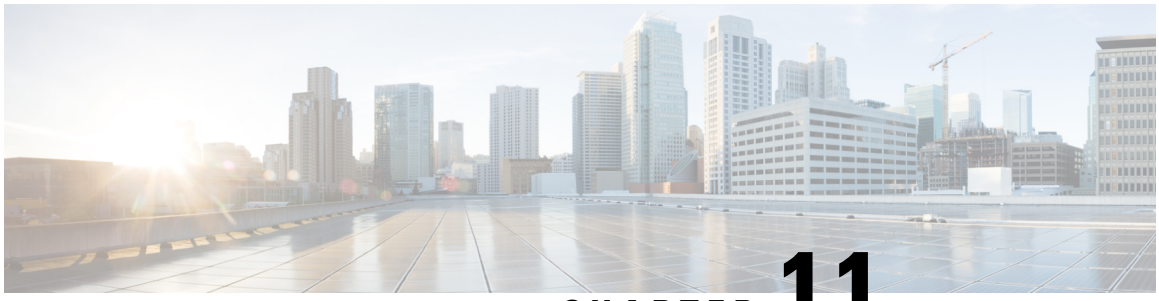
Feature Information for Encryption

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

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

Table 11: Feature Information for Encryption

Feature Name	Releases	Feature Information
Encryption	Cisco IOS-XE Release3.18.0S	This feature was introduced on the Cisco cBR Series Converged Broadband Routers.



CHAPTER 11

Global Video Configuration

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

Contents

Configuring the Default ONID

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

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

Configuring the Default PSI interval

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

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

Configuring Video Session Timeouts

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

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

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

Configuration Examples

This section provides examples for the global video configuration.

Example: Global Video Configuration

```
configure terminal
cable video
default-onid 10
default- psi-interval 50
timeout init-session 200 msec
timeout idle-session 250 msec
timeout off-session 500 sec
```

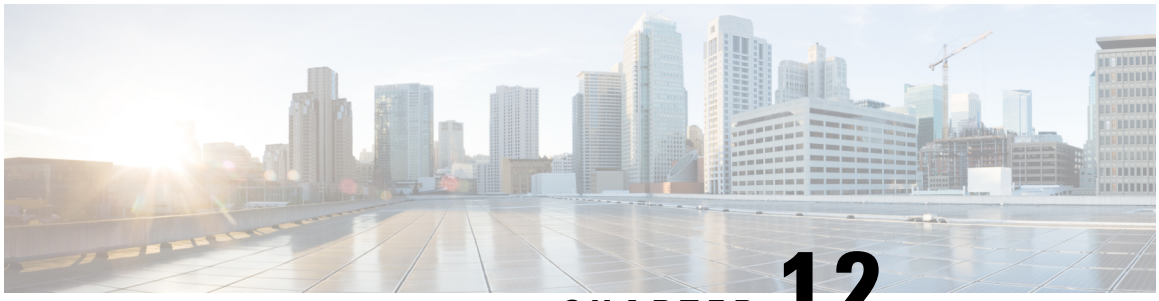
Feature Information for Global Video Configuration

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 12: Feature Information for Global Video Configuration

Feature Name	Releases	Feature Information
Global Video Configuration	Cisco IOS-XE Release 3.18.0S	This feature was introduced on the Cisco cBR Series Converged Broadband Routers.



CHAPTER 12

Advanced Video MPEG Features

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

Information about Advanced Video MPEG Features

Reserved Output PID Range

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

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

How to Configure Advanced Video MPEG Features

Configuring Reserved Output PID Range

To configure reserved output range, follow the steps below:

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

Verifying Reserved Output PID Range Configuration

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

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

Configuration Examples for Advanced Video MPEG Features

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

Example: Configuring Reserved Output PID Range

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

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

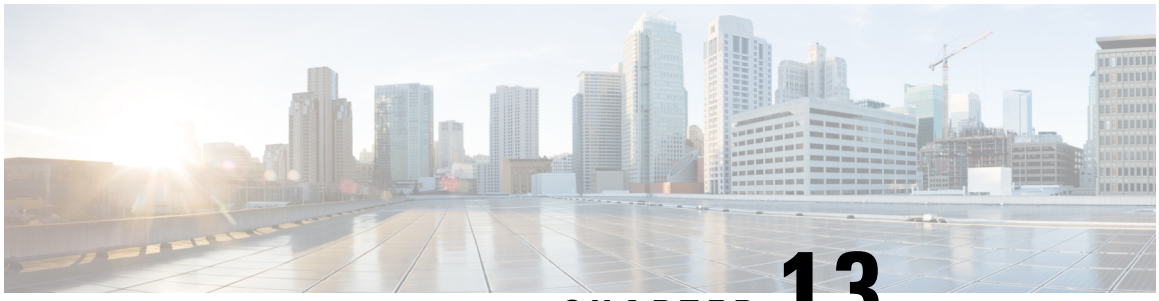
Feature Information for Advanced Video MPEG Features

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

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

Table 13: Feature Information for Advanced Video MPEG Features

Feature Name	Releases	Feature Information
Advanced Video MPEG Features	Cisco IOS-XE Release 3.18.0S	This feature was introduced on the Cisco cBR Series Converged Broadband Router s.



CHAPTER 13

Important Notes

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

Video Packet Routing Requirements

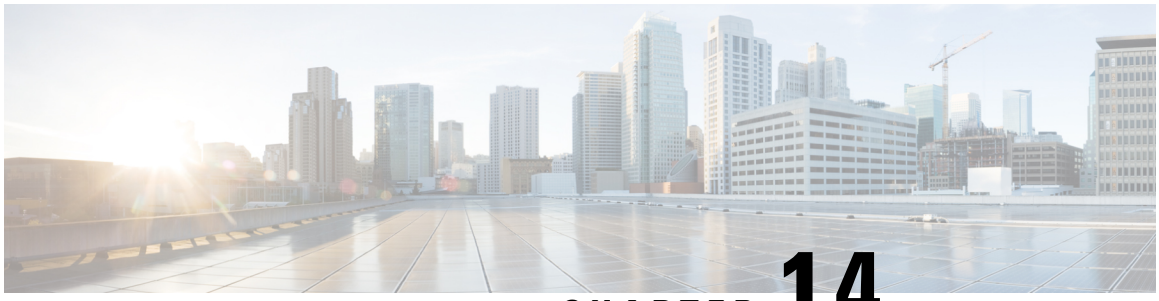
A routing protocol, such as OSPF or IS-IS, must be enabled on the cBR-8 in order for video data packets from the head end to reach the virtual QAMs. On the cBR-8, enable a routing protocol as described in the routing configuration guide.

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

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

PART II

Cisco cBR Converged Broadband Routers Video Features



CHAPTER 14

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 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 3.18.0S 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 14: 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 68.

Troubleshooting Tips

GQI Connection

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

Session Input State

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

  To display the LED, use the following command:

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

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

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

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

  show interface TenGigabitEthernet *slot/bay/port*

Session Output State

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

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

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

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

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

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

  show cable video output-port *output port number*

Session Encrypt Status

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

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

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

```
LED 1 has 8137 SCGs on 128 carriers

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

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

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

```
68157684   1048820     1     1     100
```

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

  show cable video scg id *SCG id*

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

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

Configuration Examples

This section provides configuration examples for the PowerKEY VOD feature:

Example: Configuring Encryption Type on the Line Card

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

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

Example: Configuring Encrypted Virtual Carrier Groups

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

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

Example: Configuring Service Distribution Groups and Binding

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

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

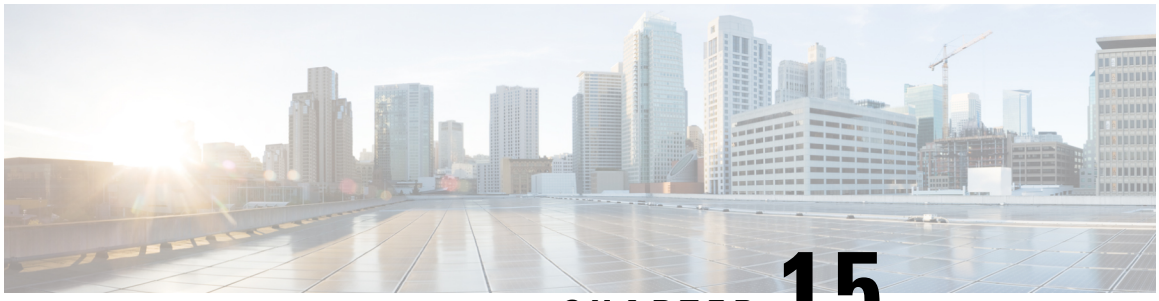
Feature Information for PowerKEY VOD

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

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

Table 15: Feature Information for PowerKEY VOD

Feature Name	Releases	Feature Information
PowerKEY VOD	Cisco IOS-XE Release 3.18.0S	This feature was introduced on the Cisco cBR Series Converged Broadband Routers.



CHAPTER 15

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.

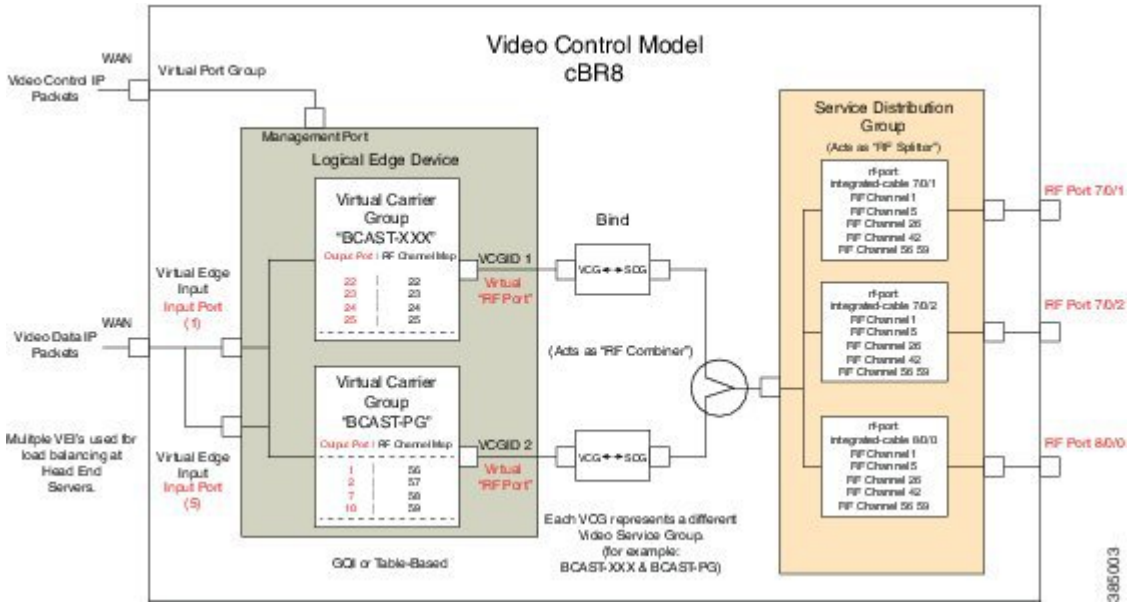
The **service-distribution-group** construct is used to perform replication. Hardware replication is supported when the replication of individual QAM Carriers is limited to the same line card.

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
```

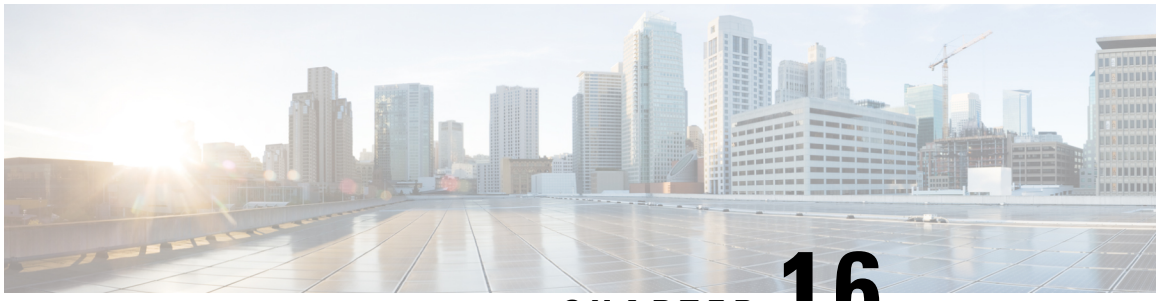
Feature Information for Replication

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

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

Table 16: Feature Information for Replication

Feature Name	Releases	Feature Information
Replication	Cisco IOS-XE Release3.18.0S	This feature was introduced on the Cisco cBR Series Converged Broadband Routers.



CHAPTER 16

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 82 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:

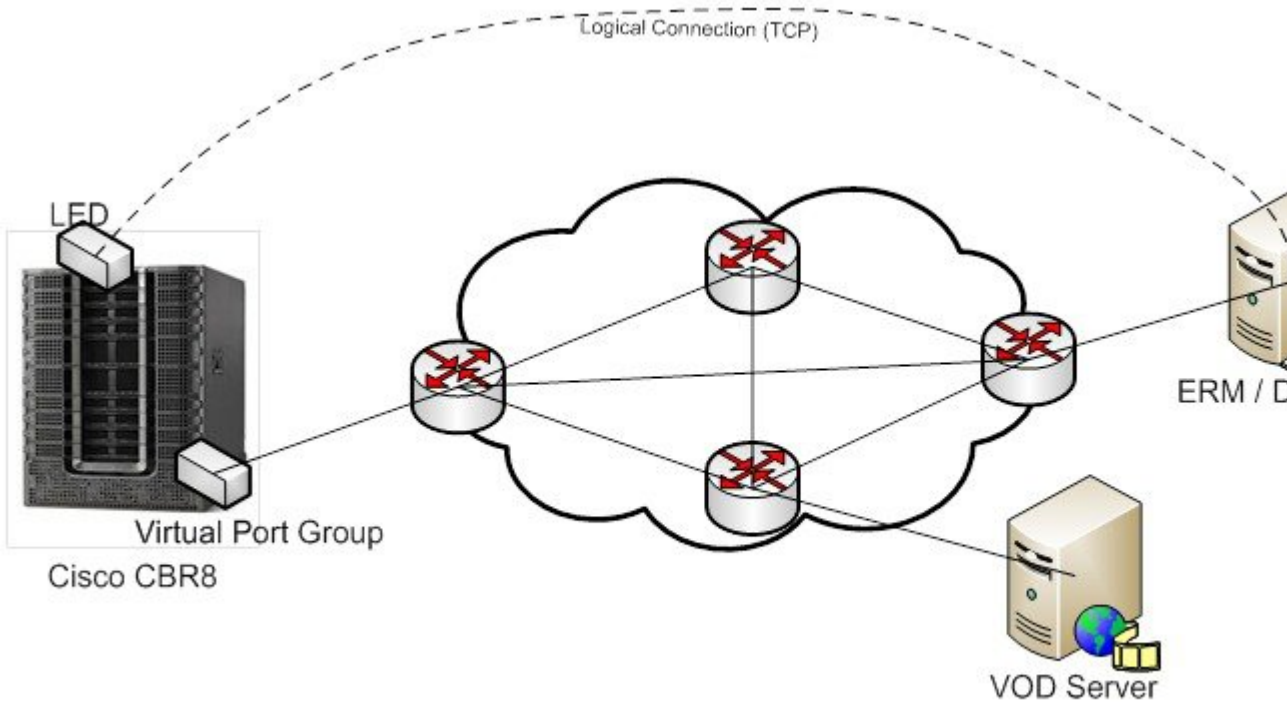
```
cable video
  mgmt-intf VirtualPortGroup 0
  encryption
    linecard 7/0 ca-system pme scrambler dvs042
    pme vodsid 111
    pme cem 1.200.1.163 5000
    pme mgmt-ip 1.25.2.6
  service-distribution-group sdg-pme id 1
    rf-port integrated-cable 7/0/7
  virtual-carrier-group vcg-pme id 1
    encrypt
    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.

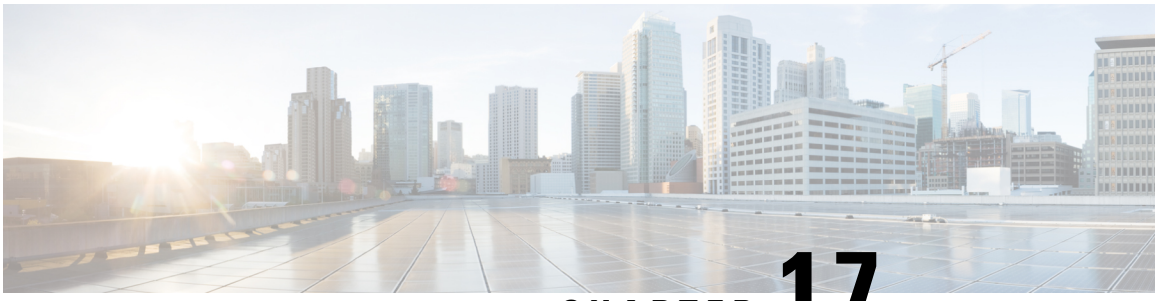
Feature Information for D6 Discovery Protocol

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 17: Feature Information for D6 Discovery Protocol

Feature Name	Releases	Feature Information
D6 Discovery Protocol	Cisco IOS-XE Release 3.18.0S	This feature was introduced on the Cisco cBR Series Converged Broadband Routers.



CHAPTER 17

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.

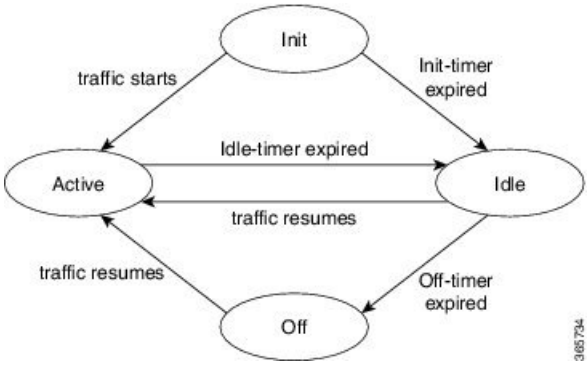
This ensures that all sessions switch to the same source IP address when a source switch occurs. Additionally, sessions configured via GQI have up to three sources available for redundancy, whereas multicast labels configured for table-based sessions have up to four sources available for redundancy.

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
```

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 mulltiсast 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
```

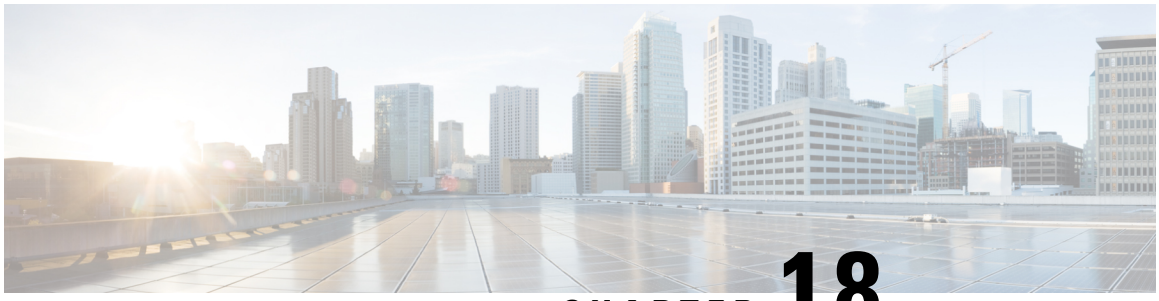
```
session SESS_PME6 group 232.2.6.7 source 175.7.2.2 processing-type data
```

Feature Information for Switched Digital Video

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

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

Feature Name	Releases	Feature Information
Switched Digital Video	Cisco IOS-XE Release 3.18.0SP	This feature was introduced on the Cisco cBR Series Converged Broadband Routers.



CHAPTER 18

Video MIBs

The SCTE-HMS-MPEG-MIB and SCTE-HMS-QAM-MIB are supported under the video management framework of Cisco cBR-8 routers.

Note For Cisco IOS-XE release 3.18.0S, only unicast traffic, that is VOD and SPTS, are supported.

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)