Cisco Remote PHY Device Video Configuration for Cisco 1x2 / Compact Shelf RPD Software 3.1

First Published: 2017-11-23

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

© 2017 Cisco Systems, Inc. All rights reserved.

CONTENTS

CHAPTER 1 **Cisco Remote PHY Video Configuration** 1

- Hardware Compatibility Matrix for Cisco Remote PHY Device 1
- Hardware Compatibility Matrix for Cisco Remote PHY Device 2
- Information About R-PHY Video Configuration 2
- How to Configure R-PHY Video 3
  - Configuring Downstream Controller Profile 3
  - Configuring RPD 3
  - Configuring Downstream Sharing 4
  - Configuring Video 4
  - Configuring Virtual Service Group 4
- Example: R-PHY Video Configuration 6
- Feature Information for Remote PHY Video 7

CHAPTER 2 **Remote PHY DVB Video on Demand** 9

- Information About DVB VOD 9
  - Overview of DVB VOD 9
  - Session based Scrambling Setup 10
  - Fail-to-Clear 10
  - Tier based Scrambling Setup 11
  - Restrictions for DVB 11
- How to Configure DVB 12
  - Configuring RPHY DVB VoD 12
  - Verifying the DVB Configuration 13
  - Troubleshooting Tips 15
- Configuration Examples 15
  - Example: Basic Session-based Scrambling Configuration 15
  - Example: Basic Tier-based Scrambling Configuration 16
  - Example: Basic Session-based Dualcrypt Scrambling Configuration 17

Additional References 18
Feature Information for RPHY DVB VoD Suppot 18

CHAPTER 3 Cisco Remote PHY PowerKEY VOD 19
Hardware Compatibility Matrix for Cisco Remote PHY Device 19
Information About PowerKEY VOD 20
Overview of PowerKEY VoD 20
How to Configure RPHY PowerKey VOD 21
Configuring the Encryption Type on the Line Card 21
Verifying the Encryption Configuration 21
Configuring the Encrypted Virtual Carrier Groups 21
Configuring the Encrypted Virtual Carrier Groups 22
Verifying the Encrypted Virtual Carrier Groups Configuration 22
Configuring the Service Distribution Groups and Binding 22
Configuring the Logical Edge Device and GQI Protocol 23
Verifying the PowerKEY VoD Configuration 23
Configuration Examples 25
Example: Configuring Encryption Type on the Line Card 25
Example: Configuring Encrypted Virtual Carrier Groups 25
Example: Configuring Service Distribution Groups and Binding 25
Feature Information for Rmote PHY PowerKEY VoD 25

CHAPTER 4 Cisco Remote PHY Pre-encrypted Broadcast Video 27
Hardware Compatibility Matrix for Cisco Remote PHY Device 27
Information About Pre-encrypted Broadcast Video 28
Multicast Table-based Sessions 28
MPTS Pass-through Session 29
How to Configure Pre-encrypted Broadcast Video Sessions 29
Configure a Port-Channel Interface 29
Configuring Pre-encrypted Broadcast Sessions 29
Configuring the Service Distribution Groups and Binding 30
Configuration Example for Pre-encrypted Broadcast Video Session 30
Feature Information for RPHY Pre-encrypted Broadcast Video 30

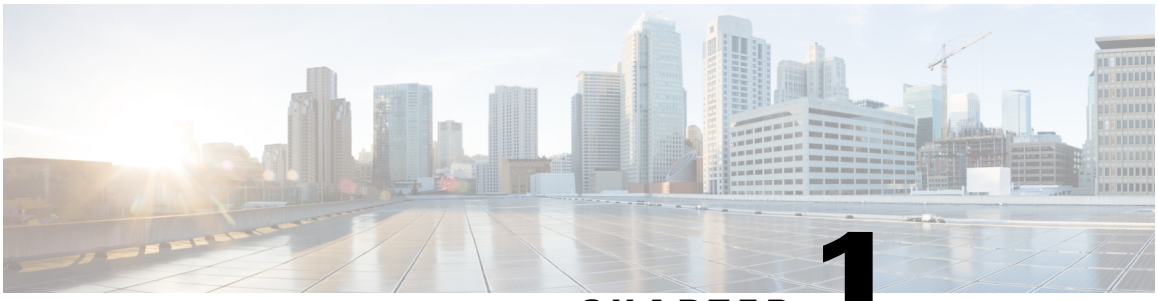
CHAPTER 5 Remote PHY BFS QAM Configuration 33

Hardware Compatibility Matrix for Cisco Remote PHY Device 33
Information About BFS QAM Support 34
How to Configure BFS QAM for EC 7.x 34
Mapping Cisco cBR-8 as a GQI QAM 35
Creating VCG with One QAM Channel 35
Creating SDG for BFS Sessions on Cisco cBR 35
Create VCG for BFS 36
Creating Logical Edge Device 36
Creating GQI QAM for BFS on EC 7.x 37
How to Configure BFS QAM for RPD 37
Creating SDG for BFS Sessions for RPD 37
Creating LED for RPD 38
Defining Cable RPD 38
How to Configure BFS QAM for EC 8.x 38
Creating VCG for VoD QAM Channels 39
Creating VCG for SDV QAM Channels 39
Creating SDG 39
Creating LEDs 40
Configuration Example for BFS QAM Configuration 40
Example: BFS QAM Configuration on Cisco cBR for EC 7.x 40
Example: BFS QAM Configuration on RPD 41
Example: BFS QAM Configuration on Cisco cBR for EC 8.x 42
Feature Information for BFS QAM Configuration 43

CHAPTER 6 **Remote PHY Switched Digital Video 45**
Switched Digital Video Services 45
Session Cloning 46
Redundant Multicast Sources 46
Benefits of Switched Digital Video 47
Prerequisites for Switched Digital Video 47
Restrictions for Switched Digital Video 47
Information About Switched Digital Video 48
QAM Sharing 48
QAM Replication 48
MPTS Pass-through Session 48

How to Configure the Switched Digital Video Services 49
Configuring Multicast Routing 49
Configuring Multicast Label 49
Configuring Multicast Table-based Sessions 49
Configuring Source Switching 50
Verifying Switched Digital Video Configuration 50
Troubleshooting Switched Digital Video Configuration 51
Configuration Examples for Switched Digital Video 52
Feature Information for Switched Digital Video 55

CHAPTER 7 **Remote PHY QAM Profile Configuration 57**
Information About QAM Profile 57
How to Configure Remote PHY QAM Profile 58
Configuring the QAM Profile on Downstream Channels 58
Verifying QAM Profile on Downstream Channels 59
Configuration Example 59
Feature Information for QAM Profile Configuration 59



CHAPTER 1

Cisco Remote PHY Video Configuration

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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

- Hardware Compatibility Matrix for Cisco Remote PHY Device, page 1
- Hardware Compatibility Matrix for Cisco Remote PHY Device, page 2
- Information About R-PHY Video Configuration, page 2
- How to Configure R-PHY Video, page 3
- Example: R-PHY Video Configuration, page 6
- Feature Information for Remote PHY Video, page 7

Hardware Compatibility Matrix for Cisco Remote PHY Device

Note The hardware components introduced in a given Cisco Remote PHY Device Software Release are supported in all subsequent releases unless otherwise specified.

Table 1: Hardware Compatibility Matrix for the Cisco Remote PHY Device

Cisco HFC Platform	Remote PHY Device
Cisco GS7000 Node	**Cisco 1x2 RPD Software 1.1 and Later Releases** Cisco Remote PHY Device 1x2 • PID—RPD-1X2= • PID—RPD-1X2-PKEY=

Note The -PKEY suffix in the PID indicates units that enable the SCTE-55-2 Out-of-Band protocol support.

Hardware Compatibility Matrix for Cisco Remote PHY Device

Note The hardware components introduced in a given Cisco Remote PHY Device Software Release are supported in all subsequent releases unless otherwise specified.

Table 2: Hardware Compatibility Matrix for the Cisco Remote PHY Device

Cisco HFC Platform	Remote PHY Device
Cisco GS7000 Node	**Cisco 1x2 RPD Software 1.1 and Later Releases** Cisco Remote PHY Device 1x2 • PID—RPD-1X2= • PID—RPD-1X2-PKEY=

Note The -PKEY suffix in the PID indicates units that enable the SCTE-55-2 Out-of-Band protocol support.

Information About R-PHY Video Configuration

The controller profile specifies the RF channels that belong to this profile and their RF parameters. Profile can either be unicast or multicast.

Multicast profile is used for downstream sharing. Multiple Remote PHY Devices (RPDs) can be configured to receive the same downstream controller. The traffic is multicast to all RPDs configured to receive the

downstream controller. Applications include Video on Demand (VOD), Switched Digital Video (SDV) and Broadcast Video.

There is one principal core interface, and up to four auxiliary core interfaces in the RPD configuration. Principal core specifies the DPIC interface with which RPD connects. Auxiliary cores specify external DPIC interfaces that can be used for downstream sharing. Auxiliary core is currently used for narrowcast video, broadcast video and out-of-band data signaling path (OOB) only.

How to Configure R-PHY Video

This section describes how to configure R-PHY video on Cisco cBR-8.

Configuring Downstream Controller Profile

To configure the donwstream controller profile, use the example below:

```
Router# configure terminal
Router(config)# cable depi multicast pool 20
Router(config-multicast-pool)# ip address 225.28.0.0  255.255.0.0
Router(config-multicast-pool)# exit
Router(config)# cable downstream controller-profile 1
Router(config-controller-profile)# multicast-pool 20
Router(config-controller-profile)# rf-chan 0 15
Router(config-prof-rf-chan)# type docsis
Router(config-prof-rf-chan)# frequency 111000000
Router(config-prof-rf-chan)# rf-output normal
Router(config-prof-rf-chan)# qam-profile 1
Router(config-prof-rf-chan)# docsis-channel-id 1
Router(config-prof-rf-chan)# exit
Router(config-controller-profile)# rf-chan 16 19
Router(config-prof-rf-chan)# type video sync
Router(config-prof-rf-chan)# frequency 699000000
Router(config-prof-rf-chan)# rf-output normal
Router(config-prof-rf-chan)# qam-profile 1
Router(config-prof-rf-chan)# exit
Router(config-controller-profile)# exit
Router(config)# cable downstream controller-profile 2
Router(config-controller-profile)# multicast-pool 1
Router(config-controller-profile)# rf-chan 20 47
Router(config-prof-rf-chan)# type video sync
Router(config-prof-rf-chan)# frequency 231000000
Router(config-prof-rf-chan)# rf-output normal
Router(config-prof-rf-chan)# qam-profile 4
```

In the above example,two profiles are configured, profile 1 is a mixed profile, profile 2 is a video only profile.

Configuring RPD

To configure the RPD to include the controller profile, follow the example below:

```
Router# configure terminal
Router(config)# cable rpd RPD01
Router(config-rpd)# identifier 0004.9f31.0455
Router(config-rpd)# core-interface Te3/1/0
Router(config-rpd-core)# principal
Router(config-rpd-core)# rpd-ds 0 downstream-cable 3/0/0 profile 1
Router(config-rpd-core)# rpd-ds 0 downstream-cable 3/0/1 profile 2
Router(config-rpd-core)# rpd-us 0 upstream-cable 3/0/0 profile 1
Router(config-rpd-core)# exit
Router(config-rpd)# core-interface te6/1/0
Router(config-rpd-core)# rpd-ds 0 downstream-cable 6/0/0 profile 2
```

```
Router(config-rpd-core)# exit
Router(config-rpd)# r-dti 1
Router(config-rpd)# rpd-event profile 0
```

Note

- All channels within the profiles of a RPD must be unique, frequencies must not overlap each other.
- There must be at least one DOCSIS downstream profile in the principal core.
- Auxiliary core must only contain video and out-of-band profiles.
- A downstream controller can only be associated to one profile.

Configuring Downstream Sharing

Downstream sharing is used for multicast (MC) traffic. To configure downstream sharing, follow the example below:

```
Router# configure terminal
Router(config)# cable rpd RPD01
Router(config-rpd)# core-interface Te3/1/0
Router(config-rpd-core)# principal
Router(config-rpd-core)# rpd-ds 0 downstream-cable 3/0/1 profile 2
Router(config-rpd-core)# exit
Router(config-rpd)# exit
Router(config)# cable rpd RPD02
Router(config-rpd)# core-interface te3/1/0
Router(config-rpd-core)# principal
Router(config-rpd-core)# rpd-ds 0 downstream-cable 3/0/1 profile 2
Router(config-rpd-core)# exit
Router(config-rpd)# exit
Router(config)# cable rpd RPD03
Router(config-rpd)# core-interface te6/1/0
Router(config-rpd-core)# principal
Router(config-rpd-core)# rpd-ds 0 downstream-cable 6/0/1 profile 3
Router(config-rpd-core)# exit
Router(config-rpd)# core-interface te3/1/0
Router(config-rpd-core)# rpd-ds 0 downstream-cable 3/0/1 profile 2
```

Note All RPDs in the same multicast group have the same controller and profile association.

Configuring Video

To configure Video, see Cisco Converged Broadband Routers Video Configuration Guide for Cisco IOS XE Everest 16.5.1.

Configuring Virtual Service Group

Virtual Service Group is supported to allow the controller configuration and removal of an RPD using that controller without removing the video configuration. To configure virtual service group, follow the example below:

1 Add controller profile:

```
Router(config)# cable downstream controller-profile 2
Router(config-controller-profile)# multicast-pool 20
Router(config-controller-profile)# rf-channel 20 47
Router(config-prof-rf-chan)# type video sync
Router(config-prof-rf-chan)# frequency 231000000
Router(config-prof-rf-chan)# rf-output NORMAL
Router(config-prof-rf-chan)# qam-profile 7
Router(config-prof-rf-chan)# exit
Router(config-controller-profile)# exit
```

2 Assign controller profile to a downstream cable for a virtual service group:

```
Router(config)# cable virtual-service-group VOD_SG1801 downstream-cable 9/0/1 profile 2
Router(config)# cable virtual-service-group VOD_SG1802 downstream-cable 9/0/3 profile 2
Router(config)# cable virtual-service-group BC_Chicago downstream-cable 9/0/31 profile
3
```

3 Create VCG, SDG, RPD downstream cable, bind VCG to SDG, assign VCG to LED, set LED active, and create sessions:

```
Router(config)# cable video
Router(config-video)# multicast-uplink Port-channel22 access-list all-multicasts
Router(config-video)# mgmt-intf VirtualPortGroup 0
Router(config-video)# service-distribution-group sdg91 id 91
Router(config-video-sdg)# rpd downstream-cable 9/0/1
Router(config-video-sdg)# exit
Router(config-video)# virtual-carrier-group vcg91 id 91
Router(config-video-vcg)# encrypt
Router(config-video-vcg)# service-type narrowcast
Router(config-video-vcg)# rf-channel 40-63 tsid 38001-38024 output-port-number 1-24
Router(config-video-vcg)# exit
Router(config-video)# bind-vcg
Router(config-video-bd)# vcg vcg91 sdg sdg91
Router(config-video-bd)# exit
Router(config-video)# logical-edge-device led-1 id 1
Router(config-video-led)# protocol table-based
Router(config-video-led-protocol)# virtual-edge-input-ip 174.102.1.1 input-port-number
1
Router(config-video-led-protocol)# vcg vcg91
Router(config-video-led-protocol)# active
Router(config-video-led-protocol)# table-based
Router(config-video-tb)# vcg vcg91
Router(config-video-tb-vcg)# rf-channel 40
Router(config-video-tb-vcg-sess)# session ss group 232.2.1.251 source 175.2.3.2
processing-type remap
```

4 Assign controller to RPD, then physical QAM id is allocated and video sessions are online:

```
Router(config)# cable rpd RPD01
Router(config-rpd)# identifier 0004.9f32.1573
Router(config-rpd)# core-interface Te9/1/0
Router(config-rpd-core)# principal
Router(config-rpd-core)# rpd-ds 0 downstream-cable 9/0/1 profile 2
Router(config-rpd-core)# rpd-ds 0 downstream-cable 9/0/3 profile 2
Router(config-rpd-core)# rpd-us 0 upstream-cable 9/0/0 profile 1
Router(config-rpd-core)# exit
Router(config-rpd)# core-interface Te9/1/6
Router(config-rpd-core)# rpd-ds 0 BC_Chicago
Router(config-rpd-core)# exit
Router(config-rpd)# r-dti 1
Router(config-rpd)# rpd-event profile 0
```

5 It is allowed to remove or replace the controller from the RPD configuration as show below, without touching any video configuration, then the video sessions are in off state which is similar to the scenario that the video QAM is shut down.

```
Router(config)# cable rpd RPD01
Router(config-rpd)# core-interface Te9/1/0
Router(config-rpd-core)# no rpd-ds 0 downstream-cable 9/0/1 profile 2
```

Note If virtual service group doesn't exist while adding controller downstream to RPD configuration, virtual service group is automatically generated when the controller profile has one or more rf-channels of the video type. If the user changes RPD downstream configuration to use another controller profile different from the one in virtual service group and in the meantime video configuration exists, the user also needs to update the controller profile in the virtual service group for that downstream as well, otherwise all the video sessions will be down.

Example: R-PHY Video Configuration

The following example shows how to configure Remote-PHY video:

```
Router# configure terminal
Router(config)# cable downstream qam-profile 7
Router(config-qam-prof)# annex B modulation 256
Router(config-qam-prof)# interleaver-depth I32-J4
Router(config-qam-prof)# symbol-rate 5361
Router(config-qam-prof)# spectrum-inversion off
Router(config-qam-prof)# description default-annex-b-256-qam
Router(config-qam-prof)# exit
Router(config)# cable depi multicast pool 20
Router(config-multicast-pool)# ip address 225.28.0.0 255.255.0.0
Router(config-multicast-pool)# exit
Router(config)# cable downstream controller-profile 1
Router(config-controller-profile)# multicast-pool 20
Router(config-controller-profile)# rf-channel 0 15
Router(config-prof-rf-chan)# type docsis
Router(config-prof-rf-chan)# frequency 111000000
Router(config-prof-rf-chan)# rf-output NORMAL
Router(config-prof-rf-chan)# qam-profile 7
Router(config-prof-rf-chan)# docsis-channel-id 1
Router(config-prof-rf-chan)# exit
Router(config-controller-profile)# exit
Router(config)# cable downstream controller-profile 2
Router(config-controller-profile)# multicast-pool 20
Router(config-controller-profile)# rf-channel 20 47
Router(config-prof-rf-chan)# type video sync
Router(config-prof-rf-chan)# frequency 231000000
Router(config-prof-rf-chan)# rf-output NORMAL
Router(config-prof-rf-chan)# qam-profile 7
Router(config-prof-rf-chan)# exit
Router(config-controller-profile)# exit
Router(config)# cable rpd RPD01
Router(config-rpd)# identifier 0004.9f31.0979
Router(config-rpd)# core-interface te6/1/0
Router(config-rpd-core)# principal
Router(config-rpd-core)# rpd-ds 0 downstream-cable 6/0/0 profile 1
Router(config-rpd-core)# rpd-ds 0 downstream-cable 6/0/1 profile 2
Router(config-rpd-core)# rpd-us 0 upstream-cable 6/0/0 profile 1
Router(config-rpd-core)# exit
Router(config-rpd)# r-dti 6
Router(config-rpd)# rpd-event profile 0
Router(config-rpd)# exit
Router(config)# cable rpd RPD2
Router(config-rpd)# identifier 0004.9f31.1437
Router(config-rpd)# core-interface Te3/1/0
Router(config-rpd-core)# principal
Router(config-rpd-core)# rpd-ds 0 downstream-cable 3/0/0 profile 1
Router(config-rpd-core)# rpd-us 0 upstream-cable 3/0/0 profile 1
Router(config-rpd-core)# exit
Router(config-rpd)# core-interface Te6/1/0
Router(config-rpd-core)# rpd-ds 0 downstream-cable 6/0/1 profile 2
Router(config-rpd-core)# exit
Router(config-rpd)# r-dti 3
```

```
Router(config-rpd)# rpd-event profile 0
Router(config-rpd)# exit
Router(config)# cable video
Router(config-video)# service-distribution-group RPD_SDG
Router(config-video-sdg)# rpd downstream-cable 6/0/1
Router(config-video-sdg)# exit
Router(config-video)# virtual-carrier-group RPC_VCG
Router(config-video-vcg)# rf-channel 20-47 tsid 20-47 output-port-number 20-47
Router(config-video-vcg)# exit
Router(config-video)# bind-vcg
Router(config-video-bd)# vcg RPC_VCG sdg RPD_SDG
Router(config-video-bd)# exit
Router(config-video)# logical-edge-device RPD_LED
Router(config-video-led)# protocol table-based
Router(config-video-led-protocol)# virtual-edge-input-ip 174.102.1.1 input-port-number 1
Router(config-video-led-protocol)# vcg RPD_VCG
Router(config-video-led-protocol)# active
Router(config-video-led-protocol)# table-based
Router(config-video-tb)# vcg RPD_VCG
Router(config-video-tb-vcg)# rf-channel 20-47
Router(config-video-tb-vcg-sess)# session tbsession-1 input-port 1 start-udp-port 49152
num-sessions-per-qam 20 processing-type remap start-program 1 bit-rate 1800000
```

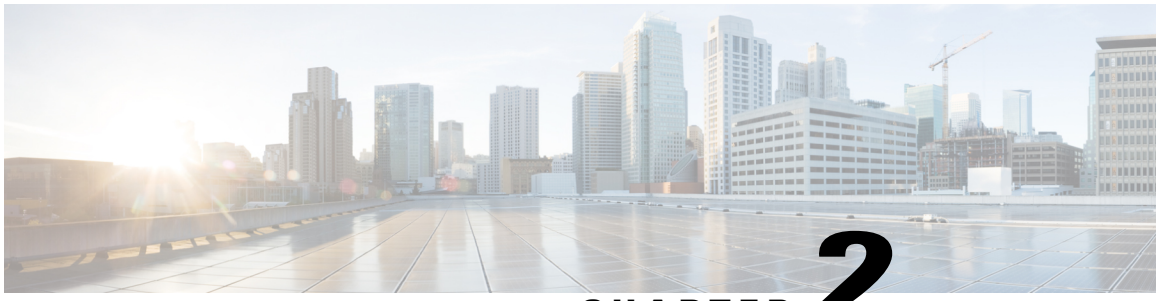
Feature Information for Remote PHY Video

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 3: Feature Information for Remote PHY Video

Feature Name	Releases	Feature Information
RPHY Video PME VOD	Cisco 1x2 / Compact Shelf RPD Software 3.1	This feature was integrated into the Cisco Remote PHY Device.
RPHY Video Pre-Encrypted MPTS Pass-Thru Support	Cisco 1x2 / Compact Shelf RPD Software 3.1	This feature was integrated into the Cisco Remote PHY Device.
RPHY Pre-encrypted Broadcast Video Support	Cisco 1x2 / Compact Shelf RPD Software 3.1	This feature was integrated into the Cisco Remote PHY Device.



CHAPTER 2

Remote PHY DVB Video on Demand

The Digital Video Broadcasting (DVB) protocol for encrypting video services as defined in the ETSI TS 103 197 DVB Simulcrypt specification has been implemented on the line card for DVB R-PHY on Cisco cBR-8. This document contains an overview of the commands for configuring DVB and the commands for viewing the status of the encryption of services.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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

- Information About DVB VOD, page 9
- How to Configure DVB, page 12
- Configuration Examples, page 15
- Additional References, page 18
- Feature Information for RPHY DVB VoD Suppot, page 18

Information About DVB VOD

Overview of DVB VOD

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

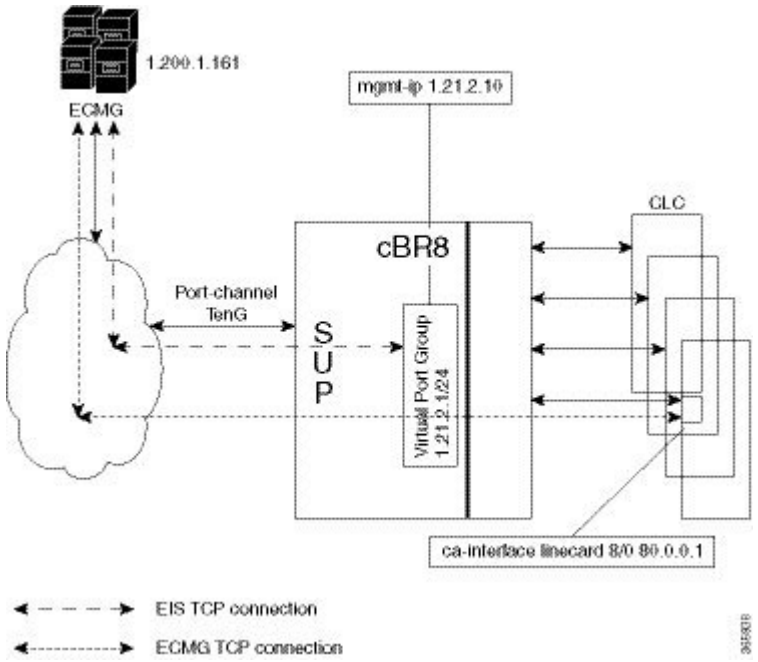
The two primary modes of scrambling are: session based scrambling and tier-based scrambling. The basic difference between the two modes is that the manner in which the Entitlement Control Messages (ECM) are

requested from the ECMG. For session based scrambling, a control word (CW) is generated once every Crypto Period (CP) and the ECM is requested for each session. For tier-based scrambling, the control word is generated once every CP and the ECM generated by the ECMG for the CW is used by all the sessions in the chassis.

Session based Scrambling Setup

The connection with the external EIS Server is established via the Virtual Port Group in the Supervisor. The connection with the external ECMG server is established via the linecard.

Figure 1: Session based Setup



Fail-to-Clear

The fail-to-clear-duration feature is supported on DVB sessions and DualCrypt encryption modes. Based on the session encryption, the following two features are supported on the Cisco cBR Series Converged Broadband Routers.

Fail-to-Clear Duration for DVB Session-based Encryption

This feature is used along with DVB or DualCrypt encryption with external Event Information Scheduler (EIS) configuration. When encryption for a session fails in Cisco cBR-8, this feature enables the operator to control the configured DVB-encrypted sessions to function without encryption for a configured duration. If the encryption still fails, the DVB session is marked as `Fail-to-black` after the fail-to-clear duration timeout.

Fail-to-Clear for DVB Tier-based Encryption

This feature is used along with Tier-based configuration. When encryption for a session fails in Cisco cBR-8, this feature enables the operator to control the configured DVB-encrypted sessions to function without encryption.

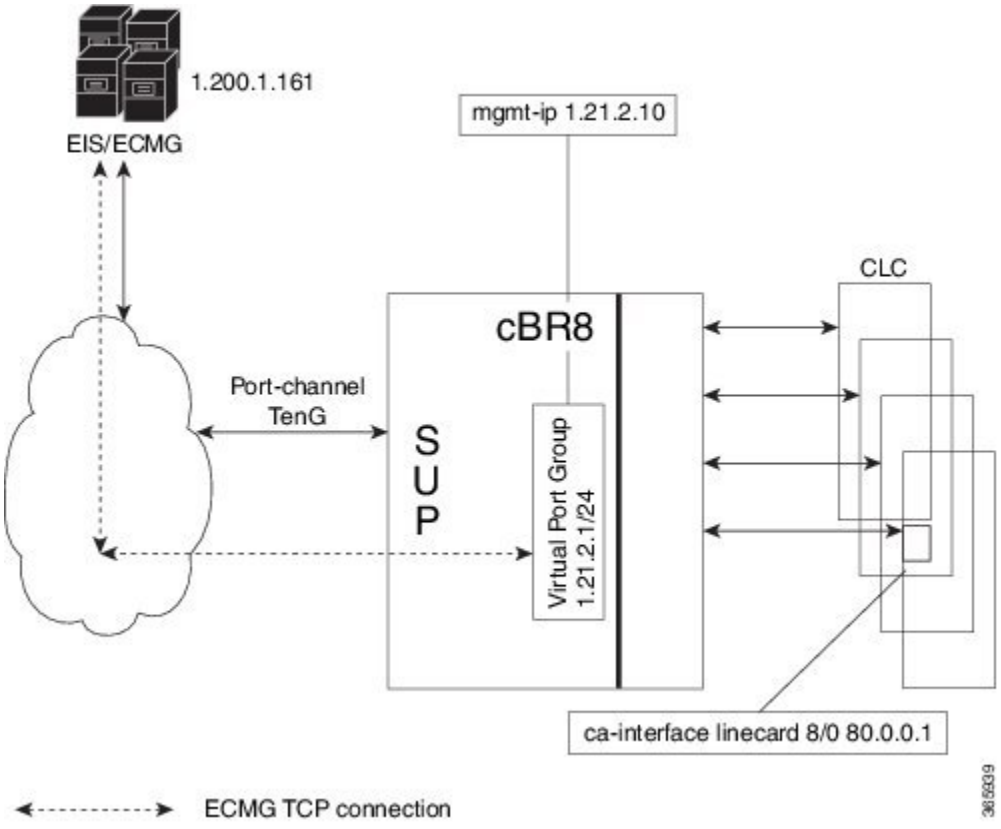
If fail-to-clear is configured, tier-based configuration is enabled, and then if the encryption fails, the DVB session's `Encrypt Status` is marked as `clear`. The status changes to `Encrypted` when the encryption starts.

This feature is not enabled by default.

Tier based Scrambling Setup

The connection with the external ECMG server is established via the Virtual Port Group in the Supervisor.

Figure 2: Tier based Setup



Restrictions for DVB

- This feature is applicable only for remapped table based sessions.
- Fail-to-clear-duration feature is applicable only to session-based scrambling for DVB CAS encryption.
- Fail-to-clear feature is applicable only to DVB tier-based scrambling sessions.

How to Configure DVB

Configuring RPHY DVB VoD

Before You Begin

- Virtual Port Group interface must be configured and the management IP for DVB must be identified.
- Management interface is set to this Virtual Port Group interface under cable video configuration.
- Logical Edge Device is configured with the table based protocol.
- The encryption algorithm of the linecard is set to DVB-CSA.
- For session based scrambling, the CA interface on the linecard and the route for reaching the ECMG server must be specified.

To configure session based scrambling, follow the steps below:

```
enable
config terminal
  interface int_id
    vrf forwarding vrf_script_red_1
    ip address ip-address subnet-mask
    no mop enabled
    no mop sysid
    exit
  cable video
    mgmt-intf VirtualPortGroup group_id
    encryption
      linecard slot/bay ca-system dvb scrambler dvb-csa
      dvb
        route-ecmg ECMG_Server_IP_Address Netmask Interface Forwarding_Router_IP_Address
        mgmt-ip management ip address
        eis EIS_name id EIS_id
          listening-port <1-65535> bind led id <led id | led name>
        ca-interface linecard slot/bay IP_Address
        ecmg ECMG_Name id ECMG_ID
          mode vod linecard slot/bay
          type standard
          ca-system-id CA_System_ID CA_Subsystem_ID
          auto-channel-id
          ecm-pid-source sid
          connection id ID priority connection_priority IP_Address Port
    service-distribution-group sdg name id SDG ID onid onid number
      rpd downstream-cable slot/subslot/bay
    virtual-carrier-group vcg-name id vcg_id
      encrypt
      service-type narrowcast
      rf-channel channel tsid tsid_number output-port-number number
    bind-vcg
      vcg vcg-name sdg sdg-name
    logical-edge-device led-name id led_id
      protocol gqi
        mgmt-ip IP_Address
        mac-address MAC address
        server server_ip_address
        keepalive retry 3 interval 10
        reset interval 8
        virtual-edge-input-ip IP address input-port-number 1
        vcg vcg-name
        active
```

The fail-to-clear-duration is measured in seconds. The valid values are in the range from 0 to 10800 seconds. The default value is 0.

To configure tier based scrambling, follow the steps below:

```
enable
config terminal
  interface VirtualPortGroup group_id
    vrf forwarding Mgmt-intf
    ip address ip-address subnet-mask
    no mop enabled
    no mop sysid
    exit

  cable video
    mgmt-intf VirtualPortGroup group_id
    encryption
      linecard slot/bay ca-system dvb scrambler dvb-csa
      dvb
        route-ecmg ECMG_Server_IP_Address Netmask Interface Forwarding_Router_IP_Address
        ecmg ECMG_Name id ECMG_ID
          mode tier-based
          type standard
          ca-system-id CA_System_ID CA_Subsystem_ID
          auto-channel-id
          ecm-pid-source sid
          connection id ID priority connection_priority IP_Address Port
        tier-based
          ecmg id ECMG_ID access- criteria access_criteria_in_hex
          fail-to-clear
          enable
    service-distribution-group sdg name id SDG ID onid onid number
      rpd downstream-cable slot/subslot/port
    virtual-carrier-group vcg-name id vcg_id
      encrypt
      service-type narrowcast
      rf-channel channel tsid tsid_number output-port-number number
    bind-vcg
      vcg vcg-name sdg sdg-name
    logical-edge-device led-name id led_id
      protocol table-based
        virtual-edge-input-ip IP address input-port-number 1
        vcg vcg-name
        active
    table-based
      vcg vcg-name
        rf-channel channel
          session session_name input-port id start-udp-port udp port number processing-type
 remap start-program 1 cbr
```

Note If the tier-based configuration is already enabled, you must first disable the tier-based configuration using the **no enable**, before you configure fail-to-clear feature.

Verifying the DVB Configuration

To verify the configuration of the encryption algorithm on the linecard, use the **show cable video encryption linecard** command as shown in the example below:

```
Router# show cable video encryption linecard 7/0
Line card: 7/0
CA System       Scrambler       DVB-Conformance
================================================
```

```
dvb             dvb-csa         Enabled
```

To verify the ECMG connection, use the **show cable video encryption dvb ecmg id** *id* **connection** command as shown in the example below:

```
Router# show cable video encryption dvb ecmg id 1 connection
------------------------------------------------------------------------------------------------
ECMG ECMG           ECMG     CA Sys CA Subsys PID    Lower Upper Streams/ Open Streams/
Auto Chan Slot ECMG        ECMG
ID   Name           Type     ID     ID        Source limit limit ECMG     ECMG          ID
             Connections Application
------------------------------------------------------------------------------------------------
1    polaris_ecmg01 standard 0x4748 0x0       sid    0     0     1        1
Enabled   RP   1           Tier-Based

ECMG Connections for ECMG ID = 1

-----------------------------------------------------------
Conn Conn     IP          Port    Channel  Conn    Open
-ID  Priority Address     Number  ID       Status  Streams
-----------------------------------------------------------
1    1        10.10.1.1  8888    1        Open    1
```

The sample output of the session based scrambling configuration verification command is shown below:

```
Router# show cable video encryption dvb ecmg id 7 connection
------------------------------------------------------------------------------------------------
ECMG ECMG           ECMG     CA Sys CA Subsys PID    Lower Upper Streams/ Open Streams/
Auto Chan Slot ECMG        ECMG
ID   Name           Type     ID     ID        Source limit limit ECMG     ECMG          ID
             Connections Application
------------------------------------------------------------------------------------------------
7    ecmg-7         standard 0x950  0x1234    sid    0     0     1680     1680
Enabled   7    1           VOD

ECMG Connections for ECMG ID = 1

-----------------------------------------------------------
Conn Conn     IP          Port    Channel  Conn    Open
-ID  Priority Address     Number  ID       Status  Streams
-----------------------------------------------------------
1    1        10.10.1.10  8888    1        Open    1
```

The status of the connection with the ECMG Server is indicated by the Conn Status. The Open Streams field indicates the number of Active ECM Streams.

To verify the EIS connection, use the **show cable video encryption dvb eis id** *id* command as shown in the example below:

```
Router# show cable video encryption dvb eis id 1
-------------------------------------------------------------------------------------------
EIS EIS  Peer       Management TCP  CP       CP       Overwrite Fail-To-Clear Connection
ID  Name IP         IP         Port Overrule Duration SCG       Duration      Status
-------------------------------------------------------------------------------------------
1   test 10.10.1.11 10.10.1.1  9898 DISABLED 0        DISABLED  400           Connected
```

To verify the CA Interface configuration in the case of session based scrambling, use the **show cable video encryption dvb ca-interface brief** command as shown in the example below:

```
Router# show cable video encryption dvb ca-interface brief
CA Interface configuration

------------------------------
Linecard    IP Address    VRF
------------------------------
7           10.10.1.1     N/A

ECMG Route configuration

-----------------------------------------------------
IP Address    NetMast         Interface
-----------------------------------------------------
10.10.1.10    255.255.255.224   TenGigabitEthernet4/1/2
```

To verify the encryption status of the sessions, use the **show cable video session logical-edge-device id** command as shown in the example below:

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

Session Output Streaming Session Session Source               UDP   Output  Input
Output Input   Output  Encrypt Encrypt   Low     Session
Id      Port   Type      Type    Ucast Dest IP/Mcast IP (S, G) Port  Program State
State  Bitrate Bitrate Type    Status    Latency Name
-------------------------------------------------------------------------------------------------------------
1048576 1      Remap     UDP     10.10.1.1                   49167 20      ACTIVE-PSI
   1695161 1689747 DVB     Encrypted N       dvbsess.1.0.1.0.23167
```

To verify the ECM PID and whether the CA Descriptor is added to the PMT, use the **show cable video session logical-edge-device id session-id** command as shown in the example below:

```
Router# show cable video session logical-edge-device id 1 session-id 1048576
Output PMT Info:
============================
  Program 20, Version 3, PCR 49, Info len 18,  (CA SYS-ID 4748, PID 79)
  PID 49: Type 2, Info len 0
  PID 50: Type 3, Info len 6, (lang eng)
```

Troubleshooting Tips

If some configuration errors occur, see the following troubleshooting tips:

- The Management IP must be unique and in the subnet of virtual port group.
- Ensure that the ECMG Server is pingable with source interface as the virtual port group from the Cisco cBR-8 console. This indicates that the ECMG Server is reachable and route is valid.
- Ensure that the TCP port number configured for the ECMG Server in the Cisco cBR-8 is the same as that of the ECMG Server listening port.
- Ensure that the management IP is pingable from the EIS Server. Otherwise, check the routing between the cBR-8 chassis and the EIS server.
- Ensure that the listening port that is configured for the EIS is used for establishing the connection from the EIS Server.
- Ensure that the Virtual Port Group interface is active.
- Ensure that the TenGigabitEthernet interface using which the management traffic reaches the Cisco cBR-8 and the interface through which the CA interface route is configured are active.

Configuration Examples

This section provides examples for the DVB configuration.

Example: Basic Session-based Scrambling Configuration

```
enable
config terminal
  interface VirtualPortGroup0
    vrf forwarding vrf_script_red_1
    ip address 10.10.1.1 255.255.255.224
```

```
    no mop enabled
    no mop sysid
    exit
  cable video
    mgmt-intf VirtualPortGroup 0
    encryption
      linecard 7/0 ca-system dvb scrambler dvb-csa
      dvb
        route-ecmg 10.20.1.1 255.255.255.224 TenGigabitEthernet4/1/2 10.20.1.1
        mgmt-ip 10.10.1.2
        eis eis-1 id 1
          listening-port 8890 bind led id 1
        ca-interface linecard 7/0 10.30.1.1
        ecmg ecmg-7 id 7
          mode vod linecard 7/0
          type standard
          ca-system-id 950 1234
          auto-channel-id
          ecm-pid-source sid
          connection id 1 priority 1 10.20.1.3 8888
    service-distribution-group sdg-1 id 1 onid 1
      rpd downstream-cable 7/0/1
    virtual-carrier-group vcg-1 id 1
      encrypt
      service-type narrowcast
      rf-channel 0 tsid 1 output-port-number 1
    bind-vcg
      vcg vcg-1 sdg sdg-1
    logical-edge-device led-1 id 1
      protocol table-based
      virtual-edge-input-ip 192.0.2.0 input-port-number 1
      vcg vcg-1
      active
    table-based
      vcg vcg-1
    rf-channel 0
    session dvb-1 input-port 1 start-udp-port 49152 processing-type
remap start-program 1 cbr
```

Example: Basic Tier-based Scrambling Configuration

```
enable
config terminal
  interface VirtualPortGroup0
    vrf forwarding vrf_script_red_1
    ip address 10.10.1.1 255.255.255.224
    no mop enabled
    no mop sysid
    exit
  cable video
    mgmt-intf VirtualPortGroup 0
    encryption
      linecard 7/0 ca-system dvb scrambler dvb-csa
      dvb
        route-ecmg 10.20.1.0 255.255.255.224 TenGigabitEthernet4/1/2 10.20.1.1
        ecmg ecmg-7 id 7
          mode tier-based
          type standard
          ca-system-id 950 1234
          auto-channel-id
          ecm-pid-source sid
          connection id 1 priority 1 10.20.1.3 8888
        tier-based
          ecmg id 7 access-criteria 1122334455
          fail-to-clear
          enable
    service-distribution-group sdg-1 id 1 onid 1
      rpd downstream-cable 7/0/1
    virtual-carrier-group vcg-1 id 1
```

```
      encrypt
      service-type narrowcast
      rf-channel 0 tsid 1 output-port-number 1
    bind-vcg
      vcg vcg-1 sdg sdg-1
    logical-edge-device led-1 id 1
      protocol table-based
        virtual-edge-input-ip 192.0.2.0 input-port-number 1
        vcg vcg-1
        active
    table-based
      vcg vcg-1
        rf-channel 0
         session dvb-1 input-port 1 start-udp-port 49152 processing-type remap start-program
 1 cbr
```

Example: Basic Session-based Dualcrypt Scrambling Configuration

```
enable
config terminal
  interface VirtualPortGroup0
    vrf forwarding vrf_script_red_1
    ip address 10.10.1.1 255.255.255.224
    no mop enabled
    no mop sysid
    exit
  cable video
    mgmt-intf VirtualPortGroup 0
    encryption
      linecard 7/0 ca-system dvb scrambler dvb-csa
      dvb
        route-ecmg 10.20.1.0 255.255.255.224 TenGigabitEthernet4/1/2 10.20.1.1
        mgmt-ip 10.10.1.2
        eis eis-1 id 1
          listening-port 8890 bind led id 1
        ca-interface linecard 7/0 10.30.1.1
        ecmg ecmg-7 id 7
          mode vod linecard 7/0
          type standard
          ca-system-id 950 1234
          auto-channel-id
          ecm-pid-source sid
          connection id 1 priority 1 10.20.1.3 8888
    service-distribution-group sdg-1 id 1 onid 1
      rpd downstream-cable 7/0/1
    virtual-carrier-group vcg-1 id 1
      encrypt
      service-type narrowcast
      rf-channel 0 tsid 1 output-port-number 1
    bind-vcg
      vcg vcg-1 sdg sdg-1
    logical-edge-device led-1 id 1
      protocol gqi
        mgmt-ip 10.10.1.3
        mac-address xxxx.yyyy.zzzz
        server 10.20.1.2
        keepalive retry 3 interval 10
        reset interval 8
        virtual-edge-input-ip 192.0.2.0 input-port-number 1
        vcg vcg-1
        active
```

Additional References

Related Documents

Related Topic	Document Title
Configuring Tier-Based Scrambling	*Cisco RF Gateway 10 Software Configuration Guide*

Technical Assistance

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

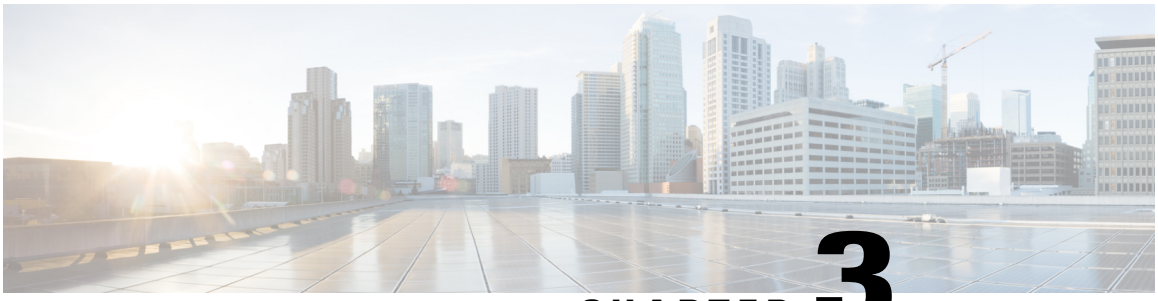
Feature Information for RPHY DVB VoD Suppot

Use Cisco Feature Navigator to find information about 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 http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note The table below 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.

Table 4: Feature Information for RPHY DVB VoD Suppot

Feature Name	Releases	Feature Information
RPHY DVB VoD Support	Cisco 1x2 / Compact Shelf RPD Software 3.1	This feature was introduced on the Cisco Remote PHY Device.



CHAPTER 3

Cisco Remote PHY 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 line card in R-PHY mode on Cisco cBR-8, specifically for each request.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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

- Hardware Compatibility Matrix for Cisco Remote PHY Device, page 19
- Information About PowerKEY VOD, page 20
- How to Configure RPHY PowerKey VOD, page 21
- Configuration Examples, page 25
- Feature Information for Rmote PHY PowerKEY VoD, page 25

Hardware Compatibility Matrix for Cisco Remote PHY Device

Note The hardware components introduced in a given Cisco Remote PHY Device Software Release are supported in all subsequent releases unless otherwise specified.

Table 5: Hardware Compatibility Matrix for the Cisco Remote PHY Device

Cisco HFC Platform	Remote PHY Device
Cisco GS7000 Node	**Cisco 1x2 RPD Software 1.1 and Later Releases** Cisco Remote PHY Device 1x2 • PID—RPD-1X2= • PID—RPD-1X2-PKEY=

Note The -PKEY suffix in the PID indicates units that enable the SCTE-55-2 Out-of-Band protocol support.

Information About PowerKEY VOD

The line cards in R-PHY mode on Cisco cBR-8 supports session-based PowerKey VOD. In both RPHY and integrated modes, the Cisco cBR-8 router establishes a GQI Remote Procedure Call (RPC) connection to the Edge Resource Manager (SRM), which may be an Explorer Controller (EC), USRM, or any other session manager. The Cisco cBR-8 supports 40G-R line cards, which can be configured for RPHY.

Configure the PowerKey VOD carriers in a GQI protocol LED. The Virtual Carrier Groups (VCG) in the LED, must be bound to a Service Distribution Group (SDG) with downstream-cable ports (instead of the integrated-cable ports).

Overview of PowerKEY VoD

PowerKEY VOD allows the operator to provide secure, encrypted video streams to a particular subscriber over the RF plant. PowerKEY video-on-demand is used in a Cisco cable environment to provide edge-encrypted video-on-demand movies and other content to subscribers. A subscriber can select the content through 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 intended for the RF carrier into a Multi-Program Transport Stream (MPTS), encapsulates it using R-DEPI protocol, and sends it out on Ethernet port to the Converged Interconnect Network (CIN) between the cBR-8 RPHY core and the RPHY Device (RPD).

How to Configure RPHY PowerKey VOD

Note To know more about the commands referenced in this section, see the Cisco IOS Master Command List.

Configuring the Encryption Type on the Line Card

The Cisco IOS-XE supports PowerKey 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 [powerkey] scrambler scrambler-type
exit
```

PowerKey currently supports DES type of encryption.

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 following example:

```
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
encrypt
rf-channel channel range tsid tsid range output-port-number port num range
exit
```

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 channels.

The following example shows how to configure the SDGs and binding:

```
configure terminal cable video
  mgmt-intf VirtualPortGroup 0

service-distribution-group sdg1 id 1
    rpd downstream-cable 7/0/0
virtual-carrier-group vcg1 id 1
    service-type narrowcast
    encrypt
    rf-channel 0-10 tsid 1-11 output-port-number 1-11

bind-vcg
    vcg vcg1 sdg sdg1
```

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.

Note 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:

```
cable video
logical-edge-device led1 id 1
    protocol gqi
      mgmt-ip management ip address
      mac-address mac address from this chassis range
      server ip address of srm
      keepalive retry 3 interval 10
      reset interval 8
      virtual-edge-input-ip ip addr for content input-port-number num
      vcg virtual edge qam name (may be multiple vcgs in an LED)
      active
```

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 the 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
  ```

  After 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 "-".

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 6/0 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 RPC_VCG
encrypt
rf-channel 20-47 tsid 20-47 output-port-number 20-47
virtual-edge-input-ip 174.102.1.1 input-port-number 1
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
  mgmt-intf VirtualPortGroup 0

service-distribution-group sdg1 id 1
    rpd downstream-cable 7/0/0
virtual-carrier-group vcg1 id 1
    service-type narrowcast
    encrypt
    rf-channel 0-10 tsid 1-11 output-port-number 1-11

bind-vcg
    vcg vcg1 sdg sdg1
logical-edge-device led1 id 1
    protocol gqi
      mgmt-ip 1.22.2.10
      mac-address c414.3c17.e001
      server 1.200.1.189
      keepalive retry 3 interval 10
      reset interval 8
      virtual-edge-input-ip 174.102.1.1 input-port-number 1
      vcg vcg2
      active
```

Feature Information for Rmote PHY PowerKEY VoD

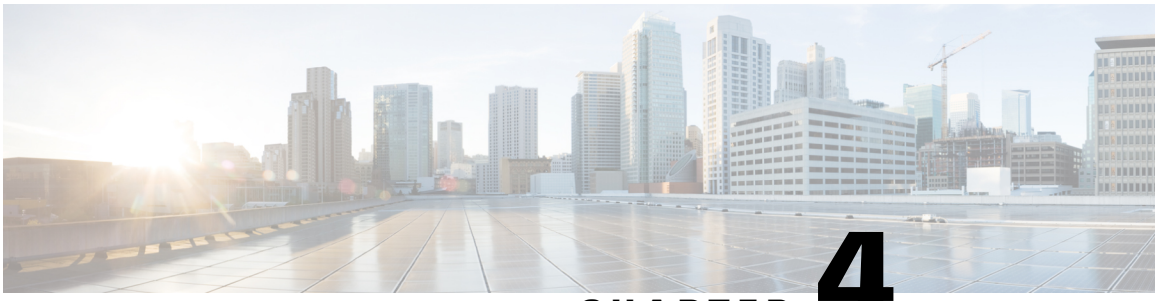
Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release,

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

Note The table below 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.

Table 6: Feature Information for RPHY PowerKEY VoD

Feature Name	Releases	Feature Information
Remote PHY PowerKEY VoD	Cisco 1x2 / Compact Shelf RPD Software 3.1	This feature was integrated into Cisco Remonte PHY Device.



CHAPTER 4

Cisco Remote PHY Pre-encrypted Broadcast Video

This document describes how to configure pre-encrypted Broadcast Video sessions on Cisco cBR-8 routers.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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

- Hardware Compatibility Matrix for Cisco Remote PHY Device, page 27
- Information About Pre-encrypted Broadcast Video, page 28
- How to Configure Pre-encrypted Broadcast Video Sessions, page 29
- Configuration Example for Pre-encrypted Broadcast Video Session, page 30
- Feature Information for RPHY Pre-encrypted Broadcast Video, page 30

Hardware Compatibility Matrix for Cisco Remote PHY Device

Note The hardware components introduced in a given Cisco Remote PHY Device Software Release are supported in all subsequent releases unless otherwise specified.

Table 7: Hardware Compatibility Matrix for the Cisco Remote PHY Device

Cisco HFC Platform	Remote PHY Device
Cisco GS7000 Node	**Cisco 1x2 RPD Software 1.1 and Later Releases** Cisco Remote PHY Device 1x2 • PID—RPD-1X2= • PID—RPD-1X2-PKEY=

Note The -PKEY suffix in the PID indicates units that enable the SCTE-55-2 Out-of-Band protocol support.

Information About Pre-encrypted Broadcast Video

The Cisco cBR-8 line card supports broadcast video. It also provides support to the WAN ports for receiving Multi program Transport Streams (MPTS). The Cisco cBR passes the MPTS streams in its entirety to multiple RPDs in the network to provide an output on their RF ports.

The content is multiplexed and encrypted during upstream traffic and reaches Cisco cBR-8 router as pre-encrypted in a constant bit-rate MPTS with all the PSI present. The Cisco cBR routers perform the following:

- De-jittering
- Clock recovery
- PCR re-stamping
- Regenerates PAT with correct TSID

Typically, multi-system operators (MSO) have between 64 and 75 carriers of Broadcast video content in their system. In the RPHY environment, the Cisco cBR routers convert the Broadcast carriers into DEPI multicast streams and send them to an unlimited number of RPDs over the Converged Interconnect Network.

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. To configure multicast video session, you must configure a port-channel interface.

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.

MPTS Pass-through Session

The Cisco cBR-8 router supports multicast MPTS pass-session type. For a pass-through session:

- 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 Pre-encrypted Broadcast Video Sessions

Note To know more about the commands referenced in this section, see the Cisco IOS Master Command List.

This section contains the following:

Configure a Port-Channel Interface

The following example shows how to configure a port-channel interface.

```
interface Port-channel27
description connection for Core A
ip address 2.27.1.1 255.255.255.252
ip pim sparse-mode
ip access-group 101 out
ip igmp version 3
ip ospf 64512 area 27
load-interval 30
carrier-delay msec 500
```

Configuring Pre-encrypted Broadcast Sessions

The following example shows how to configure the pre-encrypted Broadcast Video sessions on Cisco cBR routers.

```
cable video
multicast-uplink Port-channel32 access-list all-multicasts

table-based
   multicast-label label group group-ip source source-ip source2 source-ip source3 source-ip
 source4 source-ip
   multicast-label label group group-ip source source-ip source2 source-ip source3 source-ip
 source4 source-ip

    vcg vcg-name
  rf-channel channel
    session session-name multicast-label label processing-type {remap | passthru | data}
```

```
cbr
  rf-channel channel
    session session-name multicast-label label processing-type {remap | passthru | data}
cbr
```

Configuring the Service Distribution Groups and Binding

The Service Distribution Group (SDG) 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 channels.

The following example shows how to configure the SDGs and binding:

```
configure terminal
cable video
service-distribution-group sdg99 id 99
    rpd downstream-cable 9/0/31

  virtual-carrier-group vcg99 id 99
    service-type broadcast
    rf-channel 64-78 tsid 38901-38915 output-port-number 1-15
    rf-channel 80-127 tsid 38917-38964 output-port-number 17-64

  bind-vcg
    vcg vcg99 sdg sdg99

logical-edge-device led31 id 31
protocol table-based
vcg vcg99
active
```

Configuration Example for Pre-encrypted Broadcast Video Session

The following example shows an example of configuring pre-encrypted Broadcast Video sessions on Cisco cBR routers.

```
cable video
table-based
   multicast-label mpts1 group 236.0.1.1 source 175.10.5.2 source2 175.10.6.2 source3
175.10.7.2 source4 175.10.8.2
   multicast-label mpts2 group 236.0.1.2 source 175.10.5.2 source2 175.10.6.2 source3
175.10.7.2 source4 175.10.8.2
   vcg vcg99
  rf-channel 64
    session mpts1 multicast-label mpts1 processing-type passthru cbr
  rf-channel 65
    session mpts2 multicast-label mpts2 processing-type passthru cbr
```

Feature Information for RPHY Pre-encrypted Broadcast Video

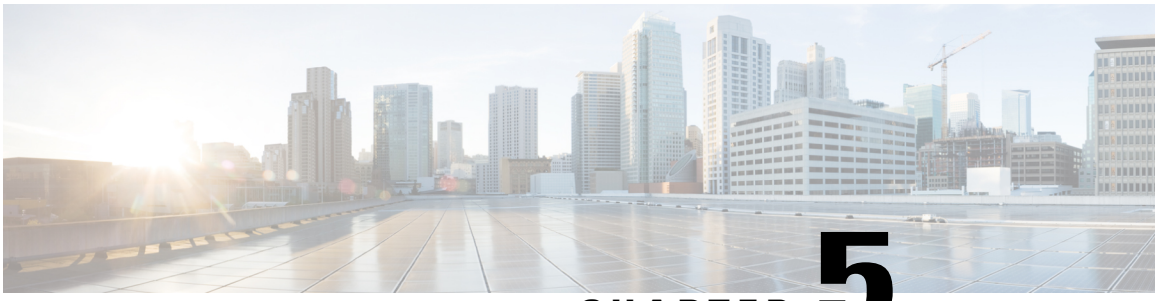
Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release,

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

Note The table below 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.

Table 8: Feature Information for RPHY Pre-encrypted Broadcast Video

Feature Name	Releases	Feature Information
RPHY Pre-encrypted Broadcast Video	Cisco 1x2 / Compact Shelf RPD Software 3.1	This feature was integrated into Cisco Remote PHY Device.



CHAPTER 5

Remote PHY BFS QAM Configuration

This document provides information on how to configure Cisco cBR-8 as a Broadcast File System (BFS) Quadrature Amplitude Modulation (QAM), which interfaces with Explorer Controller (EC) versions 7.x and 8.x.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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

- Hardware Compatibility Matrix for Cisco Remote PHY Device, page 33
- Information About BFS QAM Support, page 34
- How to Configure BFS QAM for EC 7.x, page 34
- How to Configure BFS QAM for RPD, page 37
- How to Configure BFS QAM for EC 8.x, page 38
- Configuration Example for BFS QAM Configuration, page 40
- Feature Information for BFS QAM Configuration, page 43

Hardware Compatibility Matrix for Cisco Remote PHY Device

Note The hardware components introduced in a given Cisco Remote PHY Device Software Release are supported in all subsequent releases unless otherwise specified.

Table 9: Hardware Compatibility Matrix for the Cisco Remote PHY Device

Cisco HFC Platform	Remote PHY Device
Cisco GS7000 Node	**Cisco 1x2 RPD Software 1.1 and Later Releases** Cisco Remote PHY Device 1x2 • PID—RPD-1X2= • PID—RPD-1X2-PKEY=

Note The -PKEY suffix in the PID indicates units that enable the SCTE-55-2 Out-of-Band protocol support.

Information About BFS QAM Support

The BFS provides a mechanism for a standardized downloading of applications, games, images, and other data formats required by the applications. The BFS QAM enables the router to transfer the broadcast data from an EC to the target platform such as a set-top unit. All forms of BFS data from EC flows as IP multicast, except the CVT carousel, which is through the GQI insert packets.

The BFS QAM configuration on the Cisco cBR-8 router varies based on the version of EC, which interfaces with the router.

- For EC 7.x-Model a GQI-based LED as BFS QAM. One for each LC on Cisco cBR-8.

  For Remote PHY-A single GQI-based LED as BFS QAM for the entire Cisco cBR-8 chassis, as the Cisco cBR-8 can support DEPI multicast for all Remote PHY devices (RPD).

  For EC 8.x-EC 8.x multicasts CVT carousel data in addition to GQI insert packets, but only in the presence of GQAM configured as BFS QAM. Hence, in this setup, a single table-based LED, modeled as BFS QAM, for each Cisco cBR-8 chassis is sufficient. Using cross LC replication, this BFS data can be replicated to other LCs on the Cisco cBR.

How to Configure BFS QAM for EC 7.x

This configuration applies to Cisco cBR-8 routers running Converged Cable Access Platform (CCAP) with Ethernet input and RF output.

If Cisco cBR-8 interacts with EC 7.x, configure an LED on each line card. Use the following procedure to configure BFS QAM on Cisco cBR router.

- Configure an LED with GQI protocol on each line card.
- On EC 7.x, provision BFS QAM.
- Manually create sessions on EC 7.x.
- Generate the QAM, based on GQI model.

- Generate a new source definition and use the new QAM as a target using the same PIDs.
- Ensure that everything is set up on the EC to match the Cisco cBR-8 LED configuration.

Note To know more about the commands referenced in this section, see the Cisco IOS Master Command List.

This section contains the following:

Mapping Cisco cBR-8 as a GQI QAM

On the EC 7.x, configure BFS sessions on the registered BFS QAM by using one of the following:

- Proprietary Remote Procedure Call (RPC) (with GQAM)
- GQI (with RFGW-1)

You can use a standard GQI model where the sessions will be generated on the individual line card on a single LED per line card basis. Individual BFS sessions are added to the LEDs at the Source Definition for all in-band BFS sources. Sessions must be unique in numbering and QAM selection, although all other settings must be duplicates of the original settings.

Creating VCG with One QAM Channel

The following example shows how to create a video virtual carrier group (VCG) with one QAM channel, which can carry the BFS data.

```
enable
configure terminal
cable video

virtual-carrier-group (name) id (id)
    service-type broadcast
    rf-channel (rf-channel number 1) tsid (id) output-port-number (port number 1)
  virtual-carrier-group (name 2) id (id 2)
    service-type broadcast
    rf-channel (rf-channel number 1) tsid (id 2) output-port-number (port number 1)
```

Creating SDG for BFS Sessions on Cisco cBR

The following example shows how to create Service Distribution Group (SDG) for BFS sessions and map this to as many RF ports as required.

```
enable
configure terminal
cable video

service-distribution-group sdg_bdcast id 20
    rf-port integrated-cable 8/0/0
    rf-port integrated-cable 8/0/1
    rf-port integrated-cable 8/0/2
    rf-port integrated-cable 8/0/3
    rf-port integrated-cable 8/0/4
    rf-port integrated-cable 8/0/5
    rf-port integrated-cable 8/0/6
    rf-port integrated-cable 8/0/7
```

```
  service-distribution-group sdg_bdcast-9 id 21
    rf-port integrated-cable 9/0/0
    rf-port integrated-cable 9/0/1
    rf-port integrated-cable 9/0/2
    rf-port integrated-cable 9/0/3
    rf-port integrated-cable 9/0/4
    rf-port integrated-cable 9/0/5
    rf-port integrated-cable 9/0/6
    rf-port integrated-cable 9/0/7
```

Create VCG for BFS

The following example shows how to create VCG for BFS.

```
configure terminal
cable video

virtual-carrier-group vcg_bdcast id 20
    service-type broadcast
    rf-channel 76 tsid 1011 output-port-number 1
  virtual-carrier-group vcg_bdcast-9 id 21
    service-type broadcast
    rf-channel 76 tsid 1012 output-port-number 1



vcg vcg_bdcast sdg sdg_bdcast
    vcg vcg_bdcast-9 sdg sdg_bdcast-9

bind-vcg
    vcg vcg_bdcast sdg sdg_bdcast
    vcg vcg_bdcast-9 sdg sdg_bdcast-9
```

Creating Logical Edge Device

The following example shows how to create an LED.

Note Ensure that the LED settings are the same as GQI QAM settings on the EC. For more details, see Creating GQI QAM for BFS on EC 7.x

```
enable
configure terminal
cable video

logical-edge-device led_BFS id 20
    protocol gqi
      mgmt-ip 192.0.2.1
      mac-address <MAC address>
      server 198.51.100.1
      keepalive retry 3 interval 10
      reset interval 8
      virtual-edge-input-ip 203.0.113.1 input-port-number 1
      vcg vcg_bdcast
      active
  logical-edge-device led_BFS-9 id 21
    protocol gqi
      mgmt-ip 192.0.2.1
      mac-address <MAC address>
      server 198.51.100.1
      keepalive retry 3 interval 10
```

```
reset interval 8
virtual-edge-input-ip 203.0.113.1 input-port-number 1
vcg vcg_bdcast-9
active
```

Creating GQI QAM for BFS on EC 7.x

Prerequisites

- To create the GQI QAM on the EC, enable packet insertion in the QAM Model.
- You can duplicate the standard RFGW model to ensure that no interference occurs with the current operations.
- The router must have a GQI QAM per LED.
- The individual QAM must be BFS-capable.

Procedure

Use the following procedure to create GQI QAM for BFS.

1. Choose EC > GQI Based QAM Model List > Edit GQI Based QAM.
2. (Optional) Select the BFS Capable checkbox.
3. Choose RF Carriers from the left pane.
4. Ensure that the Carriers and Ethernet Port values are the same as those on the LEDs.

You can create the sessions for each BFS source by generating a Multicast Through GQI Based QAM session through each BFS source's Source Definition.

How to Configure BFS QAM for RPD

This configuration applies to Cisco cBR-8 routers running CCAP with Ethernet input and Ethernet output.

The configuration procedure for RPD is similar to the configuration on Cisco cBR-8 routers with EC 7.x. However, only one LED is needed for BFS QAM configuration.

You can use the sessions configured on the LED on every RPD by defining an Auxiliary Core on each RPD as needed for BFS distribution.

Creating SDG for BFS Sessions for RPD

The following example shows how to create SDG for BFS sessions on RPDs.

```
service-distribution-group sdg_bdcast id 20
    rpd downstream-cable 2/0/30

virtual-carrier-group vcg_bdcast id 20
    service-type broadcast
    rf-channel 79 tsid 1013 output-port-number 1
```

Creating LED for RPD

The following example shows how to create an LED.

```
logical-edge-device led_BFS id 20
    protocol gqi
      mgmt-ip 192.0.2.1
      mac-address <MAC address>
      server 198.51.100.1
      keepalive retry 3 interval 10
      reset interval 8
      virtual-edge-input-ip 203.0.113.1 input-port-number 1
      vcg vcg_bdcast
```

Defining Cable RPD

The RPD definition must include the RPD defined in the BFS SDG for every RPD to which you want to distribute BFS data: The following example shows how to define RPD.

```
cable rpd RPD07
 identifier xxxx.xxxx.xxxx
  core-interface Te2/1/4
  principal
  rpd-ds 0 downstream-cable 2/0/16 profile 11
  rpd-us 0 upstream-cable 2/0/12 profile 1
 core-interface Te2/1/6
  rpd-ds 0 downstream-cable 2/0/30 profile 10
 r-dti 3
 rpd-event profile 0
!
cable rpd RPD08
 identifier xxxx.xxxx.xxxx
 core-interface Te2/1/4
  principal
  rpd-ds 0 downstream-cable 2/0/17 profile 11
  rpd-us 0 upstream-cable 2/0/14 profile 1
 core-interface Te2/1/6
  rpd-ds 0 downstream-cable 2/0/30 profile 10
 r-dti 3
 rpd-event profile 0
```

For information on how to create GQI QAM on the EC, see Creating GQI QAM for BFS.

How to Configure BFS QAM for EC 8.x

When Cisco cBR-8 interfaces with EC 8.x, all sessions on the router are configured as multicast and perform a multicast join.

The Cisco cBR routers are not directly mapped on the EC. Hence, this BFS QAM configuration requests and processes the multicast BFS sessions that are setup on the actual BFS QAM. If the Cisco cBR-8 routers have to process these sessions, you must set up table-based multicast sessions, which are similar to the ones available on the BFS QAM.

Configure QAM replication group (QRG), spanning across line cards (LC) to replicate these BFS sessions on every RF port (if each RF port is a service group) of every LC.

To replicate across line cards, you must configure table-based sessions. You can perform cross-line-card-replication only through table-based sessions.

Use the following procedure to configure BFS QAM on Cisco cBR router for EC 8.x.

1. Create a VCG with one QAM channel for carrying this BFS data.
2. Within the same VCG, allocate a few more QAM channels for MPTS pass-through sessions.
3. Create VCG for VoD QAM channels.
4. Create VCG for SDV QAM channels.

Creating VCG for VoD QAM Channels

The following example shows how to create VCG for VoD QAM channels.

```
enable
configure terminal
cable video

virtual-carrier-group vcg_VoD
service-type narrowcast
rf-channel 1-32 tsid 2-33 output-port 2-33
```

Creating VCG for SDV QAM Channels

The following example shows how to create VCG for SDV QAM channels.

```
enable
configure terminal
cable video

virtual-carrier-group vcg_SDV
service-type narrowcast
rf-channel 33-48 tsid 34-49 output-port 34-49
```

Creating SDG

The following procedures are applicable when you create an SDG.

1. Create SDG for broadcast sessions and map this to as many RF ports as required, depending on the Service Groups which need this broadcast data.
2. Create separate SDG for VoD.
3. Create separate SDG for SDV, which probably contains replication.

```
enable
configure terminal
cable video

service-distribution-group sdg_bdcast
  rf-port integrated-cable 1/0/0
  rf-port integrated-cable 1/0/1
  rf-port integrated-cable 2/0/0
  rf-port integrated-cable 2/0/1
  rf-port integrated-cable 3/0/0
  rf-port integrated-cable 3/0/1

service-distribution-group sdg_VoD
  rf-port integrated-cable 1/0/0
```

```
service-distribution-group sdg_SDV
  rf-port integrated-cable 1/0/0
  rf-port integrated-cable 1/0/1

bind-vcg
  vcg vcg_BFS sdg sdg_BFS
  vcg vcg_VoD1 sdg sdg_VoD
  vcg vcg_SDV sdg sdg_SDV
```

Creating LEDs

The following procedures are applicable for creating LEDs.

1. Create a table based LED for broadcast carrying BFS and MPTS pass-through sessions.
2. Create separate LEDs for VoD and SDV.

```
logical-edge-device led_BFS id 1
    protocol table-based
      virtual-edge-input-ip 203.0.113.1 input-port-number 1
      vcg vcg_bdcast
      active
  table-based
    vcg vcg_bdcast
      rf-channel 0
        session BFS group 203.0.113.4 start-udp-port 49152 num-sessions-per-qam 1
processing-type remap start-program 20 bit-rate 300000 jitter 100 vbr
      rf-channel 48 session MPTS_passthru group 203.0.113.5 start-udp-port 49152
num-sessions-per-qam 1 processing-type passthru jitter 100 vbr
      rf-channel 49 session MPTS_passthru group 203.0.113.6 start-udp-port 49152
num-sessions-per-qam 1 processing-type passthru jitter 100 vbr

logical-edge-device led_VoD id 2
    protocol gqi
      virtual-edge-input-ip 203.0.113.1 input-port-number 1
      vcg vcg_VoD
      active
```

Configuration Example for BFS QAM Configuration

This section provides examples for BFS QAM support.

Example: BFS QAM Configuration on Cisco cBR for EC 7.x

The following example shows the BFS QAM configuration for EC 7.x.

```
virtual-carrier-group vcg_bdcast id 20
    service-type broadcast
    rf-channel 76 tsid 1011 output-port-number 1
  virtual-carrier-group vcg_bdcast-9 id 21
    service-type broadcast
    rf-channel 76 tsid 1012 output-port-number 1

service-distribution-group sdg_bdcast id 20
    rf-port integrated-cable 8/0/0
    rf-port integrated-cable 8/0/1
    rf-port integrated-cable 8/0/2
```

```
    rf-port integrated-cable 8/0/3
    rf-port integrated-cable 8/0/4
    rf-port integrated-cable 8/0/5
    rf-port integrated-cable 8/0/6
    rf-port integrated-cable 8/0/7
  service-distribution-group sdg_bdcast-9 id 21
    rf-port integrated-cable 9/0/0
    rf-port integrated-cable 9/0/1
    rf-port integrated-cable 9/0/2
    rf-port integrated-cable 9/0/3
    rf-port integrated-cable 9/0/4
    rf-port integrated-cable 9/0/5
    rf-port integrated-cable 9/0/6
    rf-port integrated-cable 9/0/7

virtual-carrier-group vcg_bdcast id 20
    service-type broadcast
    rf-channel 76 tsid 1011 output-port-number 1
  virtual-carrier-group vcg_bdcast-9 id 21
    service-type broadcast
    rf-channel 76 tsid 1012 output-port-number 1

vcg vcg_bdcast sdg sdg_bdcast
    vcg vcg_bdcast-9 sdg sdg_bdcast-9

bind-vcg
    vcg vcg_bdcast sdg sdg_bdcast
    vcg vcg_bdcast-9 sdg sdg_bdcast-9

logical-edge-device led_BFS id 20
    protocol gqi
      mgmt-ip 192.0.2.1
      mac-address <MAC address>
      server 198.51.100.1
      keepalive retry 3 interval 10
      reset interval 8
      virtual-edge-input-ip 203.0.113.1 input-port-number 1
      vcg vcg_bdcast
      active
  logical-edge-device led_BFS-9 id 21
    protocol gqi
      mgmt-ip 192.0.2.1
      mac-address <MAC address>
      server 198.51.100.1
      keepalive retry 3 interval 10
      reset interval 8
      virtual-edge-input-ip 203.0.113.1 input-port-number 1
      vcg vcg_bdcast-9
      active
```

Example: BFS QAM Configuration on RPD

The following example shows the BFS QAM configuration on RPD.

```
service-distribution-group sdg_bdcast id 20
    rpd downstream-cable 2/0/30

virtual-carrier-group vcg_bdcast id 20
    service-type broadcast
    rf-channel 79 tsid 1013 output-port-number 1

logical-edge-device led_BFS id 20
    protocol gqi
      mgmt-ip 192.0.2.1
      mac-address <MAC address>
      server 198.51.100.1
      keepalive retry 3 interval 10
      reset interval 8
      virtual-edge-input-ip 203.0.113.1 input-port-number 1
```

```
      vcg vcg_bdcast
cable rpd RPD07
 identifier xxxx.xxxx.xxxx
 core-interface Te2/1/4
  principal
  rpd-ds 0 downstream-cable 2/0/16 profile 11
  rpd-us 0 upstream-cable 2/0/12 profile 1
 core-interface Te2/1/6
  rpd-ds 0 downstream-cable 2/0/30 profile 10
 r-dti 3
 rpd-event profile 0
!
cable rpd RPD08
 identifier xxxx.xxxx.xxxx
 core-interface Te2/1/4
  principal
  rpd-ds 0 downstream-cable 2/0/17 profile 11
  rpd-us 0 upstream-cable 2/0/14 profile 1
 core-interface Te2/1/6
  rpd-ds 0 downstream-cable 2/0/30 profile 10
 r-dti 3
 rpd-event profile 0
```

Example: BFS QAM Configuration on Cisco cBR for EC 8.x

The following example shows the BFS QAM configuration for EC 8.x.

```
virtual-carrier-group vcg_bdcast
service-type broadcast
rf-channel 0 tsid 1 out 1
rf-channel 49-63 tsid 50-64 output-port 50-64

virtual-carrier-group vcg_VoD
service-type narrowcast
rf-channel 1-32 tsid 2-33 output-port 2-33

virtual-carrier-group vcg_SDV
service-type narrowcast
rf-channel 33-48 tsid 34-49 output-port 34-49


service-distribution-group sdg_bdcast
rf-port integrated-cable 1/0/0
rf-port integrated-cable 1/0/1
rf-port integrated-cable 2/0/0
rf-port integrated-cable 2/0/1
rf-port integrated-cable 3/0/0
rf-port integrated-cable 3/0/1

service-distribution-group sdg_VoD
rf-port integrated-cable 1/0/0

service-distribution-group sdg_SDV
rf-port integrated-cable 1/0/0
rf-port integrated-cable 1/0/1

bind-vcg
vcg vcg_BFS sdg sdg_BFS
vcg vcg_VoD1 sdg sdg_VoD
vcg vcg_SDV sdg sdg_SDV

logical-edge-device led_BFS id 1
    protocol table-based
      virtual-edge-input-ip 203.0.113.1 input-port-number 1
      vcg vcg_bdcast
      active
  table-based
    vcg vcg_bdcast
```

```
      rf-channel 0
        session BFS group 203.0.113.4 start-udp-port 49152 num-sessions-per-qam 1
processing-type remap start-program 20 bit-rate 300000 jitter 100 vbr
      rf-channel 48
        session MPTS_passthru group 203.0.113.5 start-udp-port 49152 num-sessions-per-qam
1 processing-type passthru jitter 100 vbr
       rf-channel 49
        session MPTS_passthru group 203.0.113.6 start-udp-port 49152 num-sessions-per-qam
1 processing-type passthru jitter 100 vbr

logical-edge-device led_VoD id 2
    protocol gqi
      virtual-edge-input-ip 203.0.113.1 input-port-number 1
      vcg vcg_VoD
      active
```

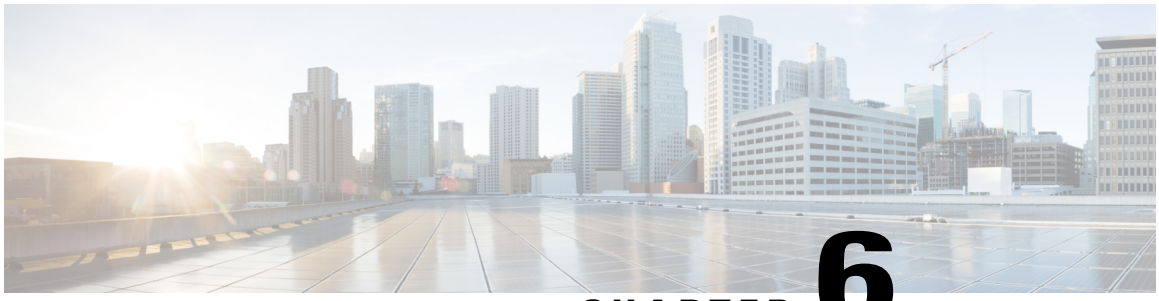
Feature Information for BFS QAM Configuration

Use Cisco Feature Navigator to find information about 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 http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note The table below 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.

Table 10: Feature Information for BFS QAM Configuration

Feature Name	Releases	Feature Information
BFS QAM Configuration	Cisco 1x2 / Compact Shelf RPD Software 3.1	This feature was integrated into Cisco Remote PHY Device.



CHAPTER 6

Remote PHY Switched Digital Video

This document provides information on how to configure Switched Digital Video for Cisco Remote PHY Device.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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

- Switched Digital Video Services, page 45
- Information About Switched Digital Video, page 48
- How to Configure the Switched Digital Video Services, page 49
- Configuration Examples for Switched Digital Video, page 52
- Feature Information for Switched Digital Video, page 55

Switched Digital Video Services

The Switched Digital Video (SDV) services are supported for the MPEG video subsystem on the Cisco Remote PHY Device. It consists of Multicast IP Packet based video streams that are managed as "Video Sessions".The Cisco Remote PHY Device 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.

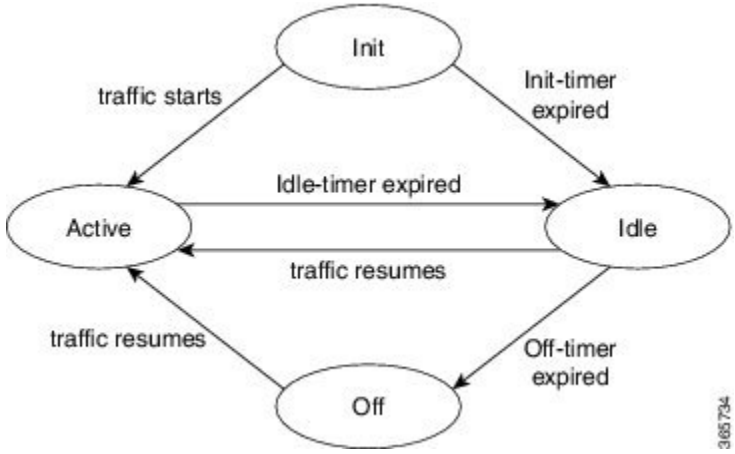
This ensures that all sessions switch to the same source IP address when a source switch occurs. Additionally, sessions configured via GQI have up to three sources available for redundancy, whereas multicast labels configured for table-based sessions have up to four sources available for redundancy.

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 Remote PHY Device 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 Remote PHY Device supports up to four multicast address pairs per multicast session for backup purpose. To specify additional sources for a multicast session for table-based, a label needs to be configured and attached to the session configuration. A maximum of 2000 multicast labels can be created but only 2048 multicast addresses can be active at a time.

Multicast label is used for table-based session configuration when more than one multicast source [S, G] is used as backup for the sessions. A mullticast label can only be created or deleted; it cannot be modified. The multicast label cannot be deleted before the sessions using it are removed.

Groups used by multicast labels must be unique like the multicast S/G pairs. However, sources may be used by more than one label as long as the group is unique. A maximum of 4 multicast sources is allowed in one label. If the label is used in multiple sessions, the sessions are considered as cloned sessions.

enable
configure terminal
cable video
table-based
multicast-label *label* **group** *group-ip* **source** *source-ip* **source2** *source-ip* **source3** *source-ip* **source4** *source-ip*

Configuring Multicast Table-based Sessions

Similar to table-based unicast session configuration, sessions can be configured as individual sessions under each QAM carrier that is assigned to a table-based LED.

A multicast session can be configured with a single input multicast input source or multiple input sources for backup purpose. For multiple backup sources, a label is required to be associated with the session configuration.

Same label can be applied to multiple sessions on different QAM channel. These sessions are considered as cloned sessions.

For session cloning on multiple QAMs within the same line card, only one copy of the traffic is forwarded to the line card. The line card replicates the input packets and forwards them to multiple QAMs. Each cloned copy of a remapped session will have the same or different output program number.

enable
configure terminal
cable video
table-based
vcg *vcg-name*
rf-channel *channel*
session *session-name* **group** *group-ip* **source** *source-ip* **processing-type** {**remap** | **passthru** | **data**} **start-program** *program-num* [**bit-rate** *bit-rate-number*] [**jitter** *jitter-number*] [**cbr** | **vbr**]

Configuring Source Switching

Source switching happens automatically when the current source goes down. If more than one source IP is configured, the software will automatically switch to the next valid source IP, if it is available. However, to force switch from one valid source to another valid source, use the following commands:

`Router(config)#` **cable video source-switch from-group** *group-ip* **from-source** *source-ip*

or

`Router(config)#` **cable video source-switch to-group** *group-ip* **to-source** *source-ip*

Verifying Switched Digital Video Configuration

```
Router#show cable video session logical-edge-device id 2
Total Sessions = 4

Session    Output     Streaming   Session Session Source                 UDP   Output
Input      Output Input    Output   Encrypt  Encrypt        Session
Id         Port       Type        Type    Ucast Dest IP/Mcast IP (S,G)    Port  Program
State      State  Bitrate  Bitrate  Type     Status         Name
-------------------------------------------------------------------------------------
2097152    142        Remap       SSM     175.2.5.6,232.5.6.7            0     1       OFF
        ON     0        0        CLEAR    -              SESS_PME2.1.7.338
2097153    163        Remap       SSM     175.6.1.13,232.2.1.6           0     2
INIT       ON     0        0        CLEAR    -              SESS_PME3.1.7.497
2097154    184        Passthru    SSM     175.2.6.7,232.5.6.15           0     -       OFF
        ON     0        0        CLEAR    -              SESS_PME4.1.7.656
2097155    230        Data-Piping SSM     175.7.2.2,232.2.6.7            0     -       OFF
        ON     0        0        CLEAR    -              SESS_PME6.1.7.978

Router#show cable video session logical-edge-device id 2 session-id 2097152
Session Name        : SESS_PME2.1.7.338
Session Id:         : 2097152
Creation Time:      : Fri Jun 24 16:30:45 2016

Output Port         : 142
TSID                : 142
ONID                : 0
Number of Sources   : 1
  Source IP         : 175.2.5.6
  Group IP          : 232.5.6.7
  UDP Port          : 0
```

```
Config Bitrate      : not specified
Jitter              : 100 ms
Processing Type     : Remap
Stream Rate         : VBR
Program Number      : 1
Idle Timeout        : 2000 msec
Init Timeout        : 2000 msec
Off Timeout         : 60 sec
Encryption Type     : CLEAR
Encryption Status   : -

Input Session Stats:
====================
  State: OFF, Uptime: 0 days 00:26:35
  IP Packets: In 0, RTP 0, Drop 0
  TP Packets: In 0, PCR 0, PSI 0, Null 0
              Unreference 0, Discontinuity 0
  Errors: Sync loss 0, CC error 0, PCR Jump 0,
          Underflow 0, Overflow 0, Block 0
  Bitrate: Measured 0 bps, PCR 0 bps

Output Session Stats:
=====================
  State: ON, Uptime: 0 days 00:26:35
  TP Packets: In 0, PCR 0, PSI 0,
              Drop 0, Forward 0, Insert 0
  Errors: Info Overrun 0, Info Error 0, Block 0, Overdue 0,
          Invalid Rate 0, Underflow 0, Overflow 0
  Bitrate: Measured 0 bps
```

Troubleshooting Switched Digital Video Configuration

Problem	Possible Causes	Recommended Solution
%ERROR: Duplicate multicast source 175.2.5.6 group 232.5.6.7 not allowed for use in label groupDuplicate.	Group and Source are already used in an existing label.	Assign unique group and source IPs across multicast labels.
%ERROR: Duplicate multicast source 178.3.3.3 group 232.222.222.222 not allowed within label DuplicateSourceHere.	Source has been repeated within a label.	Assign unique source IP within a multicast label.
%ERROR: Duplicate multicast source 175.2.5.6 group 232.5.6.7 not allowed for use in this session.	Session has been created with a duplicate group IP. This group IP has been used in an existing multicast label.	Create the session with a unique group IP.
%ERROR Only one multicast session can be created per multicast session command; rf-channel range values, such as rf-channel 20-30, not allowed.	Session has been created on a range of RF channels.	RF channel range is not allowed. Create the session on an RF channel.

Configuration Examples for Switched Digital Video

Example 1: Table-based Multicast Session Configuration

```
enable
configure terminal
ip pim rp-address 9.1.1.1
ip pim ssm range all-multicasts
ip access-list standard all-multicasts
 permit 233.0.0.0 0.255.255.255
 permit 234.0.0.0 0.255.255.255
 permit 235.0.0.0 0.255.255.255
 permit 236.0.0.0 0.255.255.255
 permit 237.0.0.0 0.255.255.255
 permit 238.0.0.0 0.255.255.255
 permit 232.0.0.0 0.255.255.255
 permit 224.0.0.0 0.255.255.255
 permit 239.0.0.0 0.255.255.255
interface TenGigabitEthernet4/1/2
 ip address 2.33.1.1 255.255.255.252
 ip pim sparse-mode
 ip igmp version 3
 ip ospf 64512 area 9
 load-interval 30
cable video
  multicast-uplink TenGigabitEthernet4/1/2 access-list all-multicasts
  service-distribution-group sdg-1 id 1
    rf-port downstream-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 downstream-cable 7/0/0
    rf-port downstream-cable 7/0/1
    rf-port downstream-cable 7/0/2
    rf-port downstream-cable 7/0/3
    rf-port downstream-cable 7/0/4
```

```
    rf-port downstream-cable 7/0/5
    rf-port downstream-cable 7/0/6
    rf-port downstream-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 downstream-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 downstream-cable 7/0/0
```

```
    rf-port downstream-cable 7/0/1
    rf-port downstream-cable 8/0/0
    rf-port downstream-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
```

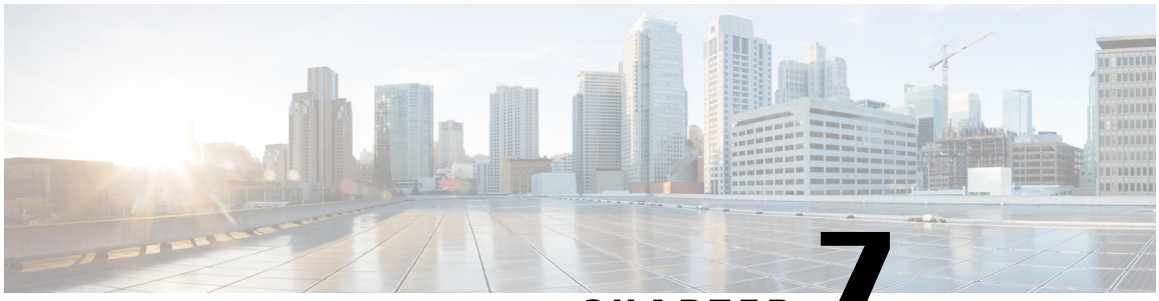
```
      rf-channel 22
        session SESS_PME2 multicast-label a2 processing-type remap start-program 1
    vcg VCG_PME3
      rf-channel 23
        session SESS_PME3 multicast-label exampleLabel processing-type remap start-program
2
    vcg VCG_PME4
      rf-channel 24
        session SESS_PME4 group 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 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 http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note The table below 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.

Feature Name	Releases	Feature Information
Switched Digital Video	Cisco 1x2 / Compact Shelf RPD Software 3.1	This feature was integrated into the Cisco Remote PHY Device.



CHAPTER 7

Remote PHY QAM Profile Configuration

This document describes how to configure the QAM profile on the Cisco cBR Series Converged Broadband Router.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

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

- Information About QAM Profile, page 57
- How to Configure Remote PHY QAM Profile, page 58
- Configuration Example, page 59
- Feature Information for QAM Profile Configuration, page 59

Information About QAM Profile

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

The QAM profile is described by CCAP DownPhyParams object. Default QAM profiles are supported and customized for DOCSIS or MPEG Video, which are described as DocsisPhyDefault and VideoPhyDefault objects, respectively.

A maximum of 32 QAM profiles can be defined. There are four system-defined QAM profiles (0 to 3), which cannot be deleted or modified. You can define profiles 4 to 31.

The system defined profiles are:

- Profile 0 - default-annex-b-64-qam
    - interleaver-depth: I32-J4

- symbol rate: 5057 kilo-symbol/second
- spectrum-inversion: off

- Profile 1 - default-annex-b-256-qam
  - interleaver-depth: I32-J4
  - symbol rate: 5361 kilo-symbol/second
  - spectrum-inversion: off

- Profile 2 - default-annex-a-64-qam
  - interleaver-depth: I12-J17
  - symbol rate: 6952 kilo-symbol/second
  - spectrum-inversion: off

Profile 3 - default-annex-a-256-qam
- interleaver-depth: I12-J17
- symbol rate: 6952 kilo-symbol/second
- spectrum-inversion: off

How to Configure Remote PHY QAM Profile

Note To know more about the commands referenced in this section, see the Cisco IOS Master Command List.

Configuring the QAM Profile on Downstream Channels

```
Enable
configure terminal
  cabledownstream qam-profile Qam_Profile_ID D

   annex {A | B | C}
   description LINE
   interleaver-depth {I12-J17 | I128-J1 | I128-J2 |
I128-J3 | I128-J4 | I128-J5 | I128-J6 | I128-J7 |
I128-J8 | I16-J8 | I32-J4 | I64-J2 | I8-J16}
  modulation {256 | 64}   spectrum-inversion {off | on}
  symbol-rate value
exit
```

You can configure symbol rate for Annex A video and Annex C video. The valid range for Annex A video is 3500 to 7000 kilo-symbols/sec. The valid range for Annex C video is 3500 to 5309 kilo-symbols/sec. The channel width in kHz is symbol-rate * (1 + alpha) with 0.15 alpha for Annex A and 0.13 alpha for Annex C.

Verifying QAM Profile on Downstream Channels

Use the following commands to verify the QAM Profile on Downstream Channels:

```
Router#show running-config | section downstream controller-profile
cable downstream controller-profile 0
 rf-chan 0 3
  type DOCSIS
  frequency 111000000
  rf-output NORMAL
  qam-profile 1
  docsis-channel-id 1
```

Configuration Example

QAM Profile Configuration

```
configure terminal
  cable downstream controller-profile 1
    multicast-pool 20
    Rf-channel 0 15
     Type docsis
     Frequency 111000000
     Rf-output NORMAL
     Qam-profile 1
     Docsis-channel-id 1
  cable downstream controller-profile 2
    multicast-pool 20
    Rf-channel 20 47
     Type video sync
     Frequency 231000000
     Rf-output NORMAL
     Qam-profile 14
```

Feature Information for QAM Profile Configuration

Use Cisco Feature Navigator to find information about 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 http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note The table below 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.

Table 11: Feature Information for QAM Profile Configuration

Feature Name	Releases	Feature Information
QAM Profile Configuration-RPHY Annex B	Cisco 1x2 / Compact Shelf RPD Software 1.1	This feature was introduced on the Cisco Remote PHY Device.
QAM Profile Configuration-RPHY Annex A and C	Cisco 1x2 / Compact Shelf RPD Software 3.1	This feature was introduced on the Cisco Remote PHY Device.