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 that are documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. The Feature Information Table at the end of this document provides information about the documented features and lists the releases in which each feature is supported.

- Hardware Compatibility Matrix for Cisco Remote PHY Device, on page 1
- Information About DVB VOD, on page 2
- How to Configure DVB, on page 4
- Configuration Examples, on page 8
- Additional References, on page 10
- Feature Information for RPHY DVB VoD Support, on page 11

Hardware Compatibility Matrix for Cisco Remote PHY Device

Note

Unless otherwise specified, the hardware components introduced in a given Cisco Remote PHY Device Software Release are supported in all subsequent releases.

Table 1: Hardware Compatibility Matrix for the Cisco 2x2 Remote PHY Device

<table>
<thead>
<tr>
<th>Cisco HFC Platform</th>
<th>Remote PHY Device</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco GS7000 BAU</td>
<td>Cisco 2x2 RPD Software 2.x and Later Releases</td>
</tr>
<tr>
<td></td>
<td>Cisco Remote PHY Device 2x2</td>
</tr>
<tr>
<td></td>
<td>PID—RPD-2X2=</td>
</tr>
</tbody>
</table>
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 the Cisco cBR-8, this feature enables the operator to control the configured DVB-encrypted sessions to function without encryption for a configured duration. If the encryption still fails, the DVB session is marked as Fail-to-black after the fail-to-clear duration timeout.

Fail-to-Clear for DVB Tier-based Encryption

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

If fail-to-clear is configured, tier-based configuration is enabled, and then if the encryption fails, the DVB session’s Encrypt Status is marked as clear. The status changes to Encrypted when the encryption starts. This feature is not enabled by default.

Tier based Scrambling Setup

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

Figure 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 the 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:

```bash
enable
cfg 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```
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:

```plaintext
enable
cfg term
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
```
If the tier-based configuration is already enabled, you must first disable the tier-based configuration using the `no enable` command before you configure the 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:

```yaml
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:

```yaml
Router# show cable video encryption dvb ecmg id 1 connection

<table>
<thead>
<tr>
<th>ECMG</th>
<th>ECMG</th>
<th>CA Sys</th>
<th>Subsys</th>
<th>PID</th>
<th>Lower</th>
<th>Upper</th>
<th>Streams/</th>
<th>Open</th>
<th>Streams/</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>polaris_ecmg01</td>
<td>standard</td>
<td>0x4748</td>
<td>0x0</td>
<td>sid 0 0 1 1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enabled</td>
<td>RF</td>
<td>1</td>
<td>Tier-Based</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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:

```yaml
Router# show cable video encryption dvb ecmg id 7 connection

<table>
<thead>
<tr>
<th>ECMG</th>
<th>ECMG</th>
<th>CA Sys</th>
<th>Subsys</th>
<th>PID</th>
<th>Lower</th>
<th>Upper</th>
<th>Streams/</th>
<th>Open</th>
<th>Streams/</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>ecmg-7</td>
<td>standard</td>
<td>0x950</td>
<td>0x1234</td>
<td>sid 0 0 1680 1680</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enabled</td>
<td>7</td>
<td>1</td>
<td>VOD</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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
```

<table>
<thead>
<tr>
<th>EIS EIS Peer Management TCP CP CP</th>
<th>Overwrite Fail-To-Clear Connection</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID Name IP</td>
<td>IP</td>
</tr>
<tr>
<td>1 test 10.10.1.11 10.10.1.1</td>
<td>9898 DISABLED 0 DISABLED 400</td>
</tr>
</tbody>
</table>

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
```

<table>
<thead>
<tr>
<th>Total Sessions = 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session Output Streaming Session Source</td>
</tr>
<tr>
<td>Output</td>
</tr>
<tr>
<td>Id</td>
</tr>
<tr>
<td>1048576</td>
</tr>
<tr>
<td>1695161</td>
</tr>
</tbody>
</table>

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 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
cfg 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
```
Example: Basic Tier-based Scrambling Configuration

```
enable
cfg 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

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
cfg 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

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-i 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

<table>
<thead>
<tr>
<th>Related Topic</th>
<th>Document Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring Tier-Based Scrambling</td>
<td>Cisco RF Gateway 10 Software Configuration Guide</td>
</tr>
</tbody>
</table>
Technical Assistance

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

Feature Information for RPHY DVB VoD Support

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

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

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>RPHY DVB VoD Support</td>
<td>Cisco 2x2 RPD Software 2.x</td>
<td>This feature was introduced on the Cisco 2x2 Remote PHY Device.</td>
</tr>
</tbody>
</table>