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

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
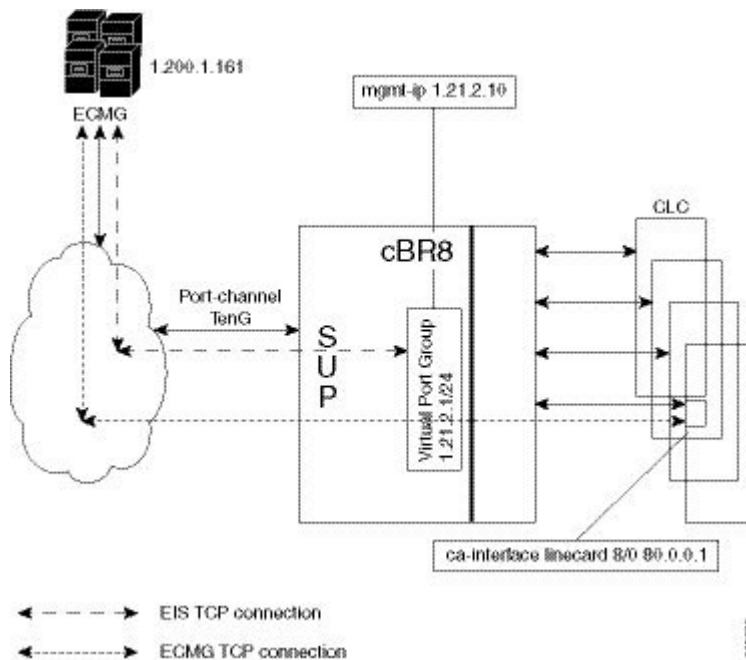
Fail-to-Clear

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
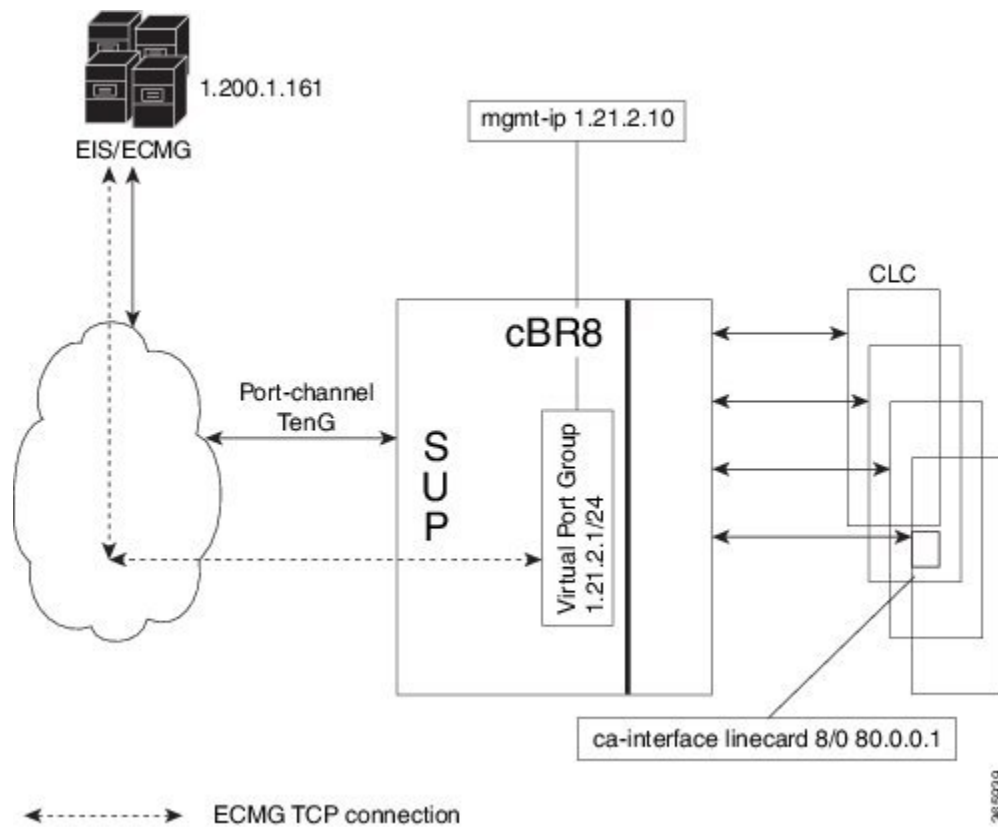
Restrictions for DVB

- 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 1: 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.