DualCrypt Encryption Mode Support

The Dualcrypt Encryption feature enables the Session and Resource Manager (SRM) to configure the PowerKey and DVB CAS sessions on the same line card (LC) of the Cisco cBR-8 Converged Broadband Router.

Finding Feature Information

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

- Hardware Compatibility Matrix for the Cisco cBR Series Routers, on page 1
- Information about DualCrypt Encryption Mode, on page 2
- How to Configure Dualcrypt Encryption Mode, on page 4
- Configuration Examples, on page 9
- Feature Information for DualCrypt Encryption Mode, on page 12

Hardware Compatibility Matrix for the Cisco cBR Series Routers

Note

The hardware components that are introduced in a given Cisco IOS-XE Release are supported in all subsequent releases unless otherwise specified.
Table 1: Hardware Compatibility Matrix for the Cisco cBR Series Routers

<table>
<thead>
<tr>
<th>Cisco CMTS Platform</th>
<th>Processor Engine</th>
<th>Interface Cards</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco cBR-8 Converged Broadband Router</td>
<td>Cisco IOS-XE Release 16.5.1 and Later Releases</td>
<td>Cisco IOS-XE Release 16.5.1 and Later Releases</td>
</tr>
<tr>
<td></td>
<td>Cisco cBR-8 Supervisor:</td>
<td>Cisco cBR-8 CCAP Line Cards:</td>
</tr>
<tr>
<td></td>
<td>• PID—CBR-SUP-250G</td>
<td>• PID—CBR-LC-8D30-16U30</td>
</tr>
<tr>
<td></td>
<td>• PID—CBR-CCAP-SUP-160G</td>
<td>• PID—CBR-LC-8D31-16U30</td>
</tr>
<tr>
<td></td>
<td>• PID—CBR-CCAP-SUP-60G</td>
<td>• PID—CBR-RF-PIC</td>
</tr>
<tr>
<td></td>
<td>• PID—CBR-SUP-8X10G-PIC</td>
<td>• PID—CBR-RF-PROT-PIC</td>
</tr>
</tbody>
</table>

Cisco cBR-8 Downstream PHY Modules:

- PID—CBR-D30-DS-MOD
- PID—CBR-D31-DS-MOD

Cisco cBR-8 Upstream PHY Modules:

- PID—CBR-D30-US-MOD
- PID—CBR-D31-US-MOD

Information about DualCrypt Encryption Mode

You can use this feature when you want the PowerKey and DVB sessions on the same QAM channel. This feature is applicable only to GQI-based sessions, as it uses the Generic QAM Interface (GQI) protocol.

To configure the dualcrypt encryption mode, you should set up connections with Event Information Scheduler (EIS) and Entitlement Control Message Generator (ECMG).

Prerequisites for Dualcrypt Encryption Mode

- Ensure that the following components are available on your system before configuring dualcrypt encryption for sessions.
  - Service Distribution Group (SDG)
  - Virtual Carrier Group (VCG) with encrypt
  - Logical Edge Device (LED) with GQI protocol
  - Event Information Scheduler (EIS)
• Entitlement Control Message Generator (ECMG)

• Ensure that the VCG is bound to SDG

• Ensure that the VCG is associated to LED

• Ensure that the Virtual Edge Input is configured only on LED

• Ensure that the following configurations are available on your system:
  
  • The encryption algorithm of the line card is set to DVB-CSA.
    
    You can set it using the following command:
    ```
    linecard <slot>/<bay> ca-system dualcrypt scrambler dvb-csa
    ```
  
  • The virtual port group interface is configured and the same is set for the management interface under cable video, because the DVB requires a management IP address for communicating with external servers.
    
    Use the following commands to set the virtual port group interface as management interface for cable video:
    ```
    configure terminal
cable video
mgmt-intf VirtualPortGroup <id>
    ```
  
  • The CA interface on the line card and the route for reaching the ECMG server are specified for session-based scrambling.
    
    Use the following commands to specify CA interface and the route:
    ```
    ca-interface linecard <slot>/<bay> <IP_Address>
route-ecmg <ECMG_Server_IP_Address> <Netmask> <Interface> <Forwarding_Router_IP_Address>
    ```
  
  • The `vrf <vrf_name>` keyword is configured for routes to populate on the respective VRFs, if you are using VRF for traffic or management separately. Configure the CA interface with specific VRF name.
    ```
    ca-interface linecard <slot>/<bay> <IP_Address> vrf <vrf_name>
    ```

• (Optional) The bind option is used to associate EIS with specific IP address or GQI-based LED

To use a single IP address for GQI (create and delete sessions) and EIS (provision/de-provision SCGs), the operator should bind the EIS with GQI-based LED using the IP option and configure the required IP address. The IP address should be the subnet of the configured virtual port group. By default, the EIS uses the management IP address configured under DVB and the GQI uses the management IP address configured under LED for session control.

The following sample commands show how to bind the EIS:
```
configure terminal
cable video
encryption
dvb
eis <name of eis>
listening-port <1-65535> bind ip <ip address>
or
listening-port <1-65535> bind led <id | name> <led id | led name>
```
Restrictions for DualCrypt Encryption Mode

The following restrictions are applicable for configuring DualCrypt encryption mode:

- The DualCrypt Encryption feature is applicable only to GQI-based remapped sessions.
- Use this feature only for PowerKey, DVB, and Clear sessions.
- Do not use this feature along with tier-based scrambling mode.

How to Configure Dualcrypt Encryption Mode

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

Configuring DVB Session for DualCrypt Encryption

This section explains how to configure the session-based scrambling with DualCrypt encryption mode.

Procedure

To configure a DVB session for Dualcrypt encryption, use the following commands:

```plaintext
enable
configure terminal
cable video
mgmt-intf VirtualPortGroup <group_id>
encryption
linecard <loslot/subslot> ca-system dualcrypt scrambler dvb-csa
dvb
route-ecmg ECMG_Server_IP_Address Netmask Interface Forwarding_Router_IP_Address
mgmt-ip IP_Address
eis EIS_Name id EIS_ID
listening-port port_number [bind {ip <ip address> | led < id <led id >| name <led name>>}]
ca-interface linecard <slot>/<bay> IP_Address
ecmg ECMG_Name id ECMG_ID
mode vod linecard <slot>/<bay>
type <standard/hitachi/irdeto/nagra/pkey>
ca-system-id CA_System_ID CA_Subsystem_ID
ecm-pid-source <sid/auto/ecm-id>
connection id ID priority connection_priority IP_Address Port
```
Verifying DVB Session for DualCrypt Encryption

To verify the configuration of the encryption algorithm on the linecard, use the `show cable video encryption linecard <slot>/<bay>` command as shown in the following example:

```
Router#show cable video encryption linecard 8/0
Line card: 8/0
CA System    Scrambler   DVB-Conformance
-----------------------------------------------
dualcrypt    dvb-csa     Enabled
```

To verify the scrambler configuration, use the `show cable video encryption scrambler brief` command as shown in the following example:

```
Router#show cable video encryption scrambler brief
Scrambler information
Chassis wide scrambler: none
-----------------------------------------------
Linecard      Current Configured
Scrambler     Scrambler
-----------------------------------------------
1   Not Ready None
2   Not Ready None
3   Not Ready None
4   Not Ready None
5   Not Ready None
6   Not Ready None
7   dvb-csa     dvb-csa
8   dvb-csa     None
9   des/dvs042  None
```

To verify the ECMG connection, use the `show cable video encryption dvb ecmg id <id> connection` command as shown in the following example:

```
Router#show cable video encryption dvb ecmg id <ID> connection
-----------------------------------------------------------------------------------------------------------------------
| ECMG | ECMG | ECMG CA Sys CA Subsys PID Lower Upper Streams/ Open Streams/ Auto Chan |
|------|------|---------------------|----------------|----------------|--|--|
| Slot | ECMG | ECMG Name Type ID ID Source limit limit ECMG ECMG ID |
| ID   | ID   | Connections Application |
-----------------------------------------------------------------------------------------------------------------------
1 test standard 0x950 0x0 sid 0 0 1 1 Enabled
7 1 VOD
```

ECMG Connections for ECMG ID = 1

```
<table>
<thead>
<tr>
<th>Conn</th>
<th>Conn IP</th>
<th>Channel Conn</th>
<th>Open Streams</th>
</tr>
</thead>
<tbody>
<tr>
<td>-ID</td>
<td>Priority</td>
<td>Number ID</td>
<td>Status</td>
</tr>
<tr>
<td>1</td>
<td>10.10.1.1</td>
<td>9878</td>
<td>Open 1</td>
</tr>
</tbody>
</table>
```

The `Conn Status` field shows the status of the connection with the ECMG server and the `Open Streams` field indicates the number of active ECM streams.

To verify the EIS connection, use the `show cable video encryption dvb eis id <id>` command as shown in the following example:

```
Router#show cable video encryption dvb eis id <ID>
----------------------------------------------------------------------------------------
| EIS | EIS Peer | Management TCP CP CP Overwrite Fail-To-Clear Connection |
|-----|---------|-----------------|------------------|
|     |         |                 |                  |
```

Verifying DVB Session for DualCrypt Encryption
Verifying the GQI Configuration

To verify the GQI connection, use the `show cable video gqi connection` command, as shown in the following example:

```
Router>show cable video gqi connection
LED Management Server Connection Version Event Reset Encryption
ID IP IP Status Pending Indication Discovery
2 10.10.1.1 10.100.1.1 Connected 2 0 ACKED Sent
```

To verify the statistics of GQI, use the `show cable video logical-edge-device id <ID> statistics` command, as shown in the following example:

```
Router>show cable video logical-edge-device id <ID> statistics
Create Delete Insert Cancel Switch Reset Encryption Event
Session Session Packet Packet Source Indication Discovery Notification
Success 4 0 0 0 0 3 7 0
Error 0 0 0 0 0 0 0 0
Total 4 0 0 0 0 3 7 0
```

Verifying the GQI Sessions for Encryption

To verify whether the sessions are encrypted, use the `show cable video session logical-edge-device id <ID>` command, as shown in the following example, and check the `Encrypt Status` field.

```
Router>show cable video session logical-edge-device id <ID>
Total Sessions = 4

Session Output Streaming Session Session Source UDP Output Input
Output Input Encrypt Encrypt Low Session Id Port Type Type Ucast Dest IP/Mcast IP (S,G) Port Program State State
Bitrate Bitrate Type Status Status Latency Name
1048580 20 Passthru UDP 10.10.11 49152 - ACTIVE-PSI ON
1713128 1698122 CLEAR - N 0x00000000000000000001
1048581 20 Remap UDP 10.10.11 49153 2 ACTIVE-PSI ON
1711859 1707422 DVB Encrypted N 0x00000000000000000002
1048582 23 Passthru UDP 10.10.11 49154 - ACTIVE-PSI ON
1711962 1699101 CLEAR - N 0x00000000000000000003
1048583 23 Remap UDP 10.10.11 49155 4 ACTIVE-PSI ON
1712498 1707834 DVB Encrypted N 0x00000000000000000004
```

The session's Encrypt Status should be Encrypted. The Output State should be ON to show the proper Encryption Status for DVB sessions. If the Output State is Pending, the Encrypt Status will be shown as Pending.

To get a list of SCGs, use the `show cable video scg all` command as shown in the following example:

```
Router>show cable video scg allq
SCGs: 4 Carriers with SCGs: 3
```

```
SCG ON TS SCG Ref Activation CP Duration SCG Seas LED/ ID ID ID ID Time (msec) Status Id EIS
```
Verifying ONID and TSID of the QAMs Configured for Specific LED

To get the details of ONID and TSID configured for QAMs configured under LED, use the `show cable video logical-edge-device id 1`, as shown in the following example, and verify the ONID and TSID details:

Logical Edge Device: led1
Id: 1
Protocol: GQI
Service State: Active
Discovery State: Disable
Management IP: 10.10.10.11
MAC Address:
Number of Servers: 1
  Server 1: 10.10.10.11
Reset Interval: 5
Keepalive Interval: 5  Retry Count:3
Number of Virtual Carrier Groups: 1
Number of Share Virtual Edge Input: 1
Number of Physical Qams: 39
Number of Sessions: 4
No Reserve PID Range

Virtual Edge Input:
<table>
<thead>
<tr>
<th>Port</th>
<th>VEI</th>
<th>Slot/Bay</th>
<th>Bundle</th>
<th>Gateway</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>10.10.10.11</td>
<td>7/0</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

Virtual Carrier Group:
<table>
<thead>
<tr>
<th>ID</th>
<th>Total</th>
<th>Total</th>
<th>Service-Distribution-Group</th>
<th>Service-Distribution-Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>vcg1 0</td>
<td>39</td>
<td>sdg1</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>QAM</th>
<th>Port</th>
<th>Physical Admin Operational TSID ONID Output VCG SDG Encryption</th>
</tr>
</thead>
<tbody>
<tr>
<td>7/0:0</td>
<td>RF Port 0</td>
<td>ON UP</td>
</tr>
<tr>
<td>7/0:1</td>
<td>RF Port 1</td>
<td>ON UP</td>
</tr>
<tr>
<td>7/0:2</td>
<td>RF Port 2</td>
<td>ON UP</td>
</tr>
<tr>
<td>7/0:3</td>
<td>RF Port 3</td>
<td>ON UP</td>
</tr>
<tr>
<td>7/0:4</td>
<td>RF Port 4</td>
<td>ON UP</td>
</tr>
</tbody>
</table>
Troubleshooting Tips

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

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

Configuration Examples

This section provides examples for configuring DualCrypt Encryption Mode:

Example: Basic Session-based Scrambling Configuration

cable video
mgmt-intf VirtualPortGroup 0
encryption
linecard 8/0 ca-system dualcrypt scrambler dvb-csa
dvb
route-ecmg 10.10.10.1 255.255.255.224 Port-channel26 2.26.1.2
mgmt-ip 10.10.10.11
eis test id 1
  listening-port 9898
c-a-interface linecard 8/0 10.10.10.12
ecmg test id 1
mode vod linecard 8/0
type standard
c-a-system-id 950 0
auto-channel-id
ecm-pid-source sid
connection id 1 priority 1 10.10.10.13 9878
service-distribution-group sdg1 id 1
  rf-port integrated-cable 8/0/0
virtual-carrier-group vcg1 id 1
type standard
  rf-channel 20-47 tsid 20-47 output-port-number 20-47
  bind-vcg
  vcg vcg1 sdg sdg1
  logical-edge-device led1 id 1
  protocol gqi
  mgmt-ip 10.10.10.10
  server 10.100.10.11
  virtual-edge-input-ip 10.10.10.11 input-port-number 1
  vcg vcg1
active

dualcrypt encryption

cable video
mgmt-intf VirtualPortGroup 0
encryption
linecard 8/0 ca-system dualcrypt scrambler dvb-csa
dvb
route-ecmg 10.10.10.1 255.255.255.224 Port-channel26 10.10.10.10
mgmt-ip 10.10.10.13
eis test id 1
  listening-port 9898 bind led id 1
c-a-interface linecard 8/0 10.10.10.14
ecmg test id 1

Example: Session-based Configuration with EIS Binding to LED using LED ID

cable video
mgmt-intf VirtualPortGroup 0
encryption
linecard 8/0 ca-system dualcrypt scrambler dvb-csa
dvb
route-ecmg 10.10.10.1 255.255.255.224 Port-channel26 10.10.10.10
mgmt-ip 10.10.10.13
eis test id 1
  listening-port 9898 bind led id 1
c-a-interface linecard 8/0 10.10.10.14
ecmg test id 1

Example: Configuration with EIS Binding to LED using LED Name

cable video
mgmt-intf VirtualPortGroup 0
encryption
linecard 8/0 ca-system dualcrypt scrambler dvb-csa
dvb
route-ecmg 10.10.10.11 255.255.255.224 Port-channel26 10.10.10.11
mgmt-ip 10.10.10.11
eis test id 1
  listening-port 9898 bind led name led1
c-ecmg test id 1
mode vod linecard 8/0
type standard
c-ecmg test id 1
auto-channel-id
c-acse test id 1
ecm-pid-source sid
c-connection id 1 priority 1 10.10.10.11 9878
c-service-distribution-group sdg1 id 1
onid 1
c-rf-port integrated-cable 8/0/0
c-locm-carrier-group vcg1 id 1
c-encrypt
service-type narrowcast
c-rf-channel 20-47 tsid 20-47 output-port-number 20-47
bind-vcg
vcg vcg1 sdg sdg1
logical-edge-device led1 id 1
protocol gqi
mgmt-ip 10.10.10.11
c-server 10.10.10.112
virtual-edge-input-ip 10.10.10.11 input-port-number 1
vcg vcg1
active
Example: EIS Binding to IP Address Other than Default DVB Management IP Address

cable video
mgmt-intf VirtualPortGroup 0
encryption
linecard 8/0 ca-system dualcrypt scrambler dvb-csa
dvb
route-ecmg 10.10.10.11 255.255.255.224 Port-channel26 10.10.10.11
mgmt-ip 10.10.10.11
eis test id 1
listening-port 9898 bind ip 10.10.10.11
car interface linecard 8/0 10.10.10.11
ecmg test id 1
mode vod linecard 8/0
type standard
car-system-id 950 0
auto-channel-id
ecm-pid-source sid
connection id 1 priority 1 10.10.10.11 9878
service-distribution-group sdg1 id 1
onid 1
rf-port integrated-cable 8/0/0
virtual-carrier-group vcg1 id 1
encrypt
service-type narrowcast
rf-channel 20-47 tsid 20-47 output-port-number 20-47
bind-vcg
vcg vcg1 sdg sdg1
logical-edge-device led1 id 1
protocol gqi
mgmt-ip 10.10.10.11
server 10.10.10.11
virtual-edge-input-ip 10.10.10.11 input-port-number 1
vcg vcg1
active

Example: Session-based Configuration with VRF

cable video
multicast-uplink Loopback410 access-list all-multicast vrf vrf_script_red_1 next-hop
10.10.10.11
mgmt-intf VirtualPortGroup 0
encryption
linecard 1/0 ca-system dvb scrambler dvb-csa
dvb
route-ecmg 10.10.10.11 255.255.255.224 Port-channel21 10.10.10.1
route-ecmg 10.10.10.16 255.255.255.224 Port-channel21 10.10.10.1
mgmt-ip 10.10.10.10
eis pytool1 id 1
listening-port 2500
cp-overrule 6
overwrite-scg
car interface linecard 1/0 10.10.10.0 vrf vrf_script_red_1
ecmg emcgl id 1
mode vod linecard 1/0
type standard
car-system-id 952 0
auto-channel-id
ecm-pid-source sid
connection id 1 priority 1 10.10.10.11 5678
connection id 2 priority 1 10.10.10.16 8765
ecmg emcg2 id 2
mode vod linecard 1/0
type standard
c-a-system-id 951 0
auto-channel-id
ecm-pid-source sid
c-connection id 1 priority 1 10.10.10.14 8765
ecmg emcg3 id 3
mode vod linecard 1/0
type standard
c-a-system-id 950 0
auto-channel-id
ecm-pid-source sid
c-connection id 1 priority 1 10.10.10.11 5678

interface VirtualPortGroup0
   vrf forwarding vrf_script_red_1
   ip address 10.10.10.11 255.255.224.0
   no mop enabled
   no mop sysid

Feature Information for DualCrypt Encryption Mode

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

Note

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

Table 2: Feature Information for DualCrypt Encryption Mode

<table>
<thead>
<tr>
<th>Feature Name</th>
<th>Releases</th>
<th>Feature Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>DualCrypt Encryption Mode</td>
<td>Cisco IOS XE Everest 16.6.1</td>
<td>This feature was integrated on the Cisco cBR Series Converged Broadband Routers.</td>
</tr>
</tbody>
</table>