



# Control Point Discovery

---

This document describes the Control Point Discovery (CPD) feature. This feature, along with Network Layer Signaling (NLS), enables automatic discovery of any control point associated with an end point.

## 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.

## Contents

- [Hardware Compatibility Matrix for Cisco cBR Series Routers, page 1](#)
- [Prerequisites for Control Point Discovery, page 2](#)
- [Restrictions for Control Point Discovery, page 2](#)
- [Information About Control Point Discovery, page 3](#)
- [How to Configure CPD, page 5](#)
- [Additional References, page 10](#)
- [Feature Information for Control Point Discovery, page 11](#)

# Hardware Compatibility Matrix for Cisco cBR Series Routers



## Note

---

The hardware components 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**

Cisco CMTS Platform	Processor Engine	Interface Cards
Cisco cBR-8 Converged Broadband Router	<p><b>Cisco IOS-XE Release 3.15.0S and Later Releases</b></p> <p>Cisco cBR-8 Supervisor:</p> <ul style="list-style-type: none"> <li>• PID—CBR-CCAP-SUP-160G</li> <li>• PID—CBR-CCAP-SUP-60G<sup>1</sup></li> <li>• PID—CBR-SUP-8X10G-PIC</li> </ul>	<p><b>Cisco IOS-XE Release 3.15.0S and Later Releases</b></p> <p>Cisco cBR-8 CCAP Line Cards:</p> <ul style="list-style-type: none"> <li>• PID—CBR-LC-8D30-16U30</li> <li>• PID—CBR-LC-8D31-16U30</li> <li>• PID—CBR-RF-PIC</li> <li>• PID—CBR-RF-PROT-PIC</li> </ul> <p>Cisco cBR-8 Downstream PHY Modules:</p> <ul style="list-style-type: none"> <li>• PID—CBR-D30-DS-MOD</li> <li>• PID—CBR-D31-DS-MOD</li> </ul> <p>Cisco cBR-8 Upstream PHY Modules:</p> <ul style="list-style-type: none"> <li>• PID—CBR-D30-US-MOD</li> </ul>

<sup>1</sup> Effective with Cisco IOS-XE Release 3.17.0S, CBR-CCAP-SUP-60G supports 8 cable line cards. The total traffic rate is limited to 60Gbps, the total number of downstream service flow is limited to 72268, and downstream unicast low-latency flow does not count against the limits.

## Prerequisites for Control Point Discovery

No special equipment or software is needed to use the Control Point Discovery feature.

## Restrictions for Control Point Discovery

- The CPD feature does not sync any dynamic CPD/NLS related data between the route processors (RPs). After sending a NLS challenge to the controller, the new active PRE will ignore the NLS response as a result of any RP switchover.
- The CPEs become inaccessible for a small duration during line card switchovers. During this interval, any CPD request received on CMTS will be responded to as if the endpoint is not connected or as if the control relationship is not supported.
- The CPD functionality is restricted to default VPN table id (0).
- Only manual configuration of NLS authentication pass phrase would be supported for CPD/NLS security.
- For NLS authentication, HMAC SHA1 (no configuration option) is used with MAC length truncated to 96 bits.

# Information About Control Point Discovery

To configure the Control Point Discovery feature, you should understand the following concepts:

## Control Points

Control points are points in a network that can be used to apply certain functions and controls for a media stream. In a cable environment, the control points are Cable Modem Termination Systems (CMTS) and devices that utilizes these control points are referred to as CPD Requestors (or controllers).

Cable CPD Requestors include the following:

- Call Management Server (CMS)
- Policy Server (PS)
- Mediation Device for Lawful Intercept (MD)

## Network Layer Signaling (NLS)

Network Layer Signaling (NSL) is an on-path request protocol used to carry topology discovery and other requests in support of various applications. In the CPD feature, NLS is used to transport CPD messages.

### NLS for CPD

NLS is used to transport CPD messages. The CPD data is carried under an application payload of the NLS and contains a NLS header with flow id. The NLS flow id is used during NLS authentication to uniquely identify the CPD requests and responses for an end point of interest.

### NLS Flags

All NLS headers contain bitwise flags. The CMTS expects the following NLS flag settings for CPD applications:

- HOP-BY-HOP = 0
- BUILD-ROUTE = 0
- TEARDOWN = 0
- BIDIRECTOINAL = 0
- AX\_CHALLENGE = 0/1
- AX\_RESPONSE = 0/1

**Note**

Any requests with flags other than AX flags, set to one will be rejected with an error indicating a poorly formed message.

## NLS TLVs

The following NLS TLVs are supported for all CPD applications:

- APPLICATION\_PAYLOAD
- IPV4\_ERROR\_CODE
- IPV6\_ERROR\_CODE
- AGID
- A\_CHALLENGE
- A\_RESPONSE
- B\_CHALLENGE
- B\_RESPONSE
- AUTHENTICATION
- ECHO

The following NLS TLVs are not supported for CPD applications:

- NAT\_ADDRESS
- TIMEOUT
- IPV4\_HOP
- IPV6\_HOP

## Control Point Discovery

The control point discovery feature allows CPD Requestors to determine the control point IP address between the CPD Requestor and the media endpoint.

Using Networking Layer Signaling (NLS), the control point discovery feature sends a CPD message towards the end point (MTA). The edge/aggregation device (CMTS), located between the requestor and the endpoint, will respond to the message with its IP address.



---

**Note**

For Lawful Intercept, it is important that the endpoint does not receive the CPD message. In this instance, the CMTS responds to the message without forwarding it to its destination.

---

## CPD Protocol Hierarchy

CPD messages are sent over the NLS.

The CPD Protocol Hierarchy is as follows:

- 1 CPD
- 2 NLS

- 3 UDP
- 4 IP

**Note**

Since NLS is implemented on the UDP protocol, there is a potential of message loss. If messages are lost, the controller will re-send the CPD request in any such event.

## Control Relationship

A control relationship between a control point and a controller is identified as a function on a media flow that passes through a control point. A control relationship is uniquely defined by a control relationship type (CR TYPE) and control relationship ID (CR ID). The CR ID is provisioned on CMTS as well as the controller.

The table lists the supported CR TYPEs and corresponding pre-defined CR IDs

**Table 2: Supported Control Relationship Types and Corresponding Control Relationship IDs**

Control Relationship Type	Pre-Defined Corresponding Control Relationship ID
CR TYPE = 1 (Lawful Intercept)	CR ID = 1: CMTS
	CR ID = 2: Aggregation router or switch in front of CMTS
	CR ID = 3: Aggregation router or switch in front of Media Services
	CR ID = 4: Media Gateway
	CR ID = 5: Conference Server
	CR ID = 6: Other
CR TYPE = 2 (DQoS)	CR ID = 1: CMTS
CR TYPE = 3 (PCMM)	CR ID = 1: CMTS

# How to Configure CPD

## Enabling CPD Functionality

To enable the CPD functionality, use the `cpd` command in global configuration mode. The CPD message authentication is determined by NLS configuration.

### Before You Begin

The CPD message authentication is determined by NLS configuration.

**Procedure**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>cpd</b>  <b>Example:</b> Router (config)# cpd	Enables CPD functionality <ul style="list-style-type: none"> <li>• Us the “no” form of this command to disable CPD functionality.</li> </ul>
<b>Step 4</b>	<b>end</b>  <b>Example:</b> Router# end	Exits global configuration mode and enters privileged EXEC mode.

**Examples for CPD Enable**

The following example shows the cpd enabled on a router:

```
Router (config)# cpd
```

**Debugging CPD Functionality**

To debug the CPD feature, use the **debug cpd** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

**Configuring Control Relationship Identifier**

To configure a Control relationship identifier (CR ID) for CMTS, use the **cpd cr-id** command. When CPD request comes with a wild-card CR ID, the CMTS will respond with this configured value.

**Procedure**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>cpd cr-id</b>  <b>Example:</b> Router (config)# cpd cr-id 100	Configures a control relationship identifier (CR ID) for CMTS.
<b>Step 4</b>	<b>end</b>  <b>Example:</b> Router# end	Exits global configuration mode and enters privileged EXEC mode.

**Examples**

The following example shows the cpd cr-id command configured with a cr-id number of 100 on a router.

```
Router (config)# cpd cr-id 100
```

**Enabling NLS Functionality**

To enable the NLS functionality, use the nls command in global configuration mode. It is recommended that NLS message authentication be enabled at all times.

**Procedure**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 1</b>	<b>enable</b>	Enables privileged EXEC mode.

	Command or Action	Purpose
	<b>Example:</b> Router> enable	<ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>nls</b>  <b>Example:</b> Router (config)# nls	Enables NLS functionality. <ul style="list-style-type: none"> <li>• NLS authentication is optional.</li> <li>• It is recommended that NLS message authentication be enabled at all times.</li> </ul>
<b>Step 4</b>	<b>end</b>  <b>Example:</b> Router# end	Exits global configuration mode and enters privileged EXEC mode.

## Examples

The following example shows the nls command enabled on a router.

```
Router (config)# nls
```

## Debugging NLS Functionality

To debug the NLS feature, use the **debug nls** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

## Configuring Authorization Group Identifier and Authentication Key

The Authorization Group Identifier (AG ID) and corresponding authorization key are provisioned on CMTS, as well as on controller/CPD requester.

To configure the Authorization Group Identifier and Authentication Key, use the nls ag-id command in global configuration mode. It is recommended that NLS message authentication be enabled at all times.



**Procedure**

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>nls ag-id</b>  <b>Example:</b> Router (config)# nls ag-id 100 auth-key 20	Configures the Authorization Group Identifier and Authentication Key.
<b>Step 4</b>	<b>end</b>  <b>Example:</b> Router# end	Exits global configuration mode and enters privileged EXEC mode.

**Examples**

The following example shows the nls ag-id command with an Authorization Group ID of 100 and Authentication Key of 20.

```
Router (config)# nls ag-id 100 auth-key 20
```

**Configuring NLS Response Timeout**

The NLS response timeout governs the time CMTS will wait for getting a response for a NLS authentication request.

To configure the NLS response timeout, use the nls ag-id command in global configuration mode. It is recommended that NLS message authentication be enabled at all times.

**Procedure**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 1</b>	<b>enable</b>  <b>Example:</b> Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal	Enters global configuration mode.
<b>Step 3</b>	<b>nls resp-timeout</b>  <b>Example:</b> Router (config)# nls resp-timeout 60	Configures the NLS response time.
<b>Step 4</b>	<b>end</b>  <b>Example:</b> Router# end	Exits global configuration mode and enters privileged EXEC mode.

**Examples**

The following example shows the nls resp-timeout command with a response timeout setting of 60 seconds.

```
Router (config)# nls resp-timeout 60
```

**Additional References**

The following sections provide references related to the CPD feature.

**Technical Assistance**

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	<a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a>

## Feature Information for Control Point Discovery

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://tools.cisco.com/ITDIT/CFN/>. An account on <http://www.cisco.com/> is not required.

**Note**

The below 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.

**Table 3: Feature Information for Control Point Discovery**

Feature Name	Releases	Feature Information
Control Point Discovery	Cisco IOS-XE Release 3.15.0S	This feature was introduced on the Cisco cBR Series Converged Broadband Routers.

