IKEv2 Mutual Authentication

This document describes the Remote PHY device IKEV2 mutual authentication 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.

- Hardware Compatibility Matrix for Cisco Remote PHY Device, on page 1
- Information about IKEv2 Mutual Authentication, on page 2
- Configure IKEv2 Mutual Authentication, on page 2
- Feature Information for IKEv2 Mutual Authentication, on page 3

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 Remote PHY Device

Cisco HFC Platform	Remote PHY Device
Cisco GS7000 Super High Output Node	Cisco 1x2 / Compact Shelf RPD Software 2.1 and Later Releases

Cisco HFC Platform	Remote PHY Device
Cisco GS7000 Super High Output Intelligent Node (iNode)	Cisco 1x2 / Compact Shelf RPD Software 4.1 and Later Releases Cisco Intelligent Remote PHY Device 1x2 • PID—iRPD-1X2= • PID—iRPD-1X2-PKEY=

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

Information about IKEv2 Mutual Authentication

When the RPD connects to the CCAP Core, a mutual authentication using IKEv2 with public key signatures is optionally required and a secure control session may be established which can be secured using IPsec.

Mutual authentication is optionally required between the RPD and CCAP Core, and a secure connection may not be required in all cases. Whether authentication is required for an RPD is determined by the network that it is connected to. In some cases, RPD is located in an untrusted network, and it must connect to devices inside the trusted network, which presents a potential security vulnerability.

Authentication is initiated by RPD. Whether the RPD is required to authenticate is under control of the CCAP Core.

Configure IKEv2 Mutual Authentication

This section describes how to configure IKEv2 mutual authentication for RPD.

CMTS Side Configuration

Global Configuration

To enable IKEv2 mutual authentication, use **cable rphy auth enable** command in the global configuration mode.

Per PRD Configuration

To configure the IKEv2 mutual authentication per PRD, use **ikev2-core authentication {enable | disable | bypass}** command in the RPD configuration mode.

To display the authentication state, use **show cable rpd** command as shown in the following example:

```
Router#show cable rpd
Load for five secs: 5%/1%; one minute: 4%; five minutes: 5%
Time source is NTP, 10:08:45.016 CST Mon Sep 4 2017
MAC Address     IP Address       I/F       State        Role  HA    Auth   Name
0004.9f00.0719  6.6.6.100        Te6/1/2   online       Pri   Act   Y      p1_0719
```

```
0004.9f00.0719  6.6.6.100        Te6/1/1   online       Aux   Act   Y      p1_0719
badb.ad13.411c  6.6.6.101        Te6/1/2   onlisssne    Pri   Act   Y      p2_411c
badb.ad13.411c  6.6.6.101        Te6/1/1   online       Aux   Act   Y      p2_411c
```

Note If RPD IKEv2 authentication is enabled, and RPD Core is authenticated, then the column of "auth" will show "Y". If RPD IKEv2 authentication is enabled, and RPD Core is not authenticated, then the column of "auth" will show "N". If RPD IKEv2 authentication is disabled, the column of "auth" will show "N/A".

RPD Node Side Configuration

To configure the IKEv2 mutual authentication on RPD node, use **ikev2 authentication {enable | disable}** command on RPD node.

To display the authentication configuration state, use **show ikev2** command as shown in the following examples:

```
R-PHY#show ikev2 configuration
IKEv2 authentication is currently enabled, next boot is enabled!

R-PHY#show ikev2 session
Local      Remote     Status
6.6.6.100  6.6.6.1    UP
```

Feature Information for IKEv2 Mutual Authentication

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 2: Feature Information for IKEv2 Mutual Authentication

Feature Name	Releases	Feature Information
IKEv2 Mutual Authentication	Cisco 1x2 / Compact Shelf RPD Software 4.1	This feature was introduced on the Cisco Remote PHY Device.