



## Network Authentication

This document describes the Remote PHY device network 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, page 1](#)
- [Information about Network Authentication, page 2](#)
- [How to Enable Network Authentication, page 2](#)

## Hardware Compatibility Matrix for Cisco Remote PHY Device



### Note

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

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

Cisco HFC Platform	Remote PHY Device
Cisco GS7000 Node	<b>Cisco 1x2 RPD Software 1.1 and Later Releases</b> Cisco Remote PHY Device 1x2 <ul style="list-style-type: none"><li>• PID—RPD-1X2=</li></ul>

# Information about Network Authentication

RPD must be able to operate in both authenticated and unauthenticated networks. 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. 802.1x is introduced to provide authentication services to eliminate the potential security issues.

802.1x is a Layer 2 protocol that uses EAP (Extensible Authentication Protocol) to provide authentication services. Following certificates are needed to use the network authentication:

- Cablelabs Root CA certificate: caRoot.pem
- CableLabs Device CA Certificate: deviceCA.pem
- RPD Certificate: rpdCert.pem, private key: rpd.key
- Cablelabs Service Provider CA Certificate: spCA.pem
- AAA Server Certificate: aaaCert.pem, private key: aaa.key

## How to Enable Network Authentication

This section describes how to enable network authentication for RPD.

### Installing Certificates in Radius Server

To install the certificate in Radius server, follow the steps below:

#### Procedure

---

**Step 1** Combine CA certificate for AAA server.

**Example:**

```
cat spCA.pem caRoot.pem > ca_root_srv.pem
```

**Step 2** In freeRadius Server, copy "ca\_root\_srv.pem", "spCA.pem", "aaaCert.pem" and "aaa.key" to "/etc/freeradius/certs".

---

### Configuring Radius Server

To install the certificate in RPD, follow the steps below:

## Procedure

**Step 1** Define a new client in `/etc/freeradius/clients.conf`.

**Example:**

```
client rphytest_ng13 {
    ipaddr = 20.5.0.36
    secret = rphytest
    shortname = ng13_switch
    require_message_authenticator = yes
}
```

The "ipaddr" is the switch's management ip address.

**Step 2** In `/etc/freeradius/eap.conf`, change the following lines in "tls" to specify the server's private key file and certificate files.

**Example:**

```
tls {
    ...
    private_key_file = ${certdir}/aaa.key
    certificate_file = ${certdir}/aaaCert.pem
    CA_file = ${cadir}/ca_root_srv.pem
}
```

**Step 3** Start radius in radius sever.

**Example:**

```
sudo freeradius
```

Make sure only one freeradius instance is running.

## Configuring Switch

To configure the switch, follow the steps below:



**Note**

This procedure is for Catalyst 3750 switch, other switch may use different commands.

## Procedure

**Step 1** Add the following configuration in global configuration mode.

**Example:**

```
dot1x system-auth-control /* enable 802.1x */
aaa new-model
aaa authentication dot1x default group radius
radius-server host 10.79.41.103 auth-port 1812 key rphytest
```

**Step 2** Add the following configuration under interface which connects to RPD.

**Example:**

```
authentication port-control auto
dot1x pae authenticator
```

---

## Verifying Authentication Status

To displays dot1x authentication information for RPD, use the **show dot1x** command as shown in the following example:

```
Router# show dot1x summary
Interface      Core-id
vbh0           CORE-3415960568
```

```
EAP_Received   Status
True           UP
```

```
Router# show dot1x detail
Interface      Core-id
vbh0           CORE-3415960568
bssid=01:80:c2:00:00:03
freq=0
ssid=
id=0
mode=station
pairwise_cipher=NONE
group_cipher=NONE
key_mgmt=IEEE 802.1X (no WPA)
wpa_state=COMPLETED
ip_address=30.85.40.47
address=00:04:9f:00:03:73
```

```
EAP_Received   Status
True           UP
```

**Supplicant PAE state=AUTHENTICATED**

```
suppPortStatus=Authorized
EAP state=SUCCESSselected
Method=13 (EAP-TLS)EAP TLS
cipher=ECDHE-RSA-AES256-SHA
tls_session_reused=0
eap_session_id=0c53798fb46014cc92a4c1151521bae6a14c98f919d5e8c81a701b7272be7f812e7e5a75881768d74d311795a3b1f0e37bfa7fff7d0c4685d36f216bec59850
uuid=ab722cfb-84dc-5835-a905-edfec20f78c3
```