Cisco Routed Passive Optical Network Deployment Guide, Release 26.1.x, 26.2.x

First Published: 2026-02-26

Last Modified: 2026-06-11

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

CHAPTER 1 **Cisco Routed PON Solution Overview** 1

Components of the Cisco Routed PON Solution 2

Cisco PON pluggable OLT 3

Cisco Routed PON ONT 3

Cisco PON Manager 4

MongoDB database 4

Cisco Routed PON Netconf Server 4

Cisco PON Controller 4

CHAPTER 2 **Deploying the Cisco Routed PON Solution** 5

Install the Cisco PON Pluggable OLT 5

Install the Cisco Routed PON ONT 6

Install and Configure the PON Manager 6

Install and Configure the MongoDB database 6

Configuring the PON Controller 6

Configure the PON Controller on the IOS XR Router using NETCONF 7

Activating the PON Controller 8

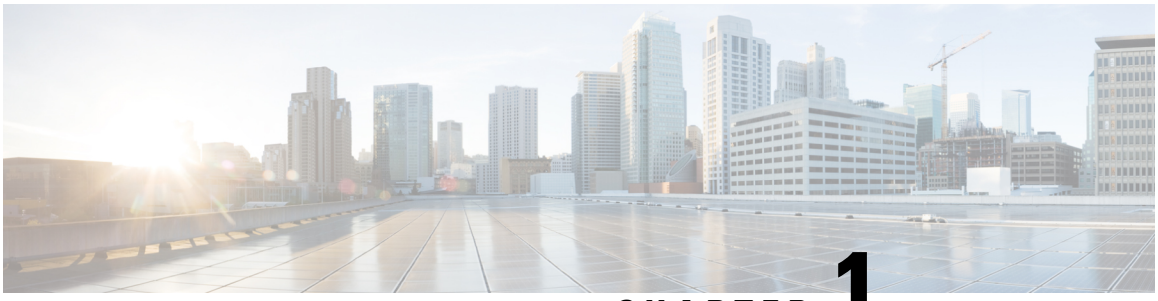
Type-B PON protection with multihoming 12

Best practices for Type-B PON protection 13

How Type-B PON protection with multihoming works 14

Enable Type-B protection with multihoming 15

CHAPTER 3 **Troubleshooting Cisco Routed PON** 19



CHAPTER 1

Cisco Routed PON Solution Overview

With the advancements in broadband technology, the customer demands have expanded to high-resolution audio and video playback, seamless audio and video streaming, immersive Virtual Reality (VR) experiences, and responsive gaming. These applications need substantial bandwidth and minimal latency to operate effectively. Currently, these requirements are met by employing an Optical Line Terminal (OLT) chassis, which connects at the access layer of the network.

Cisco's Routed PON Solution is a transformational approach that condenses the OLT chassis into a pluggable form factor. The solution becomes a part of the access router by plugging the Cisco PON SFP+ into 10G ports of NCS540, NCS5500, and NCS5700 series routers. You have the option to utilize a scalable model based on your bandwidth requirements, choosing between PON pluggable optics or Ethernet optics for your requirements.

This solution provides a network infrastructure that supports future upgrades, enabling a transition from a 10G pluggable OLT to a 25G variant when it becomes available. This solution not only uses the advanced features and capabilities of the Cisco routers but also capitalizes on the cost efficiency of PON networks. Since it uses passive devices, it doesn't require an extra power supply, leading to lower overall power consumption in the network.

The transceiver module acts as a substitute for the OLT chassis, managing the entire optical span within the access network. The Cisco PON OLT is compatible with various Optical Network Terminals (ONTs) on the market, provided they adhere to the ONU Management and Control Interface (OMCI) standard. This port-by-port network expansion approach eliminates the need for adding fixed line cards to a chassis-based OLT, allowing for a more capital-efficient network growth strategy.

Some of the advantages of the solution are:

- The transceiver module removes the need of any 3rd-party hardware for OLTs, thereby reducing the dependency on 3rd-party vendors and streamlining the network infrastructure.
- The transceiver module is a pluggable OLT that is inserted into the router. The cost of the OLT is lower than the OLT Chassis, hence reducing the cost of deployment.
- Since the device is a pluggable transceiver module, this significantly reduces the physical footprint of the network.
- Use of the PON Manager to deploy and upgrade the Routed PON solution saves time due to the use of a single point of management.

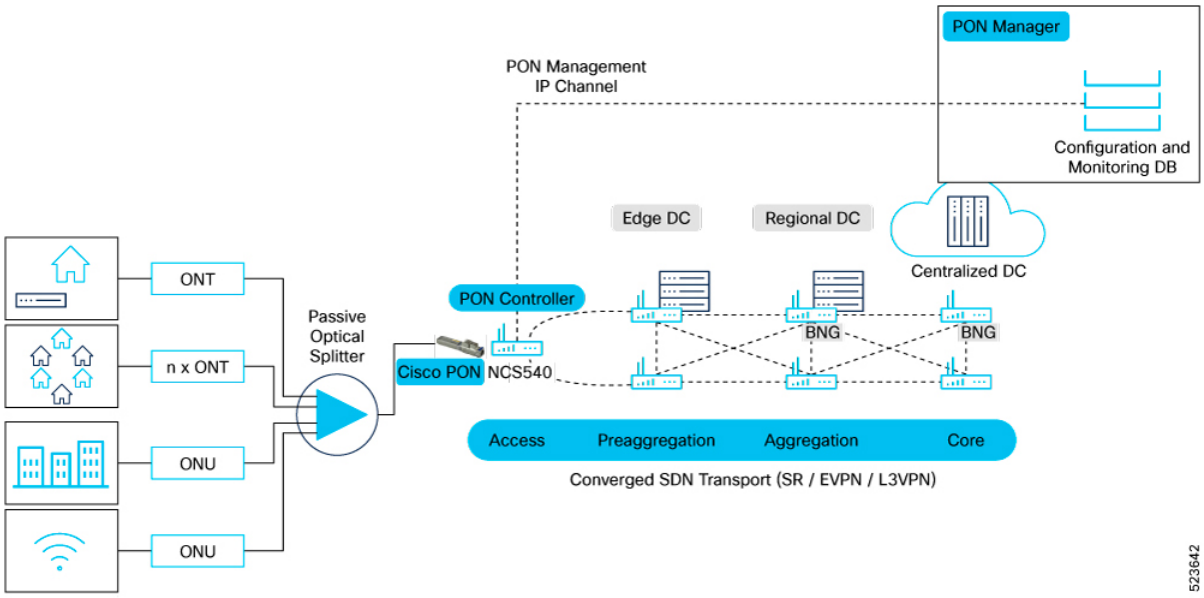
This release supports the PON Controller on the following Cisco router variants:

- N540-24Z8Q2C-SYS

- N540-ACC-SYS
- N540X-16Z4G8Q2C-A, N540X-16Z4G8Q2C-D
- N540-28Z4C-SYS-A, N540-28Z4C-SYS-D
- N540-24Q8L2DD-SYS
- NCS-55A1-24Q6H-SS
- NCS-55A2-MOD-S
- NCS-57C1-48Q6D
- NCS-57C3-MODS-SYS

Cisco Routed PON Architecture

Figure 1: Cisco Routed PON solution



The solution involves integrating the Cisco PON pluggable OLT into the 10G Ethernet ports found on the Cisco NCS 540, NCS 5500, and NCS 5700 routers. The PON manager and its corresponding database are hosted on either an external system or specialized hardware, which can be located within the core network infrastructure or hosted on a cloud platform. The PON controller establishes a protected link facilitating the exchange of data between the PON manager and the network's OLTs and ONUs. A more in-depth examination of these individual elements of the solution follows.

- Components of the Cisco Routed PON Solution, on page 2

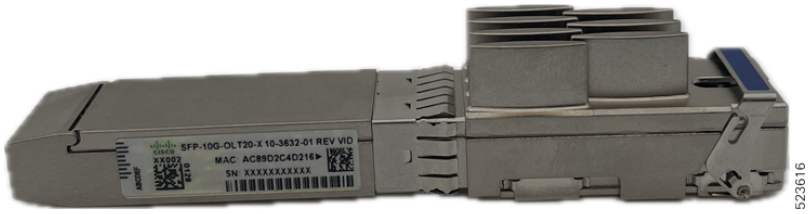
Components of the Cisco Routed PON Solution

The Various components of the solution are:

Cisco PON pluggable OLT

The Cisco PON pluggable OLT features a hot-swappable SFP+ design that enables the deployment of a software-defined broadband network. It incorporates a 10G Ethernet to XGS PON MAC Bridge IC along with a Layer 1 optical transceiver. This integration facilitates the module's connection from a PON network to a dedicated Ethernet SFP+ port on routers. The system is capable of supporting 10G data transmission speeds both upstream and downstream.

Figure 2: PON Transceiver Module



Technical specifications of the Cisco PON pluggable OLT are:

Table 1: Cisco PON pluggable OLT Technical Specifications

Dimension (H x W x D)	8.55mm x 13.4mm x 80.65mm
PID	SFP-10G-OLT20-X
Data rate	Symmetric rates: 8G upstream/8G downstream
Connector Type	SC/UPC
Maximum Distance	20 km
Operating Temperature	-20°C to 75°C
Typical Power Consumption	3.2W
Average Launch Power	4 dbm min 7 dbm max
ODN Class	N2
Cable Type	Single Mode Fiber

Cisco Routed PON ONT

Cisco 10G routed PON ONTs are fully compliant with the XGS-PON ITU-T G.9807.1 standard, supporting symmetrical 10-Gbps downstream and upstream optical connectivity via an SC/APC optical connector to meet current and future networking needs. With integrated XGS-PON optics, MAC, and Ethernet switching capabilities, these ONTs help network operators optimize Total Cost of Ownership by reducing edge transport, switching, and routing costs, as well as minimizing footprint and power consumption. Used with Cisco routed PON modules, Cisco PON ONTs provide an ideal end-to-end solution for cost-effective, agile, and diverse networking requirements.

Supported Cisco 10G Routed XGS-PON ONTs

- ENC-10G-ONT-10 for high-speed single-port RJ-45 deployments

- ENC-10G-ONT-14A for multiple business broadband and voice port option
- ENC-10G-ONT-01PR for outdoor deployments

Cisco PON Manager

The Cisco PON manager is a web application and an accompanying REST API that provides a graphical user interface for managing the PON network. The PON manager is used to set up the OLTs and ONUs, as well as downloading firmware updates for both the OLTs and ONUs. The REST API accompanies the web application for the purposes of providing access to MongoDB for managing PON users and the PON network. The PON manager facilitates:

- Alarm management
- Dashboard view
- Device monitoring and statistic
- Device provisioning and management
- Service configuration
- User management
- Database management

MongoDB database

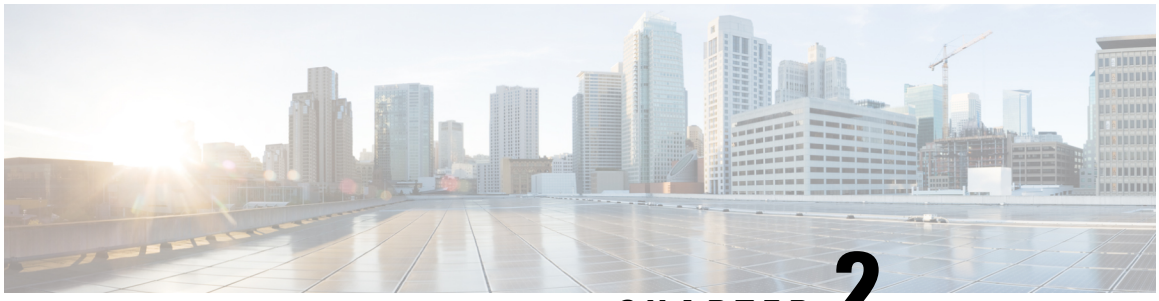
The MongoDB datastore contains all of the configuration, state, statistics, alarms, and logging data for the devices in the PON network. Northbound interfaces, such as the Routed PON Manager and the customer applications interface with MongoDB to provision and retrieve monitoring information for devices in the PON network. MongoDB serves as the interface between the PON Manager and the PON Controller.

Cisco Routed PON Netconf Server

The Cisco Routed PON Netconf Server features a Netconf-compliant interface and an API that allows clients to manage PON networks effectively. Built on Netopeer2 and ConfD, the server provides robust configuration management and connects to a MongoDB database for operational data handling. It complies with the Broadband Forum's TR-383 and TR-385 YANG models, ensuring the server can configure subscriber services reliably within the PON network infrastructure.

Cisco PON Controller

Cisco PON Controller is a light-weight application which runs as a docker container on each NCS540, NCS 5500, and NCS 5700 devices. Various configurations applied to the OLTs and ONTs in the network are fetched from the MongoDB database and provisioned on the OLT ONUs by the PON Controller. At each polling cycle, the PON controller collects state information, statistics, alarms, and logs from devices and reports the information to higher layer applications through MongoDB.



CHAPTER 2

Deploying the Cisco Routed PON Solution

Completing the implementation of the Cisco Routed PON Solution requires setting up the various components that make up the system. At a high level, the steps to configure the Cisco Routed PON Solution are as follows:

1. Install the Cisco PON pluggable OLT.
2. Install and configure the Cisco PON Manager.
3. Install and configure the MongoDB database.
4. Install and configure the the Netconf Server.
5. Configure and activate the Cisco PON Controller.

Required Versions for Cisco Routed PON Solution—PON 26.x.x Release

Ensure that you use the following PON controller, PON manager, OLT or ONU firmware, and Netconf versions for the Cisco IOS XR 26.x.x.

Table 2: PON 26.x.x Release

IOS XR Release	PON Controller	PON Manager	OLT/ONU Firmware	Netconf
26.1.1	6.10.0	6.10.0	6.10.0	6.10.0

- Install the Cisco PON Pluggable OLT, on page 5
- Install the Cisco Routed PON ONT, on page 6
- Install and Configure the PON Manager, on page 6
- Install and Configure the MongoDB database, on page 6
- Configuring the PON Controller, on page 6
- Type-B PON protection with multihoming, on page 12

Install the Cisco PON Pluggable OLT

For steps to install the Cisco PON pluggable OLT refer to *Install and Remove Transceiver Modules* in the Cisco NCS 540 Router Hardware Installation Guide.

Install the Cisco Routed PON ONT

For steps to install the Cisco Routed XGS-PON ONT refer to the Hardware Installation Guide for Cisco Routed XGS-PON ONT.

Install and Configure the PON Manager

For steps to install the PON Manager, refer to *PON Manager Installation* in the *Cisco Routed PON Installation Guide*.

Install and Configure the MongoDB database

For steps to install the MongoDB database, refer to *MongoDB Installation* in the *Cisco Routed PON Installation Guide*.

Configuring the PON Controller

The PON Controller is installed on a Docker container on the router. The PON Controller installation package is stored either on the hard disk of the router or on a network server to which the router has access.

To configure the PON controller, follow the steps:

Install the PON Controller on Cisco IOS XR7 OS

For the Cisco Routers using the Cisco IOS XR7 framework, execute the following commands to install the software package:

Note This section is applicable for the following routers:

- N540X-16Z4G8Q2C-A, N540X-16Z4G8Q2C-D
- N540-28Z4C-SYS-A, N540-28Z4C-SYS-D
- N540-24Q8L2DD-SYS
- NCS-57C1-48Q6D

1. Execute the following command to confirm if the PON Controller package is present in the router:

   ```
   show install active summary | i pon
   ```

   Sample Output

   ```
   RP/0/RP0/CPU0:PON-Rtr1-CrLk#show install active summary | i pon
   Tue Feb 27 08:45:29.246 UTC
   xr-pon-ctlr                                              24.1.1.40Iv1.0.1-1
   ```

   If the PON Controller isn't present, the command won't return any value.

2. If the PON Controller isn't present refer to the appropriate guide for steps to download and configure additional packages. The steps to configure an additional package might differ based on the router model.
   - For NCS 5500 or NCS 5700 router, refer to *Install Optional Packages to Provide Additional Functionality* in System Setup and Software Installation Guide for Cisco NCS 5500 Series Routers.
   - For NCS 540 router, refer to *Install Optional Packages to Provide Additional Functionality* in System Setup and Software Installation Guide for Cisco NCS 540 Series Routers.

Install the PON Controller on Cisco IOS XR OS

This section provides the steps to configure Cisco PON Controller software in the routers using the IOS XR framework.

Note This section is applicable for the below routers:

- N540-24Z8Q2C-SYS
- N540-ACC-SYS
- NCS-55A1-24Q6H-SS
- NCS-55A2-MOD-S
- NCS-57C3-MODS-SYS

1. Execute the following command to confirm if the PON Controller package is present in the router:

   ```
   show install active | i pon
   ```

   Sample Output

   ```
   RP/0/RP0/CPU0:PON-Rtr5-Peyto#show install active | i pon
   Tue Feb 27 08:44:53.345 UTC
   ncs5500-pon-ctlr-1.0.0.0-r241140I
   ncs5500-pon-ctlr-1.0.0.0-r241140I
   ```

   If the PON Controller isn't present, the command doesn't return any values.

2. If the PON Controller isn't present refer to the appropriate guide for steps to download and configure additional packages. The steps to configure an additional package might differ based on the router model.
   - For NCS 5500 or NCS 5700 router, refer to *Install Packages* in System Setup and Software Installation Guide for Cisco NCS 5500 Series Routers.
   - For NCS 540 router, refer to *Install Packages* in System Setup and Software Installation Guide for Cisco NCS 540 Series Routers.

Configure the PON Controller on the IOS XR Router using NETCONF

To configure the PON Controller on the router using NETCONF, use the following NETCONF RPC To configure the PON Controller on the IOS XR Router:

```
<rpc xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="101">
  <edit-config>
```

```
    <target>
      <candidate/>
    </target>
    <config>
      <pon-ctlr xmlns="http://cisco.com/ns/yang/Cisco-IOS-XR-um-pon-ctlr-cfg">
        <cfg-file>harddisk:/PonCntlInit.json</cfg-file>
        <vrf>default</vrf>
        <tls-pem>tls_file</tls-pem>
      </pon-ctlr>
    </config>
  </edit-config>
</rpc>
```

1. Replace the **PonCntlInit.json** with the appropriate JSON configuration file name.
2. Change default in the **<vrf>** element if you want to specify a different VRF instance.
3. Update tls_file in the **<tls-pem>** element to the name of the correct TLS PEM file.

For steps to configure the NETCONF server, refer to *Routed PON Netconf Server Installation* in the *Cisco Routed PON Installation Guide*.

Activating the PON Controller

After installing up the PON Controller in the router, you need to activate it by connecting to MongoDB and applying additional configurations to the controller.

Before you begin:

- Ensure that you have synchronized the XR clock with that of an NTP server.

  The steps to configure an NTP server might differ based on the router model. Refer to the appropriate guide for steps to configure an NTP server.

  - For NCS 5500 or NCS 5700 routers, refer to *Configuring Network Time Protocol* in System Management Configuration Guide for Cisco NCS 5500 Series Routers.
  - For NCS 540 router, refer to *Synchronize Router Clock with NTP Server* in System Setup and Software Installation Guide for Cisco NCS 540 Series Routers.

- Ensure that Linux Networking is configured on the router as given below:

```
linux networking
 vrf default
  address-family ipv4
   default-route software-forwarding
   source-hint default-route interface MgmtEth0/RP0/CPU0/0
  !
 !
!
```

  The steps to configure Linux Networking might differ based on the router model. Refer to the appropriate guide for steps to configure an NTP server.

  - For NCS 5500 or NCS 5700 routers, refer to *Packet I/O on IOS XR* in Application Hosting Configuration Guide for Cisco NCS 5500 Series Routers.
  - For NCS 540 router, refer to *Setup the Linux Network for Application Hosting* in Application Hosting Configuration Guide for Cisco NCS 540 Series Routers.

- Ensure that the MongoDB server is reachable from your router by executing the following command:

```
bash ping <IP address of the MongoDB server>
```

Sample Output

```
RP/0/RP0/CPU0:PON-Rtr5-Peyto#bash ping 192.0.2.0
Tue Feb 27 09:17:53.046 UTC
RP/0/RP0/CPU0:Feb 27 09:17:53.087 UTC: bash_cmd[66952]: %INFRA-INFRA_MSG-5-RUN_LOGIN :
 User lab logged into shell from con0/RP0/CPU0
PING 192.0.2.0 (192.0.2.0) 56(84) bytes of data.
64 bytes from 192.0.2.0: icmp_seq=1 ttl=64 time=0.820 ms
64 bytes from 192.0.2.0: icmp_seq=2 ttl=64 time=0.769 ms
64 bytes from 192.0.2.0: icmp_seq=3 ttl=64 time=0.703 ms
```

Edit the parameters in the **PonCntlInit.json** that is part of the PON Controller package establish connection with the MongoDB server. A sample **PonCntlInit.json** is included in the PON Controller package.

A sample **PonCntlInit.json** is given below:

```
{
    "CNTL": {
        "Auth": false,
        "CFG Version": "R4.0.0",
        "DHCPv4": false,
        "DHCPv6": false,
        "PPPoE": false,
        "UMT interface": "tibitvirt",
        "Maximum CPEs Allowed": 0,
        "Maximum CPE Time": 0
    },
    "DEBUG": {},
    "JSON": {
        "databaseDir": "/opt/cisco/poncntl/database/",
        "defaultDir": "/opt/cisco/poncntl/database/"
    },
    "Local Copy": {
        "CNTL-STATE": false,
        "OLT-STATE": false,
        "ONU-STATE": false
    },
    "Logging": {
        "Directory": "/var/log/tibit",
        "FileCount": 2,
        "FileSize": 5120000,
        "Tracebacks": false,
        "Timestamp": false,
        "Facility" : "user"
    },
    "MongoDB": {
        "auth_db": "cisco_users",
       "auth_enable": false,                                <-- field to enable CLI password
 authentication
        "ca_cert_path": "/etc/cisco/ca.pem",
        "compression": false,
        "write_concern": "default",
        "host": "192.0.2.0",                                  <-- mongoDB server IP Address
        "name": "cisco_pon_controller",
        "password": "",
        "password_opts": {
                          "type": "keyring",
                          "keyring_path": "/etc/cisco/poncntl/keyring.data",
                          "keyring_key_path": "/etc/cisco/poncntl/keyring.key"
                        },
        "port": "27017",                                      <-- mongoDB port
```

```
        "tls_enable": false,                                <-- field to enable TLS based
connection
        "username": "",
        "dns_srv": false,
        "db_uri": "",
        "replica_set_enable": false,
        "replica_set_name": "rs0",
        "replica_set_hosts":
            [
            "192.0.2.3:27017",                              <-- mongoDB replica set 1
            "192.0.2.4:27999",                              <-- mongoDB replica set 2
            "mongo02.example.com:17999"
            ],
        "validate_cfg": true
    },
    "databaseType": "MongoDB",
    "interface": "veth_pon_glb",
    "interface_namespace": ""
}
```

1. Change the **host** IP address parameter to the IP address of your MongoDB server.
2. (Optional) To enable secure connection between the PON Controller and the MongoDB server, change the value for **tls_enable** to **true**.

   If a secure connection is enabled, you'll need to configure the **username** and **password** parameters as well.
3. If you have configured a replica set for MongoDB, change the IP address for the MongoDB replica set.
4. Copy and paste the **PonCntlinit.json** file to either the hard disk of the router or to your network folder.

   When copying the file to the hard disk of the router, it is stored in `/misc/disk1` by default.
5. Confugure Controller using CLI or NETCONF RPC:

   - **CLI**

     Execute the **`cfg-file`** command to initiate the PON controller, the command is used to load the PON controller application on the router.

     Syntax

     ```
     cfg-file <tftp transfer protocol>/package_path/ or harddisk/package_path/ vrf
     <vrf-name> tls-pem <tftp transfer protocol>/pem_file_path/ db-password <password>
     ```

Parameter	Decription
tftp transfer protocol	TFTP server IP address.
package_path	Location of the .json file. **Note** If a custom VRF is used for management connectivity, include the VRF name as part of the package path.
Harddisk	Harddisk of the router. If the .json file is located on the harddisk, provide the path to on the harddisk.
vrf	Specifies VPN routing and forwarding (VRF).

Parameter	Decription
vrf-name	Name of a VRF used for MongoDB connectivity.
tls-pem	Specifies that TLS is used.
pem_file_path	Path of the .pem file. This can either be stored on the router harddisk or a TFTP server.
db-password	Password for the MongoDB server. **Note** If `auth_enable` field in the json file is set to true, you can set the password from the CLI.

Example:

```
RP/0/RP0/CPU0:ios(config)#pon-ctlr cfg-file
tftp://192.0.2.0/auto/tftp-users2/user2/PonCntlInit.json vrf default tls-pem
tftp://192.0.2.0/auto/tftp-blr-users2/user/rootCA.pem db-password cisco@123$
```

- **NETCONF RPC**

```
<rpc xmlns="urn:ietf:params:xml:ns:netconf:base:1.0" message-id="101">
  <edit-config>
    <target>
      <candidate/>
    </target>
    <config>
      <pon-ctlr xmlns="http://cisco.com/ns/yang/Cisco-IOS-XR-um-pon-ctlr-cfg">
        <cfg-file>harddisk:/PonCntlInit2411MTBDHCPTest2.json</cfg-file>
        <vrf>default</vrf>
        <tls-pem>tls_file</tls-pem>
      </pon-ctlr>
    </config>
  </edit-config>
</rpc>
```

Note In the above configuration the **PonCntlInit2411MTBDHCPTest2.json** file is a sample file used to configure the Controller.

- For NCS 5500 or NCS 5700 routers, refer to Programmability Configuration Guide for Cisco NCS 5500 Series Routers.
- For NCS 540 router, refer to Programmability Configuration Guide for Cisco NCS 540 Series Routers..

6. Ensure that the main interface for the SFP is in active.

   For example, if the Cisco PON pluggable OLT is inserted in the port 0/0/0/5:

```
RP/0/RP0/CPU0:ios(config)#interface TenGigE0/0/0/5
RP/0/RP0/CPU0:ios(config-if)#no shutdown
```

7. Create a subinterface with ID 4090 on the port where the small form-factor pluggable is inserted. The subinterface is required to receive the control packets between the PON Controller and the Cisco PON pluggable OLT.

```
interface TenGigE0/0/0/5.4090
encapsulation dot1q 4090
```

When the subinterface is created, the PON controller discovers the OLTs and ONUs in the network.

```
RP/0/RP0/CPU0:ios#run
Thu Oct 19 08:04:53.799 UTC
[xr-vm_node0_RP0_CPU0:~]$docker ps
CONTAINER ID IMAGE COMMAND CREATED STATUS PORTS NAMES
7909570b4803 cisco-poncntl.xr:R4.0.0 "/usr/bin/supervisor…" 26 hours ago Up 26 hours
pon_ctlr
[xr-vm_node0_RP0_CPU0:~]$docker logs pon_ctlr --tail 50
2023-10-19 08:07:33.482 INFO PonCntl Total Controllers: 1 OLTs: 1 ONUs: 1
RP/0/RP0/CPU0:ios(config-if)#no shutdown
```

8. Run the *lldp* command to enable Link Layer Discovery Protocol (LLDP) for the OLT port. This helps in the discovery of the OLTs and ONUs in the PON Manager.

```
RP/0/RP0/CPU0:ios(config)# lldp
```

9. Confirm if the PON Controller, OLT, and ONU details are displayed in the PON Manager.

Note If the Controller summary displays **Status:** as **offline,** then match the UTC clock on your router to that of the Cisco UCS server.

For more information on PON Controller, refer to *PON Controller* in the *Cisco Routed PON Installation Guide*.

Type-B PON protection with multihoming

Type-B PON protection with multihoming is a network redundancy mechanism for Passive Optical Network (PON) deployments that

- enables a standby PON Optical Line Terminal (OLT) to become active when the original active OLT fails or a fiber cut occurs
- facilitates PON controller level protection by enabling the secondary PON controller to take over when the primary PON controller fails without switching OLT roles, and
- assists router-level protection, so the PON controller and OLT on the secondary router take over when the router with the active PON controller fails.

Table 3: Feature History Table

Feature Name	Release Information	Feature Description
Type-B PON protection with multihoming	Release 26.2.1	You can now ensure uninterrupted subscriber service by continuously managing PON control and data traffic during equipment or link failures. Type-B PON protection with multihoming achieves this by enabling automatic switchover between active and standby Optical Line Terminals (OLTs). The automatic switchover establishes robust controller-level and router-level protection in XGS-PON deployments. This feature is supported on: • NCS-57C1-48Q6D • NCS-57C3-MOD-SYS • N540-24Q8L2DD-SYS

Limitations of Type-B PON protection with multihoming

The convergence speed is designed to ensure reliable failover, typically occurring within seconds. While it may not achieve the sub-second failover speeds required for some high-availability applications, it provides a dependable transition that supports consistent network performance.

Table 4: Comparison of protection attributes for OLT, controller, and router

Attributes	OLT-level protection	PON controller-level protection	Router-level protection
Failover action	Standby OLT assumes active role and handles traffic	Secondary PON controller manages OLTs without switching OLT roles	Secondary router's PON controller and OLTs become active

Type-B PON protection with single-homing

Type-B protection with single-homing provides redundancy for different OLTs on the same router and its fiber path. It enables a standby OLT to become active if the active OLT or fiber connection fails. This mechanism ensures service continuity by switching traffic paths at the local OLT level. It is specifically designed to protect the immediate connection between the OLT and the ONUs.

Best practices for Type-B PON protection

Ensure that you implement these best practices when designing, configuring, and managing Type-B PON protection to maximize network resilience and minimize risk.

- Avoid configuring OLTs in Cascading groups when protection is required, as these are not supported for Type-B PON protection.
- Monitor the redundancy and operational status of both OLTs and all controller links regularly; promptly investigate and address any alarms or status changes.

How Type-B PON protection with multihoming works

Summary

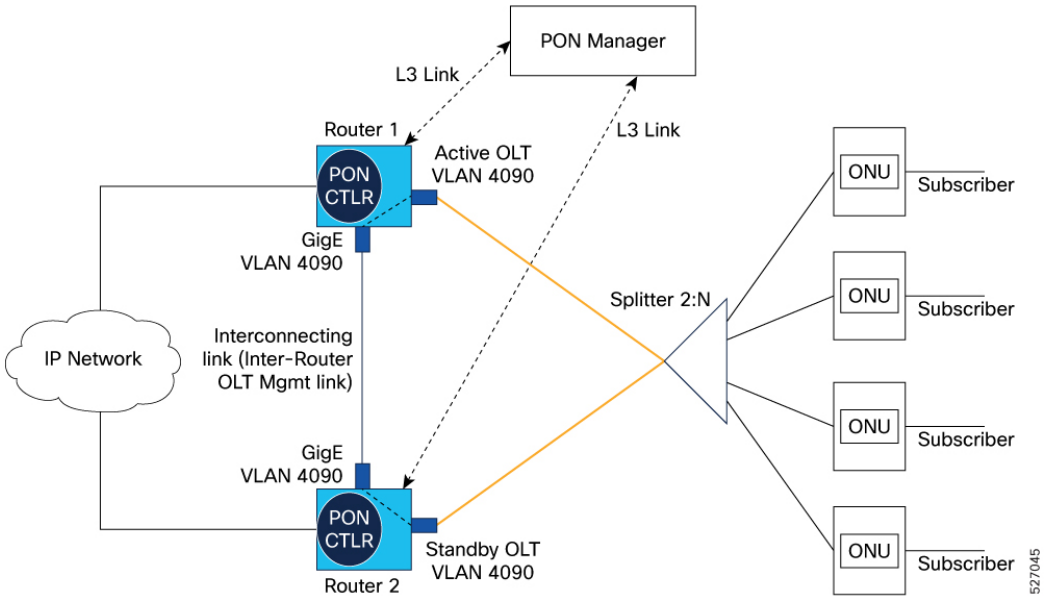
The key components involved in the process are:

- Router: Each router hosts a PON controller instance.
- PON Controller: The PON controller on each router identifies its local OLTs and discovers the OLTs on the peer router through the inter-router OLT management link. It manages both active and standby OLTs.
- PON Manager: Configures the primary and secondary PON controllers, as well as the active and standby OLTs.
- Inter-router OLT management link: A dedicated communication link between two routers that facilitates the PON controller to communicate with OLTs in the other peer routers.

This process ensures network connectivity and service continuity for subscribers by transitioning PON control from an active OLT to a standby OLT when a failure is detected .

Workflow

Figure 3: Type-B PON protection process overview



These stages describe how Type-B PON protection provides redundancy in XGS-PON deployments:

1. Initial configuration

- The inter-router OLT management link is enabled between the routers.
- Both OLTs are inventoried by the PON Manager and assigned active or standby roles.
- ONUs are registered on both OLTs.
- The system establishes protection configuration, laying the groundwork for failover.

2. Operational state
   - The designated active OLT transmits downstream traffic to subscribers; both OLTs receive upstream from ONUs.
   - The standby OLT monitors for loss of signal or inactivity, ready to take over if needed.
   - Subscribers receive uninterrupted service during this normal operation.
3. Switchover event
   - A switchover is triggered automatically by failures (link, equipment, or controller).
   - Upon trigger, the system detects the event and transitions the standby OLT to active.
   - The PON Manager updates roles and notifies controllers, ensuring continued monitoring.
4. ONU re-registration and service resumption
   - ONUs detect the new active OLT, re-register, and resume bidirectional communication.
   - Standard authentication may be performed.
   - Subscriber traffic is restored through the newly active OLT.

Result

Type-B PON protection enables rapid redirection of management traffic to a backup PON controller and subscriber traffic to a backup OLT in the event of failure, ensuring continuous network service and minimizing downtime for all subscribers.

Enable Type-B protection with multihoming

Enable chassis-level redundancy and uninterrupted PON subscriber service by configuring Type-B PON protection with multi-homing.

Configure Type-B PON protection with multihoming when continuous service for PON subscribers is critical, such as during hardware or link failures.

Before you begin

Ensure these prerequisites are met:

- PON Manager software installed to manage controllers and OLTs.
- Cisco routers with PON feature support and the XR PON software image installed.
- PON controller instances available and configured on both routers.
- Ethernet link between routers (typically a dedicated VLAN; e.g., VLAN 4090 as a Layer 2 subinterface).

- At least two OLTs, each connected to a separate router.
- All ONUs inventoried on the OLTs, with both OLTs managed as primary by the same PON Controller.

Follow these steps to configure Type-B PON protection for redundancy.

Procedure

Step 1 Enter PON controller configuration mode on each router.

Example:

```
Router(config)#pon-ctlr
```

If the controller instance does not exist, install or activate a valid instance before proceeding. Ensure XR PON software version compatibility. Repeat for each router.

PON controller configuration mode is active on both routers.

Step 2 Specify the configuration file path for each PON controller.

Example:

```
Router(config)#cfg-file tftp://192.0.2.0/auto/tftp-users2/user2/PonCntlInit.json vrf default tls-pem
 tftp://192.0.2.0/auto/tftp-blr-users2/user/rootCA.pem db-password cisco@123$
```

The controller uses the specified configuration file for setup.

Step 3 Configure inter-router OLT management links to enable bidirectional OLT/controller communication.

Example:

```
Router(config)#interRouter-olt-mgmtlink TenGigE0/0/0/24.4090
```

Step 4 Configure the subinterface under the OLT port and the inter-router OLT management link port with encapsulation 4090.

```
Router1#show running-config interface tengigE 0/0/0/24.4090
Thu Mar 26 09:06:47.144 UTC
interface TenGigE0/0/0/24.4090 l2transport
description PON TypeB IntrLnk
encapsulation dot1q 4090
!
```

```
Router2#show running-config interface tengigE 0/0/0/10.4090
Thu Mar 26 09:06:47.144 UTC
interface TenGigE0/0/0/10.4090 l2transport
description PON OLT link
encapsulation dot1q 4090
!
```

Step 5 Enable control-path communication between the OLT and the inter-router OLT management link.

```
Router#l2vpn
   bridge group 4090
  bridge-domain 4090
   interface TenGigE0/0/0/10.4090
   !
   interface TenGigE0/0/0/24.4090
   !
  !
 !
```

Step 6 Run the **show l2vpn bridge-domain** command to verify that the AC interfaces that carry the PON traffic into the router are up.

```
Router#show l2vpn bridge-domain
Tue Apr 28 14:55:17.786 UTC
Legend: pp = Partially Programmed.
Bridge group: 4090, bridge-domain: 4090, id: 0, state: up, ShgId: 0, MSTi: 0
  Aging: 300 s, MAC limit: 64000, Action: none, Notification: syslog
  Filter MAC addresses: 0
  ACs: 2 (2 up), VFIs: 0, PWs: 0 (0 up), PBBs: 0 (0 up), VNIs: 0 (0 up)
  List of ACs:
    Te0/0/0/10.4090, state: up, Static MAC addresses: 0
    Te0/0/0/24.4090, state: up, Static MAC addresses: 0
  List of Access PWs:
  List of VFIs:
  List of Access VFIs:
```

Step 7 Run the **show interface** <*inteface-name*> command to verify that the subinterface state is up and is exchanging control traffic.

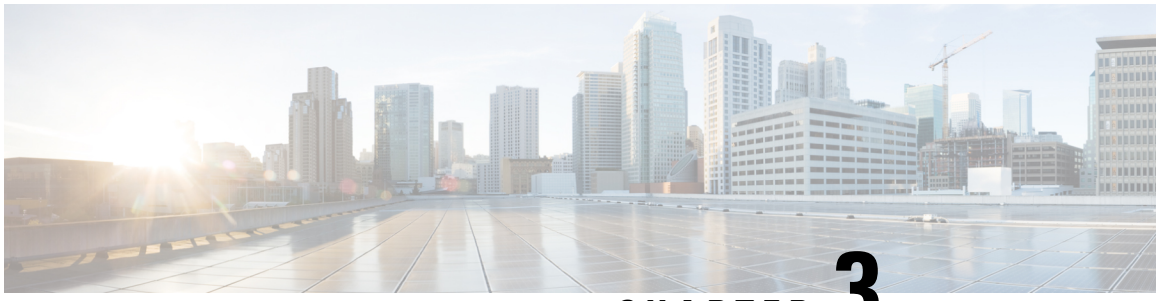
```
Router#show interfaces tengigE 0/0/0/24.4090
[22:37:58.013 UTC Tue May 26 2026]
TenGigE0/0/0/24.4090 is up, line protocol is up
Interface state transitions: 1
Hardware is VLAN sub-interface(s), address is d009.c864.362a
Layer 2 Transport Mode
MTU 1518 bytes, BW 10000000 Kbit (Max: 10000000 Kbit)
reliability Unknown, txload Unknown, rxload Unknown
Encapsulation 802.1Q Virtual LAN,
Outer Match: Dot1Q VLAN 4090
Ethertype Any, MAC Match src any, dest any
loopback not set,
Last link flapped 00:02:58
Last input 00:00:08, output 00:00:08
Last clearing of "show interface" counters never
10 packets input, 650 bytes
0 input drops, 0 queue drops, 0 input errors
109 packets output, 6779 bytes
0 output drops, 0 queue drops, 0 output errors
```

The inter-router OLT management link for PON controller communication is enabled.

What to do next

For additional configuration, refer to these sections in the Cisco Routed PON Manager User Guide:

1. Add the OLTs to the inventory on both PON Controllers.
   - Assign both OLTs as primary in the first PON Controller.
   - Assign both OLTs as secondary in the second PON Controller.
2. Configuring an OLT protection partner
3. Enabling automatic switchover for OLT active and standby
4. Enabling automatic switchover with OLT toggle
5. Forcing a switchover from active OLT to standby OLT



CHAPTER 3

Troubleshooting Cisco Routed PON

This section contains steps to troubleshoot issues related to the Cisco Routed PON solution:

Ensuring Correct Configuration for PON Controller

Confirm that the router's PON controller is configured with the correct settings, including the configuration file, file path, and Virtual Routing and Forwarding (VRF) instance.

Use the following command to review the current PON controller configuration on the router:

```
router# show running-config pon-ctlr
```

Example:

```
P/0/RP0/CPU0:router# show running-config pon-ctlr
Mon Jun 3 06:42:43.616 UTC
pon-ctlr
cfg-file harddisk:/PonCntlInit2411MTBDHCPTest2.json vrf default
```

The output displays the active configuration file (**PonCntlInit2411MTBDHCPTest2.json**) located on the hard disk and the associated VRF name (**default**). Verify that these details are accurate to ensure proper operation of the PON controller.

Checking for Errors or Trace Messages

After verifying the configurations, it's important to check for any errors or trace messages generated by the PON controller process.

Use the following command to check for errors or trace messages:

```
router# show pon-ctlr ltrace all reverse location all
```

Example:

```
RP/0/RP0/CPU0:PON-Eyrie-Rtr6#show pon-ctlr ltrace all reverse location all
Wed Jun 12 05:13:21.304 UTC
1334 wrapping entries (69760 possible, 2432 allocated, 0 filtered, 1334 total)
Jun  7 07:26:58.190 pon_ctlr/event 0/RP0/CPU0 t16459 pon_ctlr_main.c:95:Appmgr app activation
 response
Jun  7 07:26:57.936 pon_ctlr/event 0/RP0/CPU0 t16459 pon_ctlr_utls.c:357:Appmgr req request
 (4) sent
Jun  7 07:26:57.936 pon_ctlr/event 0/RP0/CPU0 t16459 pon_ctlr_utls.c:747:PON_CTLR Socket
Init completed
Jun  7 07:26:57.936 pon_ctlr/error 0/RP0/CPU0 t16459 pon_ctlr_utls.c:677:PON Socket: Bind
Passed
Jun  7 07:26:57.911 pon_ctlr/event 0/RP0/CPU0 t16459 pon_ctlr_utls.c:639:PON Create Socket
 dev veth_pon_xrns
```

```
Jun  7 07:26:57.911 pon_ctlr/event 0/RP0/CPU0 t16459 pon_ctlr_utls.c:134:CMD ip netns exec
 vrf-default ip address show veth_pon_glb - success
```

The output displays the latest trace messages from the PON controller, aiding in the diagnosis of any issues.

Verifying Linux Networking Configuration for the PON Controller

It is necessary to check the configuration of the Linux network interfaces that facilitate communication with the PON Controller Docker container to ensure they are correctly set up.

You can check the configuration of the Linux networking for the PON Controller for

- the **veth_pon_glb** interface, which is the virtual Ethernet interface on the PON Controller Docker container, by running the command:

  ```
  router# bash ifconfig veth_pon_glb
  ```

- the **veth_pon_xrns** interface, which is the XR interface that connects to the PON Controller, with the command:

  ```
  router# run ifconfig veth_pon_xrns
  ```

Example:

```
RP/0/RP0/CPU0:router#bash ifconfig veth_pon_glb
Mon Jun 3 06:36:51.808 UTC
RP/0/RP0/CPU0:Jun 3 06:36:51.841 UTC: bash_cmd[65602]: %INFRA-INFRA_MSG-5-RUN_LOGIN : User
lab logged into shell from con0/RP0/CPU0
veth_pon_glb: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500 metric 1
inet6 fe80::aa4f:b1ff:fe8c:a450 prefixlen 64 scopeid 0x20<link>
ether a8:4f:b1:8c:a4:50 txqueuelen 1000 (Ethernet)
RX packets 114 bytes 9156 (8.9 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 5699 bytes 343086 (335.0 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
RP/0/RP0/CPU0:Jun 3 06:36:52.269 UTC: bash_cmd[65602]: %INFRA-INFRA_MSG-5-RUN_LOGOUT :
User lab logged out of shell from con0/RP0/CPU0
```

The output displays the interface status, including flags indicating if the interface is up and running, MTU size, IP addresses, and counters for packets transmitted and received.

Verifying VRF-Specific Networking Configuration for the PON Controller

Ensure that the VRF-specific networking configuration is correctly established for the PON Controller within Linux is critical for proper network segmentation and routing.

To check the networking configuration within a specific VRF for the PON Controller, use the following command, replacing **<vrf-name>** with the actual name of the VRF:

```
router# bash ip netns exec vrf-<vrf-name> ifconfig veth_pon_glb
```

Example:

```
RP/0/RP0/CPU0:router#bash ip netns exec vrf-default ifconfig veth_pon_glb
Mon Jun 3 06:39:18.483 UTC
RP/0/RP0/CPU0:Jun 3 06:39:18.516 UTC: bash_cmd[66702]: %INFRA-INFRA_MSG-5-RUN_LOGIN : User
lab logged into shell from con0/RP0/CPU0
veth_pon_glb: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500 metric 1
inet6 fe80::aa4f:b1ff:fe8c:a450 prefixlen 64 scopeid 0x20<link>
ether a8:4f:b1:8c:a4:50 txqueuelen 1000 (Ethernet)
RX packets 114 bytes 9156 (8.9 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 5701 bytes 343206 (335.1 KiB)
```

```
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
RP/0/RP0/CPU0:Jun 3 06:39:18.942 UTC: bash_cmd[66702]: %INFRA-INFRA_MSG-5-RUN_LOGOUT :
User lab logged out of shell from con0/RP0/CPU0
```

This command provides the interface configuration within the specified VRF, which should show similar details as the global namespace output, but within the context of the chosen VRF.

Verifying TCP Connection Between PON Controller and MongoDB

Verify the connection status to ensure the PON Controller maintains a stable and active TCP connection with the MongoDB database, which runs on port 27017.

Run the following command in the router's shell to list all TCP connections to the MongoDB database port:

```
router#bash netstat -an | grep 27017
```

Example:

```
RP/0/RP0/CPU0:Jun 3 06:50:44.798 UTC: bash_cmd[66937]: %INFRA-INFRA_MSG-5-RUN_LOGIN : User
lab logged into shell from con0/RP0/CPU0
tcp 0 0 PON-Eyrie-Rtr6:65210 4.20.2.251:27017 ESTABLISHED
tcp 0 0 PON-Eyrie-Rtr6:65212 4.20.2.251:27017 ESTABLISHED
tcp 0 0 PON-Eyrie-Rtr6:64594 4.20.2.251:27017 ESTABLISHED
tcp 0 0 PON-Eyrie-Rtr6:65222 4.20.2.251:27017 ESTABLISHED
tcp 0 0 PON-Eyrie-Rtr6:65214 4.20.2.251:27017 ESTABLISHED
tcp 0 0 PON-Eyrie-Rtr6:65216 4.20.2.251:27017 ESTABLISHED
tcp 0 0 PON-Eyrie-Rtr6:65220 4.20.2.251:27017 ESTABLISHED
tcp 0 0 PON-Eyrie-Rtr6:65226 4.20.2.251:27017 ESTABLISHED
tcp 0 0 PON-Eyrie-Rtr6:65228 4.20.2.251:27017 ESTABLISHED
tcp 0 0 PON-Eyrie-Rtr6:65224 4.20.2.251:27017 ESTABLISHED
tcp 0 0 PON-Eyrie-Rtr6:65218 4.20.2.251:27017 ESTABLISHED
RP/0/RP0/CPU0:Jun 3 06:50:45.105 UTC: bash_cmd[66937]: %INFRA-INFRA_MSG-5-RUN_LOGOUT :
User lab logged out of shell from con0/RP0/CPU0
```

The output displays a list of established TCP connections to the MongoDB server on port 27017. Each line represents an active connection from the PON Controller to the database, indicating successful communication between the two systems.

Monitoring Packets in the Routed PON Queue

Check the number of packets that are trapped and sent to the PON queue to ensure smooth operation and identify any potential issues with packet flow.

Issue the following command to inspect the counters for packets associated with the PON:

```
router# show spp node-counters | include PON
```

Example:

```
RP/0/RP0/CPU0:router# show spp node-counters | include PON
Wed Jun 12 05:15:57.560 UTC
PON: 7082
```

The output shows the number of packets trapped and sent to the PON queue, indicated by the count next to **PON**.

Assessing Punt Rate and Policer Counters

Assess the punt rate and review accepted and dropped packet counters due to the policer. This helps ensure that the network is not discarding necessary packets and that policing mechanisms function as intended.

To display the punt rate and policer statistics, use the command

```
router# show lpts punt statistics brief location 0/0/CPU0
```

Example:

```
P/0/RP0/CPU0:router#show lpts punt statistics brief location 0/0/CPU0
Mon Jun 3 06:56:00.157 UTC
*Per-SubInterface punt policer is not HW supported on this Node
Lpts Punt Policer Statistics:
Punt_Reason - Ingress Packets type to be Punt policed
Rate - Policer rate in PPS
Accepted - No of Packets Accepted
Dropped - No of Packets Dropped
Domain - Domain name
State - Current config state
Interface Punt_Reason Rate Accepted Dropped Domain
State
any ARP 1000 1093107 0 default
Active
CDP 1000 0 0 default Active
LACP 1000 1425469 0 default Active
LLDP 1000 3045726 0 default Active
SSFP 500 261567876 0 default Active
IPv6-ND-proxy 1000 0 0 default Active
```

The output lists the punt reason, rate, number of accepted packets, number of dropped packets, domain, and the current state for each type of traffic. This information is critical for verifying that the network's policer allows or rejects traffic according to the policy.

Checking the Status of the PON Controller Docker Container

Confirm that the Docker container running the PON Controller is up and functioning properly to ensure the PON system is managed without interruption.

To verify the PON Controller container's status, run the following command:

```
[xr-vm_node0_RP0_CPU0:~]$ docker ps
```

Example:

```
CONTAINER ID        IMAGE                          COMMAND                   CREATED
   STATUS          PORTS               NAMES
e611df7e8edb        tibit-poncntl.xr:R4.0.0      "/usr/bin/supervisor…"   3 days ago
 Up 3 days                           pon_ctlr
```

The output lists all running containers. If the PON Controller (pon_ctlr) is listed with an **Up** status, the container is running correctly.

Reviewing PON Controller Log Output

Examine the log output of the PON Controller container to troubleshoot potential issues or to confirm system status and operations.

Use the following command to display the last 50 lines of the PON Controller log:

```
[xr-vm_node0_RP0_CPU0:~]$ docker logs pon_ctlr --tail 50
Example Output:
2024-06-03 06:32:59.372 PonCntl System Status
{
"ac:89:d2:c4:d2:00": {
"OLT State": "Primary",
"ONU Active Count": 1,
"ONUs": {
"TBIT94eac0bb": "Registered"
}}}
```

```
2024-06-03 06:48:02.906 PonCntl System Status
{
"ac:89:d2:c4:d2:00": {
"OLT State": "Primary",
"ONU Active Count": 1,
"ONUs": {
"TBIT94eac0bb": "Registered"
}}}
[xr-vm_node0_RP0_CPU0:~]$
```

This output provides the recent activity and status messages from the PON Controller's logs, which can be used to assess the system's current state.

Confirming Discovery of OLT

Verify that the PON Controller has discovered the OLTs and ONUs is critical to maintaining a fully operational PON network.

Run the following command to filter the log for entries related to the total number of controllers, OLTs, and ONUs discovered:

```
[xr-vm_node0_RP0_CPU0:~]$ docker logs pon_ctlr | grep "Total Controllers"
```

Example:

```
2024-02-15 10:34:47.009 INFO PonCntl Total Controllers: 1 OLTs: 0 ONUs: 0
2024-02-15 10:35:02.745 INFO PonCntl Total Controllers: 1 OLTs: 2 ONUs: 1
2024-03-02 14:06:17.379 INFO PonCntl Total Controllers: 1 OLTs: 2 ONUs: 0
```

The log messages with **Total Controllers** indicate the discovery and status of OLTs and ONUs by the PON Controller.

Monitoring Resource Usage of PON Controller Container

Monitor the CPU and memory usage of the PON Controller Docker container is necessary to ensure optimal performance and to prevent potential resource-related issues.

To check the container's resource usage, execute the following command:

```
[xr-vm_node0_RP0_CPU0:~]$ docker stats
```

Example:

```
CONTAINER ID        NAME        CPU %       MEM USAGE / LIMIT     MEM %       NET I/O
    BLOCK I/O       PIDS
9707d990b21f        pon_ctlr    26.39%      189.6MiB / 11.97GiB   1.55%       0B / 0B
    1.2TB / 0B      95
```

The output provides real-time statistics on CPU and memory usage, helping administrators to manage and allocate resources efficiently.

Accessing the PON Controller Docker Container

Access to the PON Controller Docker container's shell to perform direct operations or troubleshooting within the container.

To log into the container's bash shell, issue the following command:

```
[xr-vm_node0_RP0_CPU0:~]$ docker exec -it pon_ctlr bash
```

Note After logging in, the logs can be found in the `/var/log/tibit/` directory.

Transferring Logs from Docker Container to Router Hard Disk

Transfer log files from the Docker container to the router's hard disk may be necessary for thorough analysis or off-device troubleshooting.

Execute the command below to copy the specified log file from the Docker container to the router's hard disk:

```
[xr-vm_node0_RP0_CPU0:~]$ docker cp pon_ctlr:/var/log/tibit/umtPcap.tgz /harddisk:/
```

Retrieving the Path to the Container's Log File

Locate the complete log file path for the PON Controller Docker container may be required to access detailed log data for debugging purposes.

To view the complete path to the container's log file, use the following command:

```
[xr-vm_node0_RP0_CPU0:~]$ docker inspect --format='{{.LogPath}}' pon_ctlr
```

This output shows the full path to the Docker container's log file, enabling administrators to find and review the comprehensive log data.

The PON Controller isn't visible in the PON Manager, or the PON Controller is offline

1. Ensure that the router NTP configuration is up and running and the time reported on the node is accurate.

   The steps to configure an NTP server might differ depending on the router model. For steps to configure an NTP server, refer to the appropriate guide.

   - For NCS 5500 or NCS 5700 routers, refer to *Configuring Network Time Protocol* in the *System Management Configuration Guide for Cisco NCS 5500 Series Routers*.
   - For NCS 540 routers, refer to *Synchronize Router Clock with NTP Server* in *System Setup and Software Installation Guide for Cisco NCS 540 Series Routers*.

2. Verify that the Linux Networking configuration is present using the **`show running-config linux networking`** command.

   Example:

   ```
   Router#show running-config linux networking
   Thu Jun  6 06:39:21.206 UTC
   linux networking
   vrf default
   address-family ipv4
   default-route software-forwarding
   source-hint default-route interface MgmtEth0/RP0/CPU0/0
   !
   !
   !
   ```

   The steps to configure Linux Networking might differ depending on the router model. For steps to configure Linux Networking, refer to the appropriate guide.

- For NCS 5500 or NCS 5700 routers, refer to *Packet I/O on IOS XR* in *Application Hosting Configuration Guide for Cisco NCS 5500 Series Routers*.
- For NCS 540 routers, refer to *Setup the Linux Network for Application Hosting* in *Application Hosting Configuration Guide for Cisco NCS 540 Series Routers.*

3. Verify whether the PON Manager is pingable from the Docker using the **bash ping <IP Address>** command.

   Example:

   ```
   Router#bash ping 190.0.2.0
   ```

4. Verify that the VRF used for PON management connectivity is configured correctly using the **show running-config vrf <vrf-name>** or **show vrf <vrf-name>** commands.

   Example:

   ```
   RP/0/RP0/CPU0:router#show running-config vrf vrf1001
   Thu Jun 13 06:09:56.621 UTC
   vrf vrf1001
   address-family ipv4 unicast
   import route-target
   1001:1001
   !
   export route-target
   1001:1001
   !
   !
   address-family ipv6 unicast
   import route-target
   1001:1001
   !
   export route-target
   1001:1001
   !
   !
   !
   ```

   Example:

   ```
   RP/0/RP0/CPU0:ios#show vrf vrf1001
   Thu Jun 13 06:07:46.215 UTC
   VRF                  RD                  RT                          AFI   SAFI

   vrf1001              1.1.1.5:0

   import  1001:1001           IPV4  Unicast

   export  1001:1001           IPV4  Unicast

   import  1001:1001           IPV6  Unicast

   export  1001:1001           IPV6  Unicast
   ```

5. More troubleshooting can be done on the L3 management path between the router and the PON Manager using the **bash netstat -an | grep 27017** command.

The PON Controller container isn't running after the software upgrade or system reload

1. Ensure that the **pon-ctlr** configuration is present using the **`show running-config pon-ctrl`** command.

Example

```
RP/0/RP0/CPU0:router#show running-config pon-ctlr
Mon Jun  3 06:42:43.616 UTC
pon-ctlr
cfg-file harddisk:/PonCntlInit2411MTBDHCPTest2.json vrf default
!
```

2. Ensure that the correct **.json** file is used to activate the container. For more information on the .json file, refer to Activating the PON Controller.
3. Ensurethat the values in the **.json** file match those configured during Activating the PON Controller.

ONU isn't visible in the PON Manager

1. Click **MGMT** > **Unnamed** > **PON controller** > **OLT** in the PON Manager.
2. Go to **Ports** > **PON**.

   Ensure that **PON**is enabled on the **OLT**and that the **FEC** configuration matches on the OLT and the ONU.
3. Go to the **Monitoring** > **Logs** pane to view the OLT logs from the PON Manager to check for any ONU-specific alarms. You can also check that the PON Controller docker logs directly into the Router.
4. Check whether the OLT and ONU power levels are as expected using a power meter, and reduce attenuation if needed.

OLT and ONU aren't visible in the PON Manager

1. Ensure that the router has LLDP configuration enabled. Run the **show running-config lldp** command to view the LLDP configuration for the OLT port.

   Example

   ```
   RP/0/RP0/CPU0:router#show running-config lldp
   Thu Jun 13 06:00:54.179 UTC
   lldp
   !
   ```
2. Check if the 4090 subinterface is up and confirm that the VLAN 4090 is configured for the OLT using the **show interface tenGigE <interface number>.4090** command.

   Example

   ```
   RP/0/RP0/CPU0:router#show interfaces tengigE 0/0/0/39.4090
   Thu Jun 13 05:57:57.360 UTC
   TenGigE0/0/0/39.4090 is up, line protocol is up
   Interface state transitions: 7
   Hardware is VLAN sub-interface(s), address is 0032.1742.1427
   Internet address is Unknown
   MTU 1518 bytes, BW 10000000 Kbit (Max: 10000000 Kbit)
   reliability 255/255, txload 0/255, rxload 0/255
   Encapsulation 802.1Q Virtual LAN, VLAN Id 4090,  loopback not set,
   Last link flapped 6w6d
   Last input never, output never
   Last clearing of "show interface" counters 14w5d
   5 minute input rate 0 bits/sec, 0 packets/sec
   5 minute output rate 0 bits/sec, 0 packets/sec
   0 packets input, 0 bytes, 0 total input drops
   0 drops for unrecognized upper-level protocol
   ```

```
Received 0 broadcast packets, 0 multicast packets
0 packets output, 0 bytes, 0 total output drops
Output 0 broadcast packets, 0 multicast packets

RP/0/RP0/CPU0:router#
```

3. Troubleshoot the L2 control path between the OLT and the PON Controller using the **show spp node-counters | in PON** command.

Note This command is applicable from XR 24.2.1 release onwards.

Example

```
RP/0/RP0/CPU0:router#show spp node-counters | in PON
Wed Jun 12 05:15:57.560 UTC
PON:            7082
RP/0/RP0/CPU0:router#
```

4. For any OLT-specific information or alarms, check the PON Controller logs.

Traffic isn't flowing in one OLT and ONU Link, or traffic drops seen at the end device

1. Ensure that the correct OLT is connected to the correct ONU and the on-premise device is connected to the correct ONU.
2. Verify that the latest firmware is used in the OLT (4.0) and ONU. For the firmware upgrade procedure, refer to the Cisco PON Manager User Guide.
3. Verify the Statistics in the PON Manager for the OLT and ONU ethernet statistics.

   In the PON Manager, click on **MGMT** > **Unnamed** > **PON controller** > **OLT** > **ONU** > **Monitoring** > **stats**.
4. Compare the ONU and OLT statistics with the router interface.
5. If the router's main interface receives the traffic and not the relevant subinterface, it could be a VLAN tag-related issue.
6. If the drops are not in the PON network, you can troubleshoot in the router and in the Network-to-Network Interface (NNI) network.

OLT Firmware Upgrade Failure

The firmware upgrade process for the OLT does not complete successfully.

Solution:

Verify that the firmware file is named correctly according to the expected format, such as "R4.0.0." A mismatch in the file name can cause the upgrade process to fail.

OLT Firmware Bank Upgrade Failure

The upgrade of the firmware bank on the OLT fails.

Solution:

Ensure that the NNI firmware file is named accurately, following the required naming convention, for instance, "R4.0.0". An incorrect file name can lead to an unsuccessful upgrade.

Inability to Clear PON Statistics in the PON Manager

Attempts to clear PON statistics in the PON Manager do not yield the expected results, and the statistics remain unchanged.

Solution:

Use the **Clear** option to reset the selection and clear the PON statistics. This action should remove the current statistical data as intended.

PON Web UI Pane Selection Lost After Window Switch

The previously selected pane is not retained when navigating away from the PON web UI and returning.

Solution:

Reconfigure the settings in the PON web UI to restore the desired selection. This may involve reselecting the pane or saving the configuration to maintain the selection state between window switches.

Incorrect ONU to OLT Mapping in PON Manager Web GUI

The PON Manager Web GUI incorrectly reports the mapping of ONUs to the OLT, which is observed only with older versions of the PON Manager.

Solution:

Refresh the PON Manager interface to correct the display of the ONU to OLT mapping. If the problem persists, consider updating to a newer version of the PON Manager that addresses this issue.

PON Manager Validation

1. Verify that the MongoDB TCP Port 27017 is open. If you are using a non-standard port for the MongoDB, verify it is open/listening using **`netstat -tunl`**.

Note The standard MongoDB TCP port is 27017.

Example

```
rpon@rpon-mgr:~/PON_MANAGER_SIGNED_CCO/R4.0.0-Cisco-UB2004-sign/R4.0.0-Cisco-UB2004$
netstat -tunl
Active Internet connections (only servers)
Proto Recv-Q Send-Q  Local Address        Foreign Address State
tcp   0      0       127.0.0.53:53        0.0.0.0:*       LISTEN
tcp   0      0       127.0.0.1:27017      0.0.0.0:*       LISTEN
tcp   0      0       10.122.140.232:27017 0.0.0.0:*       LISTEN
```

2. Verify the **`mongod.conf`** file is accurate, and has the correct IP listed under **`bindIP`** parameter.

Note The MongoDB configuration file is located at `/etc/mongod.conf`.

Example

```
rpon@rpon-mgr:~/PON_MANAGER_SIGNED_CCO/R4.0.0-Cisco-UB2004-sign/R4.0.0-Cisco-UB2004$ cat
 /etc/mongod.conf
# mongod.conf

storage:
dbPath: /var/lib/mongodb
journal:
enabled: true

systemLog:
destination: file
logAppend: true
path: /var/log/mongodb/mongod.log
logRotate: reopen

# network interfaces
net:
port: 27017
bindIp: 127.0.0.1,10.122.140.232

processManagement:
pidFilePath: /var/run/mongodb/mongod.pid
timeZoneInfo: /usr/share/zoneinfo

replication:
replSetName: "rs0"
.
.
.
```

System-level logs for each service are managed within Linux. These logs are stored within the `/var/log` directory, under these folders:

- **MongoDB logs**: `/var/log/mongod/mongod.log`
- **Apache logs**: `/var/log/apache2/<filename>.log`
- **Virtual Machine Syslog**: `/var/log/syslog`