

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`