Cisco Cloud Native Broadband Router Diagnosis

The Cisco cnBR provides a suite of in-built tools to diagnose and resolve common issues.

Cable Modem Diagnosis Tool

In a Data-over-Cable Systems Interface Standard (DOCSIS) environment, various elements can affect a modem's ability to maintain a connection and remain online. When a cable modem goes offline, it is difficult to diagnose the cause and identify the issues.

The Cisco cnBR includes a Cable Modem Diagnosis Tool to enable easy diagnosis of such issues. Checkpoints are created periodically for online modems, where information such as system logs, configuration details, and system statistics are saved. When a cable modem goes offline, this system information is analyzed from the saved checkpoints.

The Cable Modem Diagnosis Tool supports the following modes:

- **On-demand mode**: System logs related to a modem is collected with a single click, when needed.

- **Background mode**: Logs, health metrics and performance metrics are actively analyzed in the background to detect, diagnose, and report modem issues.

The Cable Modem Diagnosis Tool provides the following utilities:

- Detect malfunctioning modems.

- Enable debugging for malfunctioning modems and disable debugging when modems are recovered.

- Supports interactive enabling or disabling of per modem debugging.

- Display modem logs and telemetry on the Grafana dashboard.

- Download of modem logs containing modem log messages.

Configure Cable Modem Diagnosis Tool for On-Demand Diagnosis

On-Demand diagnosis allows debugging a cable modem from the **cnBR Manager Metrics & Dashboards** dashboard. On-Demand diagnosis does not require any configuration changes. You can run the On-Demand diagnosis from the **cnBR Manager Metrics & Dashboards** dashboard.

Complete the following steps to enable On-Demand Diagnosis:

Step 1   On the Cisco Operations Hub, click **cnBR Manager** > **Metrics & Dashboards** > **Home**.

Step 2   On the Dashboards pane, search and click **Cable Modem Verbose** option.

Step 3   Select the Cisco cnBR name and modem that you want to debug from the **cnBR Name** and **Cable Modem** drop-down lists.

Step 4   Click **Cable Modem Log From cnBR**.

Step 5   Click **Debug**.

Step 6   Click **Disable** to disable debugging.

Configure Cable Modem Diagnosis Tool for Background Diagnosis

The Background diagnosis utility runs periodically, and detects malfunctioning modems. The utility runs automatically in the background, and is enabled by default.

Using the Background diagnosis method, debug functions that collect modem logs are enabled. Complete the following steps to view the logs:

Step 1   On the Cisco Operations Hub, click **cnBR Manager** > **Metrics & Dashboard**.

Step 2   Click the name of the dashboard to bring up the search box.

Note   You can find the name of the dashboard in the top left of the screen. In the **Metrics & Dashboard** home page, the dashboard name is **Home**.

Step 3   Choose **cnBR Manager** > **Diagnosis**.

The debugging information is available in the **Diagnosis Job Summary**, **cnBR Debug CMD Control**, and **Cable Modem Online Anomaly Detection Job** tables.

Step 4   To view detailed information about these tables, expand the tables and click the **i** icon at the top-left corner.

Cable Modem Troubleshooting

Table 1: Feature History

Feature Name	Release Information	Feature Description
Cable modem troubleshooting	Cisco cnBR 20.3	The Cisco Operations Hub allows you to collect troubleshooting information for cable modems on-demand. You can also retrieve troubleshooting information that the Cisco Operations Hub automatically collects when it detects L3 ping failure.
Per-CM debugging through a single location	Cisco cnBR 20.4	The Cisco Operations Hub allows you to get more cable modem debug information from Cisco cnBR.

This section describes how to:

- Collect troubleshooting information for cable modems on-demand.

- Retrieve troubleshooting information that the Cisco Operations Hub automatically collects when it detects L3 ping failure.

The cnBR Manager gathers troubleshooting information from the Cisco cnBR on-demand and automatically. L3 ping failure detection triggers automatic gathering of troubleshooting information. The troubleshooting information includes a task ID, the cable modem MAC address, and results. Results include troubleshooting information that the cnBR Manager collects from different cnBR services. Troubleshooting information is saved in the debug_info field of the logs. Currently you can receive troubleshooting information for Ranging, Vector Packet Processor (VPP), Baseline Privacy Interface (BPI), Ping, and Data Plane Vector Packet Processor (DP-VPP).

On-Demand Generation of Troubleshooting Information

To generate on-demand troubleshooting information, complete the following steps:

Step 1   Click **Cisco Operations Hub** > **cnBR Manager** > **Metrics & Dashboard**.

Step 2   On the Dashboards pane, click **Cable Modem Verbose**.

Step 3   Click **Troubleshoot**.

Wait for the **Troubleshoot** button to turn from **In Progress..** to **Save**.

Step 4   Click **Save** to save the **TroubleshootingLogs-<mac-address>.txt** file.

Example:

The following example is a sample output file: **troubleshootingLogs-0053.5577.190c.txt**

```
{
        "data": {
            "id": "f5d7fdd6-628b-4da8-917f-2487e3b8a640",
            "cm_mac": "0053.5577.190c",
            "result": {
                "root_cause_analysis": "",
                "details": [
                    {
                        "service_name": "vswitch-vpp",
                        "root_cause": "",
                        "debug_info": {
                            "log": "All interfaces are up"
                        }
                    },
                    {
                        "service_name": "cmts-cp-bpi",
                        "root_cause": "",
                        "debug_info": {
                            "well_known":
"{\"MacAddrStr\":\"0053.5577.190c\",\"SvcGrpID\":0,\"MacDomainID\":0,\"PrimSID\":3,\"BpiCurrKeySeq\":1,
 \"BpiNextKeySeq\":2,

\"BpiOddKey\":\"ZbFZ/JfHIm4Hr+hZuD+j3Q==\",\"BpiOddIV\":\"efW3mAAKUwBBpjYtVC25Pw==\",
\"BpiEvenKey\":\"n6IfiC3JLxeV4LF5vOWA4g==\",
                                        \"BpiEvenIV\":\"SqqQOTaXpHVJi2D62Ci0ZQ==\"}"
                        }
                    },
                    {
                        "service_name": "cmts-rt-ranging",
                        "root_cause": "",
                        "debug_info": {
                            "show_cmd": "{\"Ping
Results\":[{\"Id\":\"8f30cf6e-39cd-4a3b-a159-2f8816bd8580\",\"Create Time\":\"2020-12-03
00:04:29.751224356
                            +0000 UTC m=+5253.045291365\",\"SG ID\":0,\"MD ID\":0,\"MAC
```

Addr\":\"0053.5577.190c\",\"US Channel ID\":2,\"Repeat\":5,\"Verbose\":true,
\"Done\":true,\"Hit\":5,\"Results\":[{\"Result\":\"!\",\"Time
Elapsed\":18,\"Timinge Adjust\":1,\"Power Adjust\":0,\"Frequency Adjust\":583},
{\"Result\":\"!\",\"Time Elapsed\":14,\"Timinge Adjust\":1,\"Power
Adjust\":50,\"Frequency Adjust\":598},{\"Result\":\"!\",\"Time Elapsed\":12,
\"Timinge Adjust\":1,\"Power Adjust\":0,\"Frequency
Adjust\":561},{\"Result\":\"!\",\"Time Elapsed\":13,\"Timinge Adjust\":1,
\"Power Adjust\":0,\"Frequency Adjust\":585},{\"Result\":\"!\",\"Time
Elapsed\":46,\"Timinge Adjust\":1,\"Power Adjust\":0,\"Frequency Adjust\"
:571}]]},{\"Id\":\"47474871-00fb-42fd-ba31-002c52b4ebc6\",\"Create
Time\":\"2020-12-03 00:04:29.751182788 +0000 UTC m=+5253.045249807\",
\"SG ID\":0,\"MD ID\":0,\"MAC Addr\":\"0053.5577.190c\",\"US Channel
ID\":3,\"Repeat\":5,\"Verbose\":true,\"Done\":true,\"Hit\":5,\"Results\"
:[{\"Result\":\"!\",\"Time Elapsed\":18,\"Timinge Adjust\":0,\"Power
Adjust\":0,\"Frequency Adjust\":-7},{\"Result\":\"!\",\"Time Elapsed\":13,
\"Timinge Adjust\":0,\"Power Adjust\":-50,\"Frequency
Adjust\":9},{\"Result\":\"!\",\"Time Elapsed\":12,\"Timinge Adjust\":0,
\"Power Adjust\":-50,\"Frequency Adjust\":2},{\"Result\":\"!\",\"Time
Elapsed\":13,\"Timinge Adjust\":0,\"Power Adjust\":-50,
\"Frequency Adjust\":-12},{\"Result\":\"!\",\"Time Elapsed\":46,\"Timinge
Adjust\":0,\"Power Adjust\":0,\"Frequency Adjust\":2}]]},{\"Id\":
\"ddb18370-d5b7-4063-9041-4b943bbcd0ab\",\"Create Time\":\"2020-12-03
00:04:29.751212482 +0000 UTC m=+5253.045279492\",\"SG ID\":0,\"MD ID\":0,
\"MAC Addr\":\"0053.5577.190c\\",\"US Channel
ID\":1,\"Repeat\":5,\"Verbose\":true,\"Done\":true,\"Hit\":5,\"Results\":[{\"Result\":\"!\",
\"Time Elapsed\":18,\"Timinge Adjust\":0,\"Power Adjust\":0,\"Frequency
Adjust\":415},{\"Result\":\"!\",\"Time Elapsed\":13,\"Timinge Adjust\":0,
\"Power Adjust\":0,\"Frequency Adjust\":419},{\"Result\":\"!\",\"Time
Elapsed\":12,\"Timinge Adjust\":0,\"Power Adjust\":0,\"Frequency Adjust\"
:424},{\"Result\":\"!\",\"Time Elapsed\":14,\"Timinge Adjust\":0,\"Power
Adjust\":0,\"Frequency Adjust\":368},{\"Result\":\"!\",
\"Time Elapsed\":47,\"Timinge Adjust\":0,\"Power Adjust\":0,\"Frequency
Adjust\":424}]]},{\"Id\":\"b5273f03-5d79-4fe6-b8d3-0b054019357f\",
\"Create Time\":\"2020-12-03 00:04:29.751218964 +0000 UTC
m=+5253.045285972\",\"SG ID\":0,\"MD ID\":0,\"MAC Addr\":\"0053.5577.190c\",
\"US Channel
ID\":0,\"Repeat\":5,\"Verbose\":true,\"Done\":true,\"Hit\":5,\"Results\":[{\"Result\":\"!\",\"Time
Elapsed\":18,
\"Timinge Adjust\":0,\"Power Adjust\":0,\"Frequency
Adjust\":251},{\"Result\":\"!\",\"Time Elapsed\":14,\"Timinge Adjust\":0,\"Power Adjust\"
:0,\"Frequency Adjust\":270},{\"Result\":\"!\",\"Time
Elapsed\":11,\"Timinge Adjust\":0,\"Power Adjust\":0,\"Frequency Adjust\":283},
{\"Result\":\"!\",\"Time Elapsed\":13,\"Timinge Adjust\":0,\"Power
Adjust\":0,\"Frequency Adjust\":275},{\"Result\":\"!\",\"Time Elapsed\"
:47,\"Timinge Adjust\":0,\"Power Adjust\":0,\"Frequency Adjust\":234}]}]}",

"well_known":
"{\"MacAddrIeee\":\"ACUuLXJ+\",\"SvcGrpID\":0,\"MacDomainID\":0,\"PrimSID\":3,\"MacState\":25,\"MD-DS-SG-ID\":1,

\"MD-US-SG-ID\":1,\"RngTxchList\":[{\"UsChID\":3,\"RngQueue\":\"STATION_MIN_Q\",\"RngTxchState\":\"TXCH_ST_STA_MIN\",\"RngPwrLevelReported\"

:132,\"RngDynPwrWindow\":72,\"RngTxchSNR\":451850,\"RngTxchDataMER\":16777215},{\"UsChID\":1,\"RngQueue\":\"STATION_MIN_Q\",\"RngTxchState\"

:\"TXCH_ST_STA_MIN\",\"RngPwrLevelReported\":132,\"RngDynPwrWindow\":72,\"RngTxchSNR\":420410,\"RngTxchDataMER\":16777215},{\"UsChID\":0,

\"RngQueue\":\"STATION_MIN_Q\",\"RngTxchState\":\"TXCH_ST_STA_MIN\",\"RngPwrLevelReported\":130,\"RngDynPwrWindow\":74,\"RngTxchSNR\"

:420410,\"RngTxchDataMER\":16777215},{\"UsChID\":2,\"RngQueue\":\"STATION_MIN_Q\",\"RngTxchState\":\"TXCH_ST_STA_MIN\",

```
\"RngPwrLevelReported\":129,\"RngDynPwrWindow\":75,\"RngTxchSNR\":420410,\"RngTxchDataMER\":16777215}]}"

                              }
                    },
                    {
                        "service_name": "cmts-ping",
                        "root_cause": "",
                        "debug_info": {
                            "log":
"{\"minRtt\":17,\"maxRtt\":65425,\"avgRtt\":289,\"sent\":240,\"received\":240,\"MAC
Addr\":\"0053.5577.190c\",
                                    \"CmMacIeee\":\"ACUuLXJ+\",\"SvcGrp\":0,\"MacDomain\":0}",
                            "well_known":
"{\"MacAddrStr\":\"0053.5577.190c\",\"MacAddrIeee\":\"ACUuLXJ+\",\"SvcGrpID\":0,\"MacDomainID\":0}"
                        }
                    },
                    {
                        "service_name": "cmts-dp-macl3vpp-global",
                        "root_cause": "",
                        "debug_info": {
                            "show_cmd": "{\"drop_stats\":{\"name\":\"Global Drop
Stats\",\"per_cause_drops\":[{\"id\":11,\"cause\":\"icpi_inject__bad_cause\"},

{\"id\":27,\"cause\":\"dbl_fld_no_members\"},{\"id\":56,\"cause\":\"dsmac__invalid_sg\"}]},\"usmac_depi_stats\":{\"data_pw_uepi_pkt_cnt\"

:298,\"data_pw_uepi_byte_cnt\":42822,\"rng_pw_uepi_pkt_cnt\":56,\"rng_pw_uepi_byte_cnt\":9408,\"uepi_phy_burst_cnt\":354,\

"total_ccf_seg_cnt\":298,\"ccf_seg_no_hcserr_cnt\":298,\"pre30_doc_no_hcserr_cnt\":56,\"sm_rng_good_pkt_cnt\":56}}"

                        }
                    },
                    {
                        "service_name": "cmts-dp-macl3vpp-per-cm",
                        "root_cause": "",
                        "debug_info": {
                            "show_cmd":
"{\"dtrack_stats\":{\"dtrack_mac_addr\":\"00:25:2e:2d:72:7e\",\"dtrack_time_start\":1606953869,\"dtrack_time_stop\":1606953990,

\"dtrack_epoch_in\":3,\"dtrack_epoch_curr\":3,\"dtrack_us_input\":248,\"dtrack_us_xmit\":248,\"dtrack_ds_input\":248,\"dtrack_ds_xmit\":248},

\"srv_flow_stats\":[{\"id\":3,\"direction\":\"US\",\"pkts_cnt\":248,\"bytes_cnt\":15792,\"duration_seconds\":120,\"throughput_pps\":1050},

{\"id\":10003,\"direction\":\"DS\",\"pkts_cnt\":248,\"bytes_cnt\":15280,\"duration_seconds\":120,\"throughput_pps\":1016}]}"

                        }
                    }
                ]
            }
        },
        "status": 200,
        "config": {
            "method": "GET",
            "transformRequest": [
                null
            ],
            "transformResponse": [
                null
            ],
```

```
                "jsonpCallbackParam": "callback",
                "url": "https://opshub1.cisco.com/api/manager/v1/cable-modems/0053.5577.190c/debug",
                "headers": {
                    "Accept": "application/json, text/plain, */*"
                }
            },
            "statusText": "OK",
            "xhrStatus": "complete"
        }
```

Automatic Generation of Troubleshooting Information

When the cnBR Manager detects a cable modem ping failure, the cnBR Manager generates a request to get troubleshooting information from the Cisco cnBR. cnBR Manager stores the troubleshooting information responses that it receives from the Cisco cnBR.

Step 1   Click **Cisco Operations Hub** > **cnBR Manager** > **Metrics & Dashboard**.

Step 2   On the Dashboards pane, search and click **Cable Modem Verbose** option.

Step 3   In the **Cable Modem** drop-down list, select the target cable modem MAC address.

This page lists the occurrences of L3 ping loss with timestamp.

Modem IP Ping-Loss History		
Time ▾	RTT	IP Loss
2020-10-16 18:14:29	-	100.0%
2020-10-16 18:12:29	-	100.0%
2020-10-16 18:11:29	-	100.0%
2020-10-16 18:09:29	-	100.0%

1   2   3   4   5   6   7   8   9

521235

Note   You can view the top ten modems with IPv4 ping-loss from the **Top 10 IPv4 Ping-Loss Modems** panel in the **Service Group** dashboard. To view the **Service Group** dashboard, click **cnBR Manager** > **Service Group**.

Step 4   Open the following link in a browser, or use the curl command to send a GET request.

```
https://<hostname>/opshub-data/api/idocsis/v1/idm/cm-debug/tasks
```

Find the target cable modem using the MAC address to get the troubleshooting information.

Example:

```
https://opshub1.cisco.com/opshub-data/api/idocsis/v1/idm/cm-debug/tasks
```

Or

```
hostname#curl -k -L -X GET 'https://opshub1.cisco.com/opshub-data/api/idocsis/v1/idm/cm-debug/tasks'
```

See example in Step 3 for a sample response.

Step 5 Find the target cable modem MAC address, and ping failure timestamp from the information to get troubleshooting information for the ping failure.

Example:

In the following example, we can see the debug result for the cable modem 0053.2ed0.84a6.

Figure 1: JSON Data from a Cisco cnBR Response

Note If time zone settings are different, the time that is displayed in the cnBR Manager interface and the time in the Cisco cnBR response are different. The time stamp in the Cisco cnBR response is always in Greenwich Mean Time (GMT).

Cisco cnBR Metrics

The **Metrics** tab in the cnBR Manager application allows you to monitor the status of the Cisco cnBR router. The cnBR Manager receives metrics and telemetry data from Cisco cnBR. Based on the type of data, the data is saved in the Postgres or Prometheus databases. The Metrics dashboard later retrieves the data and displays it on the dashboard.

The following illustration shows the Metrics framework.
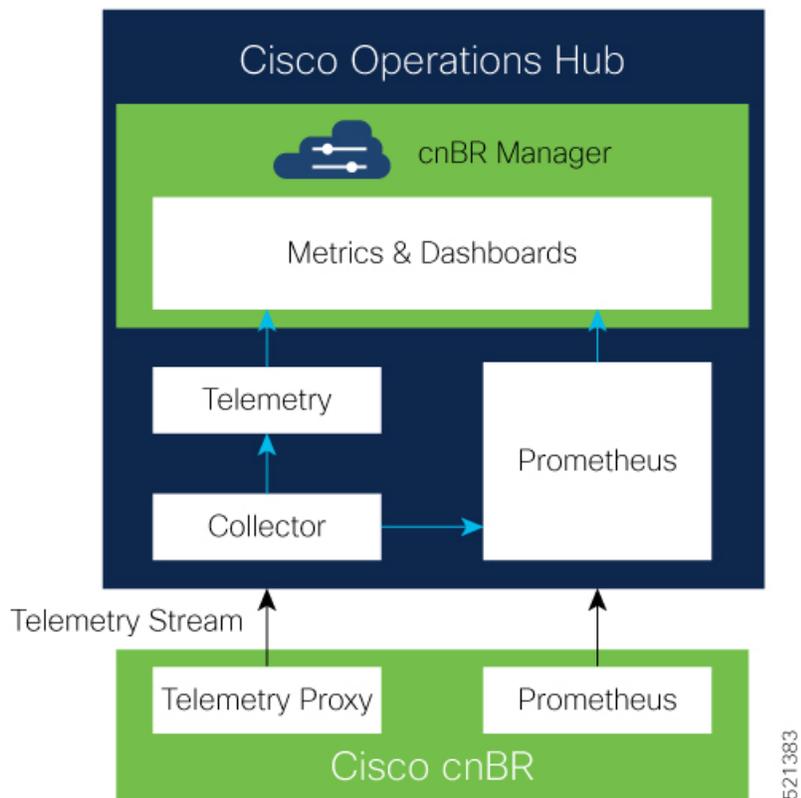
Cisco cnBR Metrics Dashboards

The Metrics Grafana dashboard displays metrics and status of the DOCSIS network, DOCSIS devices, and CMTS performance status. The Metrics dashboard is based on a hierarchical structure, which matches the Cisco cnBR system deployment exactly.

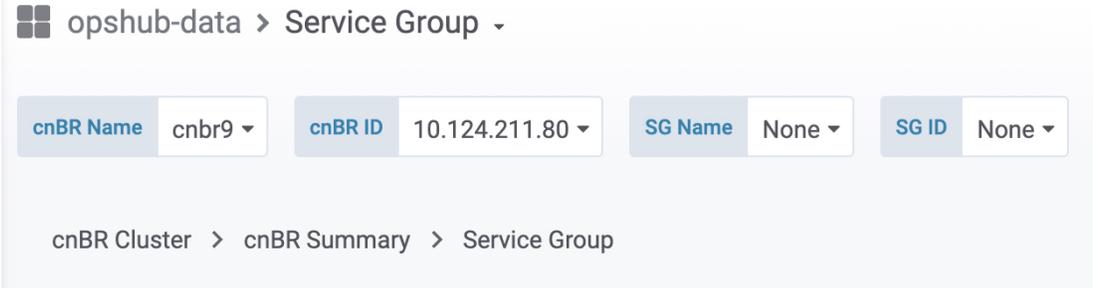The following illustration shows the hierarchical layout:
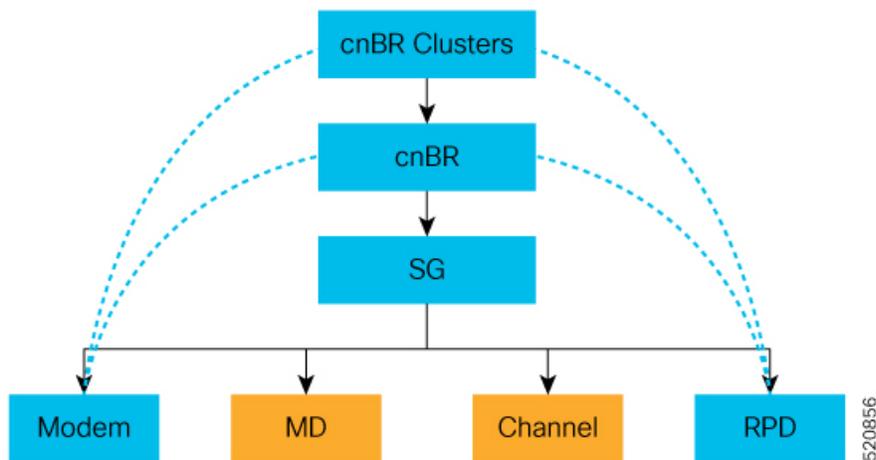
The Metrics Dashboard user interface (UI) has the following components:

Breadcrumbs Bar

The breadcrumbs bar is available on each dashboard. It shows the dashboard pages just visited. You click each link in the breadcrumbs and go to that specific dashboard.

Links

Links are marked using an underline. You click the underlined text and open the related page.
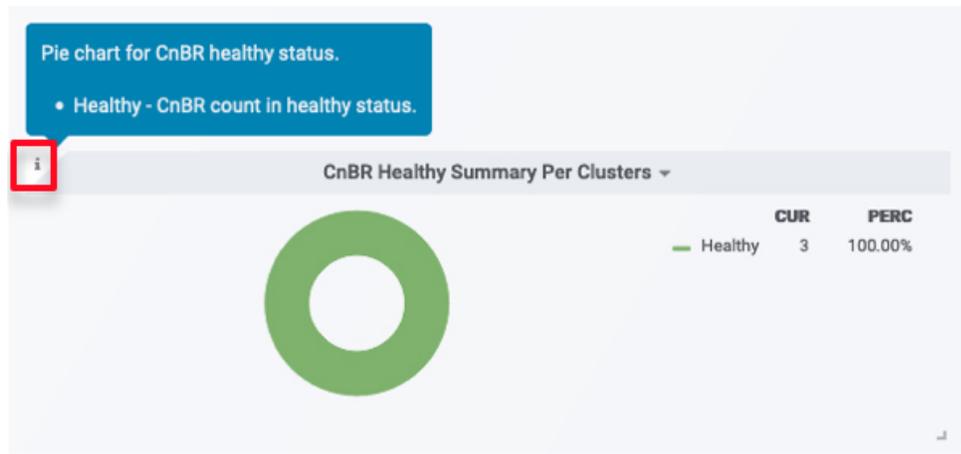

Tooltips

Tooltips are available on the dashboard to display information for each panel on the Grafana dashboard. To view a tooltip, hover your mouse over the `i` on the top-left corner of the panel.
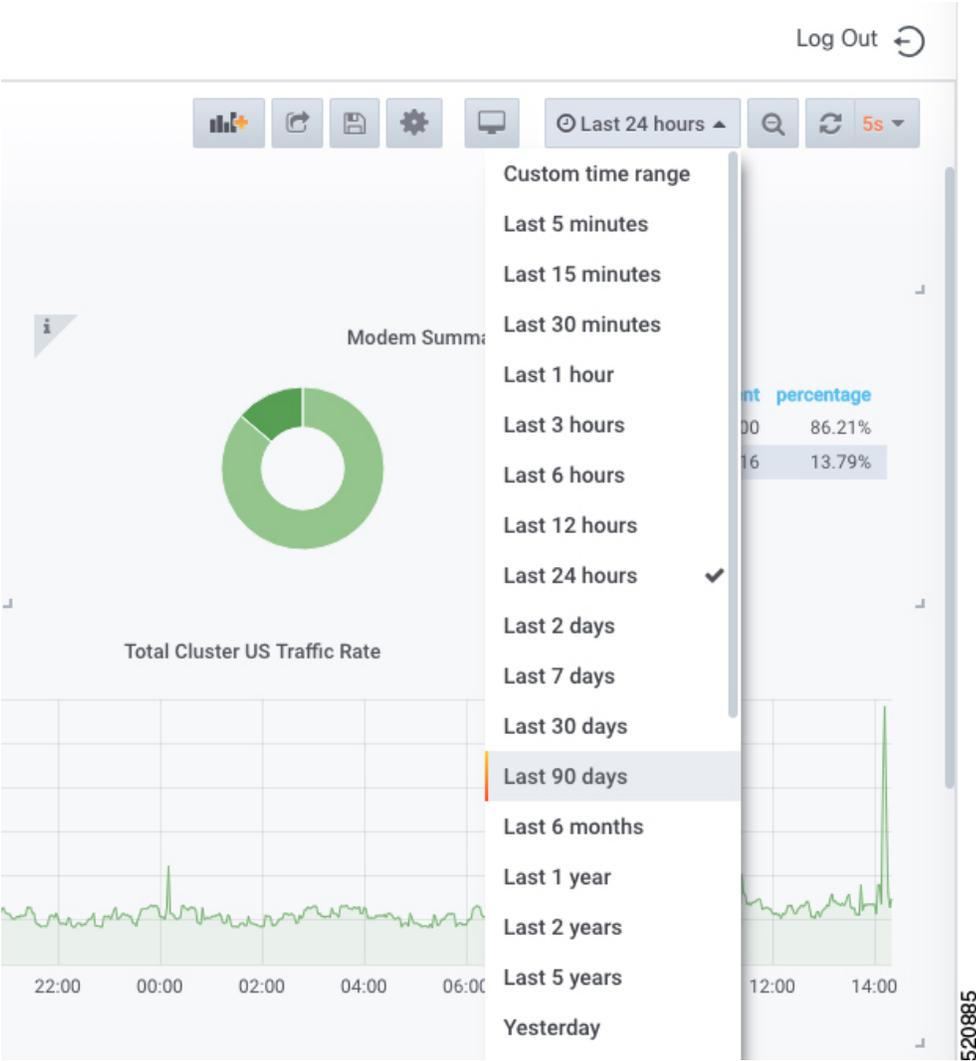
Dashboard Refresh and Time Range

To set the refresh time for each dashboard, choose the time from the drop-down list on the top-right corner of the dashboard. The default refresh time for the dashboard is 10 seconds.
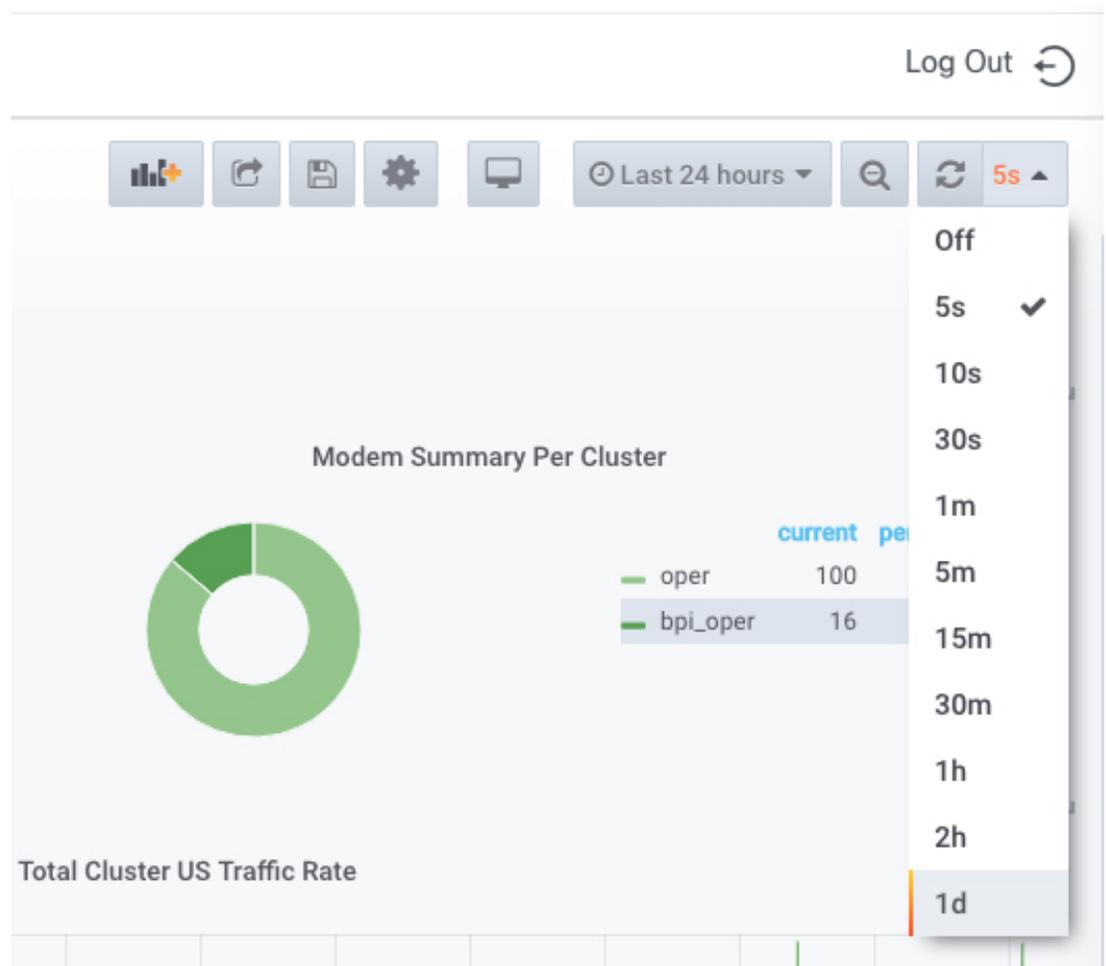
If data is retrieved from the Prometheus database, choose the required value from the **Custom time range** drop-down list as shown in the following image.

Data Display on Dashboard

For all dashboards available in the Cisco cnBR Manager application, data is represented using pie charts, tables, and live graphs.
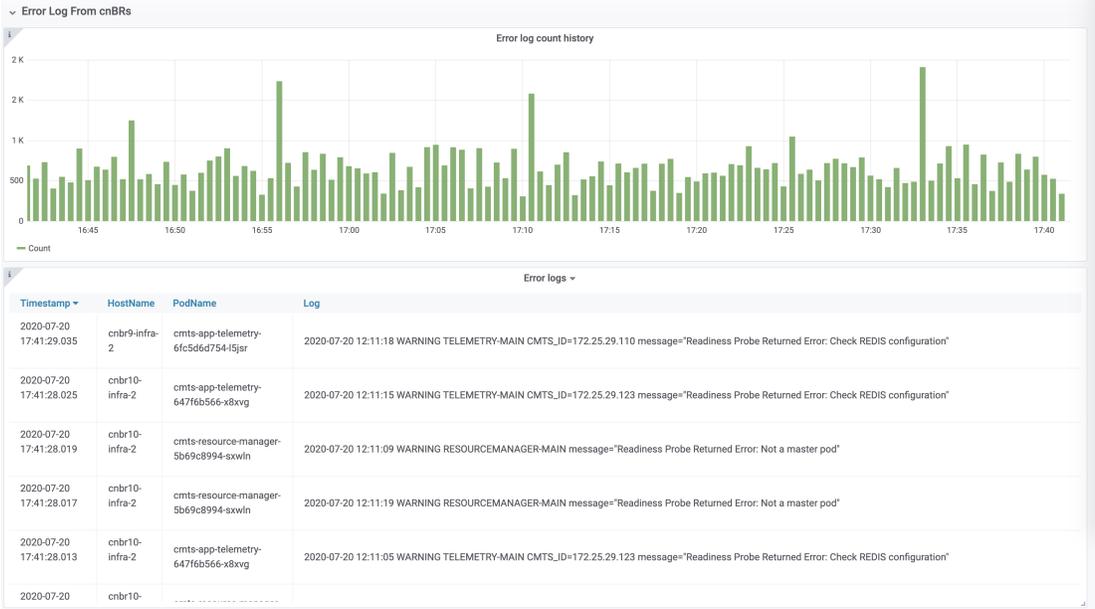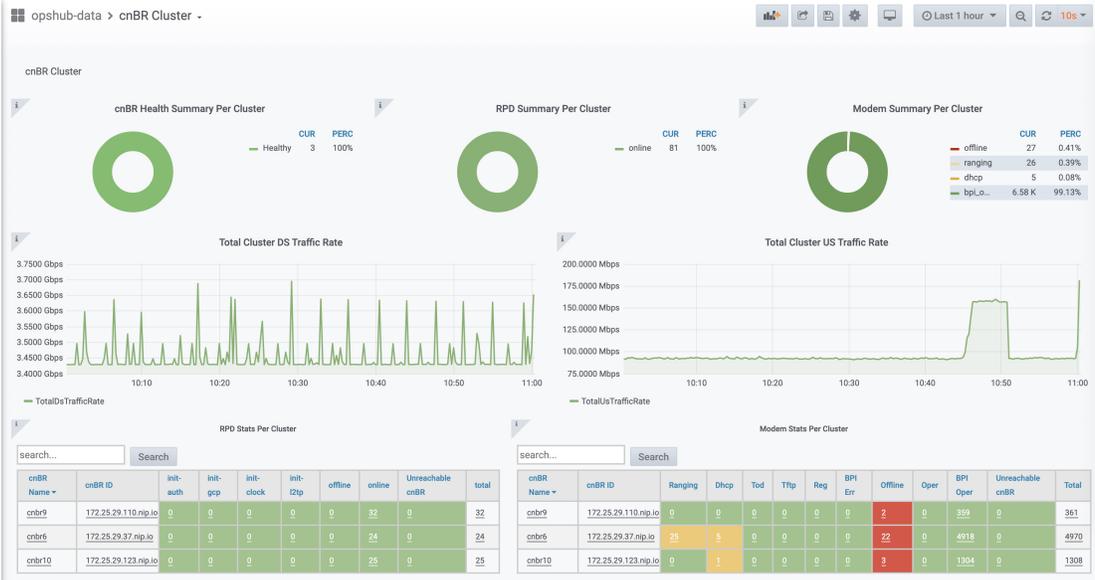
cnBR Cluster

This Dashboard displays the following information:

Panel Name	Description
cnBR health status	The pie chart shows Cisco cnBR performance status for each Cisco cnBR cluster.

Panel Name	Description
Remote-PHY device (RPD) status	The pie chart shows the status of RPDs in each Cisco cnBR cluster.
Cable Modem status	The pie chart shows the status of cable modems in the Cisco cnBR cluster.
Summary of downstream traffic rate for all cnBR clusters	The graph shows how much download happened in the set time.
Summary of upstream traffic rate for all cnBR clusters	The graph shows how much upstream traffic happened in the set time.
Summary of RPDs in different states per cnBR cluster	The table shows how many RPDs are offline or online, and the following details: • cnBR Name: Name of the cluster • cnBR ID: The IP address to reach the Cisco cnBR router. • init-auth: Authorization status of the RPD • init-gcp: GCP provision status • init-clock: Clock synchronization status • init-l2tp: L2VPN provisioning status • total: Total number of RPDs in the cluster
Summary of modems in different states per cnBR cluster	The table shows a summary of the status of cable modems in the cluster, including the following details: • Ranging: Number of ranging requests received. • DHCP: Number of DHCP requests received. • ToD: Time-of-Day (ToD) requests received. • TFTP: Number of TFTP requests received. • Reg: Number of registration requests (REG-REQ) or multipart registration request (REG-REQ-MP) received. • BPI Err: Number of Baseline Privacy Interface (BPI) errors even if the cable modem is registered. • Offline: Number of modems which are offline. • Oper: Number of cable modems which are registered without enabling BPI. • BPI Oper: Number of cable modems with BPI.
Error log count history for all cnBR clusters	The live graph shows the history of the number of error logs generated for all Cisco cnBR clusters.

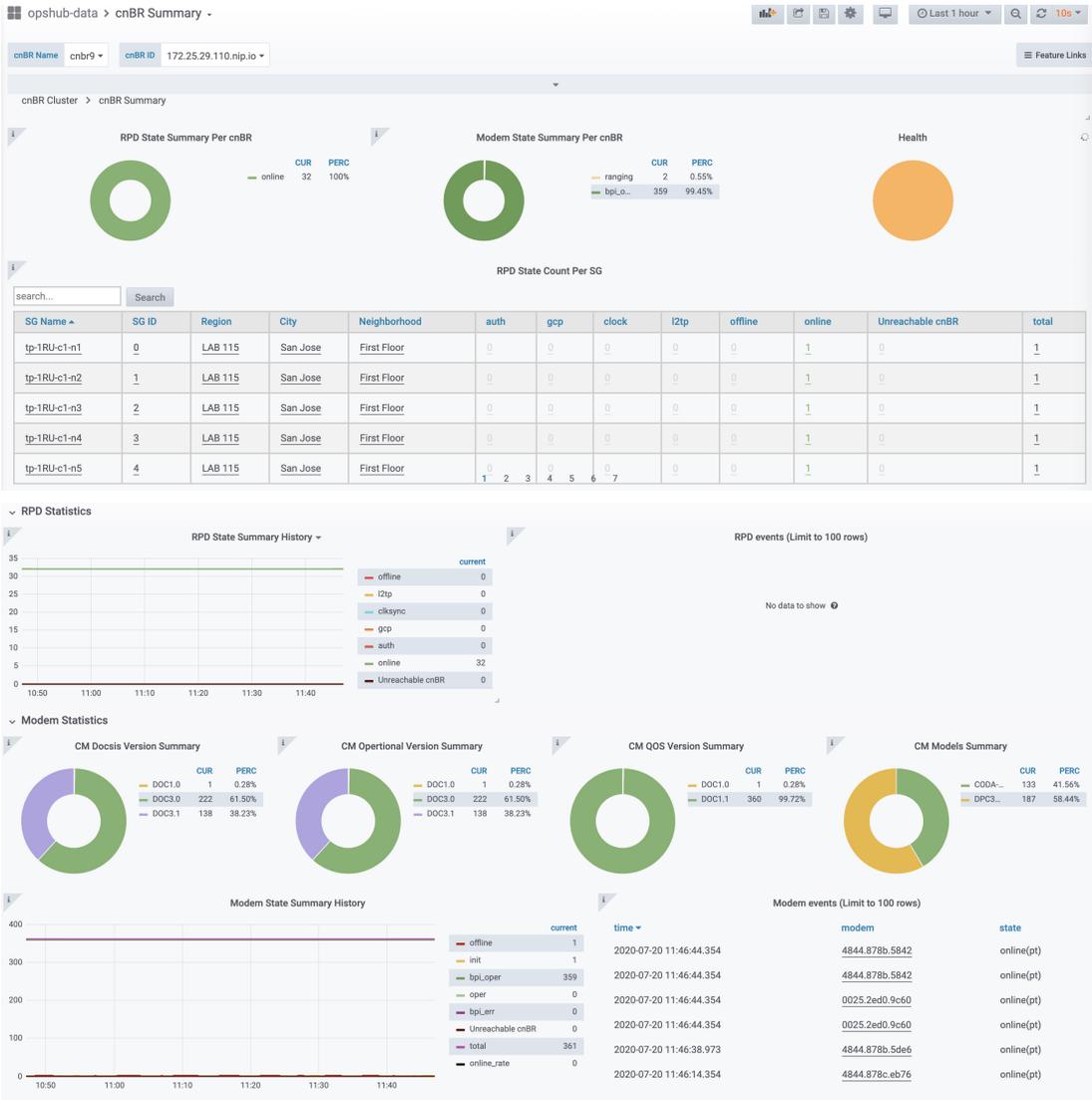| Panel Name	Description
Error logs from all cnBR clusters	The live graph shows the error logs generated for all Cisco cnBR clusters.

cnBR Summary

The Dashboard displays the following information:

Panel Name	Description
RPD state summary per cnBR	The pie chart shows a summary of RPDs in different states under the current Cisco cnBR cluster: • online: Online state • init(l2tp): Layer Two Tunneling Protocol (L2TP) provision • init(clksync): Clock sync • init(gcp): GCP provision • init(auth): Authorization • offline: Offline state
Modem state summary per cnBR	The pie chart shows a summary of modems in different states under the current Cisco cnBR cluster: • oper: Modem that is registered without BPI enabled • bpi_oper: Modem that is registered with BPI enabled • bpi_error: Modem that is registered but BPI error • reg: REG-REQ or REG-REQ-MP was received • tod: TOD request received • tftp: Trivial File Transfer Protocol (TFTP) request received • dhcp: DHCP request received • ranging: Ranging request received • offline: Offline state
RPD state count per SG	The table provides a summary of RPDs in different states per service group: • SG_ID: Service group id • auth: init(auth) state, authorization • gcp: init(gcp) state, GCP provision • clock: init(clksync) state, clock sync • l2tp: init (L2TP) state, L2TP provision • offline: offline state • online: online state

Panel Name	Description
Modem state count per SG	Summary of modems in different states per service group: • SG_ID: Service group ID • ranging: Ranging request received • tod: TOD request received • dhcp: DHCP request received • tftp: TFTP request received • reg: REG-REQ or REG-REQ-MP was received • bpi_err: Modem that is registered but BPI error • offline: Offline state • oper: Modem that is registered without BPI enabled • bpi_oper: Modem that is registered with BPI enabled
Traffic statistics for all service Groups	Shows traffic statistics for the following: • DS Service Group Traffic Rate • US Service Group Traffic Rate
RPD statistics	History summary of RPDs in different stats
RPD Events	Latest 100 RPD state change events
Modem Statistics	• CM DOCSIS version summary • CM Operational version summary • CM QoS version summary • CM models summary
Modem state summary history	Summary history of modems in different states
Modem Events	Latest 100 modem state change events

Panel Name	Description
Modem List	A detailed modem state information list. Use the Search text box to filter modems by the MAC address, IPv4 address, or IPv6 address. The number of rows in the Modem List table is limited to 256. The total is the total number of modems that are filtered by clusterIp and the search text. • Cable Modem: MAC address of the cable modem • IPv4: IPv4 address of the cable modem • IPv6: IPv6 address of the cable modem • State: State of the cable modem • SG: Service group ID of the cable modem • MD: MAC domain ID of the cable modem • Online Time: Last time when the cable modem transitioned to online • Offline Time: Last time when the cable modem transitioned to offline • Last Update: Last time when the entry was updated.

Service Group

The Dashboard displays the following information:

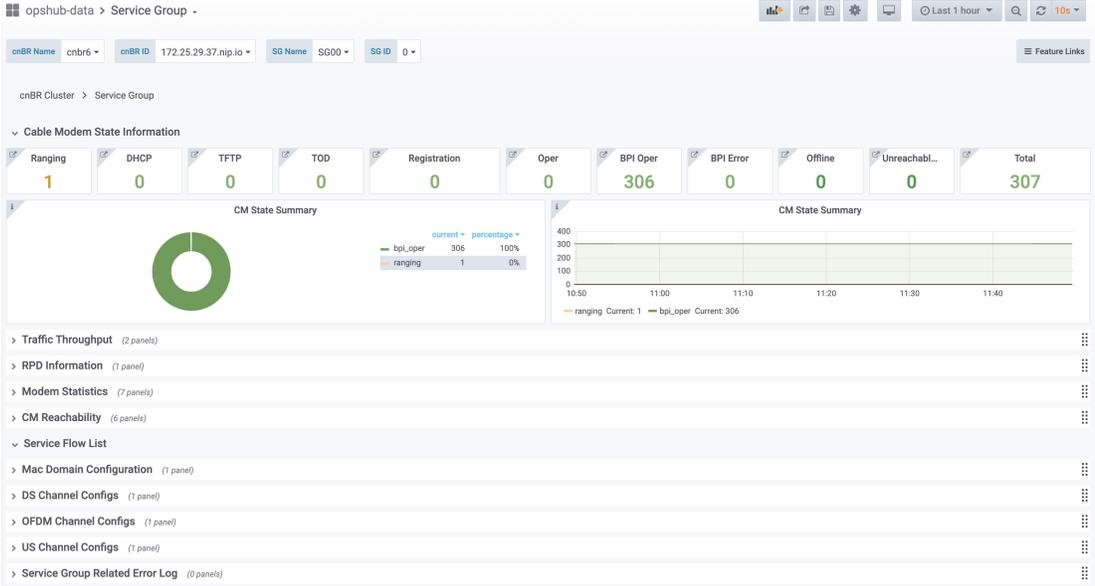| Panel Name	Description
Cable modem status information	This section shows a summary of the status of cable modems in the specified service group by using a pie chart, a live graph, and the number of modems available with each service: • Ranging: Number of ranging requests received • DHCP: Number of DHCP requests received • TFTP: Number of TFTP requests received • ToD: Time-of-Day (ToD) requests received • Registration: Number of registration requests (REG-REQ) or multipart registration request (REG-REQ-MP) received • Oper: Number of cable modems that are registered without enabling BPI • BPI Oper: Number of cable modems with BPI • BPI Error: Number of Baseline Privacy Interface (BPI) errors even if cable modem is registered • Offline: Number of modems that are offline • Unreachable: Number of modems that are unreachable
Traffic throughput information	Shows the traffic throughput for a selected service group. Provides two live graphs: • DS Traffic Throughput • US Traffic Throughput

Panel Name	Description

RPD information	The table shows a list of RPDs of this service group.
	
	• MAC Address: MAC address of the RPD, link to RPD Verbose page.
	
	• Name: Name of the RPD.
	
	• SG Name: Service group name of the RPD.
	
	• Service Group: Service group ID of the RPD.
	
	• IPv4 Address: IPv4 address of the RPD.
	
	• IPv6 Address: IPv6 address of the RPD.
	
	• State: State of the RPD.
	    • online
	    • offline
	
	• Role: Role of the RPD.
	    • principal
	    • auxiliary
	
	• cnBR ID: cnBR cluster ID of the RPD.
	
	• Online Timestamp: Timestamp when the RPD is online.

Modem Statistics	This section contains pie charts for the following summaries: • CM DOCSIS version summary • CM QoS version summary • CM OperVer summary • CM models summary • Online CM Summary on Primary DS Chan • Online CM Summary per TCS and US Chan

Panel Name	Description
Modem Table	Cable modem table for selected service group. • Cable Modem: MAC address of the cable modem. • IPv4: IPv4 address of the cable modem. • IPv6: IPv6 address of the cable modem. • State: State of the cable modem. • SG: Service group of the cable modem. • MD: MAC domain of the cable modem. • SID: Service ID of the cable modem. • DS Count: Downstream channel count of the cable modem. • US Count: Upstream channel count of the cable modem • CPE Count: CPE count of the cable modem • Online Time: Timestamp when the modem online • Offline Time: Timestamp when the cable modem offline. You can do the following from this window: • Reset: Reset the modems in the list. • Delete: Delete the modems in the list.
CM Reachability	Displays a graph and a table for the cable modems which are not reachable.

Panel Name	Description

Service Flow List	The **Downstream Service Flow List** and **Upstream Service Flow List** tables provide the following details:
	
	• SF ID: Service Flow ID.
	
	• CableModem: MAC address of the modem.
	
	• Stage: Stage of service flow:
	
	  • PRE_REGISTRATION: Service flow is provisioned before REGISTRATION.
	
	  • REGISTRATION: Service flow is provisioned in REGISTRATION.
	
	• Frame Type:
	
	  • PRE_D30: Pre-3.0 DOCSIS concatenation and fragmentation.
	
	  • CCF_ON: Continous Concatenation and Fragmentation is enabled.
	
	  • CCF_OFF: Continous Concatenation and Fragmentation is disabled.
	
	• State: State of service flow
	
	  • Prov: Service flow is in provision.
	
	  • Adm: Service flow is in admit.
	
	  • Active: Service flow is active.
	
	  • Type: Primary, Secondary
	
	  • MdID: MAC Domain ID of the modem.
	
	  • SgId: Service group ID of the modem.

MAC domain configuration	MAC domain configuration. • MAC Domain: MAC domain ID. The link opens the CMTS Mac Domain page. • cnBR: cnBR cluster. • Service Group ID: Service group ID. • Primary DS channels: Primary downstream channels for this MAC domain. • US channels: Upstream channels for this MAC domain.

Panel Name	Description

DS channel configs	Downstream channel configuration.
	
	• downstream channel ID: Downstream channel ID
	
	• annex: Annex of the downstream channel
	
	    • AnnexA
	
	    • AnnexB
	
	• frequency: Frequency of the downstream channel
	
	• modulation: Modulation of this downstream channel
	
	    • qam64
	
	    • qam256
	
	• interlevel: Interlever of the downstream channel
	
	• poweradjust: Power adjustment of the downstream channel.

OFDM channel configs	OFDM channel configuration. • ofdm chan id: OFDM channel ID • startfrequency: Start frequency • width: Width of the OFDM channel • plc: PHY Link Channel. • rolloff: Rolloff of the OFDM channel • profilencp: Profile Next Codeword Pointer • cyclicprefix: Cyclicprefix of the OFDM channel. • pilotScaling: Pilot Scaling • profiilecontrol: Profile control • interleaverdepth: Interlever depth • subcarrierspacing: Subcarrier Spacing • profiles: Link to OFDM Channel Profile Data page.

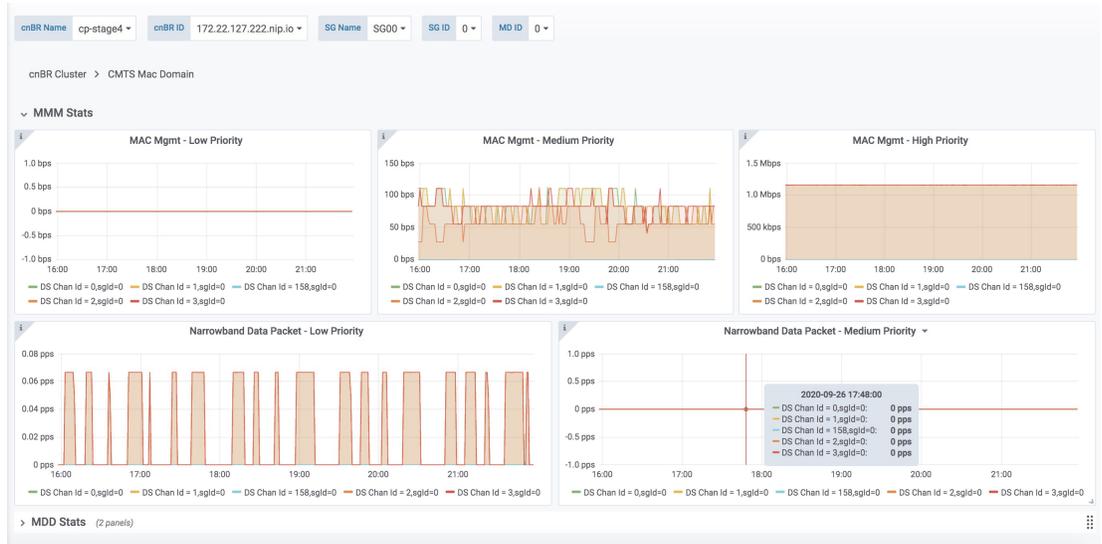| Panel Name	Description
US channel configs	Upstream channel configuration. • upstream channel id: Upstream channel ID • slotsize: Minislot size • frequency: Frequency • docsismode: DOCSIS Mode • modulation: Modulation profile • powerlevel: Power level • channelwidth: Channel width • sgid: Service group ID

CMTS MAC Domain

The Dashboard displays the following information:

Panel Name	Description
MMM stats	Rate history of MAC management messages.
MDD stats	Rate history of MDD.

DS Channel

The Downstream (DS) Channel dashboard displays the following information:

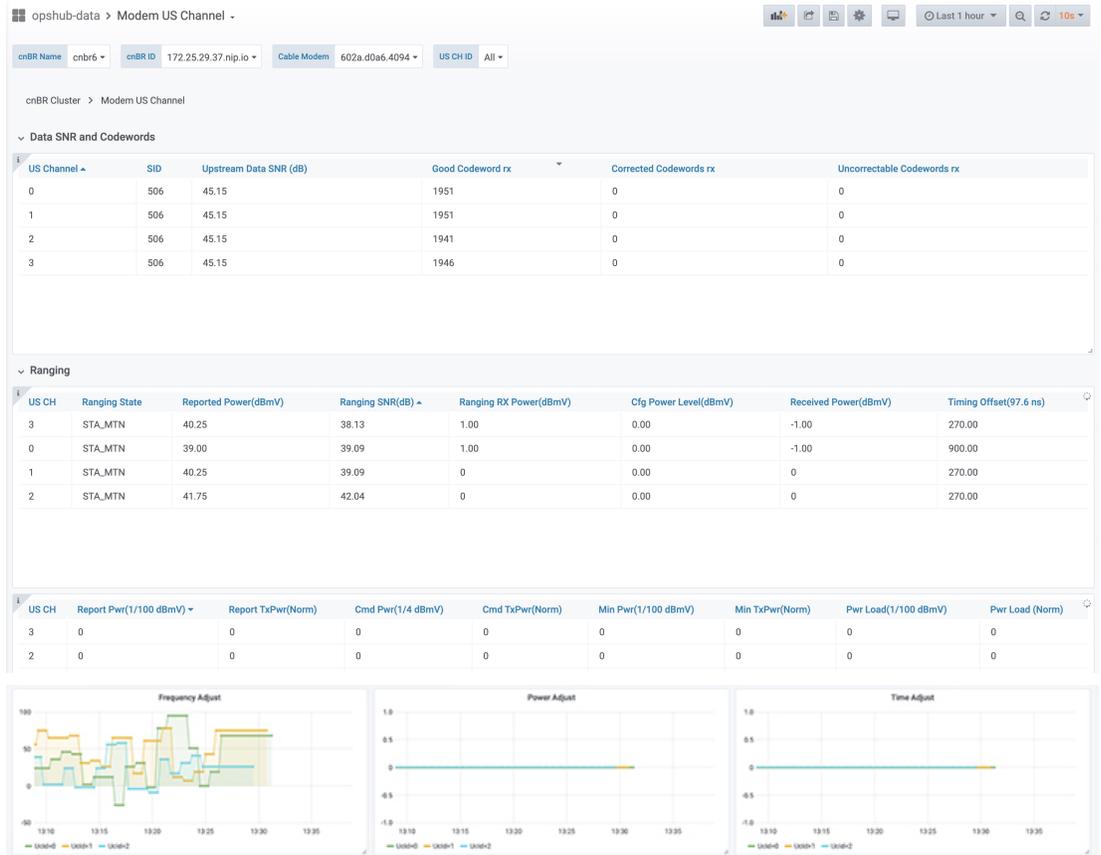| Panel Name	Description
Modem state	Summary of modems in different states for the specific Cisco cnBR cluster.
Count	Downstream channel count of the cable modem.
Rate	Downstream traffic rate for the Cisco cnBR cluster.
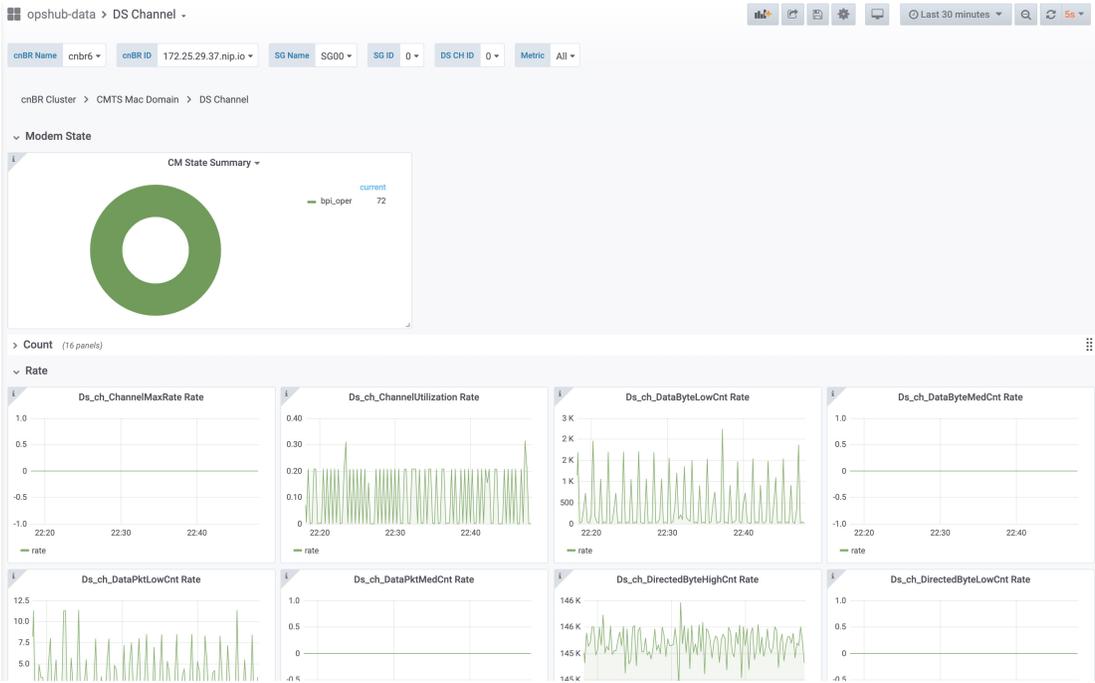
Modem US Channel

The Dashboard displays the following information:

Panel Name	Description
Data SNR and Codewords	SNR and Codeword information of the upstream channel for the cable modem.
Ranging	Ranging information of cable modems.

520887

520888

Modems List

The Dashboard displays all CMs in a list, based on the cluster, SG ID, MD, and the status:

Panel Name	Description
Download CSV	Download CSV for online and offline modems. You can download the CSV for one Cisco cnBR cluster at a time. A single CSV file for all clusters is not available for downloading.

Panel Name	Description
Modem List	Detailed modem state information list. Use the Search text box to filter modems by MAC address, IPv4 address, or IPv6 address. The number of rows in the Modem List table is limited to 256. Total is the total number of modems that are filtered by clusterIp and the search text. • Cable Modem: MAC address of the cable modem • IPv4: IPv4 address of the cable modem • IPv6: IPv6 address of the cable modem • State: State of the cable modem • SG Name: Service group name of the cable modem • SG: Service group ID of the cable modem • MD: MAC domain ID of the cable modem • cnBR ID: Cloud CMTS ID • SID: Service ID of the cable modem • DS Count: Downstream channel count of the cable modem • US Count: Upstream channel count of the cable modem • CPE Count: CPE count of the cable modem • Online Time: Time stamp when the modem became online • Offline Time: Timestamp when the cable modem transitioned to offline • Last Update: Last time when the entry was updated

Cable Modem Verbose

The Dashboard displays the following information:

Panel Name	Description
Modem Basic Info	Basic information about the cable modem.
Modem RNG Info	Ranging information of the cable modem.
Modem OFDM Info	OFDM information of the cable modem.
Modem Other Info	Additional information of the cable modem: • DOCSIS Version: DOC1.0, DOC1.1, DOC2.0, DOC3.0, DOC3.1 • Operational Version: DOC1.0, DOC1.1, DOC2.0, DOC3.0, DOC3.1 • QoS Version: DOC1.0, DOC1.1 • Sys Desc: System description • DBC Req Count: Count of DBC(Dynamic Bonding Change) request • DBC Res OK: Count of DBC response with OK • DBC Ack Count: Count of DBC ack • Ext Pktlen Capability: External packet length capability • DS Lowerband Edge: Downstream lower band edge • DS Upperband Edge: Downstream upper band edge • US Upperband Edge: Upstream upper band edge • DTP Mode: DOCSIS time protocol mode • DTP Performance: DOCSIS time protocol performance
Modem State History	History of the cable modem status.

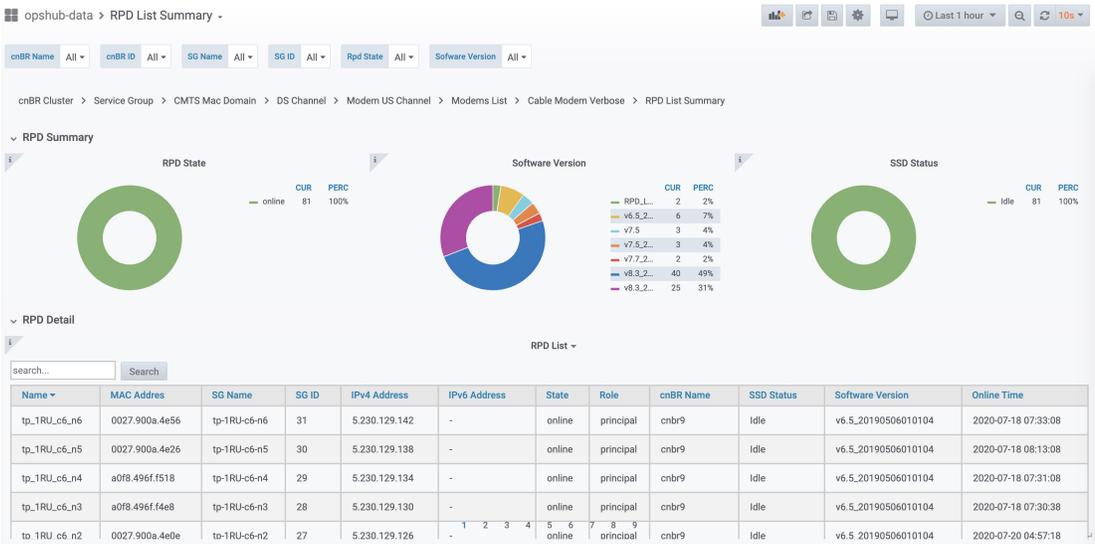| Panel Name	Description
Modem CPE List	CPE list of cable modem. • MAC: CPE MAC address • IP: IP address of the modem • Device Class: CPE device class CPE device class: • EROUTER • EMTA • SMTA • ESTB • EDVA • ECM • EPS
Modem Ping Stats	History of cable modem IP pings.
Service Flow Stats	Shows the details of upstream and downstream service flows.
Channel Stats	You can view the following details: • US CH RNG SNR History: History of upstream channel ranging SNR(Signal Noise Ratio). • US CH RNG RX Power History: History of upstream channel ranging RX power(dBm). • DS CH (RxPwr&SNR) History: History of downstream channel RX power and SNR by remote query. • US CH (TxPwr&TxTimingOffset) History: History of upstream channel TX power and timing offset by remote query. • Modem Timing Offset History: History of upstream channel timing offset of Cisco cnBR side. • Modem Ranging State History: History of upstream channel ranging state.
DBC Event	Shows the details of the Dynamic bonding change (DBC) events.
Resiliency Event	History of upstream resiliency state.

520869

520936

RPD List Summary

The Dashboard displays the following information:

Panel Name	Description
RPD Summary	Shows the following details using pie charts: • RPD state: States of the RPDs in the Cisco cnBR cluster • Software version: Software version running on the RPDs • SSD state: RPD secure software download status

Panel Name	Description

RPD Detail	The table shows details of the RPDs:
	
	• Name: Name of the RPD
	
	• MAC: MAC address of the RPD
	
	• SG: Service group
	
	• SG Name: Service group name of the RPD.
	
	• SG ID: Service group ID of the RPD.
	
	• IPv4 Address: IPv4 address of the RPD.
	
	• IPv6 Address: IPv6 address of the RPD.
	
	• State: State of the RPD.
	
	    • online
	
	    • offline
	
	• Role: Role of the RPD.
	
	    • principal
	
	    • auxiliary
	
	• cnBR Name: Name of the cluster
	
	• SSD state: RPD secure software download status
	
	• Software version: Software version running on the RPDs
	
	• Online Time: RPD online timestamp

opshub-data > RPD List Summary ▾

cnBR Name All ▾ cnBR ID All ▾ SG Name All ▾ SG ID All ▾ Rpd State All ▾ Sofware Version All ▾

cnBR Cluster > Service Group > CMTS Mac Domain > DS Channel > Modem US Channel > Modems List > Cable Modem Verbose > RPD List Summary

RPD Summary

RPD State

	CUR	PERC
online	81	100%

Software Version

	CUR	PERC
RPD_L...	2	2%
v6.5_2...	6	7%
v7.5	3	4%
v7.5_2...	3	4%
v7.7_2...	2	2%
v8.3_2...	40	49%
v8.3_2...	25	31%

SSD Status

	CUR	PERC
Idle	81	100%

RPD Detail

RPD List ▾

search...   Search

Name ▾	MAC Addres	SG Name	SG ID	IPv4 Address	IPv6 Address	State	Role	cnBR Name	SSD Status	Software Version	Online Time
tp_1RU_c6_n6	0027.900a.4e56	tp-1RU-c6-n6	31	5.230.129.142	-	online	principal	cnbr9	Idle	v6.5_20190506010104	2020-07-18 07:33:08
tp_1RU_c6_n5	0027.900a.4e26	tp-1RU-c6-n5	30	5.230.129.138	-	online	principal	cnbr9	Idle	v6.5_20190506010104	2020-07-18 08:13:08
tp_1RU_c6_n4	a0f8.496f.f518	tp-1RU-c6-n4	29	5.230.129.134	-	online	principal	cnbr9	Idle	v6.5_20190506010104	2020-07-18 07:31:08
tp_1RU_c6_n3	a0f8.496f.f4e8	tp-1RU-c6-n3	28	5.230.129.130	-	online	principal	cnbr9	Idle	v6.5_20190506010104	2020-07-18 07:30:38
tp_1RU_c6_n2	0027.900a.4e0e	tp-1RU-c6-n2	27	5.230.129.126	-	online	principal	cnbr9	Idle	v6.5_20190506010104	2020-07-20 04:57:18

1 2 3 4 5 6 7 8 9

520875

RPD Verbose

The Dashboard displays the following information:

Panel Name	Description
Basic information	Shows basic information about the RPD. • MAC: MAC address of the RPD • Name: Name of the RPD • SG: Service group • IPv4: IPv4 address • IPv6: IPv6 address • State: init(auth), init(gcp), init(clksync), init(l2tp), online, offline • GCP State: Generic control plane state • Role: principle, auxiliary • cnBR ID: Cloud CMTS ID • Last State: The previous status of RPD • Last GCP State: The previous generic control plane state • Auth Time: RPD authentication timestamp • Online Time: RPD online timestamp

Panel Name	Description
RPD identification	Shows the basic RPD identification detials. • RPD ID: RPD MAC address • Vendor Name: Vendor name • Vendor ID: Vendor ID • Model Number: Model number of the RPD • Sw Version: Current software version running on the RPD • Boot Rom Sw Version: Boot read-only memory software version • Device Description: Device description • Device Alias: Device alias • Serial Number: Serial number • Rcp Protocol Ver: R-PHY control protocol version • Rpd Rcp Protocol Ver: R-PHY control protocol version • Rpd Rcp Schema Version: R-PHY control protocol schema version • Hw Revision: Hardware revision • Asset Id: Asset ID of the RPD • Vsp Selector: Vendor-Specific Pre-configuration. • Us Burst Receiver Vendor Id: Upstream burst receiver vendor ID • Us Burst Receiver Driver Version: Upstream burst receiver driver version

Panel Name	Description
RPD Capability	

Panel Name	Description
	Shows the basic capabilities.
	• RPD ID: RPD MAC address
	• Bi-direction RF Ports: Bi-directional radio frequency ports
	• DS RF Ports: Downstream radio frequency ports
	• US RF Ports: Upstream radio frequency ports
	• 10G Eth Ports: 10 Gigabit Ethernet port number
	• 1G Eth Ports: 1 Gigabit Ethernet port number
	• DS SC-QAM Channels Per Port: Downstream single carrier quadrature amplitude modulation (qam) channels per port
	• DS OFDM Channels Per Port: Downstream orthogonal frequency division multiplexing (OFDM) channels per port
	• US SC-QAM Channels Per Port: Upstream single carrier QAM channels per port
	• US OFDMA Channels Per Port: Upstream OFDM channels per port
	• DS SCTE-55-1 Channels Per Port: Downstream SCTE-55-1 channels per port
	• US SCTE-55-1 Channels Per Port: Upstream SCTE-55-1 channels per port
	• SCTE-55-2 Modules: SCTE-55-2 Modules
	• US SCTE-55-2 Demodulator Num: Upstream SCTE-55-2 demodulator numbers
	• NDF Channels Per Port: Remote-PHY narrowband digital forward channels per port
	• NDR Channels Per Port: Remote-PHY narrowband digital return channels per port
	• UDP Encapsulation On L2TPv3: User datagram protocol (UDP) encapsulation on layer 2 tunneling protocol version 3
	• DS Distinct PSP Flows: Downstream distinct packet streaming (DPS) protocol flows
	• US Distinct PSP Flows: Upstream DPS protocol flows
	• Asyn MPEG Video Channels Per Port: Asynchronous MPEG video channels per port
	• Flow Tags support capability: Shows whether flow tags support is available or not.

Panel Name	Description
	• Freq Tilt support: Shows whether frequency tilt is supported on the RPD • Range of tilt setting: Range of tilt setting • ucd processing time: RPD upstream channel descriptor processing time • ucd change null grant time: RPD upstream channel descriptor change null grant time • Buffer depth monitor alert support: Buffer depth monitor alert support • Buffer depth config support: Buffer depth monitor configuration support • Multi section timing mer reporting support: Multiple section timing mer reporting support • Max DS Psp Seg Count: Max Downstream packet streaming protocol seg count • Direct DS Flow Queue Mapping: Direct downstream flow queue mapping • DS scheduler PhbId list: Downstream scheduler per hop behavior ID list • Pending EvRep Queue Size: RPD pending event report queue size • Local Event Log Size: RPD local event log size • Supported Optical Node RF: Shows whether optical node radio frequency is supported on the RPD • MAX DS Freq: RPD maximum downstream frequency • MIN DS Freq: RPD minimum downstream frequency • MAX Base Power: RPD maximum base power • MIN Tilt Value: RPD minimum tilt value • MIN Power Adjust for ScQam Chan: RPD minimum power adjust for single carrier quadrature amplitude modulation channels • MAX Power Adjust for ScQam Chan: RPD maximum power adjust for single carrier quadrature amplitude modulation channels • MIN Power Adjust for OFDM Chan: RPD minimum power adjust for orthogonal frequency division multiplexing channels • MAX Power Adjust for OFDM Chan: RPD maximum power adjust for orthogonal frequency division multiplexing channels

Panel Name	Description

Update history	Update history of the previous 50 RPDs.
	
	• MAC Address: MAC address of the RPD
	
	• State: Shows in which state the RPD is functioning:
	
	   • init(auth)
	
	   • init(gcp)
	
	   • init(clksync)
	
	   • init(l2tp)
	
	   • online
	
	   • offline
	
	• GCP State: offline, c1, c2 ready
	
	• TimeStamp: TimeStamp

show cable modem	The table provides basic details of the cable modem.
	
	• Cable Modem: Cable modem MAC address
	
	• IPv4: IPv4 address of the modem
	
	• IPv6: IPv6 address of the modem
	
	• State: Shows in which state the modem is functioning:
	
	   • init(auth)
	
	   • init(gcp)
	
	   • init(clksync)
	
	   • init(l2tp)
	
	   • online
	
	   • offline
	
	• SG: Service group
	
	• MD: MAC domain
	
	• cnBR ID: Cloud CMTS ID
	
	• Online Time: RPD online time
	
	• Offline Time: RPD offline time
	
	• Last Update: Last update time

Panel Name	Description
RPD configuration	The table shows the basic configuration of RPD. • Ds Channel: Downstream channel configuration • DsChan Base Power: Base power of downstream channel • DsChan Admin State: Admin state • Us Channel: Upstream channel configuration • Fiber Node: Fiber node configuration

Search for Dashboards

Follow this procedure to search for dashboards:

Step 1 Choose **cnBR Manager** > **Metrics & Dashboards** from the Cisco Operations Hub main menu.

Step 2 Click the name of the dashboard to bring up the search box.

> **Note** You can find the name of the dashboard in the top left of the screen. In the **Metrics & Dashboards** home page, the dashboard name is **Home**.

Step 3 Enter the dashboard name in the **Search dashboards by name** text field.

Or alternatively, you can click the **cnBR Manager** folder or **cee-data** folder and browse through it.

KPI Alert Management

Table 2: Feature History

Feature Name	Release Information	Feature Description
KPI Alert Management	Cisco cnBR 20.4	Expands the alerts in Subscriber, RF Plant, and Infra KPI Alert categories.

KPIs (Key Performance Indicator) of Cisco cnBR clusters help in getting information on the overall system stability and on the components that are not functioning normally and are impacting the system stability.

The cnBR Manager supports the following KPI Alert categories:

- Subscriber

- RF Plant

- Infra

Subscriber

This KPI Alert category provides an overview of the subscriber health status of the Cisco cnBR cluster. The following parameters are available in this KPI:

- **CMNotHealthyCMState**: If the percentage of online modems is higher than the configured threshold(95%), we can consider this parameter as healthy, otherwise, unhealthy.

- **CMNotHealthyPartialUS**: If the percentage of modems in upstream partial-service mode is less than the configured threshold(10%), we can consider this parameter as healthy, otherwise, unhealthy.

- **CMNotHealthyPartialDS**: If the percentage of modems in downstream partial-service mode is less than the configured threshold(10%), we can consider this parameter as healthy, otherwise, unhealthy.

- **CMNotHealthyPingLoss**: If the ping loss rate is less than the configured percentage threshold(20%), we can consider this parameter as healthy, otherwise, unhealthy.

- **CMNotHealthyPingLatency**: If the ping latency is less than the configured threshold(200 ms), we can consider this parameter as healthy, otherwise, unhealthy.

- **RPDNotHealthy**: If all the RPDs are online, we can consider this parameter as healthy, otherwise, unhealthy.

RF Plant

This KPI Alert category provides an overview of the RF plant health status of the Cisco cnBR cluster. The following parameters are available in this KPI:

- **DSCHNotHealthyMER**: If the primary downstream channel has a Modulation Error Ratio higher than the configured threshold(30 dB), we can consider the channel as healthy, otherwise, unhealthy.

- **USCHNotHealthySNRRanging**: If the primary upstream channel has an upstream ranging Signal to Noise Ratio (SNR) higher than the configured threshold(20 dB), we can consider the channel as healthy, otherwise, unhealthy.

- **USCHNotHealthySNRData**: If the primary upstream channel has a data-SNR higher than the configured threshold(30 dB), we can consider the channel as healthy, otherwise, unhealthy.

- **DSCHPartialNotHealthy**: If the percentage of modems in downstream partial-service mode is less than the configured threshold(10%), we can consider the channel as healthy, otherwise, unhealthy.

- **USCHPartialNotHealthy**: If the percentage of modems in upstream partial-service mode is less than the configured threshold(10%), we can consider the channel as healthy, otherwise, unhealthy.

Infra

This KPI Alert category provides the following information:

- An overview of the pod CPU, memory, and file descriptor usage status of the Cisco cnBR and the Cisco Operations Hub clusters.

- An overview of the node CPU, memory, and disk usage of the Cisco cnBR cluster.

- Cisco cnBR reachability and token refresh status.

The following parameters are available in this KPI:

- **NodeNotHealthyMEMIssue**: If the available memory of a node is higher than the configured threshold(10%), we can consider the node as healthy, otherwise, unhealthy. Available memory is an estimate of the memory available for starting new applications without swapping.

- **NodeNotHealthyCPUIssue**: If the 1-minute CPU load of a node is lower than the configured threshold(90%), we can consider the node as healthy, otherwise, unhealthy.

- **NodeNotHealthyDiskIssue**: If the disk usage of a node is less than the configured threshold(80%), we consider the node as healthy, otherwise, unhealthy.

- **PodNotHealthy**: If all pods of a node are ready, we consider the node as healthy, otherwise, unhealthy.

- **CriticalPodNotHealthy**: If all critical pods(configured in the config map) of a node are ready, we can consider the node as healthy, otherwise, unhealthy.

- **PodNotHealthyHighCPU**: If a pod is consuming fewer CPU cores than the configured limit, we can consider the pod as healthy, otherwise, unhealthy.

- **PodNotHealthyHighMEM**: If a pod is consuming less memory than the configured limit, we can consider the pod as healthy, otherwise, unhealthy.

- **PodNotHealthyTooManyOpenFileDescriptor**: If a pod has less open file descriptors than the configured limit(2048), we can consider the pod as healthy, otherwise, unhealthy.

- **cnBRNotReachable**: If the cnBR host is reachable from the Cisco Operations Hub, we can consider the Cisco cnBR as healthy, otherwise, unhealthy.

- **cnBRRefreshTokenFailure**: If the token refresh is working for a Cisco cnBR host, consider the host as healthy, otherwise, unhealthy.

Alert Management

The cnBR Manager Alert Management is based on the KPIs. Cisco cnBR records all alerts for users to view. You can configure the alert-manager to manage alerts.

Follow this procedure to view the KPI Alert Management page:

Choose **cnBR Manager** > **API Summary** from the Cisco Operations Hub main menu and click **KPI Alert Management** from the left side bar.

Alert Definition

All alerts are built based on the KPI metrics and divided into several alert groups. Each KPI metric generates one alert that belongs to a predefined alert group. For example, KPI metrics: CM state (Summary of CM online state) generates one alert that is named CMNotHealthy, which is part of the Subscriber alert group. The Alert Management supports the following alerts and alert groups.

Group	Alert
Subscriber	• CMNotHealthy • RPDNotHealthy
RF	• USCHNotHealthy • DSCHNotHealthy
Infra	• NodeNotHealthy • PodNotHealthy

Alert Record

Alert Management records all alerts that are generated in the Cisco cnBR router. The dashboards display an alert summary and detailed information about those alerts.

KPI Alert Summary

Alert summary dashboards show the number of current alerts and total resolved alerts. In addition, the dashboards display the distribution of alerts based on severity. Cisco cnBR supports two levels of alerts:

- critical

- warning

You can view this pane on the Cisco cnBR cluster dashboard under **Dashboards** > **Manage** > **cnBR Manager**.
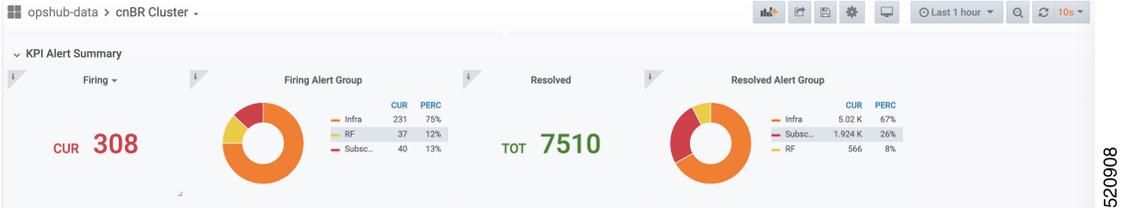
KPI Alert Information

The dashboard shows two lists of Firing Alerts and Resolved Alerts. The following details are available in these tables:

Panel Name	Description
Firing Time	Alert fired time.

Panel Name	Description
Name	Alert name.
Severity	Critical or warning.
cnBR ID	Cisco cnBR where the alert is fired.
Alert Group	Category of the KPI alert.
Acknowledge status	Shows whether acknowledged or not.
Action	Acknowledge or view an alert. Click the **View** link. The **Alert Action** pane on the right side shows the details of the alert.

You can view details and acknowledge firing alerts. For the resolved alerts, you can view the details of each alert.

Acknowledge KPI Alert

You can acknowledge the firing alerts. By default, every three hours, you are notified about the firing alerts by email. You can stop receiving the alert emails by setting the silence time, creator, and comments.
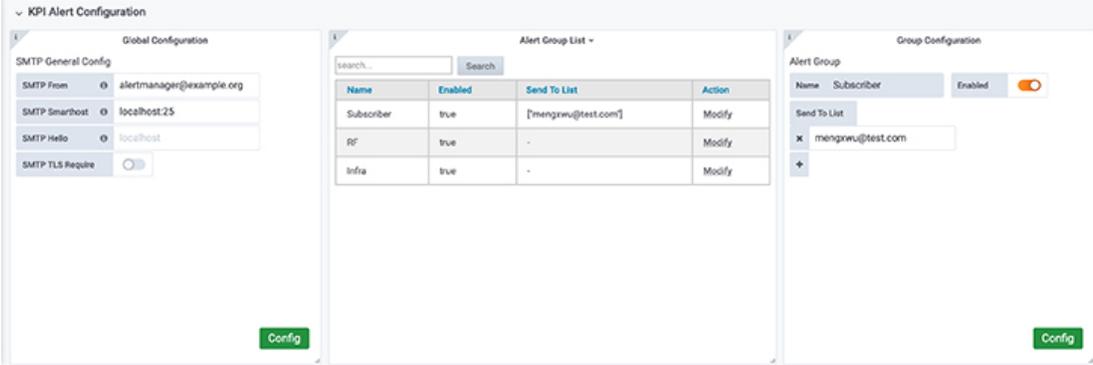
Configure Alerts

You can configure global alerts through Alert Management. For global configuration, update the SMTP (Simple Mail Transfer Protocol) settings. By default, this option is disabled.

On the **Global Configuration** pane, configure the notification channel. The **SMTP General Config** pane is available under the **KPI Global Configuration** pane of the **KPI Alert Configuration** dashboard.

Field	Description
SMTP From	The default **SMTP From** header field.
SMTP Smarthost	The default SMTP smarthost used for sending emails, including the port number. The port number is 25 or 587 for SMTP over TLS (STARTTLS). Example: `smtp.example.org:587`
SMTP Hello	The default hostname to identify to the SMTP server.
SMTP TLS Require	The default SMTP TLS requirement (Default: false).

KPI Alert Configuration

You can enable or disable an alert group and add or delete email addresses of receivers for each alert group. When you enable an alert group and add email addresses, those users are notified when an alert is generated in the respective group.

KPI Alert Email

Monitor and Troubleshoot

The KPI of one Cisco cnBR-Core is displayed on this dashboard.
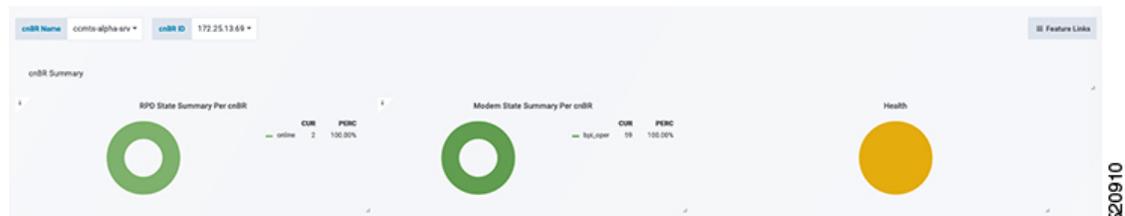
The state of each category is displayed on this dashboard.

This dashboard shows the details of the subscriber.

This dashboard shows the details of the RF.

Log Aggregation and Management

Table 3: Feature History

Feature Name	Release Information	Feature Description
Log Aggregation and Management	Cisco cnBR 21.1	The Cisco Operations Hub provides multiple log aggregation tools, various visualization techniques, and customizations that help you to view, debug, visualize, and customize your log information. The Cisco Operations Hub enables Log Aggregation and Management through the Audit Dashboard, Debug Dashboard, and a host of other utilities.

The Cisco Operations Hub provides the Audit Dashboard, Debug Dashboard, and a host of other utilities for log aggregation and management activities.

By using the various visualization techniques and customizations, you can search, visualize, and create dashboards to have macro and micro views.

Configure Operations Hub for Log Management

The following configuration steps are needed only when the Cisco cnBR is added in Cisco Operations Hub using Cisco Operations Hub UI or API. You can skip this section if you added the Cisco cnBR using Autodeployer.

During deployment, the Cisco Operations Hub is preconfigured to forward logs from all the components to Operations Hub. However, to get the logs forwarded, you must manually configure Cisco cnBR..

To manually configure the Audit Dashboard to receive the Cisco Operations Hub logs, complete the following steps:

Step 1 Log in to the CEE Data OpsCenter CLI. Ensure that you provide a valid Cisco cnBR user ID and password.

https://cli.cee-data-ops-center.*<cnBRIP>*.nip.io

Step 2 Key in these commands at the prompt:

```
logging fluent host fluentd.ccmts-infra
logging fluent port 24224
logging fluent disable-tls true
commit
end
```

Step 3 Log in to Cisco cnBR OpsCenter. Ensure that you provide a valid user ID and password.

https://cli.*<cnBR NameSpace>*-ops-center.*<cnBRIP>*.nip.io

Step 4 Key in these commands at the prompt:

```
logging forward kafka-blockers <OpsHub_IP>
```

```
commit
end
```

Working with Logs

The Cisco Operations Hub provides you with a host of utilities that helps you to view, debug, visualize, and customise your log information.

View Audit Logs

The Audit dashboard leverages Kibana to provide meaningful visualization and a search interface for the raw log data.

You can view the Audit Logs dashboard by completing these steps:

Step 1 Click **Cisco Operations Hub** > **System** > **Logs**.

Step 2 Click **Audit Dashboard**.

The Audit Dashboard provides the following information:

- A visualization of the count of audit logs against time. You can view this as a histogram.

- All user initiated events from UI or using API interface are logged and available as audit logs.

- For every log file, the Audit Dashboard provides the following facets of information:

  - **Time**: The time of logging the event.

  - **User**: The user initiating the event.

  - **API**: The API call used.

  - **Status**: The HTTP response status code that returns when API was called.

  - **Response Time**: The time taken by the API to execute.

  - **Method**: The HTTP method the API used.

  - **Service Host**: The application that served the request.

View Debug Logs

You can view the Debug logs dashboard by completing these steps:

Step 1 Click **Cisco Operations Hub** > **System** > **Logs**.

Step 2 Click **Debug Dashboard**.

The Debug Dashboard provides the following information:

- A visualisation of the count of logs from different components against time is provided as a histogram.

• All internal application events logged by respective services or software components are captured as debug logs.

• For every log file, the Debug Dashboard provides the following facets of information:

　　• **Time**: The time of logging the event.

　　• **Source**: The application where the event happened.

　　• **ContainerName**: The applications microservice that generated the event.

　　• **LogLevel**: The log level.

　　• **Message**: The entire log content.

Discover Logs

The Discover option allows you to search and find logs based on custom search definitions.

You can view the Discover option by completing these steps:

Step 1　　Click **Cisco Operations Hub** > **System** > **Logs**.

Step 2　　Click **Discover**.

Step 3　　Search for the log files.

You can perform basic text search, or advanced search by using KQL (Kibana Query Language) or Lucene search. Alternatively, you can also customize your search query based on time, debug-log type, selected fields, inspect option, and so on.

You can choose to save the search for later use from the dashboard.

Visualize Logs

You can create intuitive visualizations for your log data.

To create a visualization, complete these steps:

Step 1　　Click **Cisco Operations Hub** > **System** > **Logs**.

Step 2　　Click **Visualize** > **Create visualisation**.

Step 3　　Choose one of these visualization type:

• Area

• Control

• Coordinate Map

• Data Table

• Gauge

- Goal

- Heat Map

- Horizontal Bar

- Line

- Markdown

- Metric

- Pie

- Region Map

- TSVB

- Tag Cloud

- Timelion

- Vega

- Vertical Bar

Step 4 Choose a source type. You can choose from `audit-log`, `debug-log`, or `logstash` objects.

You can choose to save the visualizations to generate panels when you Create Dashboards , on page 50.

Create Dashboards

The Dashboard option allows you to create a new dashboard by adding panels from the saved Discover Logs option or Visualize Logs option. You can also create a new Dashboard from scratch.

Complete these steps to create a Dashboard:

Step 1 Click **Cisco Operations Hub** > **System** > **Logs**.

Step 2 Click **Dashboard** > **Create dashboard**.

Step 3 Click **Add**.

Step 4 On the Add panels menu, select the required searched and saved logs and visualizations.

Step 5 You can choose to change existing filters or add filters.

Step 6 Click **Create new** to choose a visualization type. You can choose from these visualization types:

- Area

- Control

- Coordinate Map

- Data Table

- Gauge

- Goal

- Heat Map

- Horizontal Bar

- Line

- Markdown

- Metric

- Pie

- Region Map

- TSVB

- Tag Cloud

- Timelion

- Vega

- Vertical Bar

Step 7   Choose a source type. You can choose from `audit-log`, `debug-log`, or `logstash` objects.

You can view the saved dashboards on the dashboard list.

Query on Data Store

The Dev Tools option allows you to query the data store.

Complete these steps to use the Dev Tools option:

Step 1   Click **Cisco Operations Hub** > **System** > **Logs**.
Step 2   Click **Dev Tools**.

Manage Indices and Objects

The Management option allows you to manage your indices and index patterns, list your saved objects, and enables you to customize the logs with advanced options.

Complete these steps to use the Management option:

Step 1   Click **Cisco Operations Hub** > **System** > **Logs**.
Step 2   Click **Management**.

You can choose from these tools:

- **Index Patterns**: Lists all available patterns. The list includes all fields for the selected pattern and the field's associated core type as recorded by Elasticsearch.

- **Saved Objects**: Lists all saved objects. You can choose to delete saved objects and saved searches. You can also edit the raw data of saved objects.

- **Advanced Settings**: These are advanced settings, and must be handled with caution. For more detailed information, go through Kibana Advanced Settings.