Cisco Cloud Native Broadband Router User's Guide, Release 21.2

First Published: 2021-07-12

CONTENTS

CHAPTER 4

CHAPTER 1

Overview of Cisco Cloud Native Broadband Router

This chapter provides an overview of Cisco Cloud Native Broadband Router (cnBR) and its key features and benefits. It also describes the key components of the Cisco cnBR and how the router is deployed in a network.

Transformation of the Cable Network

To support the increasing needs of the customers, cable networks are undergoing major transformations. They are:

- migrating from analog to digital systems

- adding capacity and scale

- deploying new and improved service features

Replacing analog systems with digital devices, such as Remote PHY and Converged Interconnect Network (CIN) routers and switches, is preparation for what is to come: the transformation of the cable headend. With a digital access network, cable services that are reliant on headend hardware are no longer tied to physical hardware–based solutions.

The Cisco Cloud Native Broadband Router (cnBR) is a fundamental rewrite of the CCAP, virtualizing the earlier hardware-based services with a truly cloud-native design, thus offering unprecedented service velocity, highly simplified operations, and economic scalability for profitably operating your network. The Cisco cnBR is built from the ground up, taking decades of experience and expertise in networking technologies and completely rewriting the hardware-based Converged Cable Access Platform (CCAP) code to be cloud native. Instead of lifting and shifting existing code from legacy hardware and placing it in the cloud to run as a virtual machine, the Cloud Native Broadband Router is a full software rewrite for CCAP-enabled services, built as a composable set of microservices that utilize standard tools, such as Kubernetes for container orchestration and Docker for creating, deploying, and running containerized applications.

Features and Benefits of Cisco cnBR

The previous generations of Cable Modem Termination Systems (CMTS) products integrated cable modem RF connectivity, Data-over-Cable Service Interface Specifications (DOCSIS) control plane signaling, data forwarding, platform monitoring, and back office reporting into a single purpose-built hardware platform. The Cisco cnBR is a containerized, virtual CCAP solution, which is designed to take the service capabilities of physical hardware and virtualize them into a customizable, scalable, and resilient set of microservices.

The Cisco cnBR offers the following features and benefits:

- **Increased feature velocity**: The increased feature velocity is achieved by hosting the functionality on more generic hardware platforms, making it easier to develop and test features as well as leverage Open Source Software and continuous integration technologies.

- **Flexible placement of CMTS Core and PHY**: With the Cisco cnBR on general-purpose hardware and physically not containing the PHY interface, the CMTS Core can be deployed anywhere there is network connectivity to the RPDs and service provider IP network.

- **Enhanced monitoring**: With the Cisco cnBR and Operations Hub deployed on a container platform, industry leading monitoring technologies like Prometheus and ELK are readily accessible and easy to deploy.

- **Easier scaling**: Scaling up the Cisco cnBR in a datacenter is as easy as adding new cnBR service containers on existing or new clusters.

- **Rapid feature and configuration deployment**: By employing CI/CD tools in combination with a container platform, new features can be quickly tested and deployed in the service provider network.

- **DevOps support**: Increased monitoring visibility, CI/CD capabilities, use of industry-standard container platforms, and the need to keep the deployment updated, paves the way for DevOps support and tools. The product is more visible and technologically understandable by the service provider, thus allowing for a partnered support model.

- **Increased automation**: The kubernetes (K8S) platform has been designed to make automation easier, further reducing operational cost.

Cisco cnBR Product Components

The key components of the Cisco cnBR are:

- Cisco Operations Hub

- Cisco cnBR Manager application

- cnBR Core

- Remote PHY Device

Cisco Operations Hub

Cisco Operations Hub is an application and service hosting platform tailored for the cloud-native era. Cisco Operations Hub hosts applications and services essential to managing the Cisco cnBR, including real-time telemetry, statistics, and log collection as well as providing centralized external management access to IPDR and SNMP data.

Figure 1: Cisco Operations Hub Framework
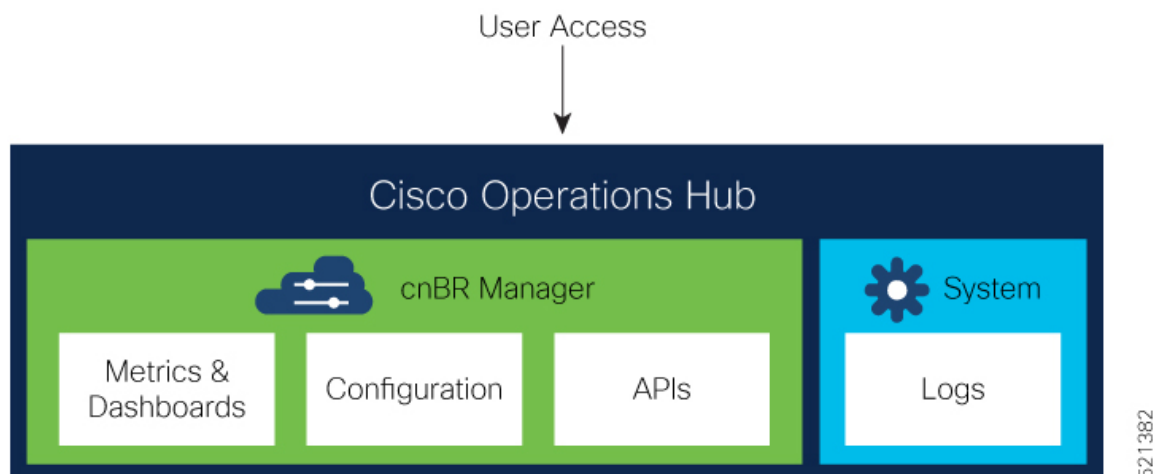
See for information on accessing and configuring Cisco Operations Hub.

In addition to application hosting, Cisco Operations Hub provides these interfaces for Customer OSS or Third-Party Vendor tool integration:

- IP Detail Record Service
- Simple Network Management Protocol

cnBR Manager

Cisco cnBR Manager provides essential tools for managing a Cisco cnBR:

- Metrics & Dashboards: Provides real-time visualizations of service & health metrics along with other information about Cisco cnBR, and DOCSIS network elements.
- Configuration: Provides a collection of management tools to view, import, export, and modify Cisco cnBR and RPD configurations.
- APIs: Provides a programmatic interface to retrieve configuration, metrics, and other information about Cisco cnBR and DOCSIS network elements.

cnBR Core

The cnBR Core interacts with RPDs to:

- receive cable modem (CM) data.

   - process CM control plane messages to establish and maintain modem sessions.

   - forward upstream and downstream data between the modem and IP network.

It also captures the KPI health of the modem and RPD network, and provides a management interface for DOCSIS features and telemetry data, including service flows.

Remote PHY Device

The Remote PHY Device (RPD) provides analogue RF connectivity to the cable modems and digital connectivity to the CMTS Core (cnBR).

Cisco cnBR Deployment

The following figure depicts a typical Cisco cnBR deployment that separates management plane, control plane, and data plane components.

Figure 2: Typical cnBR Deployment
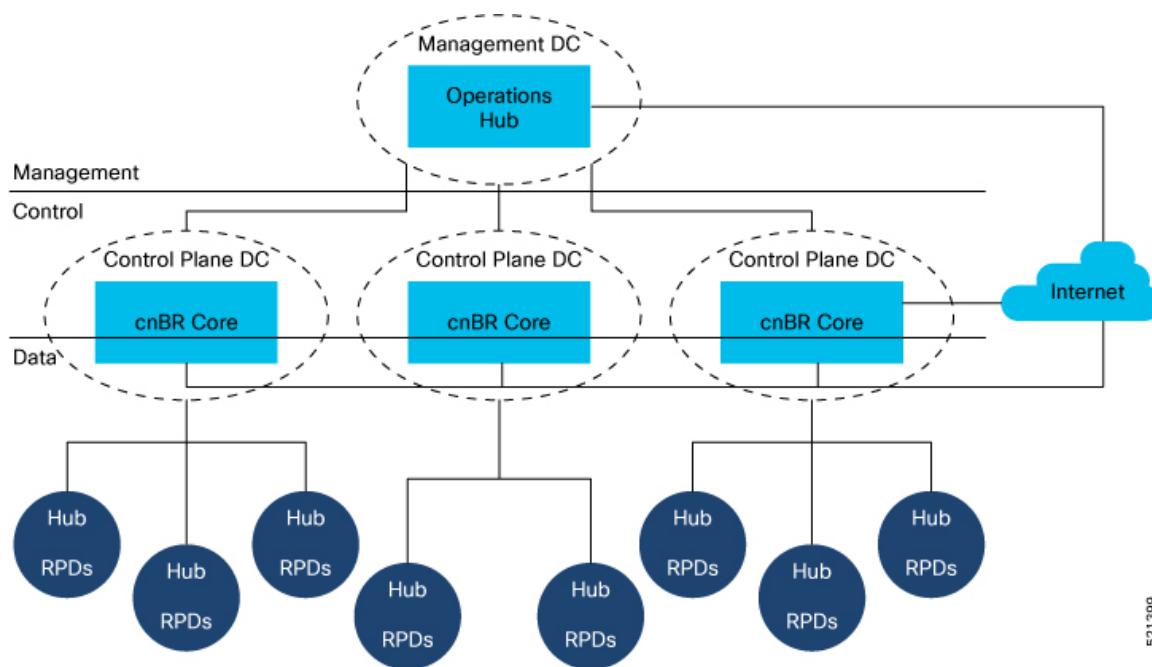
The management plane components, which include Operations Hub, are centralized within a central data center.

The Cisco cnBR, which contains the control plane components and routing for the data plane, is hosted within regional data centers.

The RPDs within hubs around the hub may connect to these regional data centers.

Because the entire solution has high availability, there can be no single point of failure, especially in the data plane.

The following diagram shows the components and networks that are configured when a Cisco cnBR is deployed in a typical service provider network.

Figure 3: Network Components
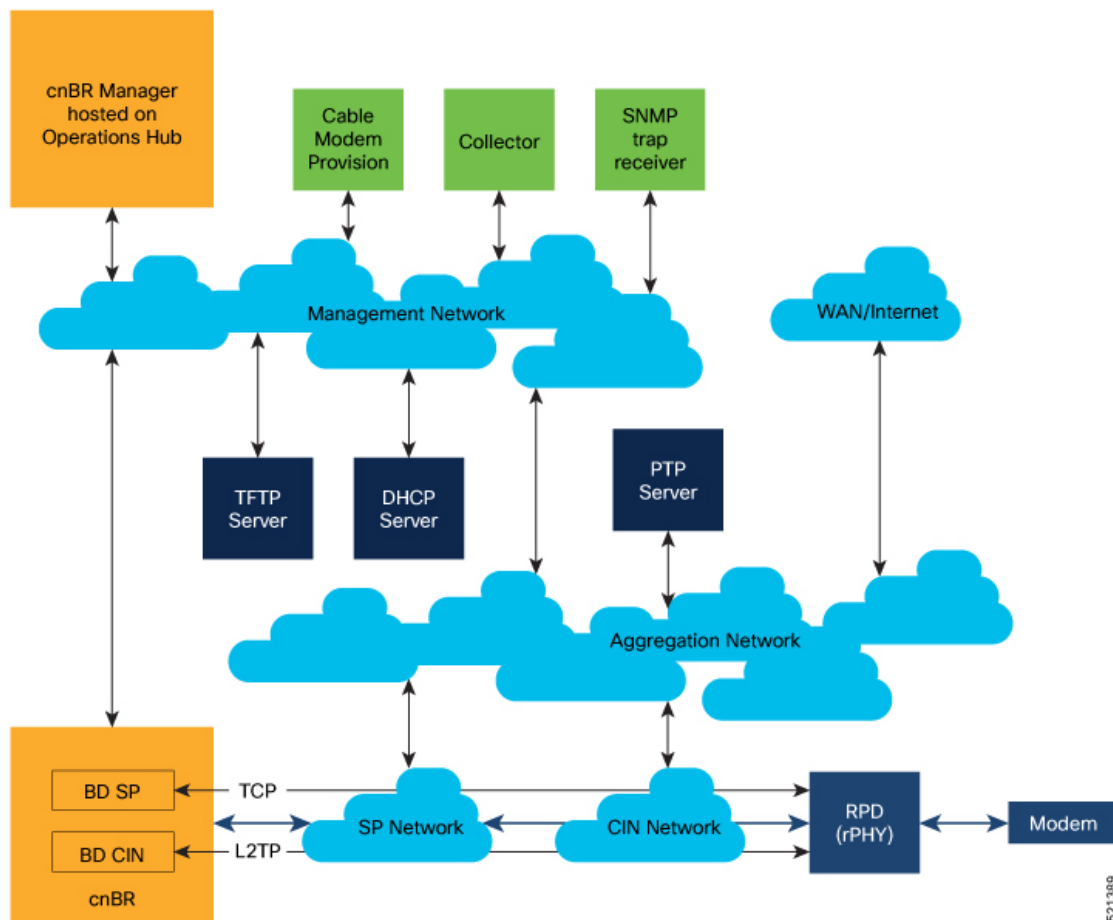
Different networks and their purposes.

Network	Purpose
Aggregation	The aggregation network provides a nexus where necessary network paths converge to provide access to all necessary services.
Converged Interconnect Network (CIN)	The CIN network is well defined in the Cisco cable architecture and brings the cable modem traffic that has been converted to IP traffic into the digital DOCSIS network. The CIN network connects to the aggregation network for non-CMTS data traffic, such as PTP timing and RPD provisioning.
Management Network	The management network provides management-level interaction between the Cisco cnBR components and back-office services, such as IPDR collectors, SNMP trap, receivers, and cable modem provisioning and monitoring.

Network	Purpose
SP Network	The service provider networks provide a path for the cable modem traffic that is processed by the CMTS to reach the internet from the service provider side of the network.
WAN/Internet	The WAN/Internet network provides a path for the cable modems to send traffic to and receive traffic from the public internet.

These networks may be realized using one or more routers configured for each network.

The TFTP, DHCP, and PTP capabilities are required to be part of the solution and may be connected to different networks than those depicted in the figure. The PTP, DHCP, and TFTP address are configured within the Cisco cnBR.

The green boxes represent common service provider management features. In the past, cable modem provisioning and monitoring used information from the CMTS collected through SNMP MIBs. However, going forward, the preference is to move to REST APIs.

In the Cisco cnBR, the CIN and SP bridge domains must be configured. The CIN and SP bridge domain configurations provide first hop routing information to correspondingly named networks.

Kubernetes Platform

The Kubernetes (K8S) platform is deployed on VMs. From Cisco cnBR 21.2, bare-metal deployment is also supported.

The Cisco cnBR and management plane services are deployed as microservices within Kubernetes (K8S) container orchestration clusters. The Kubernetes platform supports deployment of replicated restartable microservices, where requests are routed and processed. Services are therefore highly available and scalable through redundancy.

To be hardware redundant, the K8S management functionality must be spread across separate nodes, either as bare-metal servers or as VMs hosted on separate servers as shown in the following figure:

Figure 4: Kubernetes Platform
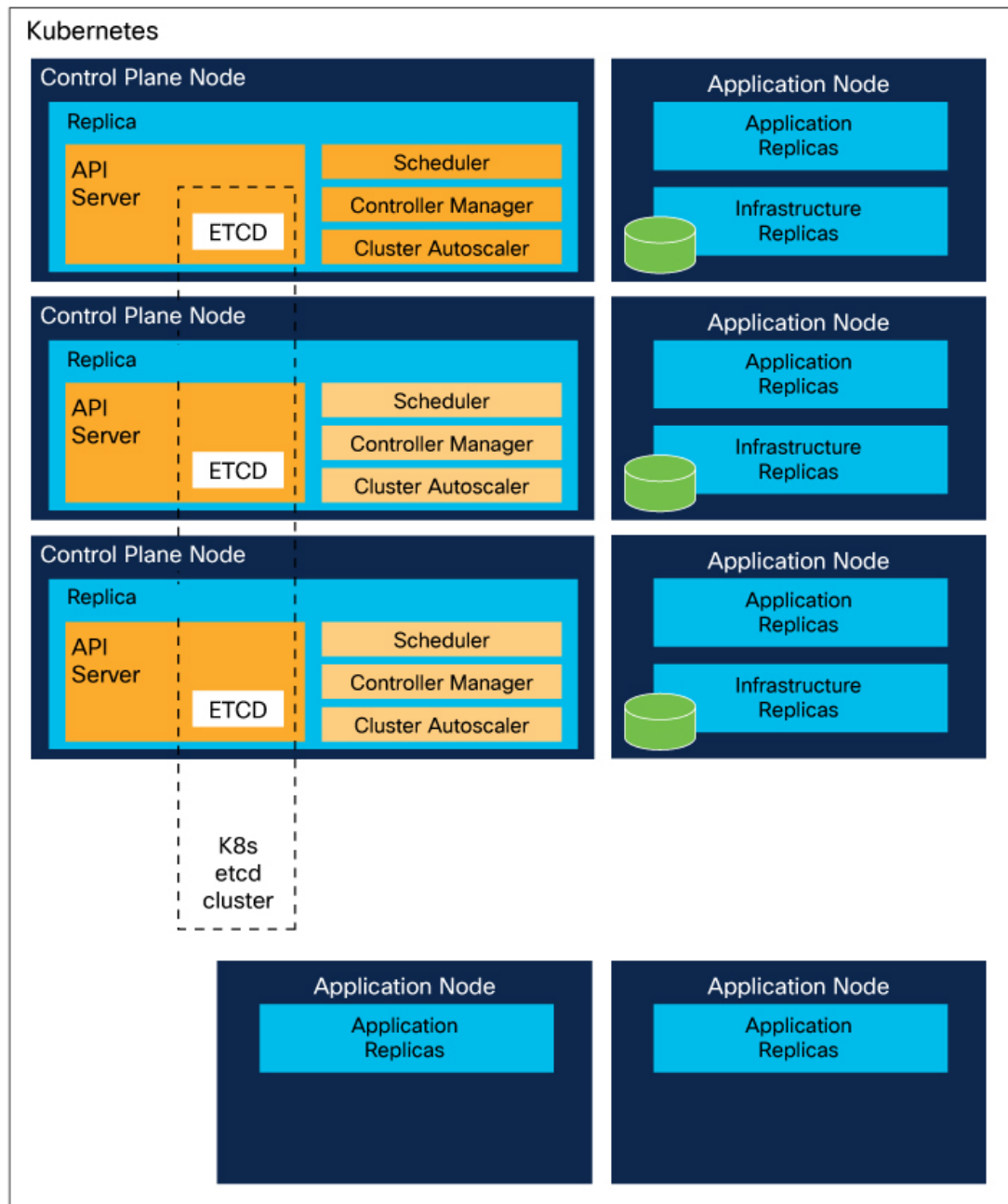
Similarly, the application load must be spread across worker nodes that are independent of the K8S control plane nodes. Separating the application workload from K8S control plane nodes protects the K8S management services from being impacted by the application workload.

The Cisco cnBR functionality and Cisco Operations Hub are hosted in a common cloud platform.

Cisco cnBR Network Topology

A typical Cisco cnBR network consists of Cisco cnBR core clusters, a SP router network, and Cisco Operations Hub, which hosts the cnBR Manager application. The following figure shows the core components and their inter-connections.

Figure 5: Cisco cnBR Inter-Connections and Data Flow
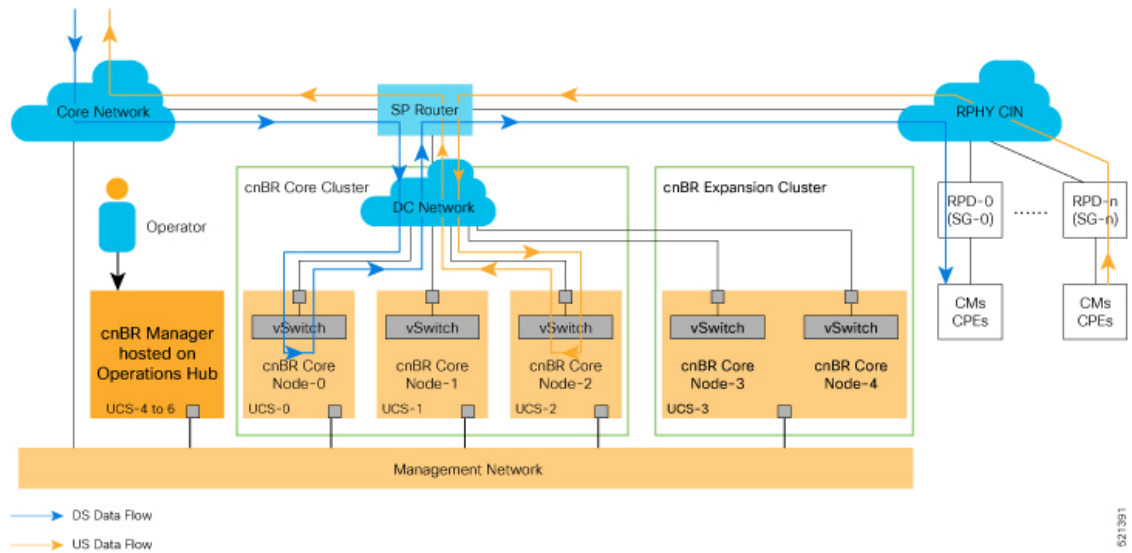
Core Components of Cisco cnBR Network Topology

- A highly available Cisco cnBR core cluster consists of three or more worker nodes, which provide core functionality of traditional CMTS: for example, DOCSIS control plane, data plane, and DOCSIS applications.

- SP Router forwards L3 packets between the uplink core network, RPHY CIN, and cnBR core services.

- Cisco Operations Hub is built in its own cluster and provides operation and management-related functionality in the Cisco cnBR system: for example, configuration, monitoring, and alert management.

Cisco cnBR Expansion Servers

Feature History

Table 1: Feature History

Feature Name	Release Information	Feature Description
Multiserver support	Cisco cnBR 20.3	You can install a Cisco cnBR cluster that includes 2 expansion servers, which is a 5-server cluster.

A Multi-Node cnBR can be deployed with increased compute capacity to accommodate larger scale deployments. Additional Cisco C220 M5 UCS Servers, which are called Expansion Servers, can be added to the Core 3 Node UCS Server Cluster to run additional DOCSIS Nodes. Cisco cnBR currently supports Static Expansion deployment. The Expansion Servers must be prepared and connected per the Prepare Supporting Software Components, on page 21 procedure in the Set Up Cisco Cloud Native Broadband Router Components, on page 11 section together with the Core 3 Node UCS Server Cluster before the initial cnBR cluster deployment.

Inter-Connections Between Core Components

- The SP router connects directly with the data center (DC) network to access multiple Cisco cnBR core nodes. The configuration is based on network virtualization technology that the UCS vSwitch uses, such as VLAN or VXLAN.

- Cisco Operations Hub communicates with the Cisco cnBR core clusters through internal RESTful messaging, which in turn is through the high-speed Management Network. The Management Network also transmits real-time telemetry data exported from Cisco cnBR core clusters to Cisco Operations Hub.

Downstream and Upstream Data Flow

Figure 5: Cisco cnBR Inter-Connections and Data Flow, on page 8 illustrates the downstream and upstream data flows with arrows shown in different colors.

- All data traffic goes in and out of the Cisco cnBR core cluster for corresponding processing. The SP router acts as a hub.

- Different service groups (SG) are managed by different Cisco cnBR core nodes. For example, in Figure 5: Cisco cnBR Inter-Connections and Data Flow, on page 8, SG-0 is managed by cnBR-Core Node-0, while SG-n is managed by cnBR-Core Node-2.

Control Flow

As shown in the following figure, network data flows between the subscriber devices and the Cisco cnBR core for control and data. It also flows between the Cisco cnBR core and the Cisco Operations Hub for management.

Figure 6: Cisco cnBR Control and Management Flows
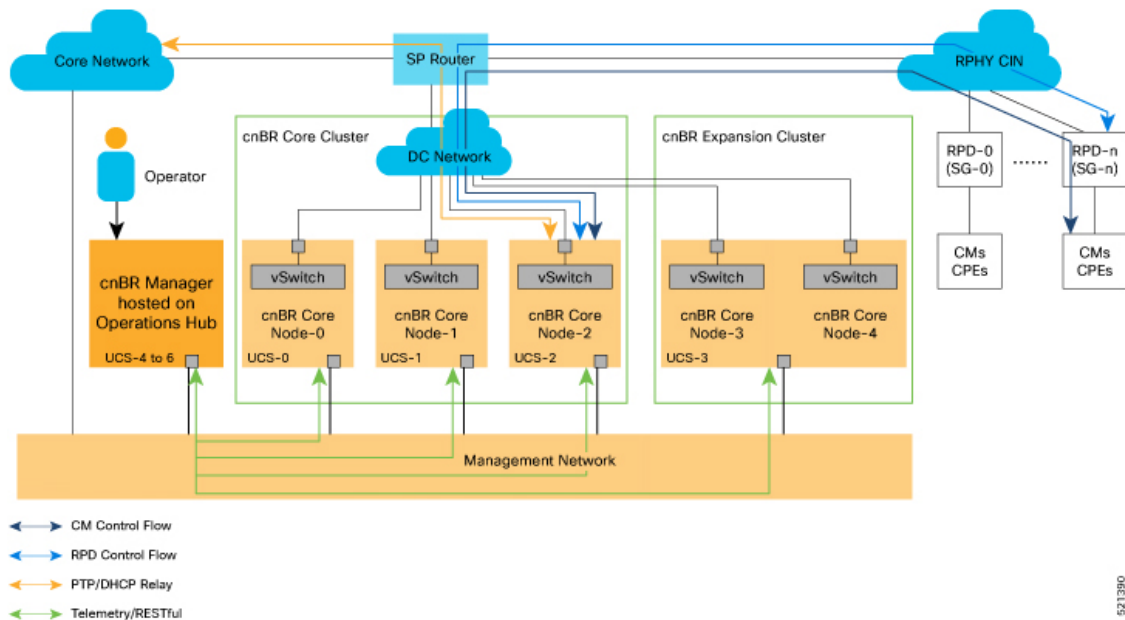
The major Cisco cnBR control and management flows are:

- Cable modem control flow—between DOCSIS service and cable modems, for cable modem provisioning and management

- RPD control flow—between RPD service and RPD nodes, for RPD node provisioning and management

- Control flow—for PTP and DHCP relay service

- Cisco Operations Hub management flow—between Cisco Operations Hub and Cisco cnBR core services, for telemetry data export and RESTful interface messaging

C H A P T E R **2**

Set Up Cisco Cloud Native Broadband Router Components

This chapter provides information about the required prerequisite hardware and software, describes key components of Cisco cnBR, its topology, and how the router is deployed in a network. This chapter also provides information about how you can set up the Cisco cnBR core and the Cisco Operations Hub, and how you configure Cisco cnBR for service resiliency.

cnBR Prerequisites

Feature History

Table 2: Feature History

Feature Name	Release Information	Feature Description
100G NIC Support	Cisco cnBR 21.3	100G NIC allows you to use 100G or 400G ports on the SPR and a breakout cable to connect multiple 100G NICs to a single SPR port. It makes significant difference in how to size, order, and architect your network for cnBR.

Feature Name	Release Information	Feature Description
Deployment on Customer Managed VMware ESXi Infrastructure	Cisco cnBR 21.3	This feature allows you to deploy Cisco Operations Hub on a customer managed VMware ESXi infrastructure. It supports normal and small size multi-node cluster deployment to fit in different application environments.

The following components are required to install, operate, and manage a Cisco cnBR:

- Cisco cnBR servers

- Cisco Operations Hub servers

- Cisco cnBR Network Components

- VMware vSphere Infrastructure including vCenter Server

Hardware Prerequisites for the Cisco cnBR

The Cisco cnBR runs exclusively on Cisco Unified Computing System (UCS) servers.

- Cisco UCS server requirement

  Three Cisco UCS C220 M5 servers are required to run Cisco cnBR. The UCSC-C220-M5SX is supported in two configurations with minimum compute, storage, and networking requirements listed in the following tables:

  Minimum Requirements for the Cisco UCS Server

  Table 3: Minimum Requirements for the Cisco UCS Server

Component	Specification
Chassis	UCSC-C220-M5SX
Processor	Intel 6248 2.5GHz/150W 20C/27.5MB DCP DDR4 2933 MHz
Memory	384GB DDR4-2933-MHz RDIMM
Storage	4 x 800GB SSD
NIC	2 x Intel XL710-QDA2 (40G)

Or

Minimum Requirements for the Cisco UCS Server

Component	Specification
Chassis	UCSC-C220-M5SX

Component	Specification
Processor	Intel 6248R 3.0GHz/205W 24C/35.75MB DCP DDR4 2933 MHz
Memory	384GB DDR4-2933-MHz RDIMM
Storage	4 x 800GB SSD
NIC	2 x Intel XL710-QDA2 (40G)

Or

Minimum Requirements for the Cisco UCS Server

Component	Specification
Chassis	UCSC-C220-M5SX
Processor	Intel 6248R 3.0GHz/205W 24C/35.75MB DCP DDR4 2933 MHz
Memory	384GB DDR4-2933-MHz RDIMM
Storage	4 x 800GB SSD
NIC	2 x Mellanox UCSC-P-M5D100GF (100G)

Prerequisites for the Cisco Operations Hub

- ESXi hosts requirement

Three ESXi hosts are required to run a Cisco Operations Hub multi-node cluster.

You can deploy Cisco Operations Hub on a non-UCS environment like customer-managed VMware infrastructure. The preferred deployment environment is Cisco Unified Computing System (UCSC-C220-M5SX). Cisco Operations Hub supports two deployment options: Small and Normal.

For Normal deployment, minimum compute, storage, and networking requirements for the ESXi hosts are listed in the following table:

Minimum Requirements for Normal Deployment

Table 4: Minimum Requirements for Normal Deployment

Component	Specification
Processor	34 vCPUs
Memory	304 GB
Storage	2400 GB SSD, Minimum 50000 IOPS (Input/output operations per second) Latency of < 5 ms
NIC	2 x 10G vNIC

For Small deployment, minimum compute, storage, and networking requirements for the ESXi hosts are listed in the following table:

Minimum Requirements for Small Deployment

Table 5: Minimum Requirements for Small Deployment

Component	Specification
Processor	20 vCPUs
Memory	160 GB
Storage	1600 GB SSD, Minimum 50000 IOPS (Input/output operations per second) Latency of < 5 ms
NIC	2 x 10G vNIC

- VMware requirements

  - Hypervisor: Choose either of the following:

    - VMware ESXi 6.5, minimum recommended patch release for security updates ESXi650-202006001

    - VMware ESXi 6.7, minimum recommended patch release for security updates ESXi670-202006001

  - Host Management - VMware vCenter Server 6.5 or VMware vCenter Server 6.7

  If the VMware ESXi 6.7 is installed on host, ensure that the vCenter version is VMware vCenter Server 6.7.

- Browser support

  For the Cisco cnBR, the Cisco Operations Hub functionality is supported for the following browser versions:

  - Mozilla Firefox 86 and later

  - Google Chrome 88 and later

  - Microsoft Edge 88 and later

  > **Note** For Windows OS, the recommended resolution is 1920x1080 and a scale and layout setting of 125%.

Prerequisites components in the Cisco cnBR Topology

- Cisco cnBR Data Switch

  You must use a data center switch with the requisite 40G port density between the Cisco cnBR servers and the service provider router to aggregate the Cisco cnBR data path links.

- Management Switch

  A dedicated data center switch can be used for Cisco cnBR and Cisco Operations Hub management traffic. Cisco UCS servers provide 1G, 10G, and 40G network interface connectivity options for the different management networks that are used in the system.

  Cisco cnBR UCS servers require connectivity for Host Operating System Management and Cisco Integrated Management Controller (IMC) Lights-Out-Management.

  Cisco Operations Hub UCS servers require connectivity for VMware ESXi host management, VM traffic for Guest Operating System Management, and Cisco Integrated Management Controller (IMC) Lights-Out-Management.

- Service Provider Router

  The SP Router is responsible for forwarding L3 packets between the core network, RPHY CIN, and Cisco cnBR. The SP Router and Cisco cnBR establishes connections through BGP, SG, RPHY-core for RPD session setup and traffic forwarding.

  We recommend the following Cisco Network Convergence System 5500 Series models:

  - NCS-55A1-36H-S

  - NCS-55A1-24H

  The required software version must be Cisco IOS XR 6.5.3 or later.

- DHCP Server

  A standard Dynamic Host Configuration Protocol (DHCP) server is required, and typically included in an existing DOCSIS infrastructure. For example, the DHCP server that is included is the Cisco Network Registrar (CNR).

- PTP Server Configuration

  A Precision Time Protocol (PTP) server is required and typically included in an existing DOCSIS infrastructure. For example, an OSA 5420.

- TFTP Server

  A standard Trivial File Transfer Protocol (TFTP) server is required and typically included in an existing DOCSIS infrastructure.

- RPHY CIN

  A Remote PHY Converged Interconnect Network (CIN) is required. A Remote PHY Device, and Cable Modems are also required. For example, Cisco Smart PHY 600 Shelf.

  The following image is a simplified, high-level overview of an end-to-end system and shows how these Cisco cnBR components are connected in the topology with provisioning systems and a Remote PHY CIN:

Figure 7: Simplified cnBR Topology
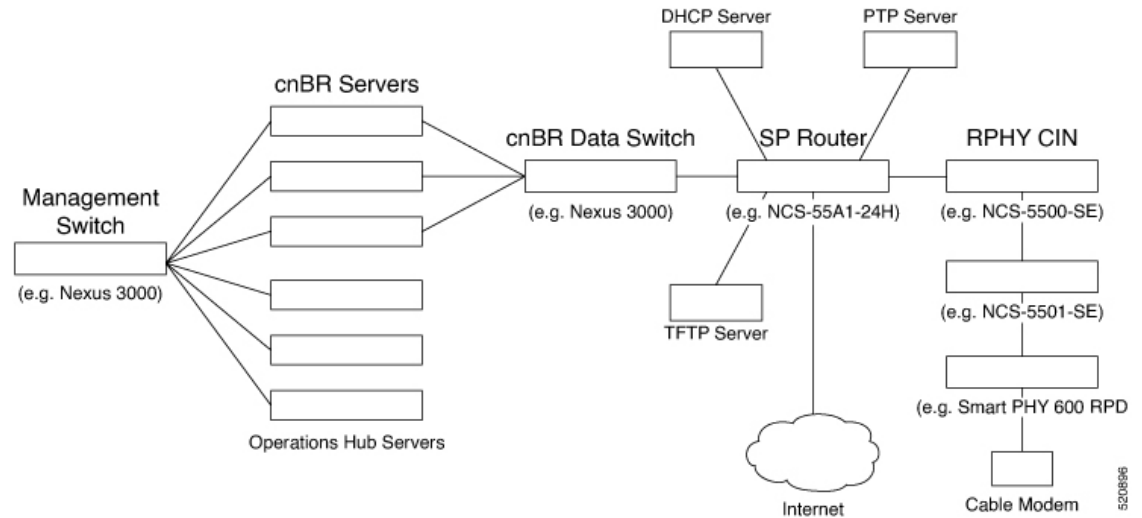
Prerequisites Required for Deployment

A VMware vSphere ESXi infrastructure with a vCenter server instance is required for end-to-end automated deployment. The SMI Deployer Cluster Manager and Cisco Operations Hub cluster nodes run as virtual machines.

A generalized Cisco cnBR deployment with the Cisco Operations Hub hosted in a VMware cluster is depicted in the following image:
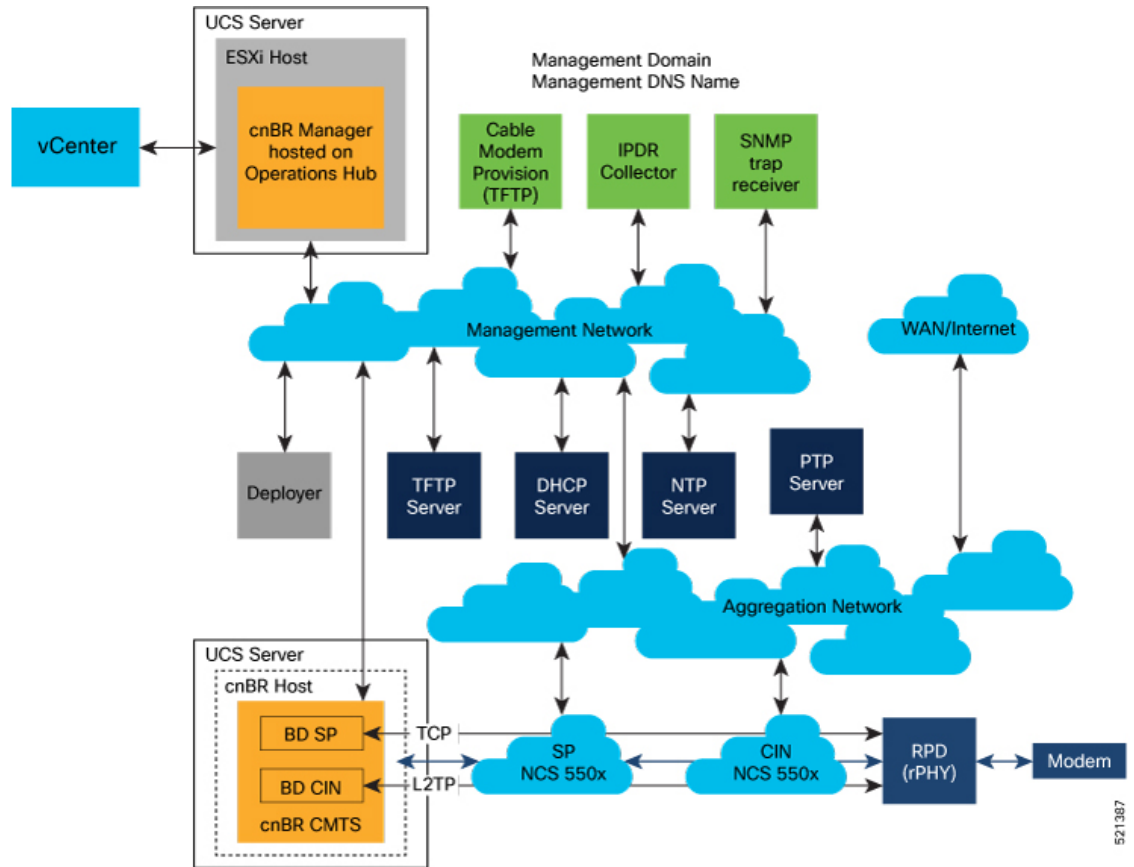
The VMware network topology in the following image is for a VLAN configuration:

Figure 9: VLAN Configuration with VMware Network Topology
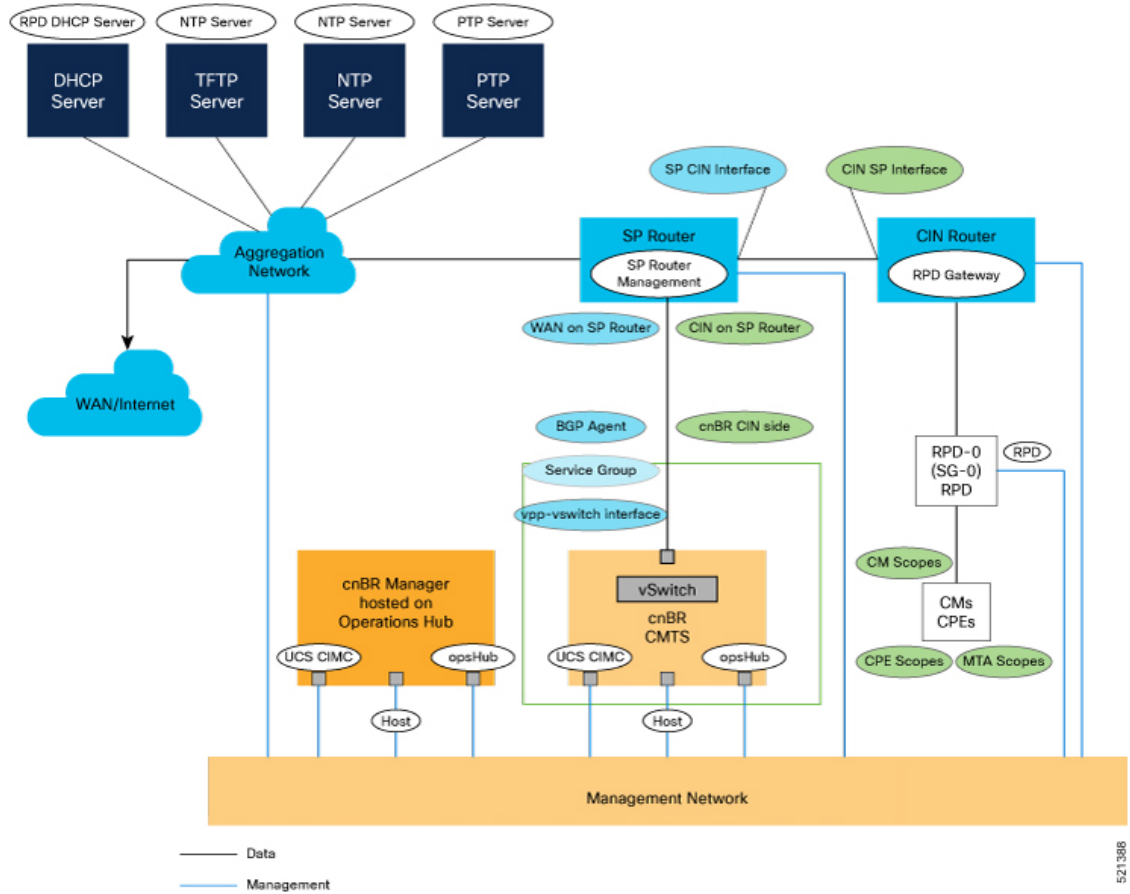
The necessary IP addresses and networks that are mapped in the diagram are described in the following sections:

- **Networks**

  The following table provides guidance for the networks that are needed in the management, WAN, and CIN routing domains:

  Network Information for Routing Domains

Table 6: Network Information for Routing Domains

Name	Subnet Mask	Function
Management	• 2 addresses for each cluster • Operations Hub/cnBR UCS • 1 for each cluster • 1 for each service device	Management
CIN	Network requirements for each customer	Connection RPD and CCAP core

Name	Subnet Mask	Function
WAN	Network requirements for each customer	Internet access for CPE
cnBR CIN side	Network requirements for each customer	-
BGP network to SP router	Network requirements for each customer	Management
Network for data	Network requirements for each customer	-
SG IP cnBR side	Network requirements for each customer	The peer IP for Service Group on cnBR
RPD address pool	Customer selected	DHCP scope for RPD sized to cover total number of RPDs.
DHCP scope for CM	Customer selected	-
DHCP scope for CPE	Customer selected	-
DHCP scope for MTA	Customer selected	-

You must provide domain and DNS name for the management network.

- **Device Addresses**

  The followings tables provide information on the IP address that is needed for device and router interfaces.

  - **Management IP Address**: Each management interface that is listed in the following table requires 1 IP address:

    Management Interface and Associated IP Addresses

    Table 7: Management Interface and Associated IP Addresses

Device name	Number of Addresses
CIMC cnBR	1 per cnBR UCS
Host OS cnBR	1 per cnBR UCS
cnBR VIP	1 per cnBR Cluster
CIMC Operations Hub	1 per Operations Hub UCS
ESXi Operations Hub	1 per Operations Hub UCS
Operations Hub	1 per Operations Hub VM
Operations Hub VIP	1 per Operations Hub Cluster
Deployer	1

Device name	Number of Addresses
vCenter	1
SP router	1
CIN router	1

- **DOCSIS Network Addresses**: The following table lists the DOCSIS network-related information:

DOCSIS Network-Related Information

Table 8: DOCSIS Network-Related Information

Device Name	Network Name	Description	Number of Addresses
SP router to CIN	CIN	SP connection to CIN router	1
CIN router to SP	CIN	CIN connection to SP router	1
SP router to WAN	WAN	SP connection to WAN/Internet	1
RPD Gateway	CIN	RPD gateway router Address	1
cnBR CIN side	CIN	cnBR connection to CIN	Customer specific
BGP Agent	WAN	WAN router BGP Agent IP	Customer specific
Service Group	WAN	Service Group WAN IP	Customer specific
WAN on SP Router	WAN	SP connection to WAN network	Customer specific

- **Customer Provisioned Services**: The following table lists the various customer services:

Customer Provisioned Services

Table 9: Customer Provisioned Services

Service	Notes
DHCP	Needed for both RPD and subscriber devices
TFTP	RPD only uses it during software upgrade
TOD	Time of day clock
PTP	One connection that is required for the cnBR and for each RPD

Service	Notes
NTP	Network Time Protocol Server
DNS	Domain Name Server

Prepare Supporting Software Components

To prepare the Cisco Unified Computing System (UCS) servers for software installation, you must do the following.

- Rack mount the servers and connect power and networking

- Configure the servers using Cisco Integrated Management Controller (CIMC)

- Cisco cnBR Server Installation and Configuration, on page 21

Cisco cnBR Server Installation and Configuration

Step 1   Cisco UCS Server Installation, on page 21

Step 2   Load Cisco cnBR Optimized BIOS Configuration, on page 22

Cisco UCS Server Installation

Step 1   Rack mount the servers. See Cisco UCS C220 M5 Server Installation and Service Guide.

Step 2   Ensure that both power supplies are connected on each server, and power on the servers.

Step 3   Connect the following network cables:

- For Cisco Integrated Management Controller (CIMC), use the 1Gb Ethernet dedicated management port.

- For Cisco cnBR Host Operating System Management, use Ethernet port 1 of the Dual 1Gb/10Gb Intel X550T on board NIC.

- For Cisco cnBR Data, if the 40G NIC is used, connect port 1 of the Intel XL710 40G NIC in PCIe Slot 1 to the SP Router/Leaf Switch using Cisco QSFP-40G-SR4. If the 100G NIC is used, connect port 1 of the Mellanox UCSC-P-M5D100GF 100G NIC in PCIe Slot 1 to the SP Router/Leaf Switch using Cisco QSFP-100G-SR4.

Step 4   Connect the UCS Kernel-based Virtual Machine (KVM) console adapter or connect a keyboard and monitor directly to the server.

Step 5   Configure CIMC through the KVM console and update the Network Settings.

Update Firmware

Download the latest Hardware Update Utility for the UCS C220 M5 Server from Cisco's Software Download site and use it to update the CIMC, BIOS, and Device Firmware for Storage Controllers, Network Adapters, SSDs, and other components.

Load Cisco cnBR Optimized BIOS Configuration

Step 1 Create a new json file "cnbr_perf.json" and add the following structure.

Cisco cnBR Optimized BIOS profile config for C220 M5 Servers

```
{
    "name":"Perf_M5",
    "description":"",
    "tokens":{
        "EnhancedIntelSpeedStep":"Enabled",
        "IntelTurboBoostTech":"Enabled",
        "IntelHyperThread":"Disabled",
        "CPUPerformance":"Enterprise",
        "ExecuteDisable":"Enabled",
        "IntelVTD":"Enabled",
        "ProcessorC1E":"Disabled",
        "ProcessorC6Report":"Disabled",
        "PsdCoordType":"HW ALL",
        "CpuEngPerfBias":"Performance",
        "PwrPerfTuning":"BIOS",
        "CpuHWPM":"HWPM Native Mode",
        "WorkLdConfig":"IO Sensitive",
        "SelectMemoryRAS":"Maximum Performance",
        "SNC":"Disabled",
        "XPTPrefetch":"Enabled",
        "DcuIpPrefetch":"Enabled",
        "PatrolScrub":"Disabled"
    }
}
```

Step 2 Load the optimized Cisco cnBR BIOS configuration into the system using "cnbr_perf.json".

Step 3 Save a backup of the current BIOS settings.

Step 4 Select the new profile "Perf_M5" and activate it.

Configure Boot Drives

Step 1 Enable the Cisco MSTOR Boot Optimized M.2 RAID Controller.

Step 2 Create a RAID 1 virtual drive from 2 x M.2 SSD Drives.

Step 3 Set Stripe Size to 64KB

Configure Data Drives

Step 1   Enable Cisco 12G SAS Modular RAID Controller.

Step 2   Create a RAID 5 enabled virtual drive using 4 x SSDs.

Step 3   Set Stripe Size to 64KB.

Step 4   Set Write Cache Policy to *Write Back with Good BBU*.

Configure UCS Servers for Hosting Operations Hub

Complete the following steps to configure UCS servers for hosting Cisco Operations Hub.

Install VMware ESXi

Step 1   Download the Cisco custom image for ESXi 6.5 U3 GA Install CD ISO from VMware.

Step 2   Install VMware ESXi 6.5 Update 3 on the M.2 RAID 1 Virtual Drive (Boot Drive).

Step 3   Use the Cisco Custom ISO - VMware_ESXi_6.5.0_13932383_Custom_Cisco_6.5.3.1.iso

Step 4   Set a password for the root user following the installation process.

Step 5   Reboot the VMware ESXi host following the installation process and execute the steps in Reboot VMware ESXi Host and Set Boot Device, on page 23.

Reboot VMware ESXi Host and Set Boot Device

Step 1   Interrupt the boot process with the F2 key after the host resets and boot into the BIOS.

Step 2   Under the Boot Options tab, set Boot Option #1 to the UEFI target - *VMware ESXi*.

Step 3   Disable all other boot options.

Step 4   Save changes and exit.

Step 5   Confirm the host boots directly into VMware ESXi.

Add Cisco cnBR ESXi Hosts to vSphere Virtual Infrastructure

Step 1   Configure VMware ESXi Host Management Networking, on page 24

Step 2   Add ESXi Hosts to VMware vCenter Server, on page 24

Step 3   Configure and Enable Required ESXi Host Features, on page 24

Step 4   Configure Virtual Machine Networking, on page 24

Configure VMware ESXi Host Management Networking

Step 1 Log into the VMware ESXi host through the Direct Console User Interface (DCUI) with the root account.

Note For Cisco cnBR PID Servers, use the password received from your Cisco representative as part of your Cisco cnBR order.

Step 2 Configure the management network.
a) Update IP configuration.
b) Update DNS configuration.
c) Update custom DNS suffixes.
d) Update VLAN ID if required.

Add ESXi Hosts to VMware vCenter Server

In VMware vCenter:

Step 1 Create a new, dedicated cluster for Cisco cnBR.

Note Do not enable DRS or any HA features.

Step 2 Add each new Cisco cnBR ESXi Host to the new Cisco cnBR cluster.

Configure and Enable Required ESXi Host Features

Step 1 Configure time on the host.
a) Enable NTP.

Step 2 Apply ESXi host licenses.

Step 3 Enable PCI Pass-through on all four Intel XL710 40G QSFP+ ports(requires host reboot).

Step 4 Create a new datastore on the data drive storage device.

Note By default, Cisco cnBR PID servers have a datastore created and PCI Pass-through enabled.

Configure Virtual Machine Networking

Step 1 Ensure VMware vSwitch connectivity to the physical switch.

Step 2 Create a PortGroup and a VMware vSwitch for the Kubernetes Cluster Node VM MGMT Network.

Deployment of cnBR and Operations Hub

Feature History

Feature Name	Release Information	Feature Description
Bare-metal support	Cisco cnBR 21.2	With the introduction of Bare Metal support, all the required software and applications for Cisco cnBR and Cisco Operations Hub installation are provided in a single release package. This provides for a simplified deployment and configuration, and eliminates any dependency on external software repositories.

Cisco cnBR supports the offline installation of the SMI Cluster Manager, Cisco Operations Hub, and Cisco cnBR clusters.

All software and applications that are required for Cisco cnBR and Cisco Operations Hub installation are provided in a single release package. This eliminates any dependency on external software repositories. All system components including the SMI Deployer Cluster Manager, Cisco Operations Hub cluster, and Cisco cnBR cluster, can be created from scratch in offline or an air-gapped environment.

Cisco cnBR and Cisco Operations Hub product tar files containing all necessary Helm charts and Docker container images are included in the release package. The product tar files are imported into the SMI Deployer during the installation process.

The installation is started from a staging server using the Autodeploy utility that is packaged in the cnBR release bundle. The staging server can be any host running docker that has access to the physical and virtual system infrastructure.

Through Autodeploy, the SMI Deployer VM is created first and in turn installs the Cisco cnBR and the Cisco Operations Hub clusters. The Autodeploy app running on the staging server must be able to reach the following components for a proper, automated end-to-end deployment:

  • For the creation of the SMI Deployer Cluster Manager VM:

    • vCenter Server server instance used to create and manage the SMI Deployer VM

    • VM MGMT Network Interface of the SMI Deployer Cluster Manager

  • For the installation and verification of Cisco cnBR clusters:

    • Cisco IMC Interface of each UCS C220 M5 Server in the Cisco cnBR cluster

    • Host Operating System Management Interfaces of all Cisco cnBR cluster nodes

    • Primary Virtual IP of each Cisco cnBR cluster

  • For the installation and verification of the Cisco Operations Hub cluster:

    • vCenter instance used to create and manage the Cisco Operations Hub cluster node VMs

> • Guest Operating System Virtual Network Management Interface of all Cisco Operations Hub cluster node VMs
>
> • Primary Virtual IP of each Cisco Operations Hub cluster

Once created, the SMI Deployer VM must be able to access:

- For the installation and management of Cisco cnBR clusters:
  - Cisco IMC Interface of each UCS C220 M5 Server in the Cisco cnBR cluster
  - Host Operating System Management Interfaces of all Cisco cnBR cluster nodes
  - Primary Virtual IP of each Cisco cnBR cluster

- For the installation and management of Cisco Operations Hub clusters:
  - vCenter instance used for the Cisco Operations Hub cluster nodes
  - Guest Operating System Virtual Network Management Interface of all Cisco Operations Hub cluster node VMs
  - Primary Virtual IP of each Cisco Operations Hub cluster

Prepare the Staging Server

Complete the following steps to prepare the staging server:

Before you begin

Ensure that you have a staging server setup with the following prerequisites:

- Docker: See https://docs.docker.com/get-docker/ for more information.
- The staging server must have network connectivity to the system components as described in .

Step 1   Untar the Cisco cnBR release bundle.

In an offline deployment scenario, you must verify the authenticity and integrity of the image before the installation and deployment. The verification script verifies the image automatically through both online (if public network connection is available) and offline mode.

A corrupted or tampered image can lead to an image verification failure. Discard the image and contact the Cisco Customer Support to get the authentic image.

a)   Extract the Cisco cnBR release bundle. Untar the `cnbr-installer-.SPA.tgz` signed release bundle as shown:

```
~/staging$ tar xvzf cnbr-installer-<release-version-tag>.SPA.tgz
  cnbr-installer-<release-version-tag>.tgz    # cnBR release bundle
  isign/                                      # folder with image verification content
  isign/cnbr-installer-<release-version-tag>.tgz.signature
  isign/CNBR-BUNDLE_pubkey.der
  isign/cisco_x509_verify_release.py3
  isign/CNBR_IMAGE_SIGN-CCO_RELEASE.cer
```

```
  explode-cnbr                              # script to be used to verify the image signature
and untar the cnbr-installer-<release-version-tag>.tgz
  cnbr-verify-image.tar                     # cnbr verification image, will be automatically
loaded through explode-cnbr
```

b) Verify and extract the Cisco cnBR image

- Run the following script to verify the image. `cnbr-installer-xxx.tgz` untars automatically if the verification is successful. A successful verification is as follows:

```
~/staging$ ./explode-cnbr
Verifying cnbr-installer-<release-version-tag>.tgz
Verified OK
Extracting cnbr-installer folder...
x cnbr-installer-<release-version-tag>/
x cnbr-installer-<release-version-tag>/isign/
x cnbr-installer-<release-version-tag>/isign/autodeploy_<version-tag>.tar.signature
x cnbr-installer-<release-version-tag>/isign/innerspace.der
x
cnbr-installer-<release-version-tag>/isign/cluster-manager-docker-deployer_<version-tag>.tar.signature
x cnbr-installer-<release-version-tag>/isign/crcam2.der
x cnbr-installer-<release-version-tag>/isign/CCMTS_IMAGE_SIGN-CCO_RELEASE.cer
x cnbr-installer-<release-version-tag>/isign/ccmts-customization_<version-tag>.tar.signature
x cnbr-installer-<release-version-tag>/isign/cee-<version-tag>.tar.signature
x cnbr-installer-<release-version-tag>/isign/crcam2.cer
x cnbr-installer-<release-version-tag>/isign/opshub-stable.tar.signature
x cnbr-installer-<release-version-tag>/isign/OPSHUB_IMAGE_SIGN-CCO_RELEASE.cer
x cnbr-installer-<release-version-tag>/isign/innerspace.cer
x cnbr-installer-<release-version-tag>/isign/cluster-deployer-<version-tag>.tar.signature
x cnbr-installer-<release-version-tag>/isign/cnbr-stable.tar.signature
x cnbr-installer-<release-version-tag>/isign/CNBR-IMAGE_pubkey.der
x cnbr-installer-<release-version-tag>/isign/cnbrmanager-stable.tar.signature
x cnbr-installer-<release-version-tag>/isign/OPSHUB-IMAGE_pubkey.der
x cnbr-installer-<release-version-tag>/isign/SMI-IMAGE_pubkey.der
x cnbr-installer-<release-version-tag>/isign/CLUSTER_MANAGER_IMAGE_SIGN-CCO_RELEASE.cer
x cnbr-installer-<release-version-tag>/examples/
x cnbr-installer-<release-version-tag>/examples/multinode-opshub-config.yaml
x cnbr-installer-<release-version-tag>/examples/day1_config_mn.yaml
x cnbr-installer-<release-version-tag>/examples/deployer-sample-config.yaml
x cnbr-installer-<release-version-tag>/examples/multinode-cnbr-config.yaml
x cnbr-installer-<release-version-tag>/examples/multinode-opshub-multi-nic-config.yaml
x cnbr-installer-<release-version-tag>/examples/aio-cnbr-config.yaml
x cnbr-installer-<release-version-tag>/examples/day1_config_aio.yaml
x cnbr-installer-<release-version-tag>/examples/multinode-cnbr-bare-metal-config.yaml
x cnbr-installer-<release-version-tag>/examples/l3_template.json
x
cnbr-installer-<release-version-tag>/examples/multinode-cnbr-expansion-link-redundancy-config.yaml
x cnbr-installer-<release-version-tag>/examples/aio-opshub-config.yaml
x cnbr-installer-<release-version-tag>/examples/sg_template_4x4.json
x cnbr-installer-<release-version-tag>/examples/multinode-cnbr-expansion-config.yaml
x cnbr-installer-<release-version-tag>/docker-images/
x cnbr-installer-<release-version-tag>/docker-images/ccmts-customization_<version-tag>.tar
x cnbr-installer-<release-version-tag>/cluster-deployer-<version-tag>.tar
x cnbr-installer-<release-version-tag>/deploy
x cnbr-installer-<release-version-tag>/smi-install-disk.iso
x cnbr-installer-<release-version-tag>/offline-products/
x cnbr-installer-<release-version-tag>/offline-products/cee-<version-tag>.tar
x cnbr-installer-<release-version-tag>/offline-products/opshub-stable.tar
x cnbr-installer-<release-version-tag>/offline-products/cnbr-stable.tar
x cnbr-installer-<release-version-tag>/offline-products/cnbrmanager-stable.tar
x cnbr-installer-<release-version-tag>/README.md
x cnbr-installer-<release-version-tag>/utility-images/
x
```

```
            cnbr-installer-<release-version-tag>/utility-images/cluster-manager-docker-deployer_<version-tag>.tar
          x cnbr-installer-<release-version-tag>/utility-images/autodeploy_<version-tag>.tar
```

Step 2   After the `cnbr-installer-.SPA.tgz` is verified:

```
> cd cnbr-installer-<release-version-tag>
```

The directory, `staging/cnbr-installer-\<release-version-tag\>`, is referred to as staging or install directory. The directory has the following content:

```
~/staging/cnbr-installer-<version-tag>$ tree
.
├── certs
│   ├── client_certificates
│   └── metrics
├── cluster-deployer-<version-tag>.tar
├── deploy
├── docker-images
│   └── ccmts-customization_<version-tag>.tar
├── examples
│   ├── aio-opshub-config.yaml       # For Experimental, Lab/Demo purpose only
│   ├── day1_config_mn.yaml
│   ├── deployer-sample-config.yaml
│   ├── l3_template.json
│   ├── multinode-cnbr-bare-metal-config.yaml
│   ├── multinode-cnbr-config.yaml
│   ├── multinode-cnbr-expansion-config.yaml
│   ├── multinode-cnbr-expansion-link-redundancy-config.yaml
│   ├── multinode-opshub-config.yaml
│   ├── multinode-opshub-multi-nic-config.yaml
│   └── sg_template_4x4.json
├── offline-products
│   ├── cee-<version-tag>.tar
│   ├── cnbrmanager-stable.tar
│   ├── cnbr-stable.tar
│   └── opshub-stable.tar
├── README.md
├── smi-install-disk.iso
└── utility-images
    ├── autodeploy_<version-tag>.tar
    └── cluster-manager-docker-deployer_<version-tag>.tar

7 directories, 22 files
```

Create the Configuration File

The configuration file is in the standard YAML descriptive language format.

Use the following steps to create the configuration file:

Step 1   **Configure the environment**: Cisco cnBR clusters, Cisco Operations Hub clusters, and the SMI Deployer each require an environment for deployment. The environment configuration defines a deployment domain and can be associated, as required, with one or more deployers or clusters.

For the Deployer and Cisco Operations Hub, the deployment domain is VMware vSphere. The environment configuration must include vCenter access information and vSphere ESXi infrastructure details that are used to create and provision the virtual machines.

For the Cisco cnBR, the deployment domain is bare-metal. The environment configuration includes minimal settings that are applied to the UCS Cisco IMC and the guest operating system of the cluster nodes.

Deployer or Cisco Operations Hub VM-based environment configuration:

```
environments:
"<<env-name>>":                                  # Environment name
      server: "<<XX.XX.XX.XX>>"                     # vCenter Server IP
      username: "<<user-name>>"                     # vCenter username, user will be prompted for
 the password
      datacenter: "<<vmware datacenter>>"           # DataCenter Name
      cluster: "<<vcenter cluster>>"                # vCenter Cluster Name
      nics: [ "<<VM Network>>", "<<VM Network1>>" ] # vCenter nics (port groups)
      nameservers: [ "<<YY.YY.YY.YY>"]              # DNS Servers
      search-domains: [ "<<yourdomain>>" ]          # Search domains
      ntp: "<<yourclock.domain>>"                   # NTP Server
      https-proxy: "<<http://proxyhost.domain:port>>"
      no-proxy: "<<127.0.0.1,localhost>>"
```

cnBR Environment config:

```
"<<env-name>>":                                  # Environment name, typically "ucs"
   ntp: "<<yourclock.domain>>"                   # NTP Server
   nameservers: [ "<<YY.YY.YY.YY>"]              # DNS Servers
   search-domains: [ "<<yourdomain>>" ]          # Search domains
```

Step 2   **Configure the deployer**: The deployer configuration requires an environment and settings that are used for the ESXi VM and the guest operating system:

```
deployers:
  "<<deployer3-test>>":                               # deployer VM name
      environment: "<<vcenter-env>>"                  # reference to vCenter environment
      address: "<<XX.XX.XX.XX/prefix_len>>"           # SSH-IP of the VM in CIDR format
      gateway: "<<XX.XX.XX.XX>>"                       # Gateway for the VM
      ingress-hostname: "<<host.domain>>"             # Custom ingress hostname for the deployer -
FQDN (Optional)
      username: "<<user-name>>"                       # Deployer VM username, user will be prompted
for the password
      # SSH private-key-file with path relative to the staging directory
      # Key will be auto-generated, if one if not provided
      private-key-file: "<<cmts.pem>>"
      host: "<<XX.XX.XX.XX>>"                          # Server IP where Deployer VM is hosted
      datastore: "<<datastore1>>"                     # Datastore for the Deployer VM
```

When you configure a custom ingress hostname for the deployer, ensure that the following entries are in the DNS:

```
<host.domain>
charts.<host.domain>
files-offline.smi-cluster-deployer.<host.domain>
deployer-ui.smi-cluster-deployer.<host.domain>
cli.smi-cluster-deployer.<host.domain>
restconf.smi-cluster-deployer.<host.domain>
docker.<host.domain>
```

Step 3   **Configure the cluster**: Both Cisco cnBR and Cisco Operations Hub cluster configurations must have at least one environment and one deployer that is defined in order to be deployed.

A cluster can be one of the following types:

- Multi-Node Cisco cnBR

- Multi-Node Cisco Operations Hub

Note
- Single-Node Cisco Operations Hub is supported for Lab or Demo purpose only.

- Single-Node Cisco cnBR clusters are not supported.

Multi-Node cnBR Configuration

- The Cisco cnBR Multi-Node Cluster config below creates a 3 node bare-metal cnBR cluster

- Four Management IP Addresses are required = 3 for the Control Plane Nodes + 1 Primary Virtual IP

- For each control-plane-node below, update the **address**, **cimc ip-address**, and **cimc username** accordingly

cnBR Multi-Node Cluster Configuration:

```
clusters:
# Name of the cluster
"<<cnbr-multi>>":                               # cnBR cluster name
    type: "<<cnbr>>"                            # Cluster type 'cnbr'
    environment: "<<ucs-env>>"                  # reference to UCS environment
    ingress-hostname: "<<FQDN>>"                # Optional ingress-hostname
    gateway: XX.XX.XX.XX                        # Gateway for the Cluster
    username: "<<user-name>>"                   # Cluster username, User will be prompted for the
 cluster password
    # SSH private-key-file with path relative to the staging directory
    # Key will be auto-generated, if not provided
    private-key-file: "<<cmts.pem>>"
    ethernet: "<interface-name>"                # Kubernetes Host MGMT Interface Name
    primary-vip: "<<XX.XX.XX.XX/prefix_len>>"      # Primary Virtual IP in CIDR format for Multi-Node
 only
    # Keepalived Virtual Router ID, value must be between 0-255
    # Each Multi-Node cluster of any type on the same MGMT Network must have a unique value configured

    vrouter-id:  "<<value>>"
    control-plane-nodes:
        - address: "<<XX.XX.XX.XX/prefix_len>>"
          cimc: {"ip-address": "<<XX.XX.XX.XX>>", "username": "<<cimc-user-name>>"}
        - address: "<<XX.XX.XX.XX/prefix_len>>"
          cimc: {"ip-address": "<<XX.XX.XX.XX>>", "username": "<<cimc-user-name>>"}
        - address: "<<XX.XX.XX.XX/prefix_len>>"
          cimc: {"ip-address": "<<XX.XX.XX.XX>>", "username": "<<cimc-user-name>>"}
```

Multi-Node and Single Node Operations Hub

- The Reference Multi-Node Configuration below distributes the Cluster Node VMs across three ESXi Hosts evenly with proper compute resource reservation

- 13 Management IP Addresses total = 12 for the Cluster Nodes + 1 Primary Virtual IP

- For each node below, update the **k8s ssh-ip**, **VMware data store**, and **VMware host** accordingly

```
clusters:
# Name of the cluster
"<<opshub-multi>>":                             # Operations Hub cluster name
    type: "<<opshub>>"                          # Cluster type 'opshub'
```

```
environment: "<<vcenter-env>>"                    # reference to vCenter environment
gateway: XX.XX.XX.XX                              # Gateway for the Cluster
username: "<<user-name>>"                         # Cluster username, User will be prompted for the
cluster password
   # SSH private-key-file with path relative to the staging directory
   # Key will be auto-generated, if not provided
private-key-file: "<<cmts.pem>>"
primary-vip: "<<XX.XX.XX.XX/prefix_len>>"     # Primary Virtual IP in CIDR format for Multi-Node
only
   # Keepalived Virtual Router ID, value must be between 0-255
  # Each Multi-Node cluster of any type on the same MGMT Network must have a unique value configured

  vrouter-id:  "<<value>>"


 # For Multi-Node only
 nodes:
   - host: "<<XX.XX.XX.182>>".                    # ESXi Host IP Address or Name in vCenter Cluster
     # IP addresses assigned to control-plane-node, etcd, infra and docsis/ops nodes respectively
     addresses: [ "<<XX.XX.XX.187>>", "<<XX.XX.XX.172>>", "<<XX.XX.XX.169>>", "<<XX.XX.XX.190>>"]
     datastore: "<<XX.XX.XX.182-datastore1>>"
   - host: "<<XX.XX.XX.176>>"
     addresses: [ "<<XX.XX.XX.188>>", "<<XX.XX.XX.173>>", "<<XX.XX.XX.170>>", "<<XX.XX.XX.191>>"]
     datastore: "<<XX.XX.XX.176-datastore1>>"
   - host: "<<XX.XX.XX.184>>"
     addresses: [ "<<XX.XX.XX.189>>", "<<XX.XX.XX.174>>", "<<XX.XX.XX.171>>", "<<XX.XX.XX.192>>"]
     datastore: "<<XX.XX.XX.184-DataStore1>>"

 # For Single-Node cluster [ Only supported, for Lab/Demo purpose for OperationsHUB ]
 nodes:
   - host: "<<XX.XX.XX.182>>"                      # ESXi Host IP Address or Name in vCenter Cluster
     addresses: [ "<<XX.XX.XX.187/prefix_len>>"]
     datastore: "<<XX.XX.XX.182-datastore1>>"
```

When you configure a custom ingress hostname for a cluster, ensure that the following entries are in the DNS:

- For Cisco cnBR

```
<host.domain>
cli.ccmts-infra-ops-center.<host.domain>
documentation.ccmts-infra-ops-center.<host.domain>
restconf.ccmts-infra-ops-center.<host.domain>
docs.cee-data-product-documentation.<host.domain>
cli.cee-data-ops-center.<host.domain>
documentation.cee-data-ops-center.<host.domain>
prometheus-hi-res.cee-data-cnat-monitoring.<host.domain>
restconf.cee-data-ops-center.<host.domain>
show-tac-manager.cee-data-smi-show-tac.<host.domain>
grafana.<host.domain>
```

- For Cisco Operations Hub:

```
<host.domain>
cli.opshub-data-ops-center.<host.domain>
documentation.opshub-data-ops-center.<host.domain>
restconf.opshub-data-ops-center.<host.domain>
docs.cee-data-product-documentation.<host.domain>
cli.cee-data-ops-center.<host.domain>
documentation.cee-data-ops-center.<host.domain>
prometheus-hi-res.cee-data-cnat-monitoring.<host.domain>
restconf.cee-data-ops-center.<host.domain>
```

```
show-tac-manager.cee-data-smi-show-tac.<host.domain>
restconf.cnbrmanager-data-ops-center.<host.domain>
```

Deploy the Cluster

Deploy the cluster by using the following command:

```
~/cnbr-installer-<release-version-tag>$ ./deploy -c <config_file>
```

The Cluster Manager is deployed first, before deploying any cluster. To deploy more clusters, run the command with the corresponding configuration files.

Deployment Example Configurations

Feature History

Table 10: Feature History

Feature Name	Release Information	Feature Description
Second NIC configuration on the Cisco Operations Hub for cable modem data	Cisco cnBR 20.3	You can configure second NIC on the Cisco Operations Hub cluster that connects to CIN network, allowing the Cisco Operations Hub to poll cable modem data such as SNR and TX/RX power.
Multiple NIC configuration on the Cisco Operations Hub for cable modem data	Cisco cnBR 21.2	You can configure multiple NIC on the Cisco Operations Hub cluster that connects to CIN network, allowing the Cisco Operations Hub to poll cable modem data such as SNR and TX/RX power.

Example configuration files are included with the installation package and are located in the examples directory. You can copy and modify the required example configuration files.

Ensure that you have gone through the Step 1 and Step 2 topics.

- **Sample Deployer Configuration**

  The following is a sample configuration to deploy the cluster manager.

  ```
  environments:
    "vcenter-env":
        server: "XX.XX.XX.XX"
        username: "vCenter username"
        datacenter: "vmware datacenter"
        cluster: "vmware cluster"
        nics: [ "VM Network" ]
        nameservers: [ "DNS1", "DNS2"]
  ```

```
        search-domains: [ "yourdomain" ]
        ntp: "yourclock.yourdomain"
        https-proxy: "http://proxyhost.domain:port"
        no-proxy: "127.0.0.1,localhost"

  deployers:
    "deployer3-test":
        environment: "vcenter-env"
        address: "XX.XX.XX.194/prefix_len"
        gateway: "XX.XX.XX.129"
        username: "cloud-user"
        private-key-file: "cmts.pem"
        host: "XX.XX.XX.184"
        datastore: "XX.XX.XX.184-DataStore1"
```

- **Multi-Node cnBR Configuration**

  Define the cluster configuration as shown:

```
  clusters:
    "cnbr-mnode":
        type: "cnbr"
        environment: "ucs"
        primary-vip: "XX.XX.XX.193/prefix_len"
        username: "cloud-user"
        private-key-file: "cmts.pem"
        ethernet: "eno1"
        vrouter-id:  "95"
        gateway: XX.XX.XX.129
        control-plane-nodes:
          - address: "XX.XX.XX.187/24"
            cimc: {"ip-address": "XX.XX.XX.125", "username": "admin"}
          - address: "XX.XX.XX.188/24"
            cimc: {"ip-address": "XX.XX.XX.126", "username": "admin"}
          - address: "XX.XX.XX.189/24"
            cimc: {"ip-address": "XX.XX.XX.127", "username": "admin"}
```

- **Multi-Node Operations Hub Configuration**

  Define the cluster configuration as shown:

```
  clusters:
    "opshub-mnode":
        type: "opshub"
        environment: "vcenter-env"
        primary-vip: "XX.XX.XX.193/prefix_len"
        gateway: XX.XX.XX.129
        vrouter-id:  "193"
        username: "cloud-user"
        private-key-file: "cmts.pem"
        size: "normal"  # By default, multi-node Operations Hub deployment config size
  is 'small', use 'normal' for deployment with higher configuration requirements.
        nodes:
          - host: "XX.XX.XX.182"
            datastore: "XX.XX.XX.182-datastore1"
            addresses: [ "XX.XX.XX.187", "XX.XX.XX.172", "XX.XX.XX.169", "XX.XX.XX.190"]

          - host: "XX.XX.XX.176"
            datastore: "XX.XX.XX.176-datastore1"
            addresses: [ "XX.XX.XX.188", "XX.XX.XX.173", "XX.XX.XX.170", "XX.XX.XX.191"]

          - host: "XX.XX.XX.184"
```

```
                datastore: "XX.XX.XX.184-DataStore1"
                addresses: [ "XX.XX.XX.189", "XX.XX.XX.174", "XX.XX.XX.171", "XX.XX.XX.192"]
```

- **Multi-Node Operations Hub Configuration with Custom Ingress Hostname and 2nd Network Interface on Ops Nodes**

  Define the cluster configuration as shown:

```
clusters:
  "opshub-mnode":
      type: "opshub"
      environment: "vcenter-env"
      primary-vip: "XX.XX.XX.193/prefix_len"
      gateway: XX.XX.XX.129
      vrouter-id:  "193"
      ingress-hostname: "opshub1.cisco.com"
      username: "cloud-user"
      private-key-file: "cmts.pem"
      size: "normal"  # By default, multi-node Operations Hub deployment config size
is 'small', use 'normal' for deployment with higher configuration requirements.
      nodes:
        -  host: "XX.XX.XX.182"
           datastore: "XX.XX.XX.182-datastore1"
           addresses: [ "XX.XX.XX.187", "XX.XX.XX.172", "XX.XX.XX.169", "XX.XX.XX.190"]

           nics: [ "OpsHub7-Remote-Query" ]
           ops:
             interfaces:
               - addresses: [ "5.202.0.40/24" ]
                 routes:
                   - {dest: [ "5.225.0.0/16" ], nhop: "5.202.0.1" }
        -  host: "XX.XX.XX.176"
           datastore: "XX.XX.XX.176-datastore1"
           addresses: [ "XX.XX.XX.188", "XX.XX.XX.173", "XX.XX.XX.170", "XX.XX.XX.191"]

           nics: [ "OpsHub7-Remote-Query" ]
           ops:
             interfaces:
               - addresses: [ "5.202.0.41/24" ]
                 routes:
                   - {dest: [ "5.225.0.0/16" ], nhop: "5.202.0.1" }
        -  host: "XX.XX.XX.184"
           datastore: "XX.XX.XX.184-DataStore1"
           addresses: [ "XX.XX.XX.189", "XX.XX.XX.174", "XX.XX.XX.171", "XX.XX.XX.192"]

           nics: [ "OpsHub7-Remote-Query" ]
           ops:
             interfaces:
               - addresses: [ "5.202.0.42/24" ]
                 routes:
                   - {dest: [ "5.225.0.0/16" ], nhop: "5.202.0.1" }
```

- **Single-Node Operations Hub Configuration**

  The Single Node Cluster is not supported for production. It is restricted for use at the Lab.

  Define the cluster configuration as shown:

```
clusters:
  "opshub-snode":
      type: "opshub"
      environment: "vcenter-env"
      gateway: XX.XX.XX.129
```

```
username: "cloud-user"
private-key-file: "cmts.pem"
nodes:
  -  host: "XX.XX.XX.139"
     datastore: "XX.XX.XX.139-datastore1"
     addresses: [ "XX.XX.XX.159/prefix_len" ]
```

Deployment Limitations

The following are the deployment limitations in this release:

- IPv6 addressing is not supported.

- The config file must comply to YAML syntax. Not conforming to the syntax might cause crash dumps.

- The configuration file must comply to all mandatory sections and attributes. You might see the autodeploy exit without warnings and errors when mandatory attributes are missing in the configuration file.

- Limited error and exception handling. When an exception or error occurs, you might see detailed crash dumps.

- Single node cluster for Cisco Operations Hub is not supported in production. Single Node Cisco Operations Hub clusters are meant for use at the Lab.

Configure Operations Hub

The Cisco Operations Hub allows you to create and configure users.

This section provides details of how to configure the Cisco Operations Hub and to use the UI and APIs.

Access Operations Hub

You can access the **Operations Hub** home page using the following URL:

`https://{Hostname}`

`Hostname` is the Fully Qualified Domain Name (FQDN) of the Cisco Operations Hub cluster, which is configured using the `ingress-hostname` key of the deployer configuration. When the Cisco Operations Hub cluster is deployed without the `ingress-hostname` key, the format of the `Hostname` is `{vip}.nip.io`, where `vip` is the virtual IP address of the Cisco Operations Hub cluster.

Customize Login Banner

Feature History

Table 11: Feature History

Feature Name	Release Information	Feature Description
Login Banner Messages	Cisco cnBR 21.2	You can create and display a customized message that appears as a banner on the Cisco Operations Hub login page.

An administrator can create and customize a banner for the Cisco Operations Hub login page.

You can also use APIs to customize the banner. For more details, see the *Cisco Cloud Native Broadband Router Operations Hub REST API Guide*.

To customize the banner, use the following procedure:

Step 1   On the Cisco Operations Hub, click the Cisco Operations Hub main menu button.

Step 2   Choose **System** > **Login Banner Message**.

Step 3   Enter the message in the text box and click Save.

A maximum of 500 characters are allowed in the banner message text box.

Navigate through Operations Hub

Feature History

Table 12: Feature History

Feature Name	Release Information	Feature Description
New dashboard home page and left navigation menu	Cisco cnBR 21.2	The Metrics & Dashboards page in the cnBR Manager has been renamed Dashboards and promoted to be a top level Cisco Operations Hub main menu item. The Dashboards home page has been updated to include a list of Suggested and Recently viewed dashboards. Additionally, the left navigation menu on the Dashboards page has been streamlined to improve usability.

After the Operations Hub is deployed successfully, you can navigate through the main menu. An overview of the navigation options is provided below.

Overview of the Navigation Options

Main Menu: 1st Level Option	Main Menu: 2nd level	Submenu and Fixed Navigation Items
cnBR Manager	cnBRs: Allows you to perform all cnBR related operations.	• Inventory: Overview of cnBR clusters. • Add cnBR: Add cnBR clusters. • Import & Export cnBR: Import and export cnBR configurations. • Service Group Operations: Overview of service groups, and allows you to move service groups across nodes. • Smart Licensing: cnBR license management operations.
	Remote PHY Devices: Allows you to perform all RPD related operations.	• Inventory: Overview of the RPDs in the network. • Add RPD: Add RPD in cnBR. • Edit RPD: Edit RPD configuration parameters. • Replace RPD: Replace MAC Address of an existing RPD. • Delete RPD: Remove a RPD from cnBR. • Image Management: View and upload RPD software images. • Secure Software Download: Apply software images to RPD. • Code Validation Check: View and apply code validation certificates. • Cutover RPD: Perform RPD cutover.
	Profiles and Templates: Allows you to add, edit and delete cnBR Profiles and Templates.	None

Main Menu: 1st Level Option	Main Menu: 2nd level	Submenu and Fixed Navigation Items
Dashboards: Allows you to view Grafana Dashboards.	None	• Suggested & Recently Viewed: Launch point of Operations Hub Grafana homepage, including a list of recently viewed dashboards. • Find a Dashboard: Search a Grafana dashboard. • Advanced: Create new dashboards and folders, navigate to existing folders and import existing dashboards.
API Explorer: Allows you to view Operations Hub and cnBR API list.	None	• List of Operations Hub and cnBR APIs.
System	Logs: Allows you to view and manage Logs.	• Audit Dashboard: Dashboard to view Audit Logs. • Debug Dashboard: Dashboard to view Debug Logs. • Advanced: Advanced configuration options to discover, visualize, and manage Kibana dashboards.
	Configuration & Upgrade: Import and export Operations Hub configuration file.	• Import & Export Configuration: Import and export Operations Hub configuration file.
	Login Banner Message: View and configure login banner message for Operations Hub.	None

User Management in Cisco Operations Hub

Cisco Operations Hub provides user management functionality where you can create local users and configure LDAP for external authentication. Refer to the following topics for details on user types and how to configure local and LDAP users.

API User Roles

Operations Hub supports three user roles based on the HTTP actions:

> • api-admin: Allowed http method: GET, POST, PUT, DELETE
>
> • api-editor: Allowed http method: GET, POST, PUT
>
> • api-viewer: Allowed http method: GET

By default, the user, admin is already under these three groups.

Configure Local Users

Administrators can perform following user management actions from **Systems > Security > Users & Roles**.

Note For users other than admin, User & Roles page isn't visible.

Add User

Step 1   On the Cisco Operations Hub, click **System > Users & Roles** to open the Users & Roles page.

Step 2   Click **Add User** in the Users & Roles page to open Add User side bar.

Step 3   Fill in the email, role, and password for the new user. Strictly follow the password requirement listed in the side bar.

   Force password change on next login option is selected by default. Newly created user must change the password during the first login.

Step 4   Click **Add User** button to confirm creating the new user.

Edit User

Step 1   On the Cisco Operations Hub, click **System > Users & Roles** to open the Users & Roles page.

Step 2   Select a user and click **Edit User** in the Users & Roles page to open Edit User side bar.

Step 3   You can change the user role and password expiration period.

Step 4   Click **Save** when you finish editing.

Remove User

Step 1   On the Cisco Operations Hub, click **System > Users & Roles** to open the Users & Roles page.

Step 2   Select a user and click **Remove User** in the Users & Roles page, a window pops up.

Step 3   Click **Remove** in the pop-up window to remove the selected user.

Export

Step 1   On the Cisco Operations Hub, click **System > Users & Roles** to open the Users & Roles page.

Step 2   Click **Export** in the Users & Roles page to export the content of the user management table.

Filter Users in the User List

You can use the **Focus** dropdown list and the **Role** buttons **Admin**, **Editor**, and **Viewer** to filter the users in the user list based on password status and user role.

View Session History

Step 1   On the Cisco Operations Hub, click **System > Users & Roles** to open the Users & Roles page.

Step 2   Click a user name in the Users & Roles page to open User Details side bar.

Step 3   Select **Sessions History** tab to view the login/logout history of the user.

Change Password

You can change the password:

- from the Cisco Operations Hub main menu by clicking the user name and updating the password in the My Account page.

- from the alert banner. Alert banner appears 30 days before password expiry. You can change your password by clicking the link in the alert banner. If your password expires, reset the password during next login.

Configure LDAP

Feature History

Table 13: Feature History

Feature Name	Release Information	Feature Description
Integration with LDAP Server	Cisco cnBR 21.3	This feature allows you to use existing LDAP credentials to log in Cisco Operations Hub and configure the LDAP parameters.

Local authentication is enabled by default. Administrators can change the authentication method to LDAP in **Systems > Authentication**.

Note   LDAP configuration page is visible to admin users only.

To configure LDAP, fill in the following fields.

LDAP Parameters	Description
LDAP Server URL	URL of the LDAP server.

LDAP Parameters	Description
Base Domain Name	Domain name as configured on your LDAP server.
LDAP User Name Domain	Validate the user name against the domain controller.
LDAP Filter	Specify a subset of data items in an LDAP data type.
LDAP Group Attribute	List of comma-separated LDAP attributes on a group object that can be used in a user member attribute.
LDAP Group Mapping	Map LDAP group to Operations Hub role.

Using REST APIs

This section explains how you can use REST APIs.

Step 1   Create a user.

Use the procedure from the section.

Step 2   Call auth REST API to create token.

Encode the username and password with base 64. Fill the encode output into the Authentication Header.

Example:

```
User: admin
Password: bell

Get the Base64 under Linux: echo -n 'admin:lab' | base64
Base64 encode output: YWRtaW46bGGFi

curl -X POST "https://{Hostname}/api/auth/v1/token" -H  "accept: application/json" -H  "authorization:
 Basic YWRtaW46bGGFi"

Response code: 201
Response body
{
"access_token": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJyb2xlIjoiYXBpLWFkbWluIiwic2FsdCI6IlViQ2daamt
IWHd6RUNzS1EiLCJleHAiOjE1NjQ2NTA2MTd9.x7ccHcOn6fLvHc_ajLJxQEY1ftvR1ZaJH9K_YZx1ues",
"refresh_token": "lYYtZqgVhnsnBJgSHbigRzeEaLnWziMpHJKVzgHA",
"refresh_token_expire": 1567221017,
"token_type": "jwt"
}
```

Step 3   With this token, call other REST APIs.

Example:

Call REST API to get the Cisco cnBR list:

```
curl -X GET "https://opshub1.cisco.com/api/manager/v1/cmts" -H  "accept: application/json" -H
  "Authorization: Bearer eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJyb2xlIjoiYXBpLWFkbWluIiwic2FsdCI6IlV
iQ2daamtIWHd6RUNzS1EiLCJleHAiOjE1NjQ2NTA2MTd9.x7ccHcOn6fLvHc_ajLJxQEY1ftvR1ZaJH9K_YZx1ues"

Response code:200
Response body
{
```

```
  "cluster_list": [
    {
      "cluster-id": "cnbr1.cisco.com",
      "cmts-name": "test",
      "namespace": "ccmts-infra",
      "ingress-host-name": "cnbr1.cisco.com"
    }
  ]
}
```

Configure TLS Certificate

When Cisco Operations Hub is deployed, a self-signed certificate is automatically created and used for TLS connections. You can replace the self-signed certificate with a CA signed certificate through the Cluster Manager CLI.

Note   If you replace the Cisco Operations Hub self-signed TLS certificate, you must update the `cert-api-ingress` secret-name in two Kubernetes (K8s) namespaces: `opshub-data` and `cnbrmanager-data`. In this case, provide the CA-signed certificate and the private key that is associated with the certificate.

The following example shows how to make the required changes. This example does not show the certificate or the private-key entries. Make sure that you include those:

```
product opshub# config terminal
Entering configuration mode terminal
product example deployer(config)# clusters {k8s-cluster-name}
product example deployer(config-clusters-******)# secrets tls opshub-data cert-api-ingress
 ?
Possible completions:
  certificate    Path to PEM encoded public key certificate.
  private-key    Private key associated with given certificate.
  <cr>
product example deployer(config-clusters-******)# secrets tls cnbrmanager-data
cert-api-ingress ?
Possible completions:
  certificate    Path to PEM encoded public key certificate.
  private-key    Private key associated with given certificate.
  <cr>
product example deployer(config-clusters-******)#commit
product example deployer(config-clusters-******)#exit
```

After exiting the configuration mode, synchronize the cluster configuration by running the following command:

```
clusters {k8s-cluster-name} actions sync run
```

Configure Cisco cnBR Using Autodeployer

You can complete the Cisco cnBR configuration using the Autodeployer.

Complete the following steps:

Step 1 Prepare Cisco cnBR configuration.

There are three categories of configuration:

- **General Configuration**

The general configuration specifies details of the Cisco cnBR and Cisco Operations Hub clusters.

```
opshub :
    ip : 'xx.xx.xx.xx'             # Operations Hub IP address
    ingress-hostname: '<host.domain>'  # Operations Hub ingress hostname - FQDN (Optional: If
the <host.domain> is not available, the default cluster ingress <IPAddress>.nip.io is used.)
cnbr   :
    name : '<name_of_cnbr>'       # Name of the Cisco cnBR cluster to be added to the Operations
 Hub
    type : 'MUL_NODES'            # cnBR cluster Type : 'MUL_NODES' Multi-Node cluster is only
option supported.
    ip   : 'xx.xx.xx.xx'          # cnBR IP address
    ingress-hostname: '<host.domain>'  # cnBR Ingress Hostname - FQDN (Optional: If the
<host.domain> is not available, the default cluster ingress <IPAddress>.nip.io is used.)
    number-of-docsis-node: 3   # Total Number of DOCSIS nodes
```

- **Mandatory Configuration**

The mandatory configuration specifies details for the PTP, BGP, CIN, Wiring, templates (SG and L3) and RPD-list.

Complete the following mandatory configurations:

- PTP Configuration

```
ptp :
    v4 :
        domain : <clock-domain>
        master: {'ip':"xx.xx.xx.xx", 'gw':"xx.xx.xx.xx"}
```

- BGP Agent Configuration

```
bgpagent :
    asn : <asn>
    max_hops : <max_hops>
    restart-time : <restart_time>
    stale-path-time: <stale_path_time>
    # list of neighbors ( IPv4 and IPv6 )
    neighbors :
      - {'address' :'xx.xx.xx.xx', 'asn':<asn>}
```

- CIN Configuration

```
# Lists of IPv4 and IPv6 gateways. IPv6 is not supported in this release.
cin :
    v4 : [ "xx.xx.xx.xx"]
```

- Wiring Configuration

```
wiring :
    # Starting IP address for the range to be used by cnBR internal interfaces
    # Make sure the range does not clash with IP addresses of RPD, COPS, and CCAPCORE
    # IP addresses that will be carved out from this pool to assign to the below interfaces
    #     PTP, VPP-DP and other interface
    cin-start-ip:
```

```
                      v4 : 'xx.xx.xx.xx'

              # SG peer IP, typically its bgp-neighbor IP address but it could be different
              #     dmic-if and relayproxy-if addresses are carved out from the same network
              sg-peer:
                 v4 : 'xx.xx.xx.xx'
                 v6 : 'xxxx::nnn'  #Needs dummy value even if IPv6 is not enabled. nnn is <0-255>

              # ccapcore IP, specified in the DHCP config, where RPD learn ccapcore from
              rphmgr-if:
                 v4 : "xx.xx.xx.xx"

              # Packet cable interface IP
              cmts-cops-if:
                 v4 : "xx.xx.xx.xx"

              # IP addresses to be used by BGP agents running in cnBR
              # AIO needs one and MultiNode needs two as that many instances of bgp agents would be
        running in the cluster
              bgp-agent-if:
                 v4 : ["xx.xx.xx.xx", "xx.xx.xx.xx"]
                 v6 : ["xxxx::xxxx", "xxxx::xxxx"]  #Needs dummy values even if IPv6 is not enabled.

              # CIN Prefix
              cin-prefix:
                 v4 : <prefix_len>
                 v6 : <prefix_len> #Needs dummy value even if IPv6 is not enabled due to known issue

              # DC link prefix to be used by CIMC interfaces within cnBR
              # v4 and v6 prefixes are mandatory for now due to an internal issue, even if v6 is not
        enabled.
              #   will have a fix in the next release.
              dc-link-prefix:
                 v4 : <prefix_len>
                 v6 : <prefix_len> #Needs dummy value even if IPv6 is not enabled due to known issue

              # VLAN or VXLAN config, whichever is applicable
              vlan :
                 cnbr-wan-ifname: "<name>/<slot>/<port>"             # 1st Interface Name -
        "Ethernet0/0/0"
                 overlay-wan-vlan: <xxxx>
                 overlay-cin-vlan: <xxxx>
                 overlay-l2vpn-vlan-vlan: <xxxx>
                 overlay-l2vpn-mpls-vlan: <xxxx>
              vxlan :
                 sp-router-wan-ip: "xx.xx.xx.xx"
                 cnbr-wan-prefix: <prefix_len>
                 cnbr-wan-ip: "xx.xx.xx.xx"
                 cnbr-wan-ifname: "<name>/<slot>/<port>"
                 cnbr-loopback-ip: "xx.xx.xx.xx"
                 sp-router-loopback-ip: "xx.xx.xx.xx"
                 overlay-cin-vni: <cin-vni>
                 overlay-l2vpn-mpls-vni: <mpls-vni>
                 overlay-l2vpn-vlan-vni: <vlan-vni>
                 overlay-wan-vni: <wan-vni>
              # MTU used by cnBR SG
              mtu : "2450"
```

• VLAN section of the wiring configuration with Link Redundancy enabled:

```
              # VLAN config, whichever is applicable
              vlan :
                 cnbr-wan-ifname: "<name>"                          # Bond Interface Name
        -"BondEthernet0"
                 cnbr-wan-bonded-interface1: "<name>/<slot>/<port>"  # 1st Interface Name -
```

```
"Ethernet0/0/0"
        cnbr-wan-bonded-interface2: "<name>/<slot>/<port>"    # 2nd Interface Name -
"Ethernet0/0/1"
        cnbr-wan-bond-mode: "<mode>"                          # Mode - lacp, roundrobin,
activebackup, xor, broadcast
        cnbr-wan-bond-loadbalance: "<type>"                   # Load Balance - L2, L34, L23,
RR, BC
        overlay-wan-vlan: <xxxx>
        overlay-cin-vlan: <xxxx>
        overlay-l2vpn-vlan-vlan: <xxxx>
        overlay-l2vpn-mpls-vlan: <xxxx>
```

- Service Group (SG) and RPD List: Specify the list of RPDs that the Cisco cnBR has to load as RPD-list. File paths are relative to the staging directory or the directory from where you are running autodeploy. Go through Autodeployer Examples, on page 49 for examples onon L3 Template, SG Template, and Video Template.

```
templates:
    # List of L3 templates in the {<name>:<file_path>} format
    L3 :
        'L3-1' : '<L3 template1 file>'
        'L3-2' : '<L3 template2 file>'

    # List of SG templates in the {<name>:<file_path>} format
    SG :
        '4x4_SG_Config'  : '<SG template1 file>'
        '33x8_SG_Config' : '<SG template2 file>'

    # List of Video Downstream SC QAM templates in the {<name>:<file_path>}
format.
    # Optional parameters: specify only while configuring Video DS SC QAM Service

    Video :
        'NC_Video_Config'  : '<Video QAM template1 file>'
        'BC_Video_Config'  : '<Video QAM template2 file>'

# Video QAM Template to Downstream Port Association.
# Optional parameters: specify only while configuring Video DS SC QAM Service
service-configs:
    VT0:
        - port: "DS-0"
          groups: ["NC_Video_Config", "BC_Video_Config"]

# RPD location
RPD-loc1: &loc1
        region: "<region>"
        city: "<city>"
        neighborhood: "<neighborhood>"
        address: "<address>"
        latitude: <latitude>
        longitude: <longitude>

# List of RPDs, 'Video_tmpl' is an optional parameter: specify only while
configuring Video DS SC QAM Service
rpd-list:
    # [ 'rpd-name', 'rpd-mac', 'SG_name', 'SG_tmpl', 'L3_tmpl', 'RPD_location',
'Video_tmpl']
        - [ 'RPD-00', 'xx:xx:xx:xx:xx:xx', 'SG00', '33x8_SG_Config', 'L3-1', *loc1,
'VT0']
        - [ 'RPD-01', 'xx:xx:xx:xx:xx:xx', 'SG01', '33x8_SG_Config', 'L3-1', *loc1 ]
        - [ 'RPD-02', 'xx:xx:xx:xx:xx:xx', 'SG02', '4x4_SG_Config', 'L3-2', *loc1 ]
```

- **Optional Configuration**

Choose the optional configurations required. The configuration specifies details for L2VPN, L3VPN, TFTP, PacketCable, RIP, SAV, and PFG:

```
# Specify, if tftpProxy is different from CIN gateway
tftpProxy:
    v4 : ["xx.xx.xx.xx"]
    v6 : ["xx:xx:xx:xx:xx:xx:xx:xx"] #specify, if IPv6 is enabled

# cops interface in wiring config needs to be set to enable this feature.
packetcable :
    enable: 'true'
    max-gate: <value>
    t0: <value>
    t1: <value>
    subscriber: 'false'

l2vpn :
    dot1qvc :
        - {'mac':"xxxx.xxxx.xxxx", 'vlan':<vlan>, 'vpn':"<name>"}
    mplsvc :
        - {'mac':"xxxx.xxxx.xxxx", 'peerip':<peerip>, 'vc': 1, 'vpn':"<name>", 'experimental':0}
    mplsvlansg :
        - {'sg':"xxxx.xxxx.xxxx", 'vlan_max':<vlan_max>, 'vlan_min':0}
    sprstat :
        - {'id':"xxxx.xxxx.xxxx", 'asn':<asn>, 'state':'Up'}

l3vpn:
    - {"name" : "<name>", "vlan" : <vlan>, "vpn" : "<name>"}

rip :
    enable : 'false'
    update-timer : <time in seconds>
    invalid-timer : <time in seconds>
    holddown-timer : <time in seconds>
    passive-mode' : 'false'

sav:
    enable : 'true'
    entries:
        - grp-name : "testSAV"
          prefixes : [ "xx.xx.xx.xx/<prefix_len>" , "xx:xx:xx:xx:xx:xx:xx/<prefix_len>" ]

pfgactive:

{"cm_ds":-1,"cm_us":-1,"host_ds":-1,"host_us":-1,"mta_ds":-1,"mts_us":-1,"stb_ds":-1,"stb_us":-1,"ps_ds":-1,"ps_us":-1}

pfg:
    - id : 1
      rules :
          - {"isPermit":0, "isIpv6":0, "srcIp":'xx.xx.xx.xx/<prefix_len>',
"dstIp":"xx.xxx.xx.xx/<prefix_len>"}
```

Step 2   Apply the configuration.

Run the deploy command to apply the configuration and monitor the status through the Cisco Operations Hub or CLI. You can update the configuration file to add, delete, or update the SGs or RPDs and rerun the command to apply the updated configuration.

```
$ ./deploy -c cnbr_config.yaml
```

The configuration file must strictly conform to YAML syntax, to avoid any crash dumps.

Note To remove Video Downstream SC QAM Service ('Video_tmpl') from specific RPDs, use the -f option to force the update. Without the -f option, the Cisco cnBR ignores this change. The -f option forces the Cisco cnBR to delete and readd the RPD.

Configure Remote cnBR Cluster Monitoring from Operations Hub

Prometheus Metrics

The CEE (Cloud Native Execution Environment) monitoring module included with Cisco cnBR and Cisco Operations Hub supports local cluster and remote cluster infrastructure monitoring. The monitoring module is based on the Prometheus, Thanos, and Node Exporter Open Source projects. Prometheus is configured to scrape the local Kubernetes resources and the node exporter. Node exporter provides all system level information, and Thanos collects these metrics and exports them to a visualization module.

The monitoring system for Cisco cnBR clusters is the Cisco Operations Hub. The monitored infrastructure and host metrics are visually displayed using Grafana, providing an overall, centralized view of clusters and metrics. The Thanos module on Cisco Operations Hub can be configured to scrape Thanos modules on multiple, remote Cisco cnBR clusters to collect metrics.

The connections to the remote clusters are TLS secured. Hence, a local system must be configured with a client certificate and remote clusters must be configured with server certificates. In the Cisco cnBR and Cisco Operations Hub topology, the local Thanos module on Cisco Operations Hub acts as the client and the Cisco cnBR remote cluster acts as the server.

The configuration process for the local and remote clusters is now automated, and is handled by the Autodeployer utility as part of the Cisco cnBR configuration phase. You can also alternatively choose to configure the local and remote clusters manually, using the CEE Ops-Center CLI.

To enable monitoring using the Autodeploy utility during the Cisco cnBR configuration phase, complete the following steps:

Step 1 Provide signed client and server ssl-keys, ssl-crts, and an ssl-ca for each cnBR.

Step 2 On the staging server, create a folder for the Cisco cnBR cluster under `certs/metrics/` in the install directory:

```
> cd cnbr-installer-<release-version-tag>/certs/metrics
> mkdir <clustername>
```

Note Ensure that the Cisco cnBR folder name matches the Cisco cnBR cluster name, that was used during deployment.

Step 3 Transfer the client and server ssl files to the new folder.

Ensure that the `ssl-ca` file supplied is named `_ca.crt`. For example:

```
[root@staging-server-1 certs]# tree
.
├── client_certificates
└── metrics
    └── cnbr1
        ├── 172.25.29.236_ca.crt
        ├── 172.25.29.236.clnt.crt
        ├── 172.25.29.236.clnt.csr
        ├── 172.25.29.236.clnt.key
```

```
                    ├── 172.25.29.236.crl
                    ├── 172.25.29.236.key
                    ├── 172.25.29.236.svr.crt
                    ├── 172.25.29.236.svr.csr
                    └── 172.25.29.236.svr.key

3 directories, 9 files
[root@staging-server-1 certs]#
```

Autodeloyer will process these files during the Cisco cnBR cluster configuration phase and configure the monitoring modules through the CEE Ops-Center APIs on both Cisco cnBR and Cisco Operations Hub.

Autodeployer Examples

- Configuration file

```
opshub : 'xx.xx.xx.xx'
cnbr :
    name : 'cnbr001'
    type : 'MUL_NODES'
    ip   : 'xx.xx.xx.xx'
ptp :
    v4 :
        domain : 0
        master: {'ip':"xx.xx.xx.xx", 'gw':"xx.xx.xx.xx"}
bgpagent :
    asn : 65224
    max_hops : 255
    restart-time : 120
    stale-path-time: 360
    neighbors :
        - {'address' :'xx.xx.xx.xx', 'asn':65534}
cin :
    v4 : ["xx.xx.xx.xx"]
wiring :
    cin-start-ip:
        v4 : 'xx.xx.xx.xx'
    sg-peer:
        v4 : 'xx.xx.xx.xx'
    bgp-agent-if:
        v4 : ["xx.xx.xx.xx", "xx.xx.xx.xx"]
        v6 : ["xx:xx:xx:xx::1", "xx:xx:xx:xx::1"]
    rphmgr-if:
        v4 : "xx.xx.xx.xx"
    cmts-cops-if:
        v4 : "xx.xx.xx.xx"
    cin-prefix:
        v4 : 24
        v6 : 64
    dc-link-prefix:
        v4 : 24
        v6 : 64
    vlan :
        cnbr-wan-ifname: "Ethernet0/0/0"
        overlay-wan-vlan: 1001
        overlay-cin-vlan: 1002
        overlay-l2vpn-vlan-vlan: 1007
        overlay-l2vpn-mpls-vlan: 1008
    mtu : "2450"
```

```
templates:
    L3 :
        # {'template_name' : 'template_file_location'}
        'L3_1' : 'l3_template1.json'
    SG :
        # {'template_name' : 'template_file_location'}
        'SG_16x4' : 'sg_template1.json'
    Video :
        # {'template_name' : 'template_file_location'}
        'NC_Video_1'  : 'NC_Video_1.json'
        'BC_Video_1'  : 'BC_Video_1.json'

 service-configs:
    VT0:
        - port: "DS-0"
            groups: ["NC_Video_Config", "BC_Video_Config"]

RPD-loc: &loc1
    region: "CA"
    city: "SanJose"
    neighborhood: "XXXX"
    address: "XXXXXXX"
    latitude: 0
    longitude: 0

rpd-list:
    # [ 'rpd-name', 'rpd-mac', 'SG_name', 'SG_tmpl', 'L3_tmpl', 'RPD_location',
'Video_tmpl']
    - [ 'RPD-00', '78:72:5D:39:26:64', 'SG00', 'SG_16x4', 'L3_1', *loc1, 'VT0']
    - [ 'RPD-01', 'F4:DB:
```

• L3 Template

```
{
  "dhcp": {
    "arpGlean": true,
    "arpProxy": true,
    "dhcpIfname": "cnr",
    "dhcpServers": [
      "xx.xx.xx.xx"
    ],
    "ipv6Lq": true,
    "mobilityScopes": [
      "xx.xx.xx.xx/<prefix_len>",
      "xx:xx:xx:xx:xx:xx:xx:xx/<prefix_len>"
    ],
    "ndProxy": true,
    # Add relayPolicies, if applicable to your setup
    "relayPolicies": [
      {
          "deviceClass": "HOST",
          "giAddr": "xx.xx.xx.xx",
          "linkAddr": "xxxx::xxxx",
          "v4ServerIp": "xx.xx.xx.xx"
      }
    ],
    "relayModeV4": 0,
    "relayModeV6": 0,
    "v4Nets": [
      "xx.xx.xx.xx/<prefix_len>"
    ],
    "v6Nets": [
      "xx:xx:xx:xx:xx:xx:xx:xx/<prefix_len>"
```

```
      ]
    },
    "spRouterName": "<SP router name>",
    "savList": {
      "prefixes": null
    },
    "sgPeerIpv4": "xx.xx.xx.xx/<prefix_len>",
    "sgPeerIpv6": "xx:xx:xx:xx:xx:xx:xx:xx/<prefix_len>"
  }
```

• SG Template

```
{
  "description": "33x8 SG Config",
  "dlb": {
    "enable": true,
    "interval": 60,
    "loadMaxThresh": 80,
    "loadMinThresh": 20,
    "cmSuccessHoldTime": 30,
    "cmFailureHoldTime": 120
  },
  "ds": [
    {
      "annex": "AnnexB",
      "attributeMask": 2147483648,
      "frequency": 255000000,
      "idInSg": 0,
      "interleaver": "fecI32J4",
      "modulation": "qam256",
      "powerAdjust": 0
    },
    {
      "annex": "AnnexB",
      "attributeMask": 2147483648,
      "frequency": 261000000,
      "idInSg": 1,
      "interleaver": "fecI32J4",
      "modulation": "qam256",
      "powerAdjust": 0
    },
    {
      "annex": "AnnexB",
      "attributeMask": 2147483648,
      "frequency": 267000000,
      "idInSg": 2,
      "interleaver": "fecI32J4",
      "modulation": "qam256",
      "powerAdjust": 0
    },
    {
      "annex": "AnnexB",
      "attributeMask": 2147483648,
      "frequency": 273000000,
      "idInSg": 3,
      "interleaver": "fecI32J4",
      "modulation": "qam256",
      "powerAdjust": 0
    },
    {
      "annex": "AnnexB",
      "attributeMask": 2147483648,
      "frequency": 279000000,
      "idInSg": 4,
```

```
                    "interleaver": "fecI32J4",
                    "modulation": "qam256",
                    "powerAdjust": 0
                },
                {
                    "annex": "AnnexB",
                    "attributeMask": 2147483648,
                    "frequency": 285000000,
                    "idInSg": 5,
                    "interleaver": "fecI32J4",
                    "modulation": "qam256",
                    "powerAdjust": 0
                },
                {
                    "annex": "AnnexB",
                    "attributeMask": 2147483648,
                    "frequency": 291000000,
                    "idInSg": 6,
                    "interleaver": "fecI32J4",
                    "modulation": "qam256",
                    "powerAdjust": 0
                },
                {
                    "annex": "AnnexB",
                    "attributeMask": 2147483648,
                    "frequency": 297000000,
                    "idInSg": 7,
                    "interleaver": "fecI32J4",
                    "modulation": "qam256",
                    "powerAdjust": 0
                },
                {
                    "annex": "AnnexB",
                    "attributeMask": 2147483648,
                    "frequency": 303000000,
                    "idInSg": 8,
                    "interleaver": "fecI32J4",
                    "modulation": "qam256",
                    "powerAdjust": 0
                },
                {
                    "annex": "AnnexB",
                    "attributeMask": 2147483648,
                    "frequency": 309000000,
                    "idInSg": 9,
                    "interleaver": "fecI32J4",
                    "modulation": "qam256",
                    "powerAdjust": 0
                },
                {
                    "annex": "AnnexB",
                    "attributeMask": 2147483648,
                    "frequency": 315000000,
                    "idInSg": 10,
                    "interleaver": "fecI32J4",
                    "modulation": "qam256",
                    "powerAdjust": 0
                },
                {
                    "annex": "AnnexB",
                    "attributeMask": 2147483648,
                    "frequency": 321000000,
                    "idInSg": 11,
                    "interleaver": "fecI32J4",
```

```
                          "modulation": "qam256",
                          "powerAdjust": 0
                        },
                        {
                          "annex": "AnnexB",
                          "attributeMask": 2147483648,
                          "frequency": 327000000,
                          "idInSg": 12,
                          "interleaver": "fecI32J4",
                          "modulation": "qam256",
                          "powerAdjust": 0
                        },
                        {
                          "annex": "AnnexB",
                          "attributeMask": 2147483648,
                          "frequency": 333000000,
                          "idInSg": 13,
                          "interleaver": "fecI32J4",
                          "modulation": "qam256",
                          "powerAdjust": 0
                        },
                        {
                          "annex": "AnnexB",
                          "attributeMask": 2147483648,
                          "frequency": 339000000,
                          "idInSg": 14,
                          "interleaver": "fecI32J4",
                          "modulation": "qam256",
                          "powerAdjust": 0
                        },
                        {
                          "annex": "AnnexB",
                          "attributeMask": 2147483648,
                          "frequency": 345000000,
                          "idInSg": 15,
                          "interleaver": "fecI32J4",
                          "modulation": "qam256",
                          "powerAdjust": 0
                        },
                        {
                          "annex": "AnnexB",
                          "attributeMask": 2147483648,
                          "frequency": 351000000,
                          "idInSg": 16,
                          "interleaver": "fecI32J4",
                          "modulation": "qam256",
                          "powerAdjust": 0
                        },
                        {
                          "annex": "AnnexB",
                          "attributeMask": 2147483648,
                          "frequency": 357000000,
                          "idInSg": 17,
                          "interleaver": "fecI32J4",
                          "modulation": "qam256",
                          "powerAdjust": 0
                        },
                        {
                          "annex": "AnnexB",
                          "attributeMask": 2147483648,
                          "frequency": 363000000,
                          "idInSg": 18,
                          "interleaver": "fecI32J4",
                          "modulation": "qam256",
```

```
                    "powerAdjust": 0
                },
                {
                    "annex": "AnnexB",
                    "attributeMask": 2147483648,
                    "frequency": 369000000,
                    "idInSg": 19,
                    "interleaver": "fecI32J4",
                    "modulation": "qam256",
                    "powerAdjust": 0
                },
                {
                    "annex": "AnnexB",
                    "attributeMask": 2147483648,
                    "frequency": 375000000,
                    "idInSg": 20,
                    "interleaver": "fecI32J4",
                    "modulation": "qam256",
                    "powerAdjust": 0
                },
                {
                    "annex": "AnnexB",
                    "attributeMask": 2147483648,
                    "frequency": 381000000,
                    "idInSg": 21,
                    "interleaver": "fecI32J4",
                    "modulation": "qam256",
                    "powerAdjust": 0
                },
                {
                    "annex": "AnnexB",
                    "attributeMask": 2147483648,
                    "frequency": 387000000,
                    "idInSg": 22,
                    "interleaver": "fecI32J4",
                    "modulation": "qam256",
                    "powerAdjust": 0
                },
                {
                    "annex": "AnnexB",
                    "attributeMask": 2147483648,
                    "frequency": 393000000,
                    "idInSg": 23,
                    "interleaver": "fecI32J4",
                    "modulation": "qam256",
                    "powerAdjust": 0
                },
                {
                    "annex": "AnnexB",
                    "attributeMask": 2147483648,
                    "frequency": 399000000,
                    "idInSg": 24,
                    "interleaver": "fecI32J4",
                    "modulation": "qam256",
                    "powerAdjust": 0
                },
                {
                    "annex": "AnnexB",
                    "attributeMask": 2147483648,
                    "frequency": 405000000,
                    "idInSg": 25,
                    "interleaver": "fecI32J4",
                    "modulation": "qam256",
                    "powerAdjust": 0
```

```
    },
    {
      "annex": "AnnexB",
      "attributeMask": 2147483648,
      "frequency": 411000000,
      "idInSg": 26,
      "interleaver": "fecI32J4",
      "modulation": "qam256",
      "powerAdjust": 0
    },
    {
      "annex": "AnnexB",
      "attributeMask": 2147483648,
      "frequency": 417000000,
      "idInSg": 27,
      "interleaver": "fecI32J4",
      "modulation": "qam256",
      "powerAdjust": 0
    },
    {
      "annex": "AnnexB",
      "attributeMask": 2147483648,
      "frequency": 423000000,
      "idInSg": 28,
      "interleaver": "fecI32J4",
      "modulation": "qam256",
      "powerAdjust": 0
    },
    {
      "annex": "AnnexB",
      "attributeMask": 2147483648,
      "frequency": 429000000,
      "idInSg": 29,
      "interleaver": "fecI32J4",
      "modulation": "qam256",
      "powerAdjust": 0
    },
    {
      "annex": "AnnexB",
      "attributeMask": 2147483648,
      "frequency": 435000000,
      "idInSg": 30,
      "interleaver": "fecI32J4",
      "modulation": "qam256",
      "powerAdjust": 0
    },
    {
      "annex": "AnnexB",
      "attributeMask": 2147483648,
      "frequency": 441000000,
      "idInSg": 31,
      "interleaver": "fecI32J4",
      "modulation": "qam256",
      "powerAdjust": 0
    }
  ],
  "dsg": {
    "cfr": null,
    "chanList": null,
    "clientList": null,
    "tg": null,
    "timer": null,
    "tunnel": null
  },
```

```
"dsmtu": 2100,
"md": [
  {
    "adminState": "Up",
    "cmInitChanTimeout": 60,
    "dataBackoff": {
      "end": 5,
      "start": 3
    },
    "dsg": {
      "dcdDisable": null,
      "tg": null
    },
    "enableBalanceUs": true,
    "idInSg": 0,
    "insertionInterval": 120,
    "ipInit": "ipv4",
    "mac": "00:00:00:00:00:00",
    "mapAdvance": {
      "advanceTime": 2000,
      "mode": "static"
    },
    "primDcid": [
      0,
      8,
      16,
      24
    ],
    "rangeBackoff": {
      "end": 6,
      "start": 3
    },
    "registrationTimeout": 3,
    "syncInterval": 10,
    "ucId": [
      0,
      1,
      2,
      3
    ]
  }
],
"modProfs": [
  {
    "entries": {
      "advPhyLongData": {
        "channelType": "atdma",
        "fecCodewordLength": 232,
        "fecErrorCorrection": 9,
        "lastCodewardShortened": true,
        "modulation": "qam64",
        "preamble": "qpsk1",
        "preambleLength": 64,
        "scrambler": true,
        "scramblerSeed": 338
      },
      "advPhyShortData": {
        "channelType": "atdma",
        "fecCodewordLength": 76,
        "fecErrorCorrection": 6,
        "lastCodewardShortened": true,
        "maxBurstSize": 6,
        "modulation": "qam64",
        "preamble": "qpsk1",
```

```
                              "preambleLength": 64,
                              "scrambler": true,
                              "scramblerSeed": 338
                            },
                            "initialRanging": {
                              "channelType": "atdma",
                              "fecCodewordLength": 34,
                              "fecErrorCorrection": 5,
                              "modulation": "qpsk",
                              "preamble": "qpsk0",
                              "preambleLength": 98,
                              "scrambler": true,
                              "scramblerSeed": 338
                            },
                            "longData": {
                              "fecCodewordLength": 2,
                              "fecErrorCorrection": 9,
                              "lastCodewardShortened": true,
                              "modulation": "qam16",
                              "preambleLength": 4,
                              "scrambler": true
                            },
                            "periodicRanging": {
                              "channelType": "atdma",
                              "fecCodewordLength": 34,
                              "fecErrorCorrection": 5,
                              "modulation": "qpsk",
                              "preamble": "qpsk0",
                              "preambleLength": 98,
                              "scrambler": true,
                              "scramblerSeed": 338
                            },
                            "request": {
                              "channelType": "atdma",
                              "fecCodewordLength": 16,
                              "modulation": "qpsk",
                              "preamble": "qpsk0",
                              "preambleLength": 36,
                              "scrambler": true,
                              "scramblerSeed": 338
                            },
                            "shortData": {
                              "fecCodewordLength": 6,
                              "fecErrorCorrection": 3,
                              "lastCodewardShortened": true,
                              "maxBurstSize": 2,
                              "modulation": "qam16",
                              "scrambler": true
                            },
                            "ugs": {
                              "channelType": "atdma",
                              "fecCodewordLength": 232,
                              "fecErrorCorrection": 9,
                              "lastCodewardShortened": true,
                              "modulation": "qam64",
                              "preamble": "qpsk1",
                              "preambleLength": 64,
                              "scrambler": true,
                              "scramblerSeed": 338
                            }
                          },
                          "idInSg": 221
                        }
                      ],
```

```
"ofdmDs": [
  {
    "cyclicPrefix": 256,
    "idInSg": 158,
    "interleaverDepth": 16,
    "pilotScaling": 48,
    "plc": 930000000,
    "profileControl": "QAM256",
    "profileNcp": "QAM16",
    "rollOff": 192,
    "startFrequency": 837000000,
    "subcarrierSpacing": "25KHZ",
    "width": 192000000
  }
],
"privacy": {
  "AcceptSelfSignCert": true,
  "BpiPlusPolicy": "capable-enforcement",
  "DsxSupport": true,
  "EaePolicy": "disable-enforcement",
  "Kek": {
    "GraceTime": 300,
    "LifeTime": 86400
  },
  "Tek": {
    "GraceTime": 300,
    "LifeTime": 1800
  }
},
"punt": {
  "icpiPerCausePuntCfgList": null
},
"rpdCfg": {
  "rfTopology": {
    "dsPort": [
      {
        "adminState": "Up",
        "basePower": 21,
        "channel": [
          0,
          1,
          2,
          3,
          4,
          5,
          6,
          7,
          8,
          9,
          10,
          11,
          12,
          13,
          14,
          15,
          16,
          17,
          18,
          19,
          20,
          21,
          22,
          23,
          24,
```

```
                         25,
                         26,
                         27,
                         28,
                         29,
                         30,
                         31,
                         158
                       ],
                       "ofdmFreqExclBand": null
                     }
                   ],
                   "fiberNode": [
                     {
                       "dsPort": [0],
                       "usPort": [0]
                     },
                     {
                       "dsPort": 0,
                       "id": 1,
                       "usPort": 1
                     }
                   ],
                   "usPort": [
                     {
                       "channel": [
                         0,
                         1
                       ],
                       "ofdmaFreqExclBand": null,
                       "ofdmaFreqUnusedBand": null
                     },
                     {
                       "channel": [
                         2,
                         3
                       ],
                       "ofdmaFreqExclBand": null,
                       "ofdmaFreqUnusedBand": null,
                       "portId": 1
                     }
                   ]
                 }
               },
               "rpdPtpCfg": {
                 "domain": 0,
                 "dtiMode": "SlaveDtiMode",
                 "priority1": 128,
                 "priority2": 255,
                 "ptpClkProfileId": "00:00:00:00:00:00",
                 "ptpPortCfg": [
                   {
                     "adminState": "Up",
                     "anncReceiptTimeout": 11,
                     "cos": 6,
                     "dscp": 47,
                     "enetPortIndex": 1,
                     "gateway": "3.208.1.2",
                     "localPriority": 128,
                     "logDelayReqInterval": -4,
                     "logSyncInterval": -4,
                     "masterAddr": "3.158.185.51",
                     "masterAdminState": "Up",
                     "ptpPortIndex": 22,
```

```
                            "unicastDuration": 300
                        }
                    ]
                },
                "us": [
                    {
                        "adminState": "Up",
                        "attributeMask": 2684354560,
                        "channelWidth": 6400000,
                        "docsisMode": "atdma",
                        "equalizationCoeffEnable": true,
                        "frequency": 11400000,
                        "idInSg": 0,
                        "ingressNoiseCancelEnable": true,
                        "modulation": 221,
                        "powerLevel": 0,
                        "slotSize": 1
                    },
                    {
                        "adminState": "Up",
                        "attributeMask": 2684354560,
                        "channelWidth": 6400000,
                        "docsisMode": "atdma",
                        "equalizationCoeffEnable": true,
                        "frequency": 17800000,
                        "idInSg": 1,
                        "ingressNoiseCancelEnable": true,
                        "modulation": 221,
                        "powerLevel": 0,
                        "slotSize": 1
                    },
                    {
                        "adminState": "Up",
                        "attributeMask": 2684354560,
                        "channelWidth": 6400000,
                        "docsisMode": "atdma",
                        "equalizationCoeffEnable": true,
                        "frequency": 24200000,
                        "idInSg": 2,
                        "ingressNoiseCancelEnable": true,
                        "modulation": 221,
                        "powerLevel": 0,
                        "slotSize": 1
                    },
                    {
                        "adminState": "Up",
                        "attributeMask": 2684354560,
                        "channelWidth": 6400000,
                        "docsisMode": "atdma",
                        "equalizationCoeffEnable": true,
                        "frequency": 30600000,
                        "idInSg": 3,
                        "ingressNoiseCancelEnable": true,
                        "modulation": 221,
                        "powerLevel": 0,
                        "slotSize": 1
                    }
                ],
                "usmtu": 2100
            }
```

Autodeployer Limitations

The Autodeployer has the following limitations:

- Rerunning the deploy command reapplies all configurations, except the wiring configuration. The wiring configuration update is not supported.

- When updating the SG or RPD, the existing service groups are deleted and the SG or RPD is then added back with the updated configuration.

- Placeholder values for IPv6 must be provided, even if IPv6 is not supported. Values for `sg-peer`, `bgp-agent-if`, `cin-prefix`, and `dc-link-prefix` must be as specified in the given example.

- The configuration file must specify all mandatory sections and attributes. You may see the autodeploy exit without warnings and errors when mandatory attributes are missing in the configuration file.

- Cisco cnBR has limited error and exception handling. Review the detailed crash dumps when an exception or error occurs.

Configure cnBR using cnBR Manager

You can complete the Cisco cnBR configuration using the cnBR Manager application in Cisco Operations Hub. We recommend that you create Profiles and Templates before initiating configuration changes.

Add Cisco cnBR to cnBR Manager

To add Cisco cnBR cores using the cnBR Manager application in Cisco Operations Hub, complete the following steps:

Step 1 From the Cisco Operations Hub, click the Cisco Operations Hub main menu button (☰).

Step 2 Click **cnBR Manager** > **cnBRs** > **Inventory**.

Step 3 Click **Add**

Step 4 Provide the mandatory information: cnBR Name, Ingress hostname, cnBR Username, and cnBR password.

Step 5 Click.**Add**.

Note The Advanced Parameters allow you to optionally configure a number of parameters during the addition of a cnBR cluster. The parameters are Wiring, PTP, BGP Agent, CIN, L2VPN, L3VPN, Packet Cable, PFG Active, PFG Group, RIP, SAV, TFP Proxy and SP Router.

For a successful Cisco cnBR addition, the Cisco cnBR Manager provides a high-level overview of the cluster. The overview includes the number of RPDs, Service Groups, associated Cable Modems, KPI Alerts, Upstream and Downstream traffic rates, and so on.

You can perform the following operations using the cnBR Manager, as shown in the table.

cnBR Operations that can be performed.

Operations	Description
Edit	Allows you to edit the cnBR Name, cnBR Username, cnBR Password, and Advanced parameters.
Remove	Remove a cnBR cluster from the cnBR Manager application. The removed cnBR cluster continues to function, but it will not be managed by cnBR Manager.
Replace cnBR Config	Overwrite the cnBR's current configuration. Configuration file should be in JSON format.
Download cnBR Config	Download the cnBR's current configuration in JSON format. This allows you to modify and upload a modified configuration later.
Export	Export the content of the cnBR overview table.

Profiles and Templates

The following table displays the Feature History information on Profiles and Templates

Feature Name	Release Information	Feature Description
Profiles and Templates	Cisco cnBR 21.2	You can use the Templates and Profiles feature to provision detailed and repetitive configurations. The configuration needs and provisioning requirements for growing networks are complex; Cisco cnBR offers a simplified data model to enable ease of network operations.
Tagging	Cisco cnBR 21.3	You can create and associate user-defined tags for cnBR cores, Profiles and Templates. This allows you to search, analyse, plan your work better, and to gather insights.

In Cisco cnBR, you can use the Profiles and Templates feature to provision various repetitive configurations. For example, you can configure a Remote PHY Device to establish connection with cnBR clusters and other networking entities, and to bring cable modems online.

In order to simplify network operations, Cisco cnBR and Cisco Operations Hub maintain a data model that is commonly known as *Templates*. Templates are schematic data about a particular type of information. For example, the SG Template contains information that is related to Service Group, which is used during Remote PHY Device (RPD) configuration. L3 Template contains information that is related to Layer 3 configuration,

which is needed for Cisco cnBR to connect to RPD and other network entities. Video QAM Templates contain information specific to Video RF Channels, Annex, Interleaver profile and so on.

As different templates are curated for different aspects of network operations, managing templates, too, may turn out to be overwhelming to configure. The Cisco Operations Hub uses smaller, reusable, data schemas that are commonly known as *Profiles* to keep template configuration simple.

Profiles are fine-tuned specific blocks of data that are used to configure a small network entity. These small building blocks stack together to eventually help build a Template. Profiles are therefore heavily reused across various types of templates, whenever applicable. For example, to help build a Service Group Template, DS Profile, US Profile, the RPD Configuration Profile and RPD PTP Configuration Profile are used. Similarly, for various Video Templates, the Video Channel Profile and Video DS Profile are used.

Templates and *Profiles* can be edited. Snapshots of templates and configuration can be taken from a live Cisco cnBR for backup, or can be used later to recreate another system at a different place and time. These snapshot files internally capture details of the configuration required to replicate an existing network, thereby making the network launch simple and fast.

Tagging: From Cisco cnBR 21.3 and later, you can associate tags to a Cisco cnBR core while creating or editing them. Existing tags are listed in the autocomplete style drop-down list. You can either assign tags to the Cisco cnBR, or complete the new tag name in the text area of the drop-down list. If an existing tag is assigned, the tag will show in capsule style UI in a colour assigned to that tag. If the tag is new, it will show in a capsule style UI in a default grey colour till the entity is created by saving it. You can perform search based on the tag names.

The following table lists the various Profiles and Template operations and their descriptions

The table lists the various Profiles and Template operations and their descriptions

Operations	Description
Create	Create a new profile or template.
Edit	Edit existing profile or template parameters.
Clone	Copy an existing profile or template. You can edit the parameters before cloning it.
Delete	Delete an existing profile or template.
Export	Download existing profiles and templates in JSON format.
Import	Upload profiles and templates.
Focus	Predefined options to quickly filter data, based on profile or template types.
Search	Search for a profile or a template.

Applying Profiles and Templates to cnBR

Complete the following steps to configure Wiring, BGP Agent, PTP, and CIN:

Step 1   Configure Wiring.

a) On the Cisco Operations Hub, click the Cisco Operations Hub main menu button.

b) Click **cnBR Manager** > **cnBRs**.

c) On the navigation panel, click **Inventory**.

   Select a cluster on the cnBR Clusters panel.

d) Click the name of the Cisco cnBR cluster to open the **cnBR Cluster Configuration** page.

   We recommend that you use the `Code` mode to configure wiring.

Figure 10: cnBR Cluster Configuration Page
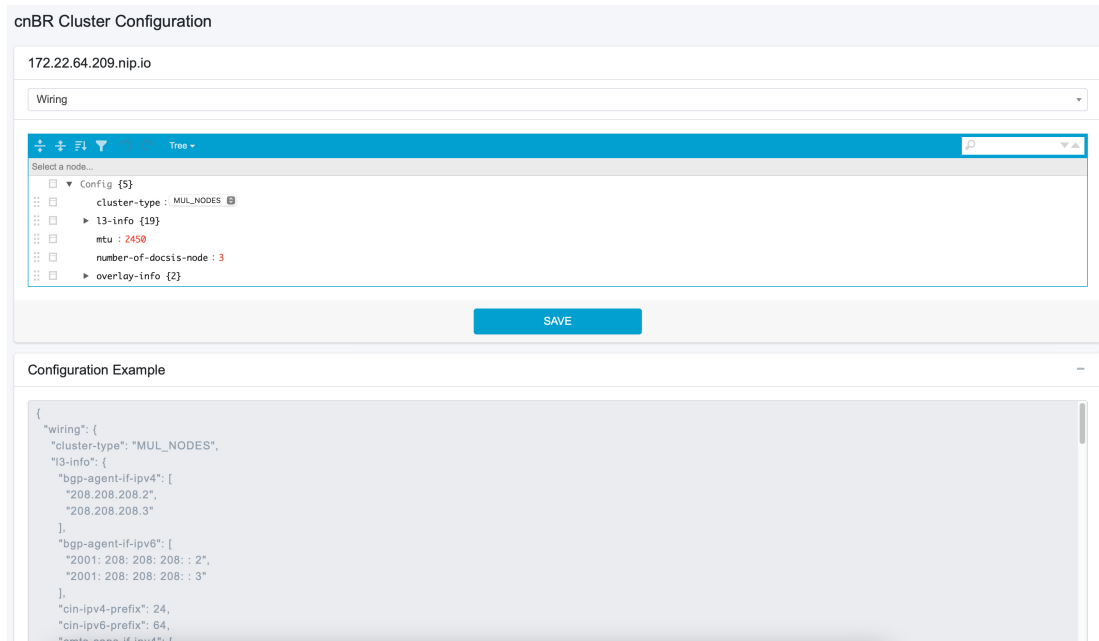
e) Click **SAVE** to apply configuration to Cisco cnBR.

   For example:

```
{
  "cluster-type": "MUL_NODES",
  "l3-info": {
    "bgp-agent-if-ipv4": [
      "208.208.208.102",      <---bgp address
      "208.208.208.103"
    ],
    "bgp-agent-if-ipv6": [
      "2001:208:208:208::102",
      "2001:208:208:208::103"
    ],
    "cin-ipv4-prefix": 24,
    "cin-ipv6-prefix": 64,
    "cmts-cops-if-ipv4": [
      "3.208.1.7",
      "3.208.1.8"
    ],
    "cmts-cops-if-ipv6": [],
    "dc-link-ipv4-prefix": 24,
    "dc-link-ipv6-prefix": 64,
    "dmic-if-ipv4": [
```

```
        "200.200.200.9",
        "200.200.200.10",
        "200.200.200.11"
      ],
      "dmic-if-ipv6": [
        "2008:199:1:1::9",
        "2008:199:1:1::10",
        "2008:199:1:1::11"
      ],
      "ptp-if-ipv4": [
        "3.208.1.4",        <---PTP local address
        "3.208.1.5",
        "3.208.1.6"
      ],
      "ptp-if-ipv6": [],
      "ptp-mac-addr": [
        "20:18:10:29:88:43",
        "20:18:10:29:88:44",
        "20:18:10:29:88:45"
      ],
      "relayproxy-if-ipv4": [
        "208.208.208.107",
        "208.208.208.108",
        "208.208.208.109"
      ],
      "relayproxy-if-ipv6": [
        "2001:208:208:208::107",
        "2001:208:208:208::108",
        "2001:208:208:208::109"
      ],
      "rphmgr-if-ipv4": [
        "3.208.1.3",
        "3.208.1.3"
      ],
      "rphmgr-if-ipv6": [],
      "vpp-dp-rpd-if-ipv4": [ <---15 addresses total
        "3.208.1.10",
        "3.208.1.11",
        "3.208.1.12",
        "3.208.1.13",
        "3.208.1.14",
        "3.208.1.15",
        "3.208.1.16",
        "3.208.1.17",
        "3.208.1.18",
        "3.208.1.19",
        "3.208.1.20",
        "3.208.1.21",
        "3.208.1.22",
        "3.208.1.23",
        "3.208.1.24"
      ],
      "vpp-dp-rpd-if-ipv6": []
    },
    "mtu": 2450,           <---Recommend value is 2450
    "overlay-info": {
      "overlay-type": "vlan",
      "vlan-info": {
        "cnbr-wan-ifname": "Ethernet0/0/0",
        "overlay-cin-vlan": 1182,          <---This vlan id should be same as vlan id in SP router

        "overlay-l2vpn-mpls-vlan": 1183,
        "overlay-l2vpn-vlan-vlan": 1184,
        "overlay-wan-vlan": 1181           <---This vlan id should be same as vlan id in SP router
```

```
      }
    }
  }
```

Step 2   Configure BGP Agent.

    a) Use the `Code` mode to configure BGP Agent.

    b) Click **SAVE** to apply configuration to Cisco cnBR.

        For example:

```
{
  "asNumber": 65001,
  "ebgpMultihop": 255,
  "gracefulRestart": {
    "enable": true,
    "restartTime": 120,
    "stalePathTime": 360
  },
  "ifname": "bgp",
  "neighbors": [
    {
      "address": "208.208.208.1",    <----IP in SP Router. Same IP with SG Peer.
      "asNumber": 65000
    },
    {
      "address": "2001:208:208:208::1",
      "asNumber": 65000
    }
  ]
}
```

Step 3   Configure PTP.

    a) Use the `Code` mode to configure PTP.

    b) Click **SAVE** to apply configuration to Cisco cnBR.

        For example:

```
PTP:
{
  "PtpDomain": 44,
  "PtpGwIp": "3.208.1.2",
  "PtpMasterIp": "3.158.185.51"
}
```

Step 4   Configure CIN.

    If RPD and RPHYMAN are in different networks, you must configure CIN. Otherwise, choose to ignore this step.

    a) Use the `Code` mode to configure CIN.

        For example:

```
{
  "CinGwIp": "3.208.1.2"
}
```

Add Service Group Configuration to cnBR

Complete the following steps to add Service Group (SG) template and L3 template:

Step 1   On the Cisco Operations Hub, click the Cisco Operations Hub main menu button.

Step 2   Choose **cnBR Manager** > **Profiles & Templates** to open the **Templates and Profiles** page.

Step 3   Click **Add Template** on the left pane and choose **SG Template** as the template type.

Step 4   Provide an appropriate template Name and Description. Click **Next**.

Step 5   On the **Add SG Template** page, choose to ignore the profile changes. Click **EXPERT**.

Figure 11: Add Service Group Template Page

Step 6   Provide the SG related configuration and click **SAVE**.

For example:

```
{
  "description": "33x8 SG Config",
  "ds": [
    {
      "annex": "AnnexB",
      "attributeMask": 2147483648,
      "frequency": 255000000,
      "idInSg": 0,
      "interleaver": "fecI32J4",
      "modulation": "qam256",
      "powerAdjust": 0
    },
    {
      "annex": "AnnexB",
      "attributeMask": 2147483648,
      "frequency": 261000000,
      "idInSg": 1,
      "interleaver": "fecI32J4",
      "modulation": "qam256",
```

```
      "powerAdjust": 0
    },
    {
      "annex": "AnnexB",
      "attributeMask": 2147483648,
      "frequency": 267000000,
      "idInSg": 2,
      "interleaver": "fecI32J4",
      "modulation": "qam256",
      "powerAdjust": 0
    },
    {
      "annex": "AnnexB",
      "attributeMask": 2147483648,
      "frequency": 273000000,
      "idInSg": 3,
      "interleaver": "fecI32J4",
      "modulation": "qam256",
      "powerAdjust": 0
    },
    {
      "annex": "AnnexB",
      "attributeMask": 2147483648,
      "frequency": 279000000,
      "idInSg": 4,
      "interleaver": "fecI32J4",
      "modulation": "qam256",
      "powerAdjust": 0
    },
    {
      "annex": "AnnexB",
      "attributeMask": 2147483648,
      "frequency": 285000000,
      "idInSg": 5,
      "interleaver": "fecI32J4",
      "modulation": "qam256",
      "powerAdjust": 0
    },
    {
      "annex": "AnnexB",
      "attributeMask": 2147483648,
      "frequency": 291000000,
      "idInSg": 6,
      "interleaver": "fecI32J4",
      "modulation": "qam256",
      "powerAdjust": 0
    },
    {
      "annex": "AnnexB",
      "attributeMask": 2147483648,
      "frequency": 297000000,
      "idInSg": 7,
      "interleaver": "fecI32J4",
      "modulation": "qam256",
      "powerAdjust": 0
    },
    {
      "annex": "AnnexB",
      "attributeMask": 2147483648,
      "frequency": 303000000,
      "idInSg": 8,
      "interleaver": "fecI32J4",
      "modulation": "qam256",
      "powerAdjust": 0
```

```
                            },
                            {
                              "annex": "AnnexB",
                              "attributeMask": 2147483648,
                              "frequency": 309000000,
                              "idInSg": 9,
                              "interleaver": "fecI32J4",
                              "modulation": "qam256",
                              "powerAdjust": 0
                            },
                            {
                              "annex": "AnnexB",
                              "attributeMask": 2147483648,
                              "frequency": 315000000,
                              "idInSg": 10,
                              "interleaver": "fecI32J4",
                              "modulation": "qam256",
                              "powerAdjust": 0
                            },
                            {
                              "annex": "AnnexB",
                              "attributeMask": 2147483648,
                              "frequency": 321000000,
                              "idInSg": 11,
                              "interleaver": "fecI32J4",
                              "modulation": "qam256",
                              "powerAdjust": 0
                            },
                            {
                              "annex": "AnnexB",
                              "attributeMask": 2147483648,
                              "frequency": 327000000,
                              "idInSg": 12,
                              "interleaver": "fecI32J4",
                              "modulation": "qam256",
                              "powerAdjust": 0
                            },
                            {
                              "annex": "AnnexB",
                              "attributeMask": 2147483648,
                              "frequency": 333000000,
                              "idInSg": 13,
                              "interleaver": "fecI32J4",
                              "modulation": "qam256",
                              "powerAdjust": 0
                            },
                            {
                              "annex": "AnnexB",
                              "attributeMask": 2147483648,
                              "frequency": 339000000,
                              "idInSg": 14,
                              "interleaver": "fecI32J4",
                              "modulation": "qam256",
                              "powerAdjust": 0
                            },
                            {
                              "annex": "AnnexB",
                              "attributeMask": 2147483648,
                              "frequency": 345000000,
                              "idInSg": 15,
                              "interleaver": "fecI32J4",
                              "modulation": "qam256",
                              "powerAdjust": 0
                            },
```

```
{
  "annex": "AnnexB",
  "attributeMask": 2147483648,
  "frequency": 351000000,
  "idInSg": 16,
  "interleaver": "fecI32J4",
  "modulation": "qam256",
  "powerAdjust": 0
},
{
  "annex": "AnnexB",
  "attributeMask": 2147483648,
  "frequency": 357000000,
  "idInSg": 17,
  "interleaver": "fecI32J4",
  "modulation": "qam256",
  "powerAdjust": 0
},
{
  "annex": "AnnexB",
  "attributeMask": 2147483648,
  "frequency": 363000000,
  "idInSg": 18,
  "interleaver": "fecI32J4",
  "modulation": "qam256",
  "powerAdjust": 0
},
{
  "annex": "AnnexB",
  "attributeMask": 2147483648,
  "frequency": 369000000,
  "idInSg": 19,
  "interleaver": "fecI32J4",
  "modulation": "qam256",
  "powerAdjust": 0
},
{
  "annex": "AnnexB",
  "attributeMask": 2147483648,
  "frequency": 375000000,
  "idInSg": 20,
  "interleaver": "fecI32J4",
  "modulation": "qam256",
  "powerAdjust": 0
},
{
  "annex": "AnnexB",
  "attributeMask": 2147483648,
  "frequency": 381000000,
  "idInSg": 21,
  "interleaver": "fecI32J4",
  "modulation": "qam256",
  "powerAdjust": 0
},
{
  "annex": "AnnexB",
  "attributeMask": 2147483648,
  "frequency": 387000000,
  "idInSg": 22,
  "interleaver": "fecI32J4",
  "modulation": "qam256",
  "powerAdjust": 0
},
{
```

```
      "annex": "AnnexB",
      "attributeMask": 2147483648,
      "frequency": 393000000,
      "idInSg": 23,
      "interleaver": "fecI32J4",
      "modulation": "qam256",
      "powerAdjust": 0
    },
    {
      "annex": "AnnexB",
      "attributeMask": 2147483648,
      "frequency": 399000000,
      "idInSg": 24,
      "interleaver": "fecI32J4",
      "modulation": "qam256",
      "powerAdjust": 0
    },
    {
      "annex": "AnnexB",
      "attributeMask": 2147483648,
      "frequency": 405000000,
      "idInSg": 25,
      "interleaver": "fecI32J4",
      "modulation": "qam256",
      "powerAdjust": 0
    },
    {
      "annex": "AnnexB",
      "attributeMask": 2147483648,
      "frequency": 411000000,
      "idInSg": 26,
      "interleaver": "fecI32J4",
      "modulation": "qam256",
      "powerAdjust": 0
    },
    {
      "annex": "AnnexB",
      "attributeMask": 2147483648,
      "frequency": 417000000,
      "idInSg": 27,
      "interleaver": "fecI32J4",
      "modulation": "qam256",
      "powerAdjust": 0
    },
    {
      "annex": "AnnexB",
      "attributeMask": 2147483648,
      "frequency": 423000000,
      "idInSg": 28,
      "interleaver": "fecI32J4",
      "modulation": "qam256",
      "powerAdjust": 0
    },
    {
      "annex": "AnnexB",
      "attributeMask": 2147483648,
      "frequency": 429000000,
      "idInSg": 29,
      "interleaver": "fecI32J4",
      "modulation": "qam256",
      "powerAdjust": 0
    },
    {
      "annex": "AnnexB",
```

```
        "attributeMask": 2147483648,
        "frequency": 435000000,
        "idInSg": 30,
        "interleaver": "fecI32J4",
        "modulation": "qam256",
        "powerAdjust": 0
      },
      {
        "annex": "AnnexB",
        "attributeMask": 2147483648,
        "frequency": 441000000,
        "idInSg": 31,
        "interleaver": "fecI32J4",
        "modulation": "qam256",
        "powerAdjust": 0
      }
    ],
    "dsg": {
      "cfr": null,
      "chanList": null,
      "clientList": null,
      "tg": null,
      "timer": null,
      "tunnel": null
    },
    "dsmtu": 2200,
    "md": [
      {
        "adminState": "Up",
        "cmInitChanTimeout": 60,
        "dataBackoff": {
          "end": 5,
          "start": 3
        },
        "dsg": {
          "dcdDisable": null,
          "tg": null
        },
        "enableBalanceUs": true,
        "idInSg": 0,
        "insertionInterval": 120,
        "ipInit": "ipv4",
        "mac": "00:00:00:00:00:00",    <----mark to all 0, cnBR will assign Mac domain mac automaticly

        "mapAdvance": {
          "advanceTime": 2000,
          "mode": "static"
        },
        "primDcid": [
          0,
          8,
          16,
          24
        ],
        "rangeBackoff": {
          "end": 6,
          "start": 3
        },
        "registrationTimeout": 3,
        "syncInterval": 10,
        "ucId": [
          0,
          1,
          2,
```

```
                3
            ]
        }
    }
],
"modProfs": [
    {
        "entries": {
            "advPhyLongData": {
                "channelType": "atdma",
                "fecCodewordLength": 232,
                "fecErrorCorrection": 9,
                "lastCodewardShortened": true,
                "modulation": "qam64",
                "preamble": "qpsk1",
                "preambleLength": 64,
                "scrambler": true,
                "scramblerSeed": 338
            },
            "advPhyShortData": {
                "channelType": "atdma",
                "fecCodewordLength": 76,
                "fecErrorCorrection": 6,
                "lastCodewardShortened": true,
                "maxBurstSize": 6,
                "modulation": "qam64",
                "preamble": "qpsk1",
                "preambleLength": 64,
                "scrambler": true,
                "scramblerSeed": 338
            },
            "initialRanging": {
                "channelType": "atdma",
                "fecCodewordLength": 34,
                "fecErrorCorrection": 5,
                "modulation": "qpsk",
                "preamble": "qpsk0",
                "preambleLength": 98,
                "scrambler": true,
                "scramblerSeed": 338
            },
            "longData": {
                "fecCodewordLength": 2,
                "fecErrorCorrection": 9,
                "lastCodewardShortened": true,
                "modulation": "qam16",
                "preambleLength": 4,
                "scrambler": true
            },
            "periodicRanging": {
                "channelType": "atdma",
                "fecCodewordLength": 34,
                "fecErrorCorrection": 5,
                "modulation": "qpsk",
                "preamble": "qpsk0",
                "preambleLength": 98,
                "scrambler": true,
                "scramblerSeed": 338
            },
            "request": {
                "channelType": "atdma",
                "fecCodewordLength": 16,
                "modulation": "qpsk",
                "preamble": "qpsk0",
                "preambleLength": 36,
```

```
                    "scrambler": true,
                    "scramblerSeed": 338
                  },
                  "shortData": {
                    "fecCodewordLength": 6,
                    "fecErrorCorrection": 3,
                    "lastCodewardShortened": true,
                    "maxBurstSize": 2,
                    "modulation": "qam16",
                    "scrambler": true
                  },
                  "ugs": {
                    "channelType": "atdma",
                    "fecCodewordLength": 232,
                    "fecErrorCorrection": 9,
                    "lastCodewardShortened": true,
                    "modulation": "qam64",
                    "preamble": "qpsk1",
                    "preambleLength": 64,
                    "scrambler": true,
                    "scramblerSeed": 338
                  }
                },
                "idInSg": 221
              }
            ],
            "ofdmDs": [
              {
                "cyclicPrefix": 256,
                "idInSg": 158,
                "interleaverDepth": 16,
                "pilotScaling": 48,
                "plc": 930000000,
                "profileControl": "QAM256",
                "profileNcp": "QAM16",
                "rollOff": 192,
                "startFrequency": 837000000,
                "subcarrierSpacing": "25KHZ",
                "width": 192000000
              }
            ],
            "privacy": {
              "AcceptSelfSignCert": true,
              "BpiPlusPolicy": "capable-enforcement",
              "DsxSupport": true,
              "EaePolicy": "disable-enforcement",
              "Kek": {
                "GraceTime": 300,
                "LifeTime": 86400
              },
              "Tek": {
                "GraceTime": 300,
                "LifeTime": 1800
              }
            },
            "punt": {
              "icpiPerCausePuntCfgList": null
            },
            "rpdCfg": [
              {
                "entries": {
                  "dsPort": [
                    {
                      "adminState": "Up",
```

```
                  "basePower": 21,
                  "channel": [
                     0,
                     1,
                     2,
                     3,
                     4,
                     5,
                     6,
                     7,
                     8,
                     9,
                     10,
                     11,
                     12,
                     13,
                     14,
                     15,
                     16,
                     17,
                     18,
                     19,
                     20,
                     21,
                     22,
                     23,
                     24,
                     25,
                     26,
                     27,
                     28,
                     29,
                     30,
                     31,
                     158
                  ],
                  "ofdmFreqExclBand": null
               }
            ],
            "fiberNode": [
               {
                  "dsPort": 0,
                  "usPort": 0
               },
               {
                  "dsPort": 0,
                  "id": 1,
                  "usPort": 1
               }
            ],
            "usPort": [
               {
                  "channel": [
                     0,
                     1
                  ],
                  "ofdmaFreqExclBand": null,
                  "ofdmaFreqUnusedBand": null
               },
               {
                  "channel": [
                     2,
                     3
                  ],
```

```
            "ofdmaFreqExclBand": null,
            "ofdmaFreqUnusedBand": null,
            "portId": 1
          }
        ]
      },
      "rpdIp": "3.2.0.2",
      "rpdMac": "00:00:20:11:11:00"
    }
  ],
  "rpdPtpCfg": {
    "domain": 44,
    "dtiMode": "SlaveDtiMode",
    "priority1": 128,
    "priority2": 255,
    "ptpClkProfileId": "00:00:00:00:00:00",
    "ptpPortCfg": [
      {
        "adminState": "Up",
        "anncReceiptTimeout": 11,
        "cos": 6,
        "dscp": 47,
        "enetPortIndex": 1,
        "gateway": "3.208.1.2",
        "localPriority": 128,
        "logDelayReqInterval": -4,
        "logSyncInterval": -4,
        "masterAddr": "3.158.185.51",
        "masterAdminState": "Up",
        "ptpPortIndex": 22,
        "unicastDuration": 300
      }
    ]
  },
  "sgName": "SG0",
  "us": [
    {
      "adminState": "Up",
      "attributeMask": 2684354560,
      "channelWidth": 6400000,
      "docsisMode": "atdma",
      "equalizationCoeffEnable": true,
      "frequency": 11400000,
      "idInSg": 0,
      "ingressNoiseCancelEnable": true,
      "modulation": 221,
      "powerLevel": 0,
      "slotSize": 1
    },
    {
      "adminState": "Up",
      "attributeMask": 2684354560,
      "channelWidth": 6400000,
      "docsisMode": "atdma",
      "equalizationCoeffEnable": true,
      "frequency": 17800000,
      "idInSg": 1,
      "ingressNoiseCancelEnable": true,
      "modulation": 221,
      "powerLevel": 0,
      "slotSize": 1
    },
    {
      "adminState": "Up",
```

```
        "attributeMask": 2684354560,
        "channelWidth": 6400000,
        "docsisMode": "atdma",
        "equalizationCoeffEnable": true,
        "frequency": 24200000,
        "idInSg": 2,
        "ingressNoiseCancelEnable": true,
        "modulation": 221,
        "powerLevel": 0,
        "slotSize": 1
      },
      {
        "adminState": "Up",
        "attributeMask": 2684354560,
        "channelWidth": 6400000,
        "docsisMode": "atdma",
        "equalizationCoeffEnable": true,
        "frequency": 30600000,
        "idInSg": 3,
        "ingressNoiseCancelEnable": true,
        "modulation": 221,
        "powerLevel": 0,
        "slotSize": 1
      }
    ],
    "usmtu": 2200
}
```

Step 7   Click **Add Template** and choose **L3 Template** as the template type.

Step 8   Provide an appropriate template Name and Description. Click **Next**.

Step 9   Choose to ignore the DHCP profile. Click **NEXT**.

Step 10   Provide the L3 related configuration updates. Click **SAVE**.

For example:

```
{
  "dhcp": {
    "arpGlean": true,
    "arpProxy": true,
    "dhcpIfname": "cnr",
    "dhcpServers": [
      "20.11.0.52"
    ],
    "ipv6Lq": true,
    "mobilityScopes": [
      "10.1.1.1/24",
      "2001::a/88"
    ],
    "ndProxy": true,
    "relayModeV4": 0,
    "relayModeV6": 0,
    "v4Nets": [
      "208.1.0.2/24"
    ],
    "v6Nets": [
      "2001:100:208:1::1/64"
    ]
  },
  "spRouterName": "ccmts8-sp-router",
  "savList": {
    "prefixes": null
  },
```

```
 "sgGWMac": "20:19:03:13:19:43",
 "sgPeerIpv4": "208.208.208.1/24",            <-----IP in SP Router. SG Peer IP and BGP Peer IP
is same
 "sgPeerIpv6": "2001:208:208:208::1/64"
}
```

Step 11   Click the Cisco Operations Hub main menu button.

Step 12   Choose **cnBR Manager** > **Remote PHY Device Management** to open the **RPD Overview** page.

Step 13   Execute **RPD Add** auto-mop to add RPD one by one.

   a)   Click **Add RPD**. Add the RPDs, one by one.

   b)   Set the target by providing all RPD related information.

   c)   Ensure that all `Pre-RPD-Add Checklist` conditions are ticked. Check the **Please confirm RPD has been connected physically and start RPD config adding** checkbox.

   d)   Click **Next Step**.

        Wait for the `RPD Add progress` wizard to complete.

   e)   To save time, you can alternatively choose to add another RPD during the `Post-check Progress`.

Step 14   Add consecutive RPDs to Cisco cnBR.

Add Service Group Configuration to cnBR

You can view the RPD and modem status using Grafana.

To check the status of RPDs and CMs, complete the following step:

Step 1   On the Cisco Operations Hub, click the Cisco Operations Hub main menu button.

Step 2   Click **Dashboards** > **DAA Overview**.

You can alternatively search for the DAA Overview by typing **DAA Overview** in the search field.

Cisco cnBR Service Resiliency

The Cisco cnBR supports service resiliency that tolerates software and hardware failures. It can dynamically balance DOCSIS service workloads among the micro service instances and DOCSIS nodes in the Cisco cnBR cluster. When a single micro service instance or node fails, to minimize service interruption, the system reassigns the affected workloads to suitable resources automatically.

Node Failure Recovery

Feature History

Table 14: Feature History

Feature Name	Release Information	Feature Description
Resiliency Support on Expansion Servers	Cisco cnBR 21.1	This feature supports service resiliency on two expansion servers. Thus, all five servers, that is three core servers and two expansion servers, are covered by service resiliency functionality. With this feature enabled, less DOCSIS services are affected in case of node failure.

In Cisco cnBR, all micro service instances, which provide DOCSIS services, are organized into a global resource pool. The system manages this resource pool and assigns workloads to micro service instances. When you add a new RPD into the cluster, the system chooses a proper node and assigns the newly increased workloads to the micro service instances running on the chosen node. In the following example, the system assigns the workloads of multiple RPDs to multiple nodes evenly.
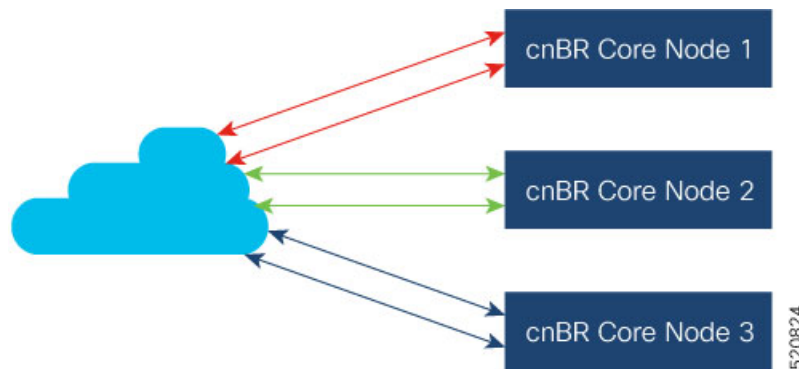
When a node fails, the system moves the workloads from the failed node to healthy nodes that have sufficient capacity to accept more workloads.
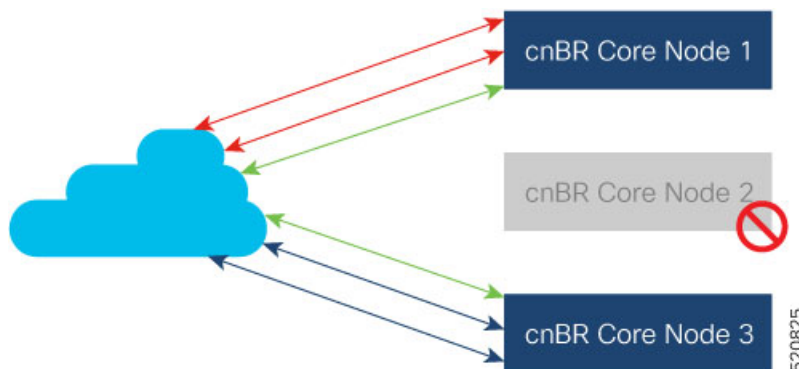
Therefore, the healthy nodes in the cluster take over the workloads from the failed node. After the failed node recovers, it returns to the resource pool and the system can assign new workloads to it. If the available capacity on the healthy node is not enough, the system moves as many workloads as possible until all resources are exhausted. The remaining workloads stay on the failed node; they are recovered after the node is recovered.

Node Failure Recovery with Expansion Servers

Cisco cnBR supports node failure recovery with the deployment of expansion servers. All service instances, which provide DOCSIS services, including service instances running on expansion servers, are treated in the same way. This allows for ease of scale without loss of node resiliency functionality.

Software Failure Recovery

In addition to node resiliency, the containerized micro services are inherently tolerant to service software failures. If a micro service instance fails, it can restart itself quickly without interrupting the overall service.
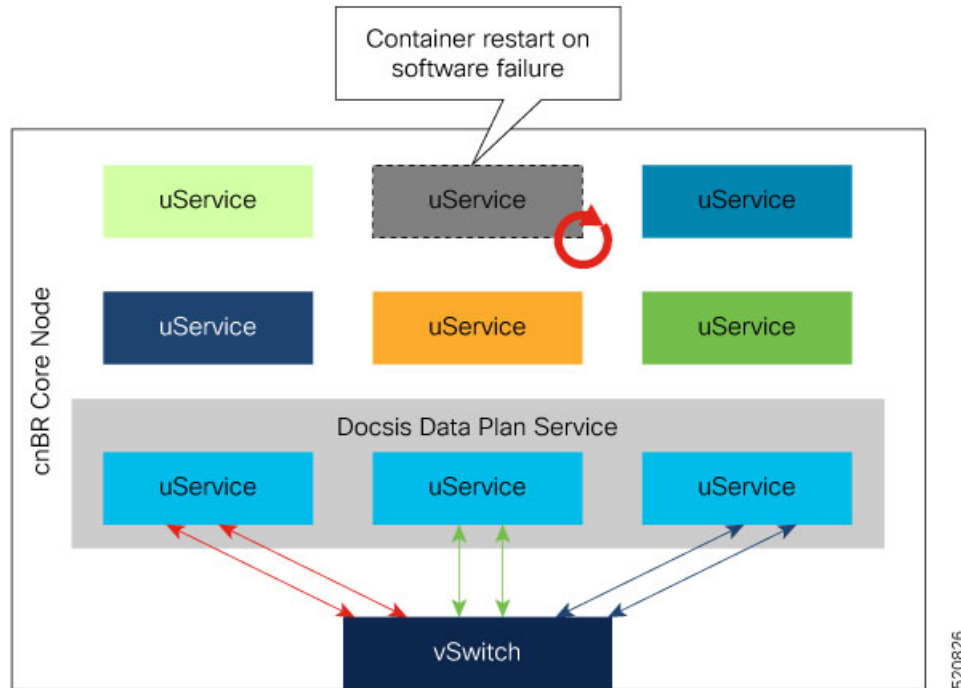
Container restart may take a few seconds; it is good enough for control plane and management services. When a container in critical services such as data plane fails to minimize the traffic interruption time, the system redirects DOCSIS traffic to other instances with free service group capacity within the same node.
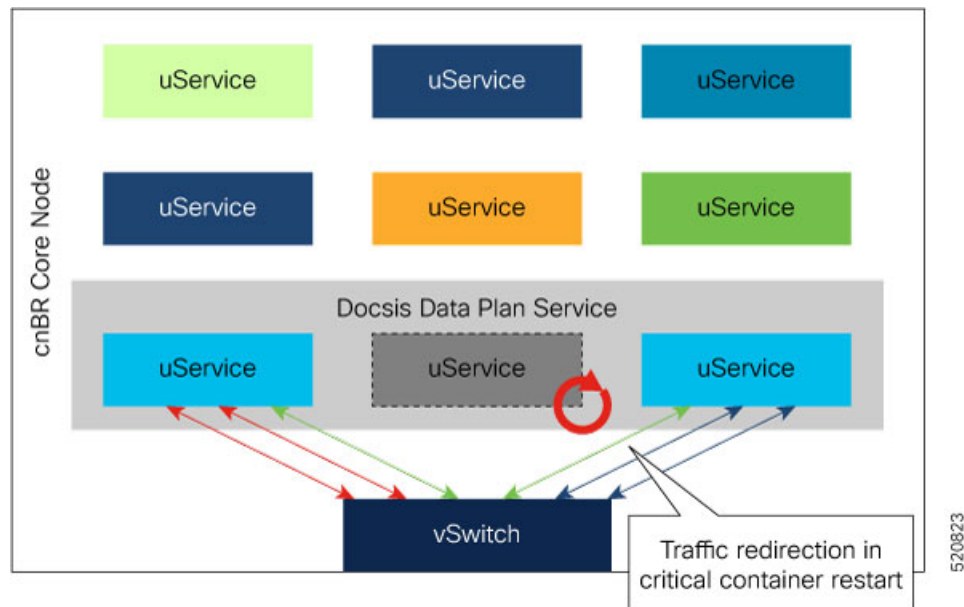
Configure Service Resiliency

Service resiliency is always enabled in Cisco cnBR cluster.

The system constantly monitors the resource (nodes and service instances) status. When there is a failure, the system automatically triggers workload reassignment. This process is transparent to the subscribers.

Workload in Cisco cnBR is measured in the unit of service group. Service groups are load balanced across DOCSIS nodes when you add them into a Cisco cnBR cluster. Make sure that there are enough capacities reserved in a Cisco cnBR cluster for resiliency.

In 20.2 release, each DOCSIS node can support up to 20 service groups. In order to tolerate one node failure without service interruption, we recommend that you do not provision more than 40 service groups for a three DOCSIS node Cisco cnBR cluster. Then, when a single DOCSIS node fails, there are enough capacities reserved for service resiliency.

Monitor and Troubleshoot

In cnBR HA Overview dashboard, you can check the overall High Availability (HA) state of the cluster.
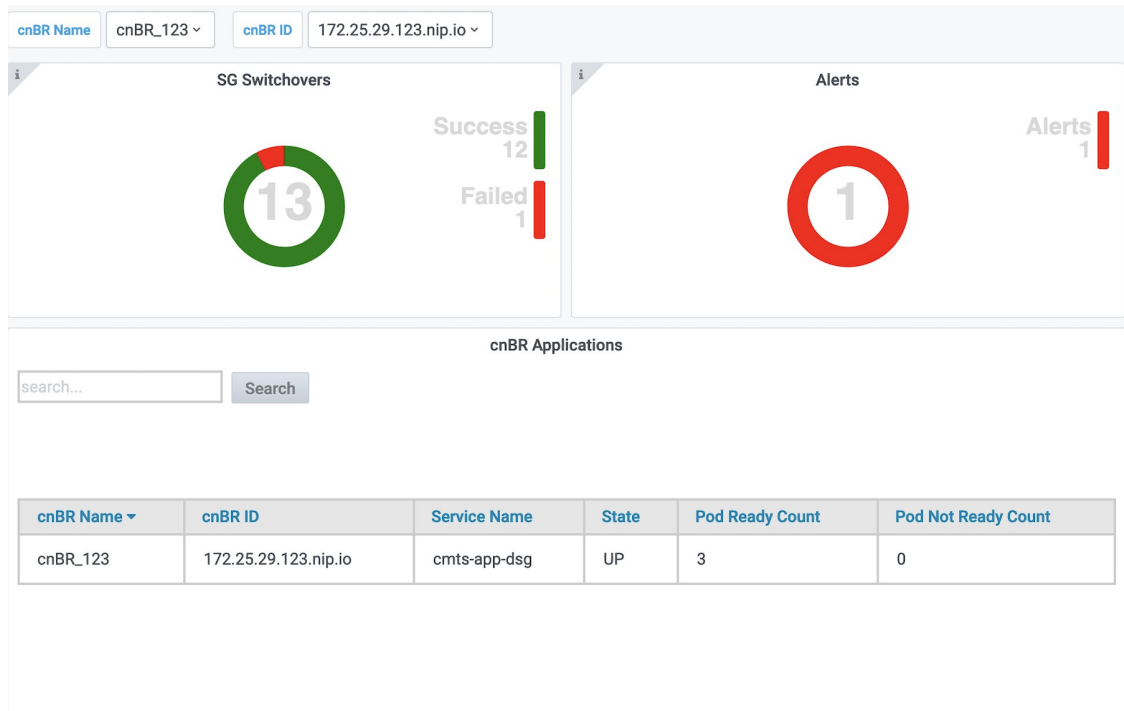
The SG Switchovers chart displays the total DOCSIS service switchover event count in the Cisco cnBR cluster. The counters increase when new service switchover occurs. In this chart:

- Success: The service switchover is complete without any issues.

- Failed: Some or all of the services failed to move workload during the service switchover. If this counter increases, click the number to check the error in the Service Group Switchover History dashboard.

Cisco cnBR Applications table lists the HA state of all the Cisco cnBR application services.

If a new switchover event occurred, access the Service Group Resiliency History dashboard to review detailed information for troubleshooting.
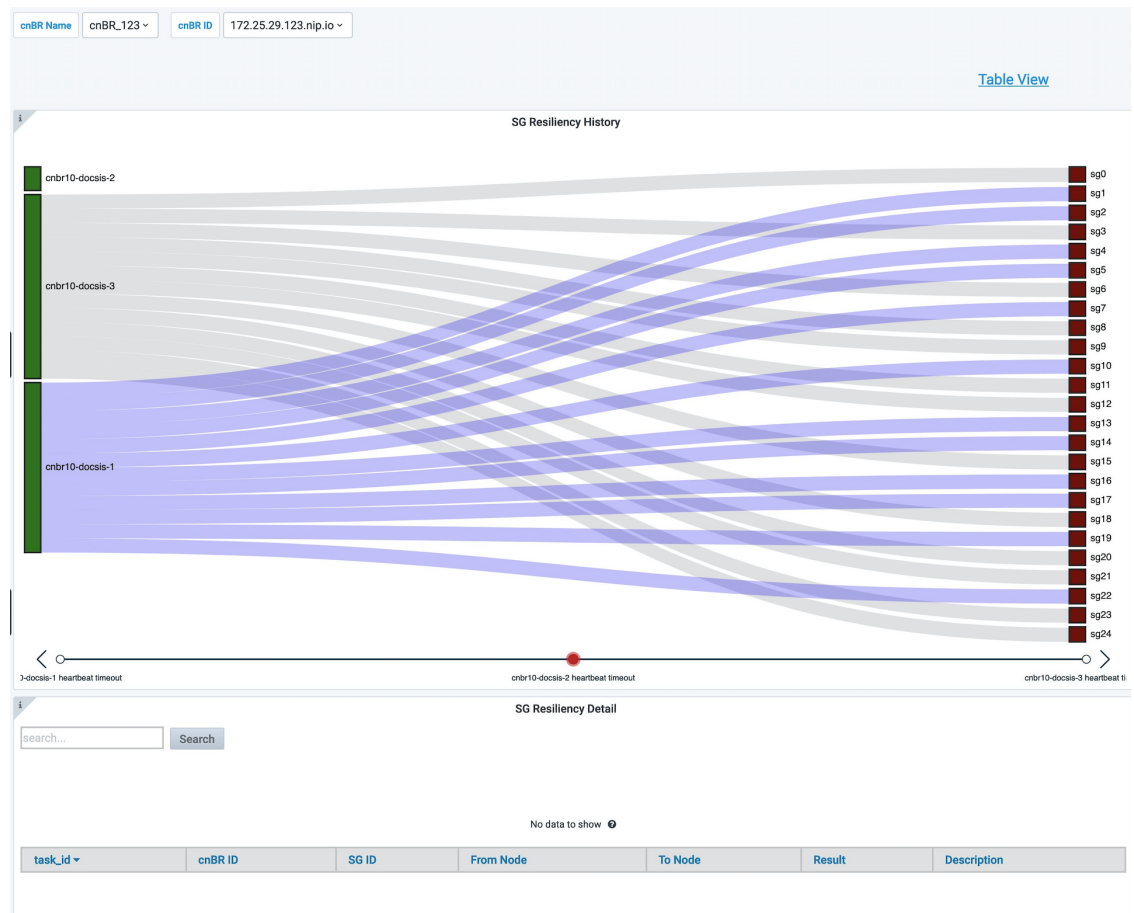
The SG Resiliency History diagram visualizes all historical DOCSIS service switchovers and SG mapping changes.

Click an event in the timeline to display the event details in the SG Resiliency Detail panel.

Cisco cnBR Link Redundancy

Feature History

Table 15: Feature History

Feature Name	Release Information	Feature Description
Cisco cnBR link redundancy	Cisco cnBR 20.3	Link redundancy protects the connection between a Cisco cnBR and a Service Provider (SP) router. When you connect a Cisco cnBR to an SP router (or uplink switch) using a 40G interface, a single link failure causes the whole service to fail. With this feature, you can enable another 40G interface to provide link redundancy.

Link redundancy protects the connection between a Cisco cnBR and a Service Provider (SP) router. When you connect a Cisco cnBR to an SP router (or uplink switch) using a 40G interface, a single link failure causes the whole service to fail. With this feature, you can enable another 40G interface to provide link-redundancy.

Link redundancy is based on the Link Aggregation Control Protocol (LACP). LACP is an 802.3ad standard. The vSwitch/Vector Packet Processor (VPP) in the Cisco cnBR provides the LACP function. The VPP has the bond interface to support link-redundancy. Bonding combines or joins two or more network interfaces together into a single logical interface. The Cisco cnBR forwards traffic over all available network interfaces of the aggregated link. Therefore, traffic can flow on the available links if one of the links within an aggregated link fails.

The following figure shows an example of a link redundancy setup between a Cisco cnBR and an SP router (or uplink switch)

Figure 12: Link Redundancy Wiring Topology in VLAN Mode
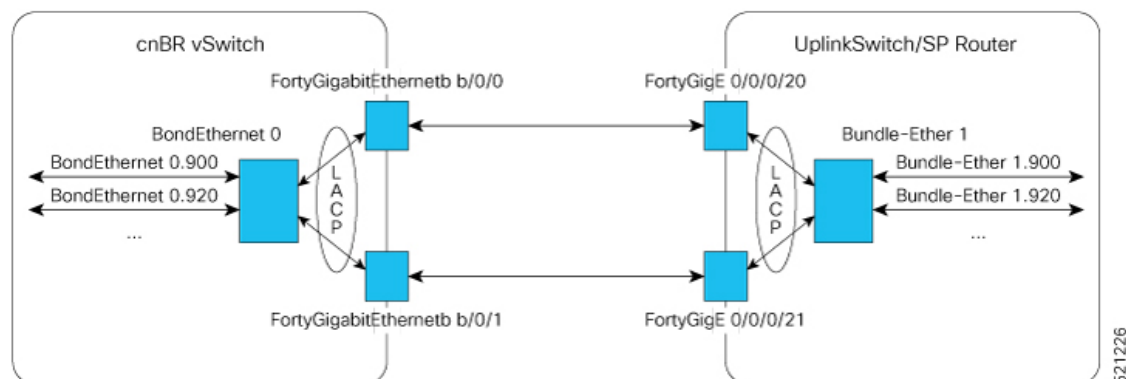
> **Note**
>
> - "bundle-ether" on router, "port-channel" on switch, and "bond-ethernet" are all terms to describe the bundling of two or more ports to form one logical Ethernet link.
>
> - Create all subinterfaces on the bond interface.
>
> - On the Cisco cnBR, an LACP bonding group supports a maximum of two members. These two members must come from the same Ethernet network-adapter card. The officially supported adapter cards include Intel X710 dual-port 40G QSPF+ NIC (Cisco product ID: UCSC-PCIE-ID40GF), and Mellanox CX-5 MCX516A-CDAT 2x100GbE QSFP PCIe NIC (Cisco product ID: UCSC-P-M5D100GF).

Configure Link Redundancy

On Cisco cnBR, use Day0 and Day1 configuration to enable link-redundancy.

Day0 Configuration

Add a second PCI device in the Day0 deployment configuration. You can configure the "pci_device" parameter as one or more PCI device entries.

See Deployment Example Configurations, on page 32 for sample configurations.

Day1 Configuration

Use the Day1 deployment configuration to configure the bond interface.

Use the following five parameters to configure the bond interface for link-redundancy.

- `cnbr-wan-ifname`

- `cnbr-wan-bonded-interface1`

- `cnbr-wan-bonded-interface2`

- `cnbr-wan-bond-mode`

- `cnbr-wan-bond-loadbalance`

These parameters are under the **wiring > overlay-info > vlan-info/vxlan-info.** "cnbr-wan-ifname" is a mandatory parameter in the wiring overlay configuration. The four bond-parameters are optional. To configure link-redundancy, define the "cnbr-wan-ifname" as "BondEthernet0" and configure the four bond-parameters. The following example shows a typical configuration:

```
wiring:

…

vlan :

    cnbr-wan-ifname: "BondEthernet0"

    cnbr-wan-bonded-interface1: "Ethernet0/0/0"

    cnbr-wan-bonded-interface2: "Ethernet0/0/1"

    cnbr-wan-bond-mode: "lacp"
```

```
                    cnbr-wan-bond-loadbalance: "L2"

                    overlay-cin-vlan: 920

                    overlay-l2vpn-mpls-vlan: 2003

                    overlay-l2vpn-vlan-vlan: 2202

                    overlay-wan-vlan: 900

              mtu : "2450"
```

Cisco cnBR Configuration

To add the bond interface, Use the cnBR Manager to configure the wiring.

Step 1 From the Cisco Operations Hub, click the Cisco Operations Hub main menu button.

Step 2 Choose **cnBR Manager** > **cnBRs** to open the **cnBR Clusters** page.

Step 3 Click the name of the target Cisco cnBR cluster to open the **cnBR Cluster Configuration** page.

Step 4 Choose Wiring from the drop-down list.

Step 5 Update the configuration and click **SAVE.**

Cisco cnBR SP Router Redundancy

Feature History

Table 16: Feature History

Feature Name	Release Information	Feature Description
Cisco cnBR SP Router Redundancy	Cisco cnBR 20.4	Enables the Cisco cnBR to set up redundant connections to different SP routers. This redundancy ensures that a single link or SP router failure does not disrupt traffic flow for the CIN and WAN networks.

Cisco cnBR bridges its internal network to the WAN and CIN networks. This bridging uses various data channels running through the provider network via the SP router. To enable high availability, the Cisco cnBR can set up redundant connections to different SP routers. This redundancy ensures that a single link or SP router failure does not disrupt the network traffic flow for the CIN and WAN networks.

You can configure redundant SP routers that the Cisco cnBR connects to, to operate in active/active or active/standby mode.

The following figure shows an example of SP router redundancy setup:

Figure 13: SP Router Redundancy Setup
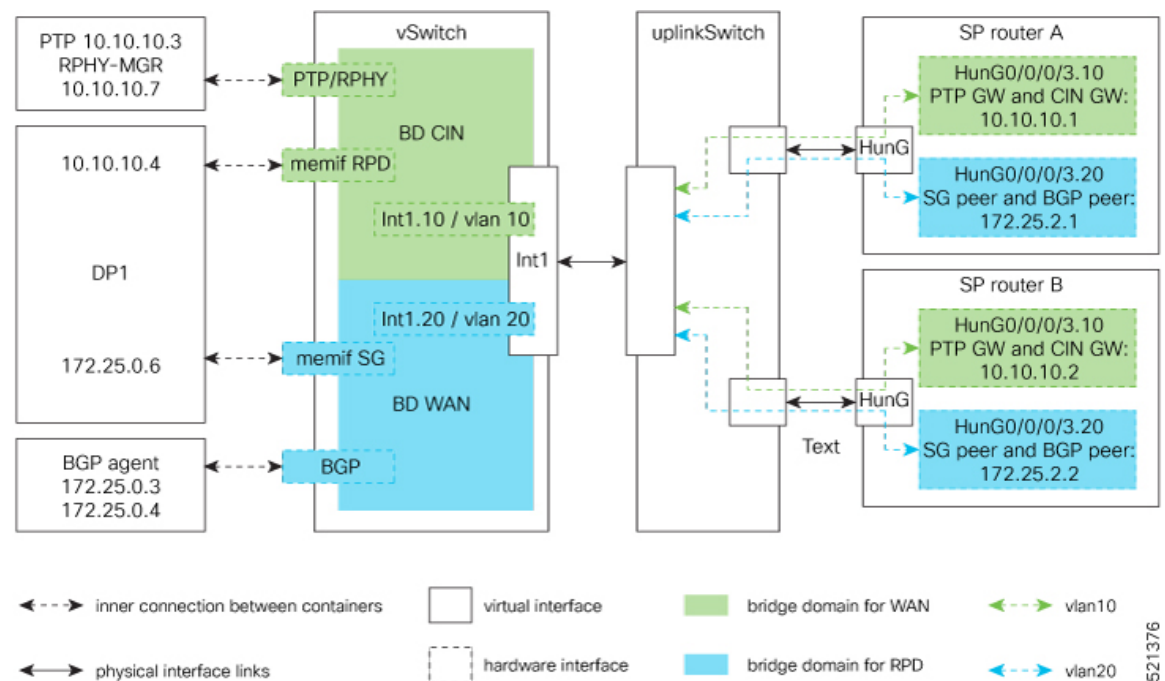
Note In VLAN mode, SP router A and SP router B are in the same VLAN. In the vlan10 for CIN and vlan20 for WAN in the preceding figure.

> **Note** Connect each UCS server to an uplink switch.

Configure SP Router Redundancy

The BGP agent and SP Router redundancy mode configurations are necessary to enable SP Router redundancy. The following configuration examples show sample BGP agent, SP Router redundancy configurations. Typically, these configurations are part of the Day1 operation.

BGP Agent Configuration

For bgpagent neighbors, configure BGP peers of both SP routers. The following example shows a typical configuration:

```
bgpagent:
    asn: 65001
    max_hops: 1
    restart-time: 120
    stale-path-time: 360
    neighbors:
       - {'address': '172.25.200.1', 'asn':65000}
       - {'address': '2001:DB8:200:200:200::1', 'asn':65000}
       - {'address': '172.25.200.254', 'asn':65000}
       - {'address': '2001:DB8:200:200:200::254', 'asn':65000}
```

SP Router Redundancy Configuration

The following example shows a typical configuration. "spr" in the following configuration refers to SP router.

```
spr:
 sp-router-redundancy-mode : "active-active"
 sp-routers :
  - {'bgp-peer' :'172.25.200.1', "sg-peer": "172.25.200.1", "router-id": "10.1.1.1",
"cin-gateway": "10.40.14.3", "ptp-gateway": "10.40.14.3"}
  - {'bgp-peer' :'2001:DB8:200:200:200::1', "sg-peer": "2001:DB8:200:200:200::1", "router-id":
 "10.1.1.1", "cin-gateway": "2001:DB8:10:40:14::3", "ptp-gateway": "2001:DB8:10:40:14::3"}
  - {'bgp-peer' :'172.25.200.254', "sg-peer": "172.25.200.254", "router-id": "20.2.2.2",
"cin-gateway": "10.40.14.254", "ptp-gateway": "10.40.14.254"}
  - {'bgp-peer' :'2001:DB8:200:200:200::254', "sg-peer": "2001:DB8:200:200:200::254",
"router-id": "20.2.2.2", "cin-gateway": "2001:DB8:10:40:14::254", "ptp-gateway":
"2001:DB8:10:40:14::254"}
```

To configure SP router redundancy for l2vpn, define the "secondary-overlay-l2vpn-vlan-vlan" and "secondary-overlay-l2vpn-mpls-vlan" for the second SP router. The following example shows a typical configuration:

```
wiring :
    .
    .
    .
    vlan :
       cnbr-wan-ifname: "Ethernet0/0/0"
       overlay-wan-vlan: 20
       overlay-cin-vlan: 10
       overlay-l2vpn-vlan-vlan: 202
       overlay-l2vpn-mpls-vlan: 203
       secondary-overlay-l2vpn-vlan-vlan: 204
       secondary-overlay-l2vpn-mpls-vlan: 205
```

Configure Cisco cnBR SP Router Redundancy Using cnBR Manager

Use the cnBR Manager to configure the BGP Agent, SP Router, and Wiring.

Step 1   Log in to the Cisco Operations Hub.

Step 2   From the Cisco Operations Hub main menu, Choose **cnBR Manager** > **cnBRs** to open the **cnBR Clusters** page.

Step 3   Click the name of the Cisco cnBR cluster to open the **cnBR Cluster Configuration** page.

Step 4   Select **BGP Agent** from the drop-down list.

Step 5   Update the configuration and click **SAVE**.

Step 6   Select **SP Router** from the drop-down list.

Step 7   Update the configuration and click **SAVE**.

Step 8   Select **Wiring** from the drop-down list.

Step 9   Update the configuration and click **SAVE**.

Smart Licensing

Feature History

Table 17: Feature History

Feature Name	Release Information	Feature Description
Smart Licensing	Cisco cnBR 21.1	The Smart Licensing feature is a standardized licensing platform that simplifies the Cisco software experience. Cisco Smart Licensing is a new, flexible way of licensing to buy, deploy, track, and renew Cisco software. With Smart Licensing, you can configure, activate, and register your device. Smart Licensing establishes a pool of software licenses or entitlements that you can use across your entire enterprise in a flexible and automated manner.
Smart Licensing	Cisco cnBR 21.2	From Cisco cnBR 21.2, the Smart Licensing workflows have been simplified. Device Registration, Permanent License Reservation, Specific License Reservation, and returning license reservations are now simple GUI driven workflows.

Cisco Smart Licensing is a new, flexible way of licensing to buy, deploy, track, and renew Cisco software. With Smart Licensing, you can configure, activate, and register your device. Smart Licensing establishes a pool of software licenses or entitlements that you can use across your entire enterprise in a flexible and automated manner.

The following sections describe several utilities and processes that are necessary to complete the registration and authorization.

Prerequisites for Smart Licensing

To enable Smart Licensing on a Cisco cnBR, ensure that you have the following components in place:

- Access to Cisco Smart Software Manager (CSSM)

- Smart Account (SA) and Virtual Account (VA). If you do not have a smart account, see Create a Smart Account.

- Smart Agent running on the device (cnBR)

- Cisco Operations Hub

- Smart Call Home (Optional)

- Cisco Smart Software Manager On-Prem (Optional)

Smart Licensing Deployment Models

You have choice of four options that are available for deploying Smart Licensing. The following list contains the deployment options from the easiest, to the most secure option:

1. **Direct cloud access**: This option allows you to transfer usage over the internet to Cisco Smart Software Manager (CSSM), directly from the devices to the cloud via HTTPs.

2. **Direct cloud access through an HTTPs proxy**: This option allows you to transfer files directly over the internet to CSSM through an HTTPs proxy. You can either use the *Smart Call Home Transport Gateway* or use an HTTPs proxy such as Apache.

3. **Mediated access through an on-premises collector-connected**: This option uses CSSM On-Prem as an internal collection device. The Cisco Smart Software Manager On-Prem is deployed in the customer environment, and periodically transmits the information to the cloud using periodic network synchronization. In this deployment option, the only system or database transferring information to the cloud is CSSM On-Prem. You can thus control what the collector database includes, which provides greater security.

4. **Mediated access through an on-premises collector-disconnected**: This option is the most secure, and uses the Cisco Smart Software Manager On-Prem. CSSM On-Prem only transfers the collected files using manual synchronization (at least once a month). In this option, the system is not directly connected to the cloud. An *air gap* exists between your network and the Cisco cloud.

cnBR License Model

Cisco cnBR offers a three-tier license model that is based on the number of channels that are configured per Service Group (SG). You need at least one of these three licenses to run a Cisco cnBR beyond the evaluation period of 90 days. You also need one basic SMI license to run the basic software infrastructure per cluster.

Cisco cnBR offers a three-tier license model:

- **Essential**: Essential is the lowest tier license which enables a Cisco cnBR. Essential is used when:

  - The number of channels per Service Group is less than or equal to 48.

  - The number of Service Groups with channels greater than 48 does not exceed 5% of all Service Groups.

- **Advantage**: Advantage is the middle tier license which enables a Cisco cnBR. Advantage is used when:

    - The number of channels per Service Group is less than or equal to 80.

    - The number of Service Groups with channels greater than 80 does not exceed 5% of total Service Groups.

- **Premier**: Premier is the highest tier license which enables a Cisco cnBR with no restrictions.

Every license has two entitlements. The entitlement types are the right-to-use (RTU) and Software Innovation Access (SIA). You must have an equal number of licenses in both RTU and SIA. Cisco cnBR automatically configures entitlements according to the criteria in the following table:

Cisco cnBR Entitlements and Required Licenses

Table 18: Cisco cnBR Entitlements and Required Licenses

Entitlement Type	Entitlement Name	Channels/SG(N)	Criteria	Licenses Required
Essential RTU	CNBR_ESS_RTU	N <= 48	Less than 5% of SGs have N < 80	1 per Subscriber
Essential SIA	CNBR_ESS_SIA	N <= 48	Less than 5% of SGs have N < 80	1 per Subscriber
Advantage RTU	CNBR_ADV_RTU	48 < N <= 80	Less than 5% of SGs have N > 80	1 per Subscriber
Advantage SIA	CNBR_ADV_SIA	48 < N <= 80	Less than 5% of SGs have N > 80	1 per Subscriber
Premier RTU	CNBR_PRE_RTU	N > 80	More than 5% of SGs have N > 80	1 per Subscriber
Premier SIA	CNBR_PRE_SIA	N > 80	More than 5% of SGs have N > 80	1 per Subscriber
Basic SMI RTU	CNBR_SMI_BS_RTU	NA	1 per Cluster	1 per Cluster
Basic SMI SIA	CNBR_SMI_BS_SIA	NA	1 per Cluster	1 per Cluster

When you exceed the usage of lower tier licenses, Cisco Smart Software Manager (CSSM) tries to borrow and consume licenses from higher tiers to keep the Cisco cnBR in compliance mode. CSSM reports noncompliance if there are no licenses available in the higher tiers.

Note

- Cisco cnBR license requirements are based on the usage of channels per Service Groups and the number of subscribers.

- Cisco cnBR configures entitlement to Essential by default.

Configure Smart License

You can configure the Smart License with Cisco cnBR using Cisco Operations Hub (Main Menu > cnBRs > Smart Licensing)..

Configure CSSM URL on Device

You must configure the Cisco Smart Software Manager (CSSM) URL on the device before configuring Smart Licensing.

Complete the following step to configure CSSM:

Click **SSM Connection Mode** in Smart License page to configure the CSSM URL.

Operations Hub provides two options to its users:

a. **Direct connection** mode requires direct internet access to the Cisco SSM cloud from the Cisco cnBR.

b. **Cisco SSM On-Prem** offers security sensitive organizations near real-time visibility and reporting of the Cisco licenses purchased and consumed, without requiring direct internet access.

Enable Smart License

Smart Licensing is enabled by default on the Cisco cnBR.

Complete the following steps to get started with Smart Licensing:

Step 1   Ensure that you meet the Prerequisites for Smart Licensing .

Step 2   Configure Call Home.

Step 3   Device Registration, on page 92.

Step 4   In case of CSSM On-Prem deployments under call-home profile, remove the default destination CSSM URL and enter your CSSM On-Prem URL.

Device Registration

Click **Register** option in Cisco Operations Hub Smart Licensing page to register your device. Also, log in to Cisco Smart Software Manager (CSSM) to generate a token. Tokens are generated to register a new product instance to the virtual account. Go through the following steps to generate a new token from the Cisco Smart Software Manager (CSSM) and register your device.

Step 1   Select a cnBR and click **Register**.
It opens a panel to accept a registration token.

Step 2   Keeping the Cisco Operations Hub open, log in to CSSM at https://software.cisco.com/. Ensure that you use a username and password that is provided by Cisco.

Step 3   Click **Inventory**.

Step 4   Select your virtual account from the Virtual Account drop-down list.

Step 5   Click **General > New Token**.

Step 6   Create a registration token. Provide a token description. Specify the number of days that the token must be active.

Step 7   Switch the Export-Controlled functionality to **Allow** for the products registered with this token.

Step 8   Click Create Token. After the token creation, click Copy to copy the newly created token.

Step 9   Come back to Cisco Operations Hub. Paste the token that is generated in the previous step under Registration Token. Complete the registration process for the device.

On successful registration, the device displays the status as Registered and receives an identity certificate. The certificate is saved to your device, and automatically used for all future communication with Cisco. The Cisco Operations Hub generates an error if device registration fails.

After successful registration, click the cnBR to view Smart License details in Cisco Operations Hub. The following is a sample of the Smart License details.

```
Smart Licensing is ENABLED
Registration:
Status: REGISTERED
Smart Account: BU Production Test
Virtual Account: CNBR-PROD-TEST
Export-Controlled Functionality: Allowed
Initial Registration: SUCCEEDED on Mar 25 03:02:38 2021 GMT
Last Renewal Attempt: SUCCEEDED on Mar 25 03:02:38 2021 GMT
Next Renewal Attempt: Sep 21 03:02:38 2021 GMT
Registration Expires: Mar 25 02:57:47 2022 GMT
License Authorization:
Status: AUTHORIZED on Mar 25 03:02:45 2021 GMT
Last Communication Attempt: SUCCEEDED on Mar 25 03:02:45 2021 GMT
Next Communication Attempt: Apr 24 03:02:45 2021 GMT
Communication Deadline: Jun 23 02:57:57 2021 GMT
License Conversion:
Automatic Conversion Enabled: true
Status: NOT STARTED
Utility:
Status: DISABLED
Transport:
Type: CALLHOME
Evaluation Period:
Evaluation Mode: Not In Use
Evaluation Period Remaining: 88 days, 3 hr, 46 min, 42 sec
License Usage
=============
License Authorization Status: AUTHORIZED as of Mar 25 03:02:45 2021 GMT
CNBR - SMI - BASIC - RTU (CNBR_SMI_BS_RTU)
Description: Cloud Native Broadband Router - SMI - BASIC - RTU
Count: 1
Version: 1.0
Status: AUTHORIZED
Export status: NOT RESTRICTED
Feature Name: <empty>
Feature Description: <empty>
Product Information
===================
UDI: PID:CNBR,SN:IP4D62A-HRFCTOY
Agent Version
=============
Smart Agent for Licensing: 3.0.13
```

Deregister a Device

Click **Deregister** in Cisco Operations Hub Smart Licensing page to deregister your device.

After successful deregistration, click the cnBR to view Smart License details. After successful deregistration. The following is a sample of the Smart License details.

```
Smart Licensing Status
======================
Smart Licensing is ENABLED

Registration:
  Status: UNREGISTERED
  Export-Controlled Functionality: Not Allowed

License Authorization:
  Status: EVAL MODE
  Evaluation Period Remaining: 88 days, 3 hr, 46 min, 42 sec
  Last Communication Attempt: NONE

License Conversion:
 Automatic Conversion Enabled: true
 Status: NOT STARTED

Utility:
  Status: DISABLED

Transport:
  Type: CALLHOME

Evaluation Period:
  Evaluation Mode: In Use
  Evaluation Period Remaining: 88 days, 3 hr, 46 min, 42 sec

License Usage
=============
License Authorization Status: EVALUATION MODE
  Evaluation Period Remaining: 88 days, 3 hr, 46 min, 42 sec

CNBR - SMI - BASIC - RTU (CNBR_SMI_BS_RTU)
  Description: Cloud Native Broadband Router - SMI - BASIC - RTU
  Count: 1
  Version: 1.0
  Status: EVAL MODE
  Export status: NOT RESTRICTED
  Feature Name: <empty>
  Feature Description: <empty>

Product Information
===================
UDI: PID:CNBR,SN:IP4D62A-HRFCTOY

Agent Version
=============
Smart Agent for Licensing: 3.0.13
```

License Reservation

License reservation is a mechanism to reserve node locked licenses and install them on the Cisco cnBR. The following are the license reservation types:

- Permanent License Reservation (PLR): All licenses are reserved.

- Specific License Reservation (SLR): Only specific licenses are reserved. Supports term licenses.

Permanent License Reservation

Permanent License Reservation (PLR) is a set of capabilities that are designed for highly secure environments. PLR restricts all communications with the outside environment. PLR enables all current and future entitlements on the Cisco cnBR device.

To create a PLR, complete the following steps:

Step 1 Generate the reservation request code on the device from **Cisco Operations Hub main menu > cnBR Manager > cnBRs > Smart Licensing**.

a) Click **License Reservation > Generate a Reservation Request Code**.

b) Click **Generate Code** to generate a **Reservation Request Code**.

c) Copy the **Reservation Request Code** displayed on the screen.

Step 2 Log in to Cisco Smart Software Manager at https://software.cisco.com/. Log in to the portal using a username and password that is provided by Cisco.

Step 3 Click **Inventory**.

Step 4 Select your virtual account from the Virtual Account drop-down list.

Step 5 Click **Licenses** > **License Reservation**.

Step 6 On the **Enter Request Code** page, enter or attach the reservation request code that you generated from the Cisco cnBR, and click **Next**.

Step 7 Select **PLR entitlement**.

Step 8 Provide and a token description. Specify the number of licenses to reserve for every entitlement.

Step 9 Click **Create Token**. After token creation, click **Copy** to copy the newly created token.

Step 10 Install the reservation key on the device in the Cisco Operations Hub.

a) Click **License Reservation > Submit Reservation Authorization Code**.

b) Paste the Reservation Authorization Code in the Reservation Authorization Code field.

c) Click **Reserve**.

The following is a sample of the Smart License details.

```
Smart Licensing Status
======================
Smart Licensing is ENABLED
License Reservation is ENABLED

Registration:
  Status: REGISTERED - UNIVERSAL LICENSE RESERVATION
  Export-Controlled Functionality: Allowed
  Initial Registration: SUCCEEDED on Wed Mar 24 14:50:18 GMT 2021
  Last Renewal Attempt: None
```

```
   License Authorization:
     Status: AUTHORIZED - RESERVED on Wed Mar 24 14:50:18 GMT 2021

   Utility:
     Status: DISABLED

   Transport:
     Type: CALLHOME

   Evaluation Period:
     Evaluation Mode: Not In Use
     Evaluation Period Remaining: 88 days, 15 hr, 56 min, 59 sec

   License Usage
   =============
   License Authorization Status:
     Status: AUTHORIZED - RESERVED on Wed Mar 24 14:50:18 GMT 2021
     Last Communication Attempt: SUCCEEDED on Mar 24 14:50:18 2021 GMT
     Next Communication Attempt: NONE
     Communication Deadline: NONE

    (CNBR_SMI_BS_RTU)
     Description: <empty>
     Count: 1
     Version: 1.0
     Status: AUTHORIZED
     Export status: NOT RESTRICTED
     Feature Name: <empty>
     Feature Description: <empty>

   Product Information
   ===================
   UDI: PID:CNBR,SN:TETB3CA-774T4BI

   Agent Version
   =============
   Smart Agent for Licensing: 3.0.13
```

Specific License Reservation

Specific License Reservation (SLR) is a Smart Licensing functionality that enables you to deploy a software license on a device without communicating usage information to Cisco. SLR allows you to reserve a license for your product instance from the Cisco Smart Software Manager (CSSM). This feature is used in secure networks.

To create an SLR, complete the following steps:

Step 1 Generate the reservation request code on the device from **Cisco Operations Hub main menu > cnBR Manager > cnBRs > Smart Licensing**.

    a) Click **License Reservation > Generate a Reservation Request Code**.

    b) Click **Generate Code** to generate a **Reservation Request Code**.

    c) Copy the **Reservation Request Code** displayed on the screen.

Step 2 Log in to Cisco Smart Software Manager at https://software.cisco.com/. You must log into the portal using a username and password that is provided by Cisco.

Step 3 Click **Inventory**.

Step 4   Select your virtual account from the Virtual Account drop-down list.

Step 5   Click **Licenses** > **License Reservation**.

Step 6   On the **Enter Request Code** page, enter or attach the reservation request code that you generated from the Cisco cnBR, and click **Next**.

Step 7   Select **SLR entitlement**.

Step 8   Provide a token description. Specify the number of licenses to be reserved for every entitlement.

Step 9   Click **Create Token**. After the token is created, click **Copy** to copy the newly created token.

Step 10   Install the reservation key on the device in the Cisco Operations Hub.

    a) Click **License Reservation > Submit Reservation Authorization Code**.

    b) Paste the Reservation Authorization Code in the Reservation Authorization Code field.

    c) Click **Reserve**.

The following is a sample of the Smart License details.

```
    Smart Licensing is ENABLED
    License Reservation is ENABLED
    Specified License Reservations:
    Status: SPECIFIC INSTALLED - SUCCEEDED on Thu Mar 25 04:26:17 GMT 2021
    Export-Controlled Functionality: Allowed
    Request Code: CB-ZCNBR:IP4D62A-HRFCTOY-BfCjVThKq-03
    Last Confirmation Code: 58aaf92a
    License Type: TERM
    Description: CNBR - SMI - BASIC - RTU
    Start Date: 2021-Mar-05 GMT
    End Date: 2021-Sep-01 GMT
    Count: 1
    Subscription ID:

  Router# show license summary
  Smart Licensing is ENABLED
  License Reservation is ENABLED
  Registration:
  Status: REGISTERED - SPECIFIC LICENSE RESERVATION
  Export-Controlled Functionality: Allowed
  Initial Registration: SUCCEEDED on Thu Mar 25 04:26:17 GMT 2021
  Last Renewal Attempt: None

License Authorization:
  Status: AUTHORIZED - RESERVED on Thu Mar 25 04:26:17 GMT 2021

Utility:
  Status: DISABLED

Transport:
  Type: CALLHOME

License Usage:
  License                      Entitlement Tag
            Count       Status

-------------------------------------------------------------------------------------------------------------

cc2b8a7b-3a10-4acd-b252-eb849e7c2885regid.2021-03.com.cisco.CNBR_SMI_BS_RTU,1.0_cc2b8a7b-3a10-4acd-b252-eb849e7c2885
  1             ReservedInCompliance
```

Return License Reservation

You can return reserved licenses through a guided workflow using the Cisco Operations Hub.

Before you begin

Make sure you can access Cisco Smart Software Manager (SSM).

Step 1 Click **License Reservation > Return License Reservation**.

Step 2 Click **Generate Code** to generate a return reservation request code. Copy the Reservation Request Code displayed on the screen.

Step 3 Log in to Cisco Smart Software Manager.

Step 4 Submit the Reservation Request Code to return your license.

CHAPTER 3

Cisco Cloud Native Broadband Router Service Configuration and Monitoring

Cisco cnBR virtualizes all hardware-based services, provides a cloud-native design, and offers a variety of features as microservices. You can quickly develop, test, and deploy new services or update features and functions without any downtime.

Network Services

Cisco cnBR empowers you to create a number of easily composable, scalable, and resilient network services.

DHCP Relay Service

Cisco cnBR acts as a Dynamic Host Configuration Protocol (DHCP) relay agent to implement features such as DHCP relay, Lease Query (LQ), IPv6 Prefix Delegation (PD), and to provision static IP addresses for subscribers by using source address verification (SAV).

DHCP Relay

When the Cisco cnBR acts as a relay agent, it forwards requests and replies between clients and servers when they are not on the same physical subnet. Relay agent forwarding is different from normal IP router forwarding. In normal IP router forwarding, IP datagrams are forwarded between networks transparently. However, in relay agent forwarding, relay agent receives a DHCP message and then generates a new DHCP message to send through another interface.

When a DHCP client requests an IP address from a DHCP server, for instance DHCPv4, the client sends a DHCPDISCOVER broadcast message to locate the DHCP server. Relay agent forwards the packets between the DHCP client and the DHCP server. The DHCP server provides configuration parameters, such as IP

address, MAC address, domain name, and a lease for the IP address, to the client in a DHCPOFFER unicast message.

User Guidelines:

- By default, DHCP relay is enabled on Cisco cnBR. DHCP relay depends on two Cisco cnBR services in the multiple instances environment - BGP agent and Relay proxy.

- DHCP relay agent configuration is based on service group.

- DHCP server receives DHCP request. If multiple DHCP servers are configured, all these servers receive relay packets.

- The v4Net/v6Net defines all the IP scopes for the subscriber's DHCP destination IP address. This configuration must be consistent with the configuration of the DHCP server. If multiple subscriber nets are configured, use the first scope as the default scope.

- Cisco cnBR can also assign a specific server or IP scope for a subscriber. For more information, see Policy Based Relay, on page 101.

- By default, the DHCPv6 Client Link-Layer Address option (RFC 6939) is enabled. You cannot disable this option.

DHCPv6 Client Link-Layer Address Option (RFC 6939)

The following table provides description of the various features and their release information

Table 19: Feature History

Feature Name	Release Information	Feature Description
Support for DHCPv6 client link-layer address (RFC 6939)	Cisco cnBR 21.2	This support provides the client's link-layer address in the DHCPv6 messages which are sent towards the server.

Cisco cnBR supports DHCPv6 client link-layer address option (RFC 6939). It defines an optional mechanism and the related DHCPv6 option to allow first-hop DHCPv6 relay agents (relay agents that are connected to the same link as the client) to provide the client's link-layer address in the DHCPv6 messages which are sent towards the server.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| OPTION_CLIENT_LINKLAYER_ADDR  |           option-length       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|   link-layer type (16 bits)   |                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+                               |
|               link-layer address (variable length)           |
|                                                               |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

The following table provides information on the DHCPv6 client link-layer address (RFC 6939) parameters and their description

Name	Description
option-code	OPTION_CLIENT_LINKLAYER_ADDR (79).
option-length	2 + length of MAC address.
link-layer type	CPE or CM MAC address type. The link-layer type must be a valid hardware type assigned by the IANA, as described in the RFC0826.
link-layer address	MAC address of the CPE or CM.

Note By default, the DHCPv6 Client Link-Layer Address option (RFC 6939) is enabled. You cannot disable this option.

Policy Based Relay

Policy Based Relay allows subscribers with different device classes to be classified into different IP ranges.

When the relay agent handles subscriber DHCP packets, Cisco cnBR can identify its device class based on the TLV (Tag, Length, Value) in the DHCP packets. Then the Cisco cnBR uses a predefined relay policy to assign a specific server to get DHCP address, or notify the server to assign its DHCP address in a specific IP range.

User Guidelines:

  • Define the v4serverip/v6serverip in the dhcpServers.

  • Define the giaddr/linkaddr with associated v4Nets and/or v6Nets. The address is the prefix of the v4Nets/v6Nets.

  • If there is no specific v4serverip/v6serverip for the device class, the subscriber requests are forwarded to all the servers defined.

  • If there is no specific giaddr/linkaddr for the device class, the subscribers get the IP from the first default range.

DHCPv6 Prefix Delegation

In the IPv6 networking, you can use the DHCPv6 prefix delegation (PD) to assign network address prefix, automate configuration, and provision the public routable addresses for the network. For example, in home networks, home routers use the DHCPv6 protocol to request a network prefix from the ISP's DHCPv6 server. After you assign the network prefix, the ISP routes this network prefix to your home router. Then the home router starts displaying the new addresses to hosts on the network.

After the PD router comes online, it gets the assigned network prefix from the DHCP server.

ARP/NDP Glean and Lease Query

As a relay agent, Cisco cnBR stores all subscriber DHCP information after DHCP is completed. Based on this information, routing is established for subscribers. However, there are several cases when subscriber

information is unavailable, such as a modem reset, resulting in routing being no longer available for subscribers. When these subscribers access the network, Cisco cnBR rebuilds the data path by using ARP/NDP glean or lease query.

When using ARP/NDP Glean, Cisco cnBR can trust the packets that come from the cable side network. After the ARP/NS is received and the source IP is updated in the configured IP ranges, Cisco cnBR rebuilds a data path for the source MAC. This method is open to MAC spoofing.

In contrast, when using Lease Query, Cisco cnBR doesn't trust the cable side network. When Cisco cnBR receives the upstream packet with no data path route, it sends a LEASEQUERY request to DHCP server. After DHCP server gets the request and confirms that the RESPONSE, the MAC and IP are released from DHCP server, Cisco cnBR rebuilds the data path. Otherwise, Cisco cnBR drops the packets.

User guidelines:

- Enable or disable ARP/NDP Glean and Lease Query on demand.

- Lease Query checks the source IP with the v4Nets/v6Nets configuration. If the source IP of the packets isn't in the range, then Lease Query discards the packet.

- Use ARP/NDP Glean and Lease Query with Source Address Verification (SAV).

Source Address Verification (SAV)

In addition to DHCP leased IP address, Cisco cnBR allows static IP address by provisioning SAV group.

A SAV group is a group of IPv4 or IPv6 prefixes. Cisco cnBR uses these prefixes to authenticate a cable modem (CM). You can configure a CM with an IPv4 or IPv6 prefix that belongs to a particular SAV group. The time, length, and the value (TLV) 43.7.1 specify the group name to which a given CM belongs. If the source IP address of a packet from a CM belongs to the configured prefix in a SAV group, the Cisco CMTS considers it as an authorized packet.

You can configure a maximum of 255 SAV groups on a Cisco cnBR. Each SAV group contains up to four IPv4s, IPv6s, or a combination of both prefixes. The total number of the prefixes is not more than four.

During registration, CMs communicate their configured static prefixes to the CMTS using TLV 43.7.1 and TLV 43.7.2. The TLV 43.7.1 specifies the SAV prefix group name that the CM belongs to, and TLV 43.7.2 specifies the actual IPv4 or IPv6 prefix. Each CM can have a maximum of four prefixes configured. When the Cisco CMTS receives these TLVs, it identifies whether the specified SAV group and the prefixes are already configured on the Cisco CMTS. If these are configured, the Cisco CMTS associates them to the registering CM. However if these are not configured, the Cisco CMTS automatically creates the specified SAV group and prefixes before associating them to the registering CM.

The Cisco CMTS considers the SAV group name and the prefixes that are provided by these TLVs to be valid. The packets received from the CM, with the source IP address belonging to the prefix specified by the TLV, are authorized packets. For example, if a given CM has an SAV prefix of 10.10.10.0/24, and the source IP address of a packet received from this CM (or CPE behind the CM) is in the subnet 10.10.10.0/24, then it is an authorized packet.

User guidelines:

- SAV configuration is global and not for each service group.

- SAV doesn't check the MAC/IP binding. You can assign the static IP to any MAC.

- By default, SAV is disabled. You can enable it on demand.

ARP/NDP Proxy

All cable modems and subscribers are behind the HFC network. As a proxy, Cisco cnBR relays the ARP/NDP requests to the CM.

With ARP/NDP proxy enabled, Cisco cnBR can respond the ARP/NDP, and the DS lease query is not to be triggered.

Mobility Scopes

If the subscribers are allowed to roam between different IPv4 and IPv6 scopes, the mobility scopes contain all the IPv4 and IPv6 scopes granted to the subscribers. This configuration is optional.

Configure DHCP Relay Service

The DHCP relay service operates in a similar way as other Cisco CMTS products. You can configure it with Autodeployer Script, or by importing the whole Cisco cnBR configuration YAML file to the desired Cisco cnBR using Cisco Operations Hub. The imported configuration file overwrites the existing configuration and activates the new configuration.

Update the DHCP Relay configuration using Autodeployer reconfig (Preferred)

After configuring the DHCP Relay using the Autodeployer during deployment, you can modify the dhcp block in the L3 profile file and run the AutoDeployer configuration script again to update the configuration.

> ✎
> **Note**   Rerunning AutoDeployer configuration script causes all the RPDs/SGs to be deleted and added.

Update DHCP Relay Configuration Using cnBR Manager

After configuring the DHCP Relay using the Autodeployer during deployment, you can also update the configuration using the cnBR Manager UI.

Use the following steps to update the DHCP Relay configuration:

Step 1   On the Cisco Operations Hub, click the Cisco Operations Hub main menu button.

Step 2   Choose **cnBR Manager** > **cnBRs** to open the **cnBR Clusters** page.

Step 3   Click **Import & Export cnBR** to open the **Export/Import** page.

Step 4   In the **Export cnBR Configuration** pane, from the drop-down list, choose the required Cisco cnBR to update.

Step 5   Click **Export** to get the current SG configuration of the selected Cisco cnBR.

Step 6   In the .json file, update one or more parameters in the dhcp section of the SG configuration.

Step 7   Save the updated configuration file on the local disk.

Step 8   In the **Import cnBR Configuration File** pane, from the drop-down list, choose the Cisco cnBR to update.

Step 9   Click **Browse** to locate the file which you updated (saved at Step 5).

Step 10   Click **Import** to upload the updated SG configuration to the selected Cisco cnBR.

Configure DHCP Relay using Autodeployer Script

In the AutoDeployer script L3 profile file, the DHCP Relay configuration is saved in the `dhcp` section. It is applied to all Service Groups on the Cisco cnBR. The following is an example configuration:

```
"Dhcp":
    {
        "ArpGlean":true,
        "ArpProxy":true,
        "ipv4Lq": false,
        "NdGlean":true,
        "NdProxy":true,
        "ipv6Lq":false,
        "dhcpServers":["80.80.80.3",
                       "81.81.81.3",
                       "2001:80:80:80::3",
                       "2001:81:81:81::3"
        ],
        "V4Nets":["90.90.90.1/24",
                  "91.91.91.1/24",
                  "92.92.92.1/24"
        ],
        "V6Nets":["2001:90:90:90::1/64",
                  "2001:91:91:91::1/64",
                  "2001:92:92:92::1/64"
        ],
        "RelayPolicies":[
          {"deviceClass": "HOST",
           "v4serverip": "80.80.80.3",
           "v6serverip": "2001:80:80:80::3",
           "giaddr": "90.90.90.1",
           "linkaddr": "2001:90:90:90::1"
           },
           {"deviceClass": "STB",
           "v4serverip": "81.81.81.3",
           "v6serverip": "2001:81:81:81::3",
           "giaddr": "91.91.91.1",
           "linkaddr": "2001:91:91:91::1"
           },
           {"deviceClass": "PS",
           "giaddr": "92.92.92.1",
           "linkaddr": "2001:92:92:92::1"
           },
           {"deviceClass": "EROUTER",
           "v4serverip": "80.80.80.3",
           "v6serverip": "2001:80:80:80::3",
           },
           {"deviceClass": "DVA",
           "giaddr": "90.90.90.1",
           "linkaddr": "2001:90:90:90::1"
           },
           {"deviceClass": "MTA",
           "giaddr": "91.91.91.1",
           "linkaddr": "2001:91:91:91::1"
           }
        ],
        "mobilityScopes":["90.90.90.1/24",
                          "91.91.91.1/24",
                          "92.92.92.1/24",
                          "2001:90:90:90::1/64",
                          "2001:91:91:91::1/64",
                          "2001:92:92:92::1/64"
        ]
    }
```

See Configure Cisco cnBR Using Autodeployer, on page 43 for additional information.

Configure DHCP Relay

The following table provides information on the DHCP relay field names, their descriptions, type and enforcement

Field Name	Description	Type	Enforcement
dhcpServers	DHCP server IPv4 and IPv6 addresses	IPv4 or IPv6	Required
v4Nets	IPv4 range to which the subscriber's DHCP address belongs	CIDR (Classless Inter-Domain Routing)	Required
v6Nets	IPv6 range to which the subscriber's DHCP address belongs	CIDR (Classless Inter-Domain Routing)	Required

```
"Dhcp":
{
    // all the DHCP servers IP, V4 and V6
    "dhcpServers":[
                "81.81.81.3",
                "24.24.24.3",
                "2001:81:81:81::3",
                "2001:24:24:24::3"
              ],
    // all the V4 subnets for the subscribers in this SG
    "v4Nets":[
                "90.90.90.1/24",
                "91.91.91.1/24",
                "92.92.92.1/24",
                "93.93.93.1/24",
                "94.94.94.1/24",
                "95.95.95.1/24"
                "96.96.96.1/24",
                "97.97.97.1/24",
          ],
    // all the V6 subnets for the subscribers in this SG
    "v6Nets":[
                "2001:90:90:90::1/64",
                "2001:91:91:91::1/64",
                "2001:92:92:92::1/64",
                "2001:93:93:93::1/64",
                "2001:94:94:94::1/64",
                "2001:95:95:95::1/64",
                "2001:96:96:96::1/64",
                "2001:97:97:97::1/64"
          ],
}
```

Configure DHCP Relay Policy

Field Name	Description	Type	Enforcement
deviceClass	The device class for each subscriber	String	Required
v4serverip	The server to which the DHCP request is forwarded	IPv4	Optional
v6serverip	The server to which the DHCPv6 request is forwarded	IPv6	Optional

Field Name	Description	Type	Enforcement
giaddr	The IP range to which the DHCPv4 address belongs; the giaddr is the IP address in the v4Nets	IPv4	Optional
linkaddr	The IP range to which the DHCPv6 address belongs; the linkaddr is the IP address in the v6Nets	IPv6	Optional

```
"Dhcp":
 {
  "RelayPolicies":[
{"deviceClass": "HOST",
 "giaddr": "92.92.92.1",
 "v4serverip": "24.24.24.3",
 "linkaddr": "2001:92:92:92::1"
},
{"deviceClass": "STB",
 "giaddr": "93.93.93.1",
 "v4serverip": "81.81.81.3",
 "linkaddr": "2001:93:93:93::1"
},
{"deviceClass": "PS",
 "giaddr": "94.94.94.1",
 "v6serverip": "2001:81:81:81::3",
 "linkaddr": "2001:94:94:94::1"
},
{"deviceClass": "EROUTER",
 "giaddr": "95.95.95.1",
 "linkaddr": "2001:95:95:95::1"
},
{"deviceClass": "DVA",
 "giaddr": "96.96.96.1",
 "v4serverip": "24.24.24.3",
 "linkaddr": "2001:96:96:96::1"
},
{"deviceClass": "MTA",
 "giaddr": "97.97.97.1",
 "v6serverip": "2001:24:24:24::3",
 "linkaddr": "2001:97:97:97::1"
}]
 }
```

Configure ARP/NDP Glean and Lease Query

The following table provides information on the ARP/NDP Glean and Lease Query field names, their descriptions, type and enforcement

Field Name	Description	Type	Enforcement
arpGlean	Enable/Disable	Boolean	Required; default is false
ndGlean	Enable/Disable	Boolean	Required; default is false
ipv4Lq	Enable/Disable	Boolean	Required; default is false
ipv6Lq	Enable/Disable	Boolean	Required; default is false

```
"Dhcp":
{
    "arpGlean":true,
    "ipv4Lq": false,
    "ndGlean":false,
    "ipv6Lq": false,
}
```

Configure SAV

The following table provides information on the SAV field names, their descriptions, type and enforcement

Field Name	Description	Type	Enforcement
savEnable	Enable/Disable	Boolean	Required
savEntires	SAV group structure	savGroup	Optional
grpName	SAV group name	String	Optional
prefixes	The SAV prefixes	CIDR (Classless Inter-Domain Routing) list	Optional

```
"sav"
{
    "savEnable": true,
    "savEntries": [{
                    "grpName": "testSAVV",
                    "prefixes": ["93.93.93.100/28",
                                 "2001:93:93:93100::0/72"]

                  }]
}
```

Configure ARP/NDP Proxy

The following table provides information on the ARP/NDP Proxy field names, their descriptions, type and enforcement

Field Name	Description	Type	Enforcement
ArpProxy	Enable/Disable	Boolean	Required; default false
NdProxy	Enable/Disable	Boolean	Required; default false

```
"ArpProxy":true,
"NdProxy":true,
```

Configure Mobility Scopes

The following table provides information on the Mobility Scopes field names, their descriptions, type and enforcement

Field Name	Description	Type	Enforcement
mobilityScopes	Scopes of ipv4 and ipv6	String	Optional

```
"mobilityScopes":["90.90.90.1/24",
                  "91.91.91.1/24",
```

```
                                    "92.92.92.1/24",
                                    "2001:90:90:90::1/64",
                                    "2001:91:91:91::1/64",
                                    "2001:92:92:92::1/64"
                                  ]
```

Monitor DHCP Relay Service

DHCP IPv4 Statistics

Figure 14: DHCPv4 panel in cnBR Manager Metrics
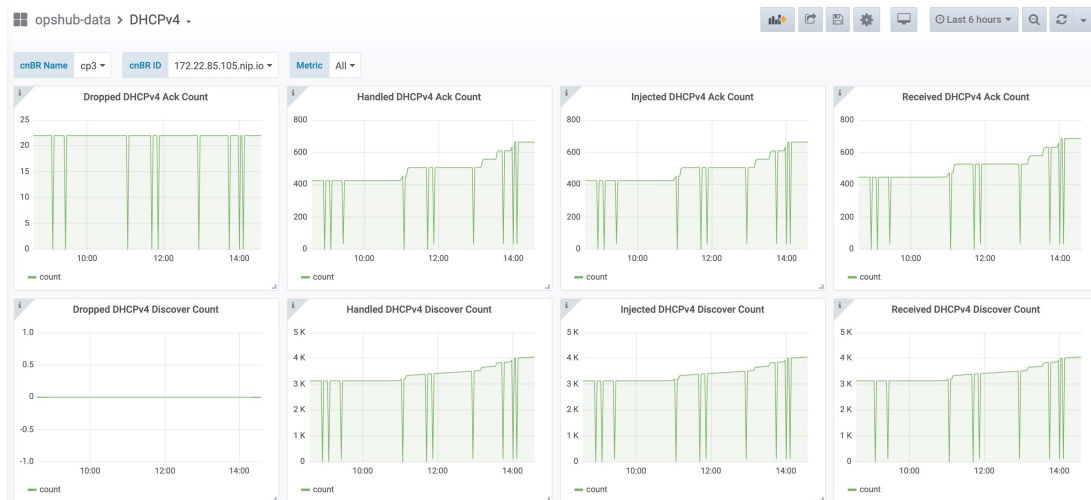
DHCPv4 dashboard displays statistics of the DHCP relay of IPv4. In all, there are 16 panels. The preceding picture shows only half the number of panels. Each panel represents the count of different states for different packet over time. There are four packet types for DHCPv4: Discover, Offer, Request, and Acknowledgment (Ack). The system processes each type of packet differently: Received, Dropped, Handled, and Injected. You can change the time span at the top-right corner. Currently, they show the count for the last six hours.

DHCP IPv6 Statistics

Figure 15: Screenshot of DHCPv6 panel in cnBR Manager Metrics
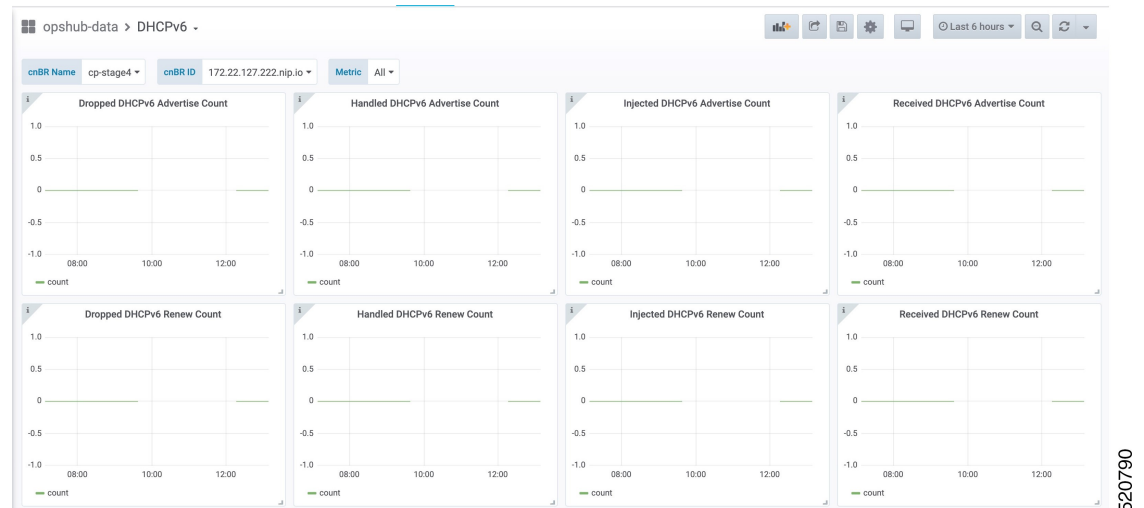
DHCPv6 dashboard displays statistics of the DHCP relay of IPv6. In all, there are 16 panels. The preceding picture shows only half the number of panels. Each panel represents the count of different states for different packet over time. There are four packet types for DHCPv6: Renew, Advertise, Request, and Reply. The system processes each type of packet differently: Received, Dropped, Handled, and Injected. You can change the time span at the top-right corner. Currently, they show the count for the last six hours.

PTP

Precision Time Protocol (PTP) is used to synchronize clocks throughout all cable networks. The Cisco cnBR cores and RPDs are managed by the Cisco cnBR, and runs an instance of the PTP client. To achieve time synchronization, the PTP client in Cisco cnBR and the PTP client in RPDs must synchronize their clocks to the same PTP primary clock. The Cable Modems (CMs) then synchronize their clock to the Cisco cnBR (and eventually to the PTP primary clock) through the DOCSIS timestamps provided by the RPD.

PTP allows creation of individual profiles for different scenarios. A profile is a specific selection of PTP configuration options that are selected to meet the requirements of a particular application. Cisco cnBR supports the PTP default profile.

To provide a high availability precision clock in the Cisco cnBR, two PTP primary clock sources can be configured in cnBR - a main PTP primary clock server and an alternate PTP primary clock server. Cisco cnBR synchronizes its clock to the best available PTP primary clock.

Some of the key parameters that are configured, or configurable, in the Cisco cnBR and RPD PTP client include:

- PTP Domain

  A PTP domain is a logical grouping of clocks that communicate with each other using the PTP protocol. A single computer network can have multiple PTP domains operating separately. For example, one set of clocks synchronized to one time scale and another set of clocks synchronized to another time scale. PTP can run over either Ethernet or IP, so a domain can correspond to a Local Area Network, or it can extend across a Wide Area Network.

In Cisco cnBR and RPD PTP client, the PTP domain is set during initial Cisco cnBR deployment. The PTP domain can be updated after deployment.

- PTP Transport

In Cisco cnBR and RPD, the PTP transport is configured to use PTP over IPv4 in unicast mode. The PTP Transport mode is not configurable in Cisco cnBR PTP client. The PTP Transport mode is configurable in the RPD PTP client.

- PTP Ports

A port can be configured to perform either fixed primary or secondary role, or can be configured to change its role dynamically. If no role is assigned to a port, it can dynamically assume a primary, passive, or secondary role, based on the Best Primary Clock Algorithm (BPCA), which is also known as Best Master Clock Algorithm (BMCA [RFCÂ 7273]).

Cisco cnBR and RPD support the PTP port secondary role. The Cisco cnBR PTP port role is not configurable. However, the RPD PTP port role is configurable, but it must be set to secondary role.

- PTP Clock Mode

PTP Clock Mode can be configured as either of the following modes:

- **1-step clock mode**: The PTP primary clock includes its timestamp in the synchronization message when the synchronization message is sent by the hardware. This mode requires hardware to insert the clock timestamp right before the synchronization message is sent through the wire.

- **2-step clock mode**: The PTP primary clock sends its timestamp in a separate message after sending the synchronization message. This mode does not require hardware support, but the timestamp messages and the synchronization messages may arrive at the PTP clients out of order in some scenarios.

Cisco cnBR and RPD support the 1-step clock mode. The PTP Clock mode is not configurable.

Configure PTP

This table lists the features, the releases in which each feature was introduced, and gives a small description of each feature.

Table 20: Feature History

Feature Name	Release Information	Feature Description
Support for redundant PTP primary clock for RPDs	Cisco cnBR 21.3	This feature adds support for a redundant PTP primary clock for the Cisco cnBR and RPDs. This additional primary clock improves redundancy.
Support for user configurable PTP intervals	Cisco cnBR 21.3	This feature allows you to configure the intervals at which the Cisco cnBR sends PTP Announce, Sync, and Delay_Req packets. This feature allows for granular control over PTP activity in the network.

Feature Name	Release Information	Feature Description
Support for DSCP marking for Cisco cnBR PTP packets	Cisco cnBR 21.3	This feature allows you to set the Differentiated Services Code Point for PTP packets. This feature enables you to set the priority for PTP packets in the network.

You can configure the PTP client in the Cisco cnBR and RPD during the initial Cisco cnBR configuration using autodeployer.

Step 1 The top-level autodeployer configuration file that you use in the deployment of Cisco cnBR must include the configuration for the PTP client in the Cisco cnBR.

The following table provides description of the PTP parameters, descriptions, and the required mandatory information.

Table 21: PTP Parameters, Descriptions, and Mandatory Information

Field Name	Description	Mandatory
ptp:v4:	PTP IPv4 related parameters for the Cisco cnBR PTP container	Yes
domain	Clock domain of the PTP primary server	Yes
master:ip	IPv4 address of the PTP clock primary server	Yes
master:gw	IPv4 address of the Gateway to access the PTP clock primary server.	Yes
alt-master:ip	IPv4 address of the PTP alternate primary clock server	No
alt-master:gw	IPv4 address of the gateway to access the PTP alternate primary clock server.	No
dscp	Differentiated services code point. Default: 46 (integer range: 0 ~ 63)	No
logAnncInterval	Interval for PTP announcement packets in log2 base; default: 1 (integer range: -3 to 5)	No
logDelayReqInterval	Interval for PTP delay-req packets in log2 base; default: -1 (integer range: -7 to 5)	No
logSyncInterval	Interval for PTP sync packets in log2 base; default: -1 (integer range: -7 to 5)	No

Field Name	Description	Mandatory
SG_template	See the SG template listed in step Step 2, on page 112	Yes

Step 2 The reference Service Group template must include the configuration of the PTP client in the RPD. Go through the following table for the detailed values.

Configuration values for the SG Template

Table 22: Configuration Values for the SG Template

Field Name	Description	Mandatory
rpdPtpCfg:	< PTP-related parameters for the PTP client in the RPD >	Yes
domain	Clock domain of the PTP primary server	Yes
dtiMode	DOCSIS Time Interface Mode	Yes
priority1	Priority1	No
priority2	Priority2	No
ptpClkProfileId	PTP clock profile ID in PTP primary server	Yes
ptpPortCfg: adminState	PTP port administration state	Yes
ptpPortCfg: anncReceiptTimeout	Announcement Receipt Timeout interval	No
ptpPortCfg: cos	COS of 802.1Q	No
ptpPortCfg: dscp	DSCP of IP Differentiated Services	No
ptpPortCfg: enetPortIndex	Ethernet port index for the clock port	No
ptpPortCfg: gateway	IPv4 address of the gateway to access the PTP primary clock server.	Yes
ptpPortCfg: gatewayAlt	IPv4 address of the Alt gateway to access the PTP primary clock server.	No
ptpPortCfg: masterAddr	IPv4 address of the PTP primary clock server	Yes
ptpPortCfg: masterAddrAlt	IPv4 address of the Alt PTP primary clock server	No
ptpPortCfg: localPriority	Local Priority	No

Field Name	Description	Mandatory
ptpPortCfg: logAnncInterval	Interval for PTP announcement packets in log2 base; Default: 0 (integer range: -3 ~ 0)	No
ptpPortCfg: logDelayReqInterval	Interval for PTP delay-req packets0-7(-7 -0)	Yes
ptpPortCfg: logSyncInterval	Interval for Sync packets	Yes
ptpPortCfg: masterAdminState	PTP Primary Administration State	Yes
ptpPortCfg: ptpPortIndex	PTP Port Index	Yes
ptpPortCfg: unicastDuration	The grant duration time in seconds for unicast	No

For more information on the listed parameters, go through the RPD documentation at
https://www.cisco.com/c/en/us/td/docs/cable/cbr/configuration/guide/b-rpd-full-book-11/b-rpd-full-book-11_chapter_011.pdf.

Example

- Cisco cnBR PTP client-related parameters in the autodeployer top-level configuration file:

```
// IPv4 address of PTP Primary Clock and alternate Primary clock servers,
// and their respective Gateway server, in the top level config file.
ptp :
    v4 :
        domain : 0
        master: {'ip':"10.158.158.158", 'gw':"10.70.78.1"}
        alt-master: {'ip':"10.150.158.159", 'gw':"10.7.78.77"}
        dscp: 46
        interval: {'announce': 1, 'delay-request': -1, 'sync': -1}

//Specify the "SG template" that contains the RPD PTP Client parameters.
    SG :
         'SG_4x4': 'sg_template.json'
```

Note

- PTP does not support IP dual stack. Please configure either IPv4 or IPv6.

- PTP primary IP must come with a PTP primary IP gateway. PTP alternate primary IP must come with a PTP alternate primary IP gateway.

- The DSCP value must be same as that in the DSCP config on the ptp primary.

- The interval value must follow the max interval restriction on the ptp primary.

- If you do not configure the DSCP and interval parameters, the Cisco cnBR applies the following default values.

    ```
    dscp: 46
    interval: {'announce': 1, 'delay-request': -1, 'sync': -1}
    ```

- RPD PTP client-related parameters in the SG_template:

```
"rpdPtpCfg": {
    "dtiMode": "SlaveDtiMode",
    "domain": 44,
    "priority1": 128,
    "priority2": 255,
    "ptpClkProfileId": "00:00:00:00:00:00",
    "ptpPortCfg": [
      {
        "adminState": "Up",
        "anncReceiptTimeout": 11,
        "cos": 6,
        "dscp": 47,
        "enetPortIndex": 1,
        "gateway": "10.70.78.1",
        "gatewayAlt": "10.7.78.77",
        "localPriority": 128,
        "logDelayReqInterval": -4,
        "logSyncInterval": -4,
        "masterAddr": "10.158.158.158",
        "masterAddrAlt": "10.150.158.23",
        "masterAdminState": "Up",
        "ptpPortIndex": 22,
        "unicastDuration": 300
      }
    ]
  }
```

Update cnBR PTP Configuration using Autodeployer

You can update the Cisco cnBR PTP configuration using the Autodeployer.

Ensure that you have configured the Cisco cnBR PTP client during deployment, and the Cisco cnBR using the Autodeployer.

See Configure Cisco cnBR Using Autodeployer, on page 43 for more information.

Go through the following steps to update the PTP configuration:

Step 1 Locate the Autodeplyer configuration files used for the initial deployment and configuration of cnBR. This includes:

- Top-level Autodeployer configuration file

- SG template

- L3 template

Step 2 Update the `PTP` section of the top-level Autodeployer configuration file.

Step 3 Run the Autodeployer configuration script.

Note All RPDs or SGs (including unchanged SGs), are first deleted and added when you rerun the Autodeployer configuration.

Update cnBR PTP Configuration using cnBR Manager

You can update the Cisco cnBR PTP configuration using the cnBR Manager.

Ensure that you have configured the Cisco cnBR PTP client during deployment and the Cisco cnBR using the Autodeployer. Also, ensure that the Cisco cnBR is added to the cnBR Manager.

To view and update the PTP configuration parameters, use the following procedure:

Step 1 On the Cisco Operations Hub, click the Cisco Operations Hub main menu button.

Step 2 Choose **cnBR Manager** > **cnBRs** to open the **cnBR Clusters** page.

Step 3 Click the name of the Cisco cnBR to open the **cnBR Cluster Configuration** page.

Step 4 Choose PTP from the drop-down list and edit the configuration using one of the following modes:

- Tree mode: Select **Tree** mode to edit each field.

- Code mode: Select **Code** mode to edit the configuration in plain text.

Step 5 Configure the Cisco cnBR PTP client with either a single primary clock or with dual primary clocks.

The following image shows the Cisco cnBR PTP client with a single primary clock.

Figure 16: Configuring cnBR PTP Client with a Single Primary Clock

cnBR Cluster Configuration

172.22.127.208.nip.io

PTP

Select a node...
▼ Config {3}
    PtpDomain : 0
    PtpGwIp : 10.40.13.3
    PtpMasterIp : 100.158.158.158

SAVE

Configuration Example —

PTP Configuration Example

```
// Ipv4 config:
{
    "PtpDomain" : 55,
    "PtpGwIp" : "4.4.4.5",
```

The following image shows the Cisco cnBR PTP client with dual primary clock.

Figure 17: Configuring cnBR PTP Client with a Dual Primary Clock

cnBR Cluster Configuration

172.25.29.123.nip.io

PTP

Select a node...
▼ Config {5}
    PtpDomain : 44
    PtpGwIp : 5.230.211.1
    PtpGwIpAlt : 5.230.211.1
    PtpMasterIp : 5.10.2.253
    PtpMasterIpAlt : 5.10.2.249

SAVE

Configuration Example —

PTP Configuration Example

```
// Ipv4 config:
{
    "PtpDomain" : 55,
    "PtpGwIp" : "4.4.4.5",
```

Update RPD PTP Configuration using Autodeployer

You can update the RPD PTP configuration using the Autodeployer. We recommend this method of updating the RPD PTP.

Ensure that you have configured the RPD PTP client during the deployment, and have configured Cisco cnBR using the Autodeployer.

See Configure Cisco cnBR Using Autodeployer, on page 43 for more information.

Step 1 Locate the complete set of Autodeplyer configuration files used in the initial deployment and configuration of cnBR. This includes:

- Top-level Autodeployer configuration file

- SG template

- L3 template

Step 2 Update the `rpdPtpCfg` section of the Service Group template.

Step 3 Run the Autodeployer configuration script.

> **Note** Rerunning the Autodeployer configuration causes all the RPDs or SGs, including unchanged SGs, to be first deleted and added.

Update RPD PTP Configuration using cnBR Manager

You can update the RPD PTP configuration using the cnBR Manager.

Ensure that you have configured the RPD PTP client during deployment, and have configured Cisco cnBR using the Autodeployer.

To view and update the RPD PTP configuration parameters, use the following procedure:

Step 1 On the Cisco Operations Hub, click the Cisco Operations Hub main menu button.

Step 2 Choose **cnBR Manager** > **cnBRs** to open the **cnBR Clusters** page.

Step 3 Click **Import & Export cnBR** to open the **Export/Import** page.

Step 4 On the **Export cnBR Configuration** pane, choose the Cisco cnBR that you want to update.

Step 5 Click **Export** to retrieve the current SG configuration of the selected Cisco cnBR.

Step 6 In the `<filename>-configuration.txt` file, update the parameters in the `rpdPtpCfg` section of the SG configuration.

Step 7 Save the updated file to the local disk.

Step 8 Update the SG configuration.

   a) In the **Import cnBR Configuration File** pane, choose the file that you updated.
   b) Click **Import** to update the SG configuration to the RPD.

Step 9 Delete the RPD and add the RPD again for the updated SG configuration to take effect.

Monitor and Troubleshoot PTP

You can view the PTP status and its details on the PTP dashboard.

To view the PTP dashboard, use the following procedure:

Step 1 Enter the Cisco Operations Hub URL `https://{Hostname}` in the web browser.

Step 2 On the Cisco Operations Hub, click the Cisco Operations Hub main menu button.

Step 3 Choose **Dashboard** to open the **Dashboard** page.

Step 4 Click **Find a Dashboard** to open the search pane.

Step 5 Enter **PTP** in the **Search dashboards by name** field and click the **PTP** row.

The PTP dashboard appears.

Figure 18: PTP Dashboard
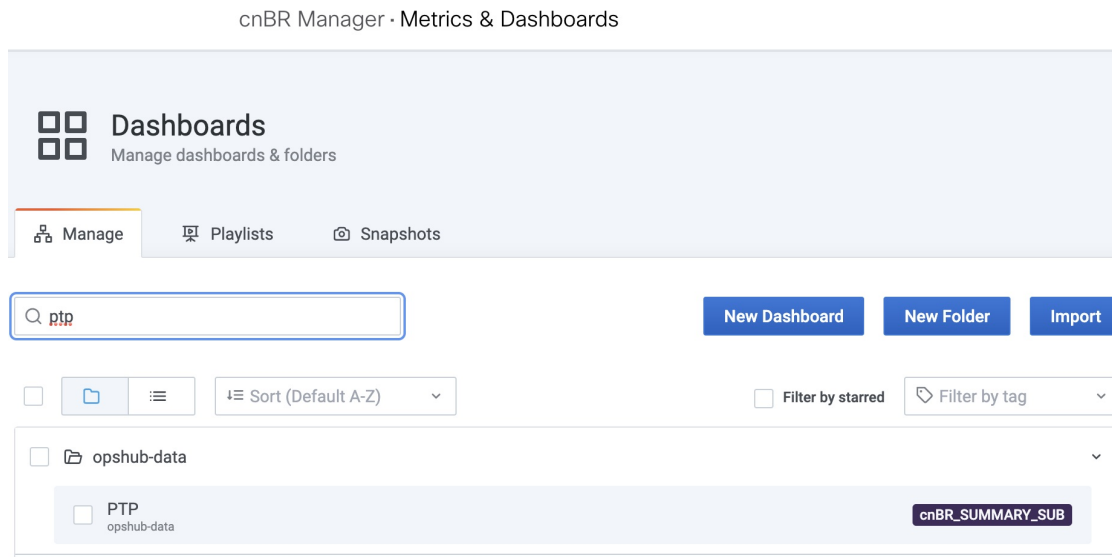
Note The `OffsetFromMaster` must be within [-1ms, 1ms].

BGP Agent

The BGP Agent is a service in Cisco cnBR. It sets up BGP sessions with the SP router and installs or withdraws subscribed routes on the SP router while the subscribed devices (e.g. CM/CPE) are online.

The Cisco cnBR BGP Agent supports BGP version 4, includes address family IPv4 unicast, address family IPv6 unicast, and supports Graceful Restart, on page 120.

Configure BGP Agent

You can perform the BGP Agent initial configurations through the Autodeployer Config file. See Configure Cisco cnBR Using Autodeployer, on page 43 for additional information.

After the initial setup, you can access BGP Agent configuration through the cnBR Manager. See instructions for Access BGP Agent Configuration, on page 120.
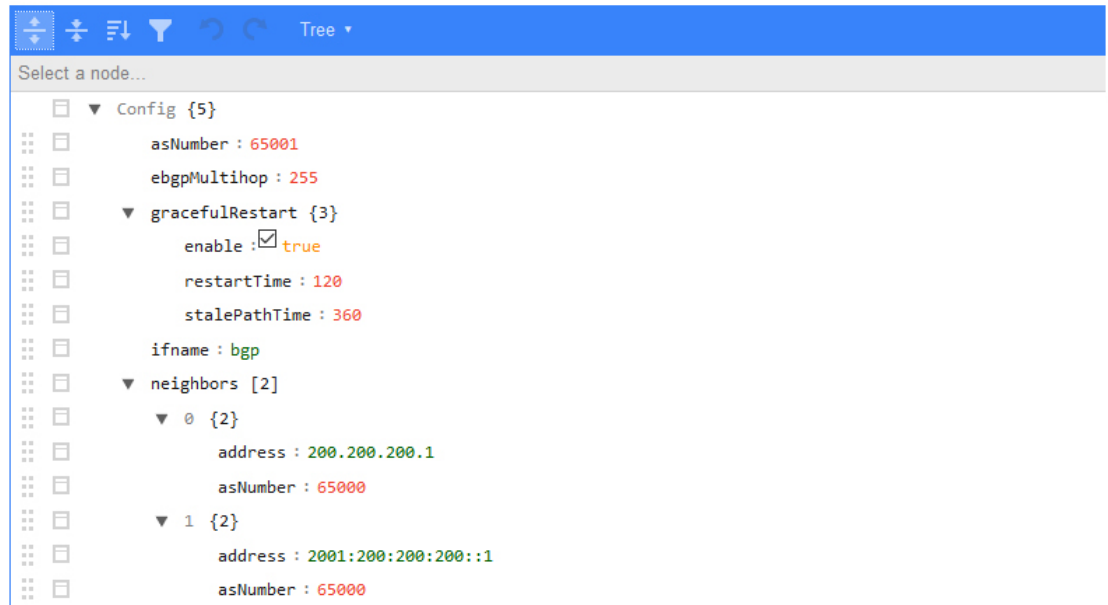
520757

Configuration Parameters

The table displays the BGP configuration parameters, their description, type and enforcement information

Field Name	Description	Type	Enforcement
asNumber	BGP supports 2-byte AS numbers	1 ~ 65535	Required
ebgpMultihop	The maximum number of eBGP hops allowed	0 ~ 255	Required
ifname	BGP Agent interface name	String, length 1 ~ 255	Required
neighbors	BGP peer; BGP uses TCP port 179 to create a TCP session with a peer		Required
weight	Weight of BGP peers; if you configure two BGP IPv4/IPv6 peers, the upstream routes sent from these peers are accepted in the order of weight. Default: 100	Unsigned integer	Optional
address	BGP peer IP/IPv6 address	String	Required
gateway	The gateway IP address if the BGP messages are transmitted to loopback interface on the SP router	String	Optional
gracefulRestart	BGP graceful restart parameters		Required
enable	True, to enable the graceful restart BGP option and False, to disable it	Bool	Required
restartTime	Determines how long the peer routers wait to delete stale routes before a BGP open message is received	1 ~ 3600 seconds	Required
stalePathTime	Determines how long a router waits before deleting stale routes after receiving an end of record (EOR) message from the restarting router	1 ~ 3600 seconds	Required

Graceful Restart

When a BGP router restarts, all its neighbors detect that the BGP router went down and has come up again. It results in the deletion and adding back of the BGP routes in the neighbors. The unnecessary recomputation of routes, called a "routing flap", causes issues on both the BGP and neighbor routers. Graceful Restart allows the system to preserve the routes during BGP restart, thus minimizing the negative effects of BGP restart.

BGP Agent Configuration

The Cisco cnBR BGP Agent allows easy modification of BGP Agent global configurations.

Access BGP Agent Configuration

Step 1   Log in to Cisco Operations Hub.

Step 2   On the Cisco Operations Hub, click the Cisco Operations Hub main menu button.

Step 3   Choose **cnBR Manager** > **cnBRs** to open the **cnBR Clusters** page.

Step 4   Click the name of the target Cisco cnBR to open the **cnBR Cluster Configuration** page.

Step 5   Choose **BGP Agent** from the drop-down list.

The BGP Agent configuration details appear.

Add BGP Neighbors

Step 1   In the BGP Agent configurator, expand `neighbors` field, and click the edit box of the last element.

Step 2   From the drop-down list, expand **Append** and select **Object**.

Step 3   In the new object, click the edit box of the `(empty object)` field.

Step 4   Choose **Append** from the drop-down list to create an object with two fields.

Step 5   In the first field, enter `address`, and in the second field, enter the IP address of the new neighbor.

Step 6   Click the edit box of the `Address` field and choose **Append** from the drop-down list to create an object with two fields.

Step 7   In the first field, enter `asNumber` and in the second field, enter the AS number of the new neighbor.

Step 8   Click **Save**.

Delete BGP Neighbors

Step 1   In the BGP Agent configuration, expand all neighbor objects to locate the neighbor to delete.

Step 2   Select the edit box of the neighbor object to delete, then select **Remove**.

Step 3   Click **Save**.

Get BGP Neighbors

BGP neighbor information is stored in the `neighbors` field in the BGP configurator.

cnBR Cluster Configuration

172.25.29.110.nip.io

BGP Agent

Tree ▼

object ► neighbors ► 1 ►

▼ Config {5}
    asNumber : 65009
    ebgpMultihop : 255
   ► gracefulRestart {3}
    ifname : bgp
  ▼ neighbors [2]
    ▼ 0 {2}
       address : 200.200.10.1
       asNumber : 65534
    ▼ 1 {2}
       address : 2001:200:200:a::1
       asNumber : 65534

SAVE
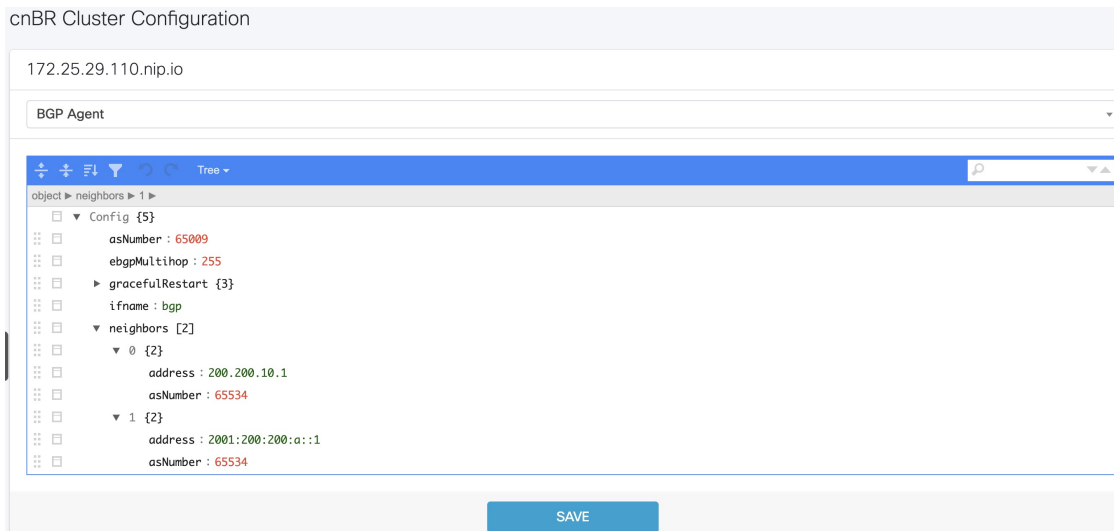
BGP Agent Dashboard

The Cisco cnBR BGP Agent Dashboard provides visibility into the BGP IPv4 and IPv6 routes and operation.

Access BGP Agent Dashboard

Step 1   Log in to the Cisco Operations Hub.

Step 2   On the Cisco Operations Hub, click the Cisco Operations Hub main menu button.

Step 3   Choose **Dashboard** to open the **Dashboard** page.

Step 4   Click **Find a Dashboard** to open the search pane.

Step 5   Enter **bgp** in the **Search dashboards by name** field and click the **BGP Agent** row.

Step 6   Choose the desired Cisco cnBR from the **cnBR Name** drop-down list.

The BGP Agent Dashboard of the desired Cisco cnBR appears.

WAN Route Table

WAN Route Table displays the default routes generated by BGP Agent, and BGP routes received by the SP Router.

The table dispalys the WAN Route Table parameters and their descriptions

Table 23: Parameters

Name	Description
Neighbor	Neighbor IP address
Prefix	Network segment of route

Name	Description
Nexthop	IP address of next hop to get to destination
Weight	Weight parameter described in Configuration Parameters, on page 119

SP Router State Table

SP Router State Table displays the connection state between the BGP Agent and the SP router. The UP state indicates that the connection is established, and the DOWN state indicates the connection is not established.

SP Router State Table		
Index ▲	SP Router	State
1	2001:200:200:200::1	UP

520765

SP Router State Table		
Index ▲	SP Router	State
1	200.200.200.1	UP

520766

The following table dispalys the SP Router State parameters and their descriptions

Table 24: Parameters

Name	Description
SP Router	The IP address of the SP Router
State	State of the connection between BGP Agent and SP Router

BGP Route Table

BGP Route Table displays the BGP routes that is sent to the SP router to route packets from CM to the correct DP.

Figure 19: BGP v4 Route Table

Figure 20: BGP v6 Route Table

The following table lists the parameters with regard to the BGP Route Table

Table 25: Parameters

Name	Description
SG Name	Service Group name corresponding to the route
SG ID	Service Group ID corresponding to the route
IP Route	Destination IP address
NextHop	Next IP address hop to get to destination

BGP Route Number

BGP Route Number displays the number of BGP routes installed into the SP router over time.

Figure 21: BGP v4 Route Number
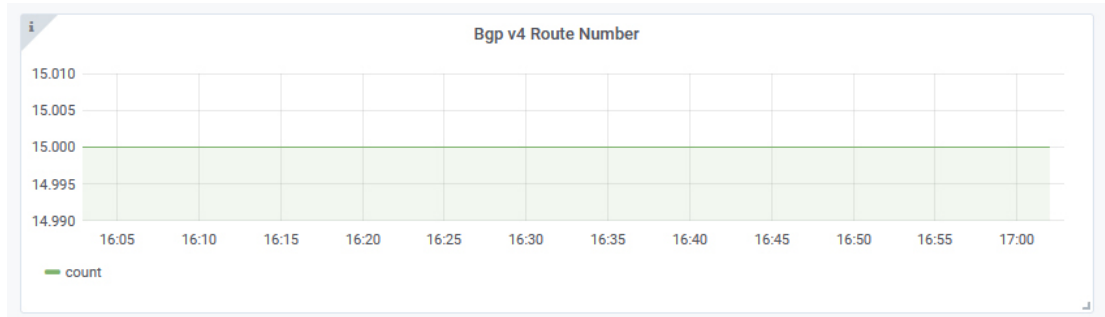
Figure 22: BGP v6 Route Number
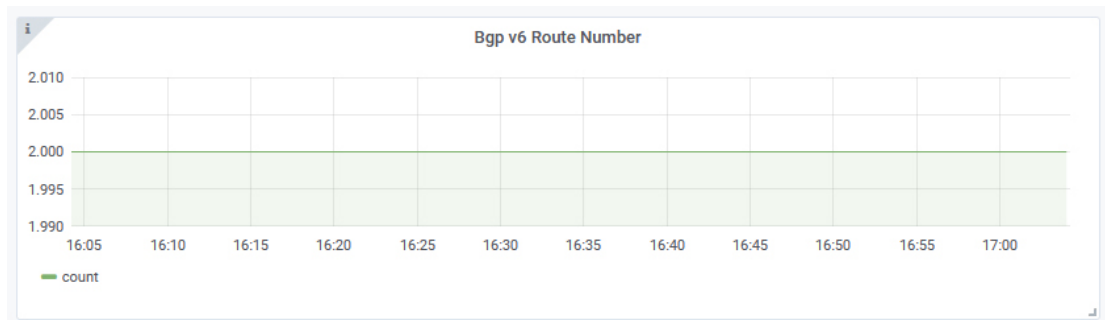
• X-axis: Time

• Y-axis: Number of BGP routes

BGP Route Rate

BGP Route Rate displays the rate of change of BGP routes over time.

Figure 23: BGP v4 Route Rate
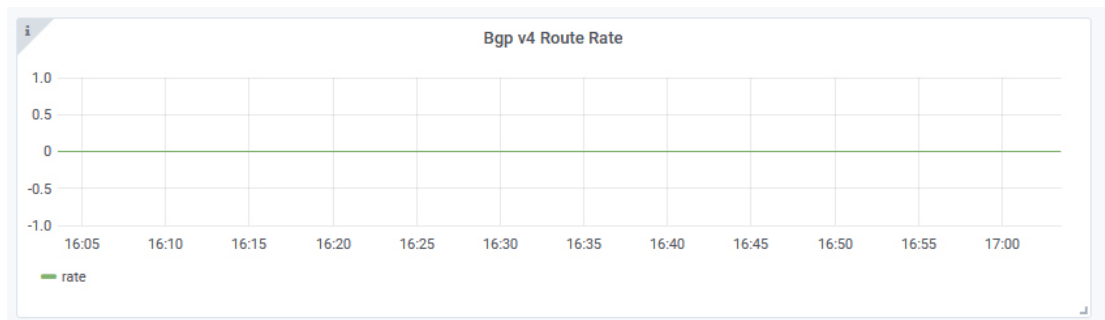
Figure 24: BGP v6 Route Rate
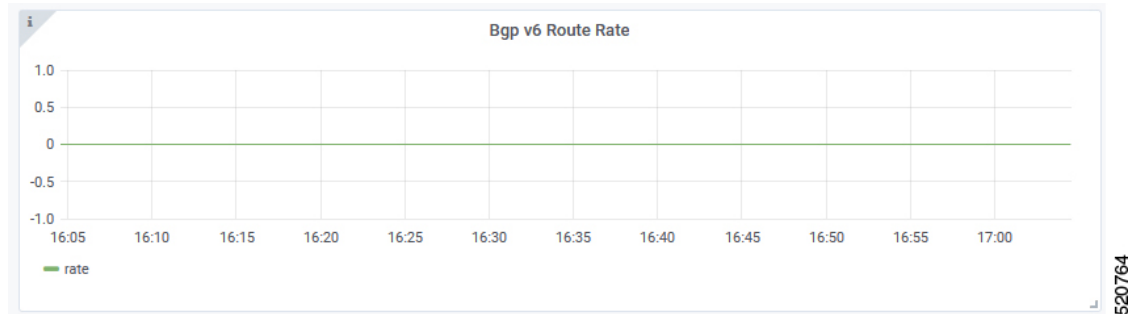
- X-axis: Time

- Y-axis: Change rate of BGP routes

L2VPN

The Cisco cnBR application emulates the Layer 2 virtual private network (L2VPN), when L2VPN devices across shared or public networks appear as computing devices that are directly connected to a switch device. Therefore, Layer 2 packets from one device can reach the other device without changes to the Layer 2 packet header, similar to the traditional Layer 2 Forwarding method.

Several tunneling protocols are used to implement L2VPN. Cisco cnBR supports the point-to-point mode L2VPN for the IEEE 802.1Q (dot1q) protocol.

For the dot1q L2VPN, Cisco cnBR adds one layer dot1q tag for the upstream packet and removes the tag at the receiving end.

Cisco cnBR supports both cable modem (CM) based L2VPN and service flow (SF) based L2VPN.

- CM-based L2VPN: One CM can configure one L2VPN service. Primary upstream and primary downstream packets are encapsulated into a L2VPN tunnel.

- Service flow-based L2VPN: One CM can configure up to four L2VPN services using the CM configure file TLV. A maximum of eight upstream SFs and eight downstream SFs are supported for each L2VPN service. The upstream classifier on the CM and downstream classifier on the Cisco cnBR router are used to classify different packets into L2VPN service flows.

Cisco cnBR supports the following types of L2VPN tunnel:

The table lists the L2VPN tunnels types and their detailed information

Tunnel Type	CM-based	SF-based
dot1q	- dot1q tunnel - Configure by Rest API - One L2VPN per CM	- dot1q tunnel - Configured by CM configuration file TLV - Up to 4 L2VPN per CM

Configure L2VPN

The dot1q L2VPN is implemented using the Cisco cnBR router with a Service Provider (SP) router.

SP routers are Cisco ASR 9000, Cisco ASR 1000, or Cisco Network Convergence System 5501.

The connection between the Cisco cnBR router and the SP router is supported by either the VxLAN mode or the VLAN mode.

VxLAN Mode

The following image shows the dot1q L2VPN packet flow from CPE to the dot1q tunnel.

Figure 25: dot1q L2VPN packet flow from CPE to the dot1q tunnel
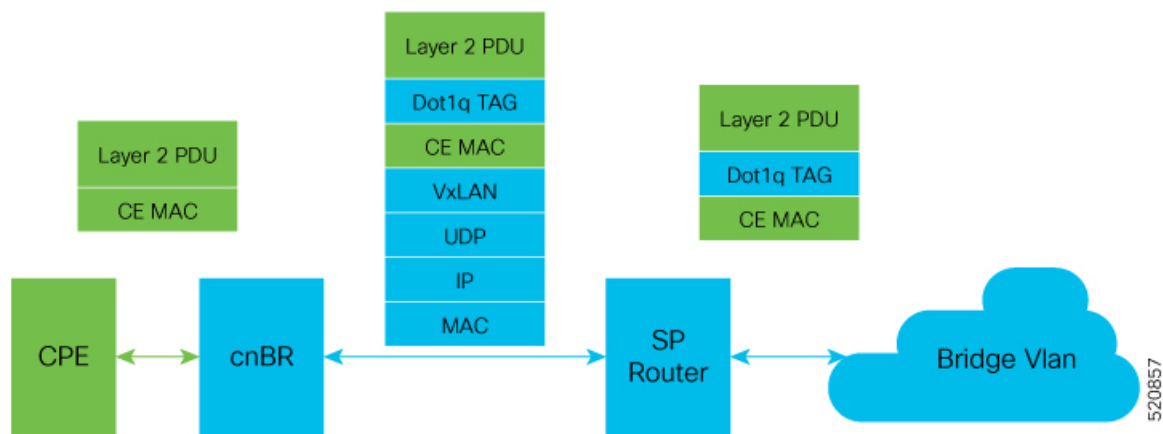
The following table summarizes the configuration that is required for the supported L2VPN types:

Supported L2VPN types and their required configuration

Tunnel Type	CM-based	SF-based
dot1q	• Cisco cnBR configuration: static dot1q L2VPN • Cisco cnBR configuration: dot1q VxLAN wiring • SP router configuration: dot1q VxLAN wiring	• CM configure file: dot1q L2VPN related TLV • Cisco cnBR configuration: dot1q VxLAN wiring • SP router configuration: dot1q VxLAN wiring

VLAN Mode

The following image shows the dot1q L2VPN packet flow from CPE to the dot1q tunnel.

Figure 26: dot1q L2VPN packet flow from CPE to the dot1q tunnel
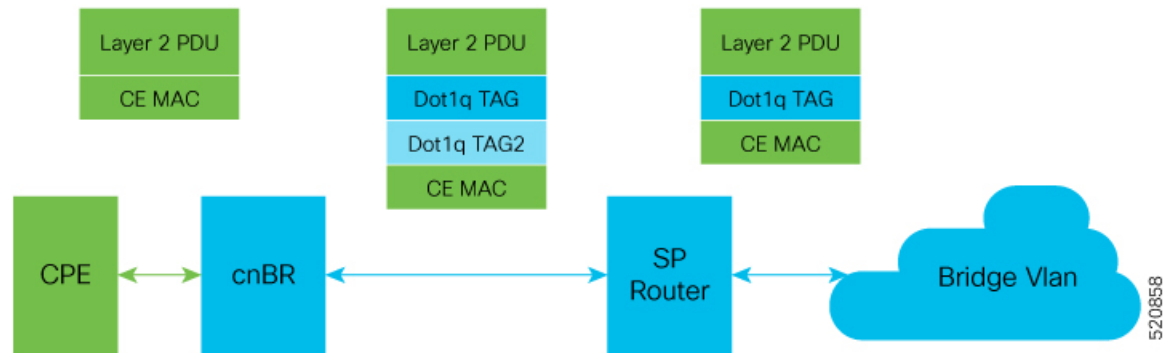
The following table summarizes the configuration that is required for the supported L2VPN types:

The table lists the supported L2VPN types and their required configuration information

Tunnel Type	CM-based	SF-based
dot1q	• Cisco cnBR configuration: static dot1q L2VPN • Cisco cnBR configuration: dot1q VxLan wiring • SP router configuration: dot1q VxLan wiring	• CM configure file: dot1q L2VPN related TLV • Cisco cnBR configuration: dot1q VxLan wiring • SP router configuration: dot1q VxLan wiring

Cisco cnBR L2VPN Configuration

For both CM-based and SF-based L2VPN, configure the L2VPN related VLAN or VxLAN that connects to the SP router. Use the **cnBR Cluster Configuration** window to configure the wiring.

For CM-based L2VPN, configure the static L2VPN map by using the REST API.

Step 1 On the Cisco Operations Hub, click the Cisco Operations Hub main menu button.

Step 2 Choose **cnBR Manager** > **cnBRs** to open the **cnBR Clusters** page.

Step 3 Click the name of the target Cisco cnBR cluster to open the **cnBR Cluster Configuration** page.

Step 4 Select **Wiring** from the drop-down list.

Step 5 Update the configuration as required and click **SAVE**.

Static Dot1q L2VPN

To configure a cable modem (CM) as dot1q CM-based L2VPN, upstream traffic (primary service flow) adds one-level dot1q tag. Each L2VPN must have a different `VLanId`.

Step 1 On the Cisco Operations Hub, click the Cisco Operations Hub main menu button.

Step 2   Choose **cnBR Manager** > **cnBRs** to open the **cnBR Clusters** page.

Step 3   Click the name of the target Cisco cnBR cluster to open the **cnBR Cluster Configuration** page.

Step 4   Choose **Layer 2 VPN** from the drop-down list.

Step 5   Update the configuration as required and click **SAVE**.

CM Configuration File TLV Definition

SF-based L2VPN depends on the CM configuration file TLV to set up L2VPN service, L2VPN service flow, and L2VPN classifier. For more details, see the CableLabs document: *Business Services over DOCSIS Layer 2 Virtual Private Networks*.

L3VPN

Layer 3 VPN (L3VPN) in Cisco cnBR is based on Multiprotocol Label Switching (MPLS) network. Cisco cnBR is at the Customer Edge (CE) and the service provider router is at the provider edge (PE), as shown in the following diagram.
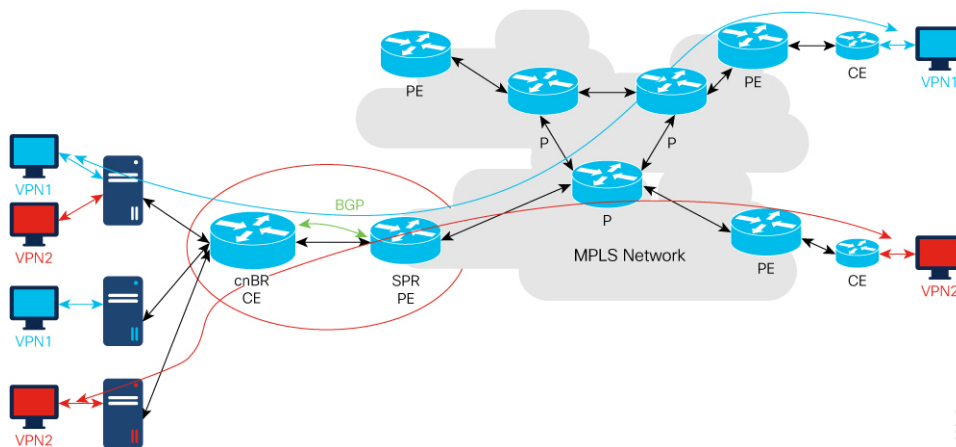
Cisco cnBR uses Border Gateway Protocol (BGP) to advertise Virtual Routing and Forwarding (VRF) (and global) routes and MPLS network uses MPLS to forward VPN packets on service provider backbones.

Figure 27: Cisco cnBR L3VPN Architecture

With L3VPN service, the system (Cisco cnBR and MPLS network) can enable cable mode (CM) or customer premises equipment (CPE) connect to host in the same VPN, and isolate CM/CPE from other VPN.

Configure L3VPN

To set up L3VPN, configure the following:

- L3VPN global configuration
- DHCP

Configure L3VPN Globally

In the initial-configuration YAML file (`day1.yaml`), under l3vpn section, add two entries for voice and video. Following is a sample configuration:

```
l3vpn:
          - {"name" : "voice", "vlan" : 1050, "vpnRd" : "65000:1050"}
          - {"name" : "video", "vlan" : 1051, "vpnRd" : "65000:1051"}
```

Configure L3VPN from Cisco Operations Hub

Use the following procedure to configure L3VPN globally through Cisco Operations Hub:

Step 1 Log in to Cisco Operations Hub.

Step 2 Click the Cisco Operations Hub main menu button on the top-left corner, choose **cnBR Manager** > **cnBRs**, and click **Inventory**.

Step 3 Choose the required Cisco cnBR core from the list.

Step 4 Choose the required cnBR, click **Edit** and click the **Advanced** tab.

Step 5 Choose **L3 VPN** from the drop-down list under **Wiring**.

You can see the L3VPN configuration details.

```
{
        "vrfList": [
        {
            "name": "voice",
            "vlan": 1050,
            "vpnRd": "65000:1050"
        },
        {
            "name": "video",
            "vlan": 1051,
            "vpnRd": "65000:1051"
        }
    }
```

Configure SG DHCP in L3 Template

DHCP configuration depends on service groups (SG). Different SGs can have different VPN configurations. The following example shows the initial DHCP configuration of one SG.

For each SG, VPNs are configured under `vrfList`, whose name maps to L3VPN global configuration.

Relay policies are supported at the device type level.

```
{
        "dhcp": {
        "arpGlean": true,
        "arpProxy": true,
        "dhcpIfname": "cnr",
        "dhcpServers": [
            "10.70.70.12",
            "2001:10:70:70::12"
        ],
        "ipv6Lq": true,
        "mobilityScopes": [
```

```
                    "1.1.1.1/24",
                ],
                "ndProxy": true,
                "v4Nets": [
                    "91.91.91.1/24"
                ],
                "v6Nets": [
                    "2001:91:91:91::1/64"
                ],
                "vrfList": [
                    {
                    "dhcpServers":["10.70.70.12","2001:10:70:70::12"],
                    "name":"voice",

"relayPolicies":[{"deviceClass":"HOST","giAddr":"93.93.93.1","linkAddr":"2001:93:93:93::1"}]

                    "v4Nets":["92.92.92.1/24","93.93.93.1/24"],
                    "v6Nets":["2001:92:92:92::1/64","2001:93:93:93::1/64"]
                    },
                    {
                    "dhcpServers":["10.70.70.12","2001:10:70:70::12"],
                    "name":"video",
                    "v4Nets":["94.94.94.1/24"],
                    "v6Nets":["2001:94:94:94::1/64"]
                    }
                ],
                "savList": {
                "prefixes": null
                },
                "sgPeerIpv4": "201.201.201.1/24",
                "sgPeerIpv6": "2001:201:201:201::1/64"
            }
```

In this example, cable modems (CM) in the VPN voice get the 92.92.92.x address and the CPEs get 93.93.93.x address.

Configure SG DHCP in L3 Template from Cisco Operations Hub

Add the L3VPN configuration in the L3 template. Use the following sample configuration:

```
{
                "dhcp": {
                "arpGlean": true,
                "arpProxy": true,
                "dhcpIfname": "cnr",
                "dhcpServers": [
                    "10.70.70.12",
                    "2001:10:70:70::12"
                ],
                "ipv6Lq": true,
                "mobilityScopes": [
                    "1.1.1.1/24",
                ],
                "ndProxy": true,
                "v4Nets": [
                    "91.91.91.1/24"
                ],
                "v6Nets": [
                    "2001:91:91:91::1/64"
                ],
                "vrfList": [
                    {
                    "dhcpServers":["10.70.70.12","2001:10:70:70::12"],
                    "name":"voice",
```

```
"relayPolicies":[{"deviceClass":"HOST","giAddr":"93.93.93.1","linkAddr":"2001:93:93:93::1"}]

            "v4Nets":["92.92.92.1/24","93.93.93.1/24"],
            "v6Nets":["2001:92:92:92::1/64","2001:93:93:93::1/64"]
            },
            {
            "dhcpServers":["10.70.70.12","2001:10:70:70::12"],
            "name":"video",
            "v4Nets":["94.94.94.1/24"],
            "v6Nets":["2001:94:94:94::1/64"]
            }
        ],
        "savList": {
        "prefixes": null
        },
        "sgPeerIpv4": "201.201.201.1/24",
        "sgPeerIpv6": "2001:201:201:201::1/64"
    }
```

Configure BGP Agent for L3VPN

In the initial-configuration YAML file (`day1.yaml`), add the BGP agent configration. Following is a sample configuration:

```yaml
yaml
bgpagent :
    asn : 65002
    max_hops : 255
    # to set bgpagent work at loopback mode, uncomment below 2 lines and set IP address for
 them
    # loaddr : ['1.1.1.1', '1.1.1.2']
    # loaddrv6 : ['2001:1:1:1::1', '2001:1:1:1::2']
    restart-time : 120
    stale-path-time: 360
    neighbors :
      - {'address' :'201.201.201.1', 'asn':65000}
```

Configure BGP Agent from Cisco Operations Hub

Use the following procedure to configure BGP Agent through Cisco Operations Hub:

SUMMARY STEPS

1. Log in to Cisco Operations Hub.
2. Click the Cisco Operations Hub main menu button on the top-left corner, choose **cnBR Manager** > **cnBRs**, and click **Inventory**.
3. Choose the required Cisco cnBR core from the list.
4. Choose the required cnBR, click **Edit** and click the **Advanced** tab.
5. Choose **BGP Agent** from the drop-down list under **Wiring**.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Log in to Cisco Operations Hub.	

	Command or Action	Purpose
Step 2	Click the Cisco Operations Hub main menu button on the top-left corner, choose **cnBR Manager** > **cnBRs**, and click **Inventory**.	
Step 3	Choose the required Cisco cnBR core from the list.	
Step 4	Choose the required cnBR, click **Edit** and click the **Advanced** tab.	
Step 5	Choose **BGP Agent** from the drop-down list under **Wiring**.	You can see the BGP Agent configuration details.

```json
{
  "asNumber": 65002,
  "ebgpMultihop": 1,
  "gracefulRestart": {
    "enable": true,
    "restartTime": 120,
    "stalePathTime": 360
  },
  "ifname": "bgp",
  "loaddr": null,
  "loaddrv6": null,
  "neighbors": [
    {
      "address": "201.201.201.1",
      "asNumber": 65000,
      "weight": 100
    },
    {
      "address": "201.201.201.250",
      "asNumber": 65000,
      "weight": 100
    }
  ]
}
```

Example of Service Provider Configuration

Example for NCS-55A1

VRF definition

```
vrf video
 rd 65000:1051
 address-family ipv4 unicast
  import route-target
   65000:1051
  !
  export route-target
   65000:1051
  !
 !
 address-family ipv6 unicast
  import route-target
   65000:1051
  !
  export route-target
   65000:1051
  !
```

```
 !
!
vrf voice
 rd 65000:1050
 address-family ipv4 unicast
  import route-target
   65000:1050
  !
  export route-target
   65000:1050
  !
 !
 address-family ipv6 unicast
  import route-target
   65000:1050
  !
  export route-target
   65000:1050
  !
 !
!
```

WAN Sub-interface for Each VRF

```
interface FortyGigE0/0/0/5.1050
 vrf voice
 ipv4 address 201.201.201.1 255.255.255.0
 ipv6 nd prefix default no-adv
 ipv6 nd suppress-ra
 ipv6 address 2001:201:201:201::1/64
 encapsulation dot1q 1000 second-dot1q 1050
!
interface FortyGigE0/0/0/5.1051
 vrf video
 ipv4 address 201.201.201.1 255.255.255.0
 ipv6 nd prefix default no-adv
 ipv6 nd suppress-ra
 ipv6 address 2001:201:201:201::1/64
 encapsulation dot1q 1000 second-dot1q 1051
!
```

BGP Configuration

```
router bgp 65000
 bgp router-id 1.1.1.1
 address-family ipv4 unicast
 !
 address-family vpnv4 unicast
 !
 address-family ipv6 unicast
 !
 address-family vpnv6 unicast
 !
 neighbor 201.201.201.198
  remote-as 65002
  bfd fast-detect
  bfd multiplier 3
  bfd minimum-interval 100
  address-family ipv4 unicast
   route-policy pass-all in
   route-policy pass-all out
  !
```

```
   address-family ipv6 unicast
    route-policy pass-all in
    route-policy pass-all out
   !
  !
  neighbor 201.201.201.199
   remote-as 65002
   bfd fast-detect
   bfd multiplier 3
   bfd minimum-interval 100
   address-family ipv4 unicast
    route-policy pass-all in
    route-policy pass-all out
   !
   address-family ipv6 unicast
    route-policy pass-all in
    route-policy pass-all out
   !
  !
  vrf video
   address-family ipv4 unicast
    label mode per-vrf
   !
   address-family ipv6 unicast
    label mode per-vrf
   !
   neighbor 201.201.201.198
    remote-as 65002
    address-family ipv4 unicast
     route-policy pass-all in
     route-policy pass-all out
    !
    address-family ipv6 unicast
     route-policy pass-all in
     route-policy pass-all out
    !
   !
   neighbor 201.201.201.199
    remote-as 65002
    address-family ipv4 unicast
     route-policy pass-all in
     route-policy pass-all out
    !
    address-family ipv6 unicast
     route-policy pass-all in
     route-policy pass-all out
    !
   !
  !
  vrf voice
   address-family ipv4 unicast
    label mode per-vrf
   !
   address-family ipv6 unicast
    label mode per-vrf
   !
   neighbor 201.201.201.198
    remote-as 65002
    address-family ipv4 unicast
     route-policy pass-all in
     route-policy pass-all out
    !
    address-family ipv6 unicast
     route-policy pass-all in
```

```
   route-policy pass-all out
  !
 !
 neighbor 201.201.201.199
  remote-as 65002
  address-family ipv4 unicast
   route-policy pass-all in
   route-policy pass-all out
  !
  address-family ipv6 unicast
   route-policy pass-all in
   route-policy pass-all out
  !
 !
!
```

IPv6

The following table provides description of the various features and their release information

Feature Name	Release	Feature Description
IPv6 WAN Protocols	Cisco cnBR 21.1	Allows you to use WAN protocols over IPv6. The WAN protocols consist of IPv6 BGP Agent, IPv6 DHCP Relay Agent and Proxy, and IPv6 DMIC.

Cisco cnBR supports IPv6 protocol when communicating with the following network devices:

- Cable Modem (CM)

- Customer Premise Equipment (CPE)-Equipment that is connected to the CM at the customer premise.

Note   Cisco cnBR supports dual-stack IPv4 and IPv6 protocols (It supports both IPv4 and IPv6 addresses at the same time).

Cisco cnBR supports WAN protocols over IPv6, along with CIN protocols. The WAN protocols consist of IPv6 BGP Agent, IPv6 DHCP Relay Agent and Proxy, and IPv6 DMIC. In the current network topology, both CIN and WAN networks are connected to the SP router through a layer 2 switch.

Configure IPv6 WAN

Configure Service Provider router BGP WAN, which includes BGP routing display, Wiring configuration, layer 3 (L3) configuration, SG template configuration, and DMIC configuration.

Following are a few sample configurations, which may be different for each vendor router. The current topology must have a Layer 2 switch between the SP router and Cisco cnBR.

Configure BGP WAN

```
interface Bundle-Ether1.1001
 description WAN-for-cnbr-mn
```

```
 mtu 9216
 ipv4 address 200.200.9.1 255.255.255.0
 ipv4 address 100.100.9.1 255.255.255.0 secondary
 ipv6 address 2001:100:100::9:1/112
 ipv6 address 2001:200:200::9:1/112
 encapsulation dot1q 1001
!
router bgp 65534
 bgp router-id <rtr-id>
 address-family ipv6 unicast
  aggregate-address fd26:ba99:aae:944::/64 summary-only
  aggregate-address fd26:ba99:aae:2244::/96 summary-only
  aggregate-address fd26:ba99:aae:2344::/96 summary-only
  aggregate-address fd26:ba99:aae:2444::/64 summary-only
  redistribute connected
  redistribute static
 !
 neighbor-group ibgp
  remote-as 65534
  update-source Loopback0
  address-family ipv6 unicast
   route-policy pass-all in
   route-policy pass-all out
  !
 neighbor 2001:200:200::9:2
  remote-as 65009
  ebgp-multihop 255
  description "For cnbr-mn eBGP"
  address-family ipv6 unicast
   route-policy pass-all in
   route-policy pass-all out
  !
 !
 neighbor 2001:200:200::9:3
  remote-as 65009
  ebgp-multihop 255
  description "For cnbr-mn eBGP"
  address-family ipv6 unicast
   route-policy pass-all in
   route-policy pass-all out
  !
```

BGP Routing Display

BGP Sync display:

```
SP RTR: show bgp ipv6 unicast summary
BGP router identifier 172.2.44.1, local AS number 65534
BGP generic scan interval 60 secs
Non-stop routing is enabled
BGP table state: Active
Table ID: 0xe0800000   RD version: 8842309
BGP main routing table version 8842309
BGP NSR Initial initsync version 8 (Reached)
BGP NSR/ISSU Sync-Group versions 0/0
BGP scan interval 60 secs

BGP is operating in STANDALONE mode.


Process       RcvTblVer   bRIB/RIB   LabelVer   ImportVer   SendTblVer   StandbyVer
```

```
Speaker          8842309    8842309    8842309    8842309    8842309          0

Neighbor         Spk    AS MsgRcvd MsgSent   TblVer   InQ OutQ  Up/Down  St/PfxRcd
2001:200:200::9:2
                  0 65009 2627876   89050   8842309    0    0 19:28:38       80
2001:200:200::9:3
                  0 65009 2625705   87694   8842309    0    0 19:25:52       80

```
```

For more details, see .

Configure Wiring

```
wiring :
    bgp-agent-if:
       v4 : ['200.200.9.2', '200.200.9.3']
       v6 : ['2001:200:200::9:2', '2001:200:200::9:3']
    sg-peer: {'v4':'200.200.9.1', 'v6':'2001:200:200::9:1'}
    vlan :
       cnbr-wan-ifname: 'Ethernet0/0/0'
       overlay-wan-vlan: 1001
       overlay-cin-vlan: 1002
bgpagent :
    asn : 65009
    max_hops : 255
    restart-time : 120
    stale-path-time: 360
    neighbors :
       - {'address' :'200.200.9.1', 'asn':65534}
       - {'address' :'2001:200:200::9:1', 'asn':65534}

tftpProxy:
    v4 : ['200.200.9.1']
    v6 : ['2001:200:200::9:1']
```

SP Router Redundancy Configuration:

```
spr :
    sp-router-redundancy-mode : "active-active"
    sp-routers :
      - {'bgp-peer' :'200.200.9.1', "sg-peer": "200.200.9.1", "router-id": "200.200.9.1",
 "cin-gateway": "100.100.9.1", "ptp-gateway": "100.100.9.1"}
      - {'bgp-peer' :'2001:200:200::9:1'}
      - {'bgp-peer' :'200.200.9.250', "sg-peer": "200.200.9.250", "router-id":
"200.200.9.250", "cin-gateway": "100.100.9.250", "ptp-gateway": "100.100.9.250"}
```

Configure Layer 3

```
{
  "dhcp": {
    "arpGlean": true,
    "arpProxy": true,
    "dhcpIfname": "cnr",
    "dhcpServers": [
      "1.2.2.91",
      "fd26:ba99:aae:102::2:91"
    ],
    "ipv6Lq": true,
    "mobilityScopes": [
      "1.1.1.1/24",
      "2001::a/88"
    ],
    "ndGlean": false,
```

```
        "ndProxy": true,
        "relayPolicies": [
         {
             "deviceClass": "CM",
             "giAddr": "9.44.6.2",
             "linkAddr": "fd26:ba99:aae:0944:6::1",
             "v4ServerIp": "1.2.2.91",
             "v6serverip": "fd26:ba99:aae:102::2:91"
          },
          {
              "deviceClass": "HOST",
              "giAddr": "24.44.6.2",
              "linkAddr": "fd26:ba99:aae:0944:6::1",
              "v4ServerIp": "1.2.2.91",
         "v6ServerIp": "fd26:ba99:aae:102::2:91"
          }
        ],
        "relayModeV4": 0,
        "relayModeV6": 0,
        "v4Nets": [
          "9.44.6.2/24",
          "24.44.6.2/24"
        ],
        "v6Nets": [
          "FD26:BA99:AAE:944:6::1/80",
          "FD26:BA99:AAE:2444:6::1/80"
        ]

      },
      "spRouterName": "NCS-55A1",
      "savList": {
        "prefixes": null
      },
      "sgPeerIpv4": "100.100.6.1/24",
      "sgPeerIpv6": "2001:100:100::6:1/112",
      "ptp-mac-addr": "20:19:06:13:15:43"
}
```

Configure SG Template

The `ipInit` can be dual-stack, IPv6 only, or IPv4 only. The following is an example of the relevant subsection of the SG template:

```
"md": [
        {
            "adminState": "Up",
            "cmInitChanTimeout": 60,
            "dataBackoff": {
                "end": 5,
                "start": 3
            },
      "disableDocsis31": false,
            "idInSg": 0,
      "ipInit": "dual-stack",
            "mac": "00:23:09:73:47:a5",
```

Configure DMIC

Dynamic Shared Secret that enables service providers to provide higher levels of security for their data-over-cable service interface specifications (DOCSIS) cable networks. This feature uses randomized, single-use shared secrets to verify the DOCSIS configuration files, which are downloaded to each cable modem.

Following is the L3 configuration for Dynamic Message Integrity Check (DMIC):

```
{
  "dhcp": {
    "arpGlean": true,
    "arpProxy": true,
    "dhcpIfname": "cnr",
    "dhcpServers": [
      "1.2.2.91",
      "fd26:ba99:aae:102::2:91"
    ],
    "dynamicSecret": true,
    "ipv6Lq": true,
```

Cisco cnBR as DHCP Relay Agent

In a Cisco cnBR system, cable modems and some of the associated CPEs acquire IP addresses from a DHCP server in the network. These cable modems, their associated CPEs, and the DHCP server are not on the same physical network. In this scenario, Cisco cnBR acts as a DHCP relay agent to relay all requests and replies between the clients (CM and CPE) and the DHCP server. The DHCP relay agent in Cisco cnBR supports both IPv4 and IPv6 addressing.

Cisco cnBR supports CMs and CPEs operating in IPv4, IPv6, and dual-stack modes.

When CMs operate in the IPv6 mode, especially only in the IPv6 mode, configure the TFTP server and operate it in the IPv6 mode. This configuration allows the CMs to connect to the TFTP server in IPv6 mode and download their CM configuration file.

Note DHCP messages from RPDs does not reach the DHCP relay agent in the Cisco cnBR router. These DHCP messages from RPDs can reach the DHCP server in the CIN without using the DHCP relay agent in Cisco cnBR.

Configure DHCP Services

Initially, you can configure the DHCP relay services using the Autodeployer script, or by importing the Cisco cnBR configuration YAML file to the desired Cisco cnBR through the Cisco Operations Hub. The imported configuration file overwrites the existing configuration and activates the new configuration. Following is an example of the DHCP relay service configuration:

```
```
"Dhcp":
    {
        "ArpGlean":true,
        "ArpProxy":true,
        "ipv4Lq": false,
        "NdGlean":true,
        "NdProxy":true,
        "ipv6Lq":false,
        "dhcpServers":["80.80.80.3",
                       "81.81.81.3",
                       "2001:80:80:80::3",
                       "2001:81:81:81::3"
        ],
        "V4Nets":["90.90.90.1/24",
                  "91.91.91.1/24",
                  "92.92.92.1/24"
        ],
```

```
                    "V6Nets":["2001:90:90:90::1/64",
                            "2001:91:91:91::1/64",
                            "2001:92:92:92::1/64"
                    ],
                    "RelayPolicies":[
                      {"deviceClass": "HOST",
                       "v4serverip": "80.80.80.3",
                       "v6serverip": "2001:80:80:80::3",
                       "giaddr": "90.90.90.1",
                       "linkaddr": "2001:90:90:90::1"
                       },
                       {"deviceClass": "STB",
                       "v4serverip": "81.81.81.3",
                       "v6serverip": "2001:81:81:81::3",
                       "giaddr": "91.91.91.1",
                       "linkaddr": "2001:91:91:91::1"
                       },
                       {"deviceClass": "PS",
                       "giaddr": "92.92.92.1",
                       "linkaddr": "2001:92:92:92::1"
                       },
                       {"deviceClass": "EROUTER",
                       "v4serverip": "80.80.80.3",
                       "v6serverip": "2001:80:80:80::3",
                       },
                       {"deviceClass": "DVA",
                       "giaddr": "90.90.90.1",
                       "linkaddr": "2001:90:90:90::1"
                       },
                       {"deviceClass": "MTA",
                       "giaddr": "91.91.91.1",
                       "linkaddr": "2001:91:91:91::1"
                       }
                    ],
                    "mobilityScopes":["90.90.90.1/24",
                                      "91.91.91.1/24",
                                      "92.92.92.1/24",
                                      "2001:90:90:90::1/64",
                                      "2001:91:91:91::1/64",
                                      "2001:92:92:92::1/64"
                    ]
                }
            ```
```

For more details, see DHCP Relay Service, on page 99.

## Cisco cnBR IPv6 CIN

From Cisco cnBR 20.4 onwards, Converged Interconnect Network (CIN) is supported over IPv6. CIN enables you to build a robust, flexible, and scalable network to interconnect the CCAP-Core and RPDs in a solution topology. You can provision RPD with IPv6 to communicate with cnBR ccap-core through IPv6.

The GCP, PTP, and L2TP protocol will be running over IPv6. You need to configure end-to-end CIN network from RPDs to SPR, and Cisco cnBR must be configured to support it. You also need to provision the RPDs to support IPv6.

### Configure cnBR IPv6 CIN

Complete the following steps to configure Cisco cnBR IPv6 CIN:

**Step 1**    Configure the SP router CIN network interface with IPv6 address.

```
  ```
interface Bundle-Ether24.1002
 ipv4 address 5.230.203.1 255.255.255.0
 ipv6 nd prefix default no-adv
 ipv6 nd ra-interval 4
 ipv6 nd suppress-ra
 ipv6 address fc00::5e6:cb01/120
 load-interval 30
 encapsulation dot1q 1002
!
  ```
```

a) Day1 configuration: Add v6 support for `rphmgr-if`, `cin-start-ip` in wiring part. The `rphmgr-if v6` address is `ccap-cores` for RPDs in DHCPv6 option 17.61.

```yaml
wiring :
    bgp-agent-if:
        v4 : ['200.200.203.201', '200.200.203.202']
        v6 : ['2001:200:200:203::201', '2001:200:200:203::202']
    cin-prefix: {'v4':24, 'v6':120}
    rphmgr-if:  {'v4':'5.230.203.3', 'v6':'fc00::5e6:cb03'}
    cmts-cops-if: { 'v4':'5.230.203.9'}
    cin-start-ip: { 'v4':'5.230.203.10', 'v6':'fc00::5e6:cb0a'}
    sg-peer: {'v4':'200.200.203.1', 'v6':'2001:200:200:203::1'}
    dc-link-prefix: {'v4':24, 'v6':64}
    vlan :
        cnbr-wan-ifname: 'BondEthernet0'
        cnbr-wan-bonded-interface1: 'Ethernet0/0/0'
        cnbr-wan-bonded-interface2: 'Ethernet0/0/1'
        cnbr-wan-bond-mode: 'lacp'
        cnbr-wan-bond-loadbalance: 'L2'
        overlay-wan-vlan: 1001
        overlay-cin-vlan: 1002
        overlay-l2vpn-vlan-vlan: 1003
        overlay-l2vpn-mpls-vlan: 1004
        secondary-overlay-l2vpn-vlan-vlan: 1103
        secondary-overlay-l2vpn-mpls-vlan: 1104
    mtu : '2450'
```

b) Add PTP and CIN IPv6 configuration:

```yaml
ptp :
    v6:
        domain : 44
        master: {'ip': '2001:420:4:ef00::50a:2f9', 'gw': 'fc00::5e6:cb01'}
cin :
    v4 : ['5.230.203.1']
    v6 : ['fc00::5e6:cb01']
```

c) Add `ipv6 cin-gateway` and `ptp-gateway` if SP router redundancy is configured:

```yaml
spr :
    sp-router-redundancy-mode : 'active-active'
    sp-routers :
        - {'bgp-peer' :'200.200.203.1', 'sg-peer': '200.200.203.1', 'router-id': '5.230.0.5',
'cin-gateway': '5.230.203.1', 'ptp-gateway': '5.230.203.1'}
```

```
                - {'bgp-peer' :'2001:200:200:203::1', 'sg-peer': '2001:200:200:203::1', 'router-id':
    '5.230.0.5', 'cin-gateway': 'fc00::5e6:cb01', 'ptp-gateway': 'fc00::5e6:cb01'}
                - {'bgp-peer' :'200.200.203.254', 'sg-peer': '200.200.203.254', 'router-id':
    '5.230.0.17', 'cin-gateway': '5.230.203.254', 'ptp-gateway': '5.230.203.254'}
                - {'bgp-peer' :'2001:200:200:203::254', 'sg-peer': '2001:200:200:203::254', 'router-id':
     '5.230.0.17', 'cin-gateway': 'fc00::5e6:cbff', 'ptp-gateway': 'fc00::5e6:cbff'}
            ```
```

Step 2   SG template configuration

Configure the `masterAddr` to PTP primary v6 address in `rpdPtpCfg` section of SG template:

```json
"rpdPtpCfg": {
  "domain": 44,
  "dtiMode": "SlaveDtiMode",
  "priority1": 128,
  "priority2": 255,
  "ptpClkProfileId": "00:00:00:00:00:00",
  "ptpPortCfg": [
    {
      "adminState": "Up",
      "anncReceiptTimeout": 11,
      "cos": 6,
      "dscp": 40,
      "enetPortIndex": 1,
      "localPriority": 128,
      "logDelayReqInterval": -4,
      "logSyncInterval": -4,
      "masterAddr": "2001:420:4:ef00::50a:2f9",
      "masterAdminState": "Up",
      "ptpPortIndex": 22,
      "unicastDuration": 300
    }
  ]
}
```

RIP

Routing Information Protocol (RIP) is used in small to medium TCP/IP networks. It uses a distance-vector algorithm to calculate routes. The RIP uses broadcast UDP data packets to exchange the routing information. Cisco cnBR can advertise the default network to the CPE devices running RIP, and collect the routing information updated by the CPE device.

Among the RIP version 2 features, Cisco cnBR supports plain text and message digest algorithm 5 (MD5) authentication, route summarization, classless interdomain routing (CIDR), and variable-length subnet masks (VLSMs). Only RIPv2 packets are sent and received.

Authentication Mode in RIP

Cisco cnBR supports two modes of authentication on RIP:

- Simple authentication: Uses a plaintext password in every RIPv2 packet.

• Message digest algorithm 5 (MD5) authentication: MD5 authentication pads digest information to each RIPv2 packet based on the packet content and preconfigured passwords. The key chain structure maintains passwords, which determines if a key can be used or valid.

Configure RIP

You can configure RIP on Cisco cnBR during the initial configuration using the Autodeployer.

The Autodeployer configuration file includes the following RIP configuration fields.

Field Name	Description	Mandatory
enable	Shows whether RIP is enabled on Cisco cnBR.	Yes
passive-mode	Shows whether RIP works in passive mode. Default is `False`.	No
update-timer	RIP update-timer in seconds. Default value is 30.	No
invalid-timer	RIP invalid-timer in seconds. Default value is 180.	No
holddown-timer	RIP hold-down timer in seconds. Default value is 180.	No
ripAuthMode	RIP authentication mode. Default is `None`.	No
ripSimplePswd	RIP simple authentication password.	Yes, if ripAuthMode is simple.
keychain	RIP md5 authentication keychain.	yes if ripAuthMode is md5.

The keychain is a list of key items and each item must contain the following attributes:

Field Name	Description	Mandatory
KeyID	ID for each individual key.	Yes
KeyString	Key phrase content.	Yes
algorithm	Hash algorithm used by the key. Currently, supports only md5.	No
sendlifetime	Time-interval to send keys.	No
acceptlifetime	Time-interval to accept incoming keys.	No

Following is an example of the RIP configuration, as part of the Autodeployer configuration:

```
rip :
    enable : 'false'
    update-timer : 30
    invalid-timer : 180
    holddown-timer : 180
    passive-mode : 'false'
```

```
        ripAuthMode : "md5"
        keychain:
            - {'key-id': 10, 'algorithm': "md5", 'accept-lifetime': { "start":
"1970-01-01T00:00:00Z07:00",
                "end": "2022-01-02T15:04:05Z07:00" }, 'send-lifetime': { "start":
"1970-01-01T00:00:00Z07:00",
                "end": "2022-01-02T15:04:05Z07:00" }
```

Update RIP Configuration using cnBR Manager

You can also update the RIP configuration using the cnBR Manager from the Cisco Operations Hub. Use the following procedure:

SUMMARY STEPS

1. Log in to Cisco Operations Hub.
2. Click the Cisco Operations Hub main menu button on the top-left corner, choose **cnBR Manager** > **cnBRs**, and click **Inventory**.
3. Choose the required Cisco cnBR core from the list.
4. Choose the required cnBR, click **Edit** and click the **Advanced** tab.
5. Choose **RIP** from the drop-down list under **Wiring**.

DETAILED STEPS

	Command or Action	Purpose
Step 1	Log in to Cisco Operations Hub.	
Step 2	Click the Cisco Operations Hub main menu button on the top-left corner, choose **cnBR Manager** > **cnBRs**, and click **Inventory**.	
Step 3	Choose the required Cisco cnBR core from the list.	
Step 4	Choose the required cnBR, click **Edit** and click the **Advanced** tab.	
Step 5	Choose **RIP** from the drop-down list under **Wiring**.	You can see the RIP configuration details.

DOCSIS

Cisco cnBR provides Data-Over-Cable Service Interface Specifications (DOCSIS) functionality, enabling next generation broadband capability for your Distributed Access Architecture.

Upstream Resiliency

A DOCSIS 3.0+ cable modem (CM) operating in upstream channel bonding mode, or Multiple Transmit Channels (MTC) mode, utilizes its assigned upstream channels, or Transmit Channel Set (TCS), to transmit data packets when Cisco cnBR grants transmission opportunities on those channels.

The Upstream (US) Resiliency feature provides the capability to automatically suspend granting transmission opportunities for a CM on one or more certain upstream channels when the Cisco cnBR determines that those upstream channels are no longer usable for the CM.

Cisco cnBR determines the usability of the upstream channel by polling the CM with Station Maintenance (SM) Ranging opportunities every 20 seconds on each of the upstream channels in the CM TCS, and waits for the Range Request from the CM on those upstream channels. If Cisco cnBR does not receive the Range Request message from the CM after granting an SM Ranging opportunity, the Cisco cnBR reduces the SM grant interval from 20 seconds to 1 second for the CM on the affected upstream channel. If the Cisco cnBR still can not receive the Ranging Request from the CM for the next 25 times, the Cisco cnBR then considers the upstream channel to be impaired for that CM.

The CM is then classified as operating in the Upstream Partial Service state. The RPTS, nRTPS service flows used by the CM, if any, will be moved to another upstream channel in the updated TCS of the CM. After the CM is able to range on all its TCS channels again, the CM exits the Partial Service state.

Note Other non-Best Effort Service Flows, such as UGS, UGS-AD, will not be moved away from the impaired upstream channel. Future Cisco cnBR releases will address this issue.

By default, upstream resiliency is enabled. It does not require any configuration; that is, you do not need to set US Resiliency parameters in the Autodeployer configuration file.

Monitor Upstream Resiliency

The Upstream Resiliency Dashboard displays the statistics of the cable modems that are in upstream partial service state, and the status of the upstream channels in the Cisco cnBR. You can use the Dashboard to identify impaired upstream channels, and help to narrow down part of the cable plant that needs servicing.

US Resiliency cnBR Manager Dashboard

To view the US Resiliency dashboard, use the following procedure:

Step 1 Enter the Cisco Operations Hub URL `https://{Hostname}` in the web browser.

Step 2 On the Cisco Operations Hub, click the Cisco Operations Hub main menu button.

Step 3 Choose **Dashboard** to open the **Dashboard** page.

Step 4 Click **Find a Dashboard** to open the search pane.

Step 5 Enter **us resiliency** in the **Search dashboards by name** field and click the **us resiliency** row to open **US Resiliency** dashboard.

Step 6 In the **US Resiliency** dashboard, click the **cnBR ID** drop-down list to choose the Cisco cnBR to monitor. You must add Cisco cnBR to the Cisco Operations Hub to see it in the drop-down list.

Step 7 After you choose the Cisco cnBR, select the desired Service Group by clicking the **SG ID** drop-down list. Similarly, you must first fill and configure the Service Group to select it in the **SG ID** drop-down list.

Cluster Statistics

The Cisco cnBR Cluster US Resiliency statistics panel provides the current and historical statistics for the selected Cisco cnBR and Service Group, which includes:

- The current number of cable modems that are in partial service mode in the selected Cisco cnBR cluster.

- The current total number of cable modems detected by the selected Cisco cnBR cluster.

- The historical count of the cable modems that are in upstream partial service mode.

- The total number of cable modems over time.

- The current list of the cable modems in upstream partial service mode.

Figure 28: The US Resiliency panel
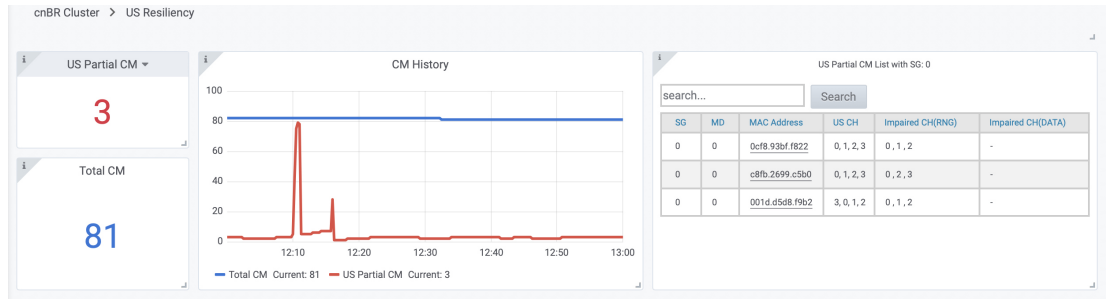
Service Group Statistics

The Service Group Statistics panel provides the current and historical statistics for the selected Service Group, which includes:

- The current number of cable modems that are in partial service mode in a specific Service Group.

- The historical count of the cable modems that are in upstream partial service mode in a specific service group.
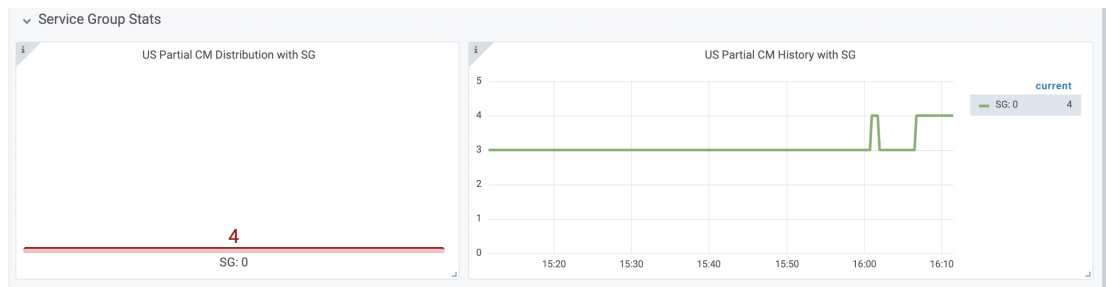
Upstream Channel Statistics

The US Channel Statistics panel provides the current and historical statistics for each upstream channel in the selected Service Group, which includes:

- The current number of cable modems that are in partial service mode for each upstream channel in the selected Service Group.

- The historical count of the cable modems that are in upstream partial service mode in each upstream channel in the selected Service Group.

When a significant number of CMs have a problem on a specific channel, there may be channel frequency interference in a certain segment of the cable plant or service neighborhood.

When a few CMs have a problem on all channels, it may indicate that there is a loose connector or deteriorating cable on certain segment of the service neighborhood, or those CMs may be close to the boundary of the supported service area. It may also indicate a cabling problem of those CMs at the customer homes.

In the preceding cases, you may need more investigation to better understand and troubleshoot the problem, and proactively implement remedies if needed (before you call the service center).

Downstream Resiliency

DOCSIS 3.0+ Cable Modems (CMs) use downstream bonding groups to receive data. In this scenario, when one or more downstream channels get impaired, it causes packet drops in that particular channel. Furthermore, as the packets need to be reordered, packet drop in one channel can cause reorder timeout and large packet delay, in a continuous manner. Therefore, detecting channel impairment and mitigating this type of condition is important for proper downstream channel bonding operation.

DOCSIS provides a mechanism that let modems detect this condition and report the issue through a CM-STATUS MAC Management Message (MMM). Therefore, CMTS can stay informed about one or more channels that are impaired. However, the DOCSIS specification does not specify how the CMTS should handle the impaired channel conditions. The implementation is up to CMTS vendor.

Upon receiving a CM-STATUS MMM indicating DS channel impairment, the Cisco cnBR temporarily removes the impaired DS channel from the bonded DS Receive Channel Set (RCS). From the CM's perspective, its current RCS persists during impairment. It allows the CM to monitor all DS channels and detect when the impairment is gone from the impacted DS channel. After the Cisco cnBR receives a CM-STATUS MMM indicating that the DS channel impairment is gone, the previously impaired DS channel is added back to the RCS.

Note DS resiliency applies to only nonprimary DS channels. DS impairment of a CM's primary channel is an event that cannot be mitigated and results in a CM dropping offline.

Current DS Resiliency Feature handles three failure modes:

- MDD timeout

- QAM lock failure

- OFDM profile failure

Four types of CM-STATUS messages are handled for supporting DOCSIS 3.0 DS resilience:

• MDD timeout (Event Code 1)

• QAM lock failure (Event Code 2)

• MDD recovery (Event Code 4)

• QAM lock recovery (Event Code 5)

Two types of CM-STATUS message are handled for supporting DOCSIS 3.1 DS resilience:

• DS OFDM Profile Failure (Event Code 16)

• DS OFDM Profile Recovery (Event Code 24)

Configure DS Resiliency

The DS Resiliency configuration is a sub-configuration of the service group configuration. To enable the DS resiliency feature, add the following sub-configuration to all SG configurations.

```
"DsResilCfg":
    {
        "DampenTime":30,
        "ResilEn":"true"
    },
```

To disable the DS resiliency feature, change the `"ResilEn":"true"` to `"ResilEn":"false"` in all SG configurations.

Note Even with DS Resiliency disabled, logs and dashboards show all events and impaired CMs, and don't change the service flow.

Note The unit of dampen time is seconds.

Update the DS Resiliency Configuration Using cnBR Manager

After the initial configuration of DS Resiliency during deployment using the Autodeployer, you can also update the configuration through the cnBR Manager using the following steps:

Step 1 On the Cisco Operations Hub, click the Cisco Operations Hub main menu button.

Step 2 Choose **cnBR Manager** > **cnBRs** to open the **cnBR Clusters** page.

Step 3 Click **Import & Export cnBR** to open the **Export/Import** page.

Step 4 On the **Export cnBR Configuration** pane, choose the Cisco cnBR that you want to update.

Step 5 Click **Export** to get the current SG configuration of the selected Cisco cnBR.

Step 6 Update the configuration in the `dsResilCfg` section of the SG configuration.

Step 7 Save the updated file on the local disk.

Step 8 In the **Import cnBR Configuration File** pane, from the drop-down list, choose the Cisco cnBR to update.

Step 9 Click **Browse** to locate the file which you updated (saved at Step 5).

Step 10   Click **Import** to upload the updated SG configuration to the selected Cisco cnBR.

DS Resiliency Monitor Statistics

Step 1   Enter the Cisco Operations Hub URL `https://{Hostname}` in the web browser.

Step 2   On the Cisco Operations Hub, click the Cisco Operations Hub main menu button.

Step 3   Choose **Dashboard** to open the **Dashboard** page.

Step 4   Click **Find a Dashboard** to open the search pane.

Step 5   Enter **ds resil** in the **Search dashboards by name** field and click the **DS Resil Dashboard** row to open the **DS Resil Dashboard**.

Step 6   Select the desired Cisco cnBR from the **cnBR Name** drop-down list.

OFDM Container

This table lists the features and the releases in which the feature was introduced and gives a small description of the feature.

Table 26: Feature History

Feature Name	Release Information	Feature Description
Support for 2 OFDM Blocks	Cisco cnBR 21.2	This feature increases the support for OFDM Blocks to two. This increase allows for up to 384 MHz of OFDM bandwidth for each Service Group.

Cisco cnBRprovides DOCSIS 3.1 support by introducing Orthogonal Frequency-Division Multiplexing (OFDM) channels in the downstream direction, and Orthogonal Frequency-Division Multiple Access (OFDMA) channels in the upstream direction. OFDM allows for higher throughput and higher spectral efficiency, while still allowing backward compatibility to DOCSIS 3.0.

The OFDM Channel support includes 2 OFDM channels per Service Group (SG) with a channel bandwidth 24–192 MHz wide per OFDM channel. These channels allow for a maximum of 384 MHz of OFDM bandwidth per SG. Cisco cnBR supports OFDM channels as nonprimary channels. The two OFDM channels do not need to be contiguous in the Downstream frequency spectrum.

DOCSIS 3.1 cable modems automatically bond with the maximum number of both OFDM and SC-QAM channels they support. For example, if you configure 16 SC-QAM and 2 OFDM channels in the SG, these modems come online bonded to all these channels. If you configure 32 or more SC-QAM and 2 OFDM channels in the SG, these modems come online bonded to 32 SC-QAM and 2 OFDM channels. If you configure one of the OFDM channels in the downstream spectrum above the downstream diplexer upper band edge of a DOCSIS 3.1 cable modem, the modem comes online using only one OFDM channel.

Each OFDM channel supports the following:

- **Control profile:** The control profile is known in CM-SP-MULTIv3.1 as Profile A, using profile ID 0. This profile ID denotes the common profile that all modems can receive and decode. A modem uses Profile A when it first initializes.

- **NCP profile**: There is a dedicated NCP profile, the Next Codeword Pointer. The NCP profile indicates which subcarriers are usable for NCP and what modulation to use on each subcarrier.

- **Data profile**: An OFDM channel supports a maximum of five data profiles. The data profiles are referred to as profile B, C, D, and so on, in CM-SP-MULTIv3.1.

Configure OFDM Port

Complete the following steps to configure the OFDM port:

Step 1 Configure the OFDM Frequency Exclusion band. The OFDM Frequency exclusion band configuration is supported at the DS port level. The OFDM configuration parameters are listed in the following table:

This table shows parameter ranges for OFDM port configuration parameters.

Table 27: OFDM Port Configuration Parameters

OFDM Frequency Exclusion Band Parameter	Minimum (MHz)	Maximum (MHz)	Default
Channel ID in SG	158	162	N/A
Start frequency	108	1217	N/A
Width	1	1110	N/A

Step 2 Configure OFDM channels in the SG. OFDM channels are numbered from 158 to 162. An OFDM channel number must be present in the `channel` set under a `dsPort` for its configuration to take effect.

Note Cisco cnBR supports a maximum of two OFDM channels for each SG.

See the following DS port configuration example for a sample single OFDM channel configuration:

```
"rpdCfg":
    [{
        "rpdIp":"$RPD0_IP",
        "rpdMac":"$RPD0_MAC",
        "entries":
        {
            "dsPort":
            [{
                "portId": 0,
                "basePower": 21,
                "rfMute": false,
                "adminState": "Up",
                "ofdmFreqExclBand": [{"startFreq":900000000,"width":10000000}],
                "channel": [0,1,2,3,158]
            }],
            "usPort":
            [{
                "portId": 0,
                "channel": [0,1,2,3]
```

```
            }],
            "fiberNode":
            [{
                "Id":0,
                "DsPort":0,
                "UsPort":0
            }]
        }
    }],
```

See the following DS port configuration example for a sample configuration for two OFDM channels:

```
"rpdCfg":
    [{
        "rpdIp":"$RPD0_IP",
        "rpdMac":"$RPD0_MAC",
        "entries":
        {
            "dsPort":
            [{
                "portId": 0,
                "basePower": 21,
                "rfMute": false,
                "adminState": "Up",
                "ofdmFreqExclBand": [{"startFreq":900000000,"width":10000000}],
                "channel": [0,1,2,3,158,159]
            }],
            "usPort":
            [{
                "portId": 0,
                "channel": [0,1,2,3]
            }],
            "fiberNode":
            [{
                "Id":0,
                "DsPort":0,
                "UsPort":0
            }]
        }
    }],
```

Configure OFDM Channel

Complete the following steps to configure the OFDM channel:

Go through the OFDM channel-level configuration parameters listed in the following table:

This table shows parameter ranges for OFDM channel configuration parameters.

Table 28: OFDM Channel Configuration Parameters

OFDM Frequency Exclusion Band Parameter	Minimum (MHz)	Maximum (MHz)	Default
Channel ID in SG	158	162	N/A
Start frequency	108	1218	N/A

OFDM Frequency Exclusion Band Parameter	Minimum (MHz)	Maximum (MHz)	Default
Width	24	192	N/A
PLC start frequency	108	1218	N/A
Cyclic prefix	192, 256, 512, 768, 1024		1024
Interleaver depth	1	32	16
Pilot scaling	48	120	48
Roll-off	64, 128, 192, 256		128
Subcarrier spacing	25 KHz, 50 KHz		50 KHz
Guard band override (optional)	0 Hz	4000000 Hz	Disabled

Note   As a Cisco cnBR convention, OFDM channels use DOCSIS Channel ID (DCID) of 158, or higher.

See the following DS channel configuration example. The OFDM channel configuration is in the `ofdmDs` block at the SG level. The following block configures OFDM channel #158:

```
"ofdmDs":
[
    {
      "cyclicPrefix": 512,
      "idInSg": 158,
      "interleaverDepth": 16,
      "pilotScaling": 48,
      "plc": 873000000,
      "profileControl": "QAM64",
      "profileData": [
        {
          "id": 1,
          "modulationDefault": "QAM1024"
        },
        {
          "id": 2,
          "modulationDefault": "QAM2048"
        },
        {
          "id": 3,
          "modulationProfile": 9
        }
      ],
      "profileNcp": "QAM16",
      "rollOff": 128,
      "startFrequency": 867000000,
      "subcarrierSpacing": "50KHZ",
      "width": 192000000
    }
],
```

The following DS channel configuration example configures OFDM channels 158 and 159.

```
    "ofdmDs":
```

```
[
    {
      "cyclicPrefix": 512,
      "idInSg": 158,
      "interleaverDepth": 16,
      "pilotScaling": 48,
      "plc": 873000000,
      "profileControl": "QAM64",
      "profileData": [
        {
          "id": 1,
          "modulationDefault": "QAM1024"
        },
        {
          "id": 2,
          "modulationDefault": "QAM2048"
        },
        {
          "id": 3,
          "modulationProfile": 9
        }
      ],
      "profileNcp": "QAM16",
      "rollOff": 128,
      "startFrequency": 867000000,
      "subcarrierSpacing": "50KHZ",
      "width": 192000000
    },
    {
      "cyclicPrefix": 512,
      "idInSg": 159,
      "interleaverDepth": 16,
      "pilotScaling": 48,
      "plc": 615000000,
      "profileControl": "QAM64",
      "profileData": [
        {
          "id": 1,
          "modulationDefault": "QAM1024"
        },
        {
          "id": 2,
          "modulationDefault": "QAM2048"
        },
        {
          "id": 3,
          "modulationDefault": "QAM4096"
        }
      ],
      "profileNcp": "QAM16",
      "rollOff": 128,
      "startFrequency": 609000000,
      "subcarrierSpacing": "50KHZ",
      "width": 192000000
    }
],
```

OFDM Channel Guard Band

This table lists the features and the releases in which the feature was introduced and gives a small description of the feature.

Table 29: Feature History

Feature Name	Release Information	Feature Description
OFDM Channel Guard Band	Cisco cnBR 21.1	You can override the default OFDM guard band configuration and configure it based on your requirement, for example, you could potentially trade off some performance margin for additional usable OFDM channel bandwidth.

Guard band is an excluded subcarrier band on both the lower and upper edges of the OFDM channel spectrum. The lower and upper guard band sizes are always identical. You can configure the size of the guard band by setting **guardbandOverride** under the **ofdmDs** block at the SG level. By default, the Cisco cnBR uses the roll-off and subcarrier spacing configuration of the OFDM channel to calculate the guard band. See the following table for the default guard band values.

This table lists the default guard band values.

Roll-off	Subcarrier Spacing: 25 kHz (freq: sc)	Subcarrier Spacing: 50 kHz (freq: sc)
64	3,350,000 Hz: 134	3,600,000 Hz: 72
128	1,725,000 Hz: 69	1,900,000 Hz: 38
192	1,175,000 Hz: 47	1,350,000 Hz: 27
256	1,000,000 Hz: 40	1,000,000 Hz: 20

Use the **guardbandOverride** parameter to configure the guard band size to any value 0–4000000 Hz. Align the guard band size with the subcarrier spacing configuration. The Cisco cnBR uses the configured guard band value for both the lower guard band and upper guard band of the OFDM channel. The following block configures OFDM channel 158 to use a guard band of 1 MHz:

```
"ofdmDs":
[
    {
      "cyclicPrefix": 512,
      "idInSg": 158,
      "interleaverDepth": 16,
      "pilotScaling": 48,
      "plc": 873000000,
      "profileControl": "QAM64",
      "profileData": [
        {
          "id": 1,
          "modulationDefault": "QAM1024"
        },
        {
          "id": 2,
          "modulationDefault": "QAM2048"
        },
        {
```

```
                "id": 3,
                "modulationProfile": 9
            }
        ],
        "profileNcp": "QAM16",
        "rollOff": 128,
        "startFrequency": 867000000,
        "subcarrierSpacing": "50KHZ",
        "width": 192000000,
        "guardbandOverride": 1000000
    }
],
```

Configure Downstream Modulation Profile

This table lists the features and the releases in which the feature was introduced and gives a small description of the feature.

Table 30: Feature History

Feature Name	Release Information	Feature Description
Configure OFDM Subcarriers Using Frequency Offset	Cisco cnBR 21.1	You can configure sub carrier ranges using the frequency offset (`freqOffset`) attribute in `ofdmModProfs` group.

A profile is a list of modulation orders which are defined for each subcarrier within an OFDM channel. The Cisco cnBR can define multiple profiles for use in an OFDM channel. The profiles may differ in the modulation orders that are assigned to each subcarrier.

Choose one of the supported modulation orders:

- Constant Modulation Orders

  When a profile has the same QAM modulation for all subcarriers, it is specified by the keyword `modulationDefault` and a modulation value (for example - `QAM256`) inside the `profileData` block for the OFDM channel configuration. See the example available in the section, Configure OFDM Channel, on page 153.

- Variable Modulation Orders

  When a profile has Variable QAM modulations for the subcarriers, it is specified using a different block within `ofdmModProfs` at the SG level. The following example defines the data-profile ID 9, named 512-1k-4k. The profile has a modulation order of 4096 QAM for all subcarriers except two ranges, where a different modulation order is defined.

  You can configure the ranges using either absolute frequency or frequency offset. When you use the frequency offset, the range begins at the frequency (startFrequency + freqOffset). In the following example, the first range begins at the absolute frequency of 935000000 Hz with a width of 7405000 Hz and has a modulation order of 512 QAM. The second range begins at a frequency offset of 12000000 Hz with a width of 6000000 Hz, and has a modulation order of 1024 QAM.

```
"ofdmModProfs":
    [
        {
            "assigns": [
```

```
                            {
                              "modulation": "QAM512",
                              "rangeSubcarriers": {
                                "freqAbs": 935000000,
                                "width": 7405000
                              }
                            },
                            {
                              "modulation": "QAM1024",
                              "rangeSubcarriers": {
                                "freqOffset": 12000000,
                                "width": 6000000
                              }
                            }
                          ],
                          "description": "512-1k-4k",
                          "idInSg": 9,
                          "modulationDefault": "QAM4096"
                        }
                  ]
```

Configure Modulation Profile Display

The profile list that is used by an OFDM channel is displayed in the OFDM Channel Profile Data dashboard in the cnBR Manager.

To view the OFDM profile data, perform either of the following steps:

- To load the OFDM Channel Profile Data dashboard:

  a. On the Cisco Operations Hub, click the Cisco Operations Hub main menu button.

  b. Choose **Dashboard** to open the **Dashboard** page.

  c. Click **Find a Dashboard** to open the search pane.

  d. Enter **OFDM Channel Profile Data** in the **Search dashboards by name** field and click the **OFDM Channel Profile Data** row to open the **OFDM Channel Profile Data** dashboard.

- To load the OFDM Modulation Profile Data dashboard:

  a. On the Cisco Operations Hub, click the Cisco Operations Hub main menu button.

  b. Choose **Dashboard** to open the **Dashboard** page. Click **Find a Dashboard** to open the search pane.

  c. Enter **OFDM Modulation Profile Data** in the **Search dashboards by name** field

  d. Click the **OFDM Modulation Profile Data** row to open the **OFDM Modulations Profile Data** dashboard.

  Note The data profile that is defined for variable modulation orders is displayed in the **OFDM Modulation Profile Data** page in the Cisco Operations Hub.

Update Configuration Using cnBR Manager

The configuration of the DS port, OFDM channel, and OFDM Modulation Profile can all be updated using the cnBR Manager. After the initial configuration during deployment using the Autodeployer, the configuration can be updated through the cnBR Manager.

Use the following procedure to update the configuration:

Step 1   On the Cisco Operations Hub, click the Cisco Operations Hub main menu button.

Step 2   Choose **cnBR Manager** > **cnBRs** to open the **cnBR Clusters** page.

Step 3   Click **Import & Export cnBR** to open the **Export/Import** page.

Step 4   In the **Export cnBR Configuration** section, from the drop-down list, choose the required to cnBR cluster to update.

Step 5   Click **Export** to get the current SG configuration of the selected cnBR cluster.

The file is downloaded in JSON format. You can choose to update the following parameters in the downloaded JSON file.

- To update the OFDM Modulation Profile, edit the values in the `ofdmModProfs` section of the SG configuration.

- To update the DS port, edit the values in the `rpdCfg` section of the SG configuration.

- To update the OFDM channel, edit the values in the `ofdmDs` section of the SG configuration.

Step 6   Save the updated file.

Step 7   In the **Import cnBR Configuration File** pane, from the drop-down list, choose the Cisco cnBR to update.

Step 8   Click **Browse** to locate the file which you updated (saved at Step 4).

Step 9   Click **Import** to push the updated SG configuration.

Downstream Modulation Profile Selection

Cisco cnBR has the following DS modulation profiles:

- Default Data Profile

  When a CM registers, it is assigned a default data profile. The default data profile is `profile-data 1`. If `profile-data 1` is not configured, `profile-control` is assigned to the CM.

- Recommended Profile

  The Cisco cnBR chooses a profile from existing configured modulation profiles having the highest speed and sufficient Signal to Noise Ratio (SNR) margin. The profile selection is based on the Receive Modulation Error Ratio (RxMER) values collected from a modem.

  This allows optimum use of the OFDM channel while allowing the modem to receive codewords with acceptable error rate. The selected profile is the *recommended profile* for that modem.

  To compute the recommended profile, the modem's RxMER values are first mapped to desired bit loading values. The desired bit loading values are compared to those in the configured profiles. Ideally, the desired bit loading value must be higher than that in the profile for the same subcarrier.

  However, due to the error correction capabilities provided by the channel coding and interleaving, this rule allows certain exceptions. The exemptions are made a configurable value, and is called *exempt subcarrier percentage*.

Recommended Profile Age

All recommended profiles have a configurable age that is associated with it. If the recommended profile exceeds this age, it is no longer valid for that modem.

RxMER to Bit Loading Mapping

There are various methods to map the Receive Modulation Error Ratio (RxMER) values to a modem's desired bit loading values. Cisco cnBR recommends the following mapping, which is listed in CM-SP-CCAP-OSSIv3.1, as the baseline mapping:

This table shows therecommended RxMER to Bit Loading values mapping.

Table 31: RxMER to Bit Loading Values

RxMER (¼ DB)	QAM	Bit Loading
60	16	4
84	64	6
96	128	7
108	256	8
136	1024	10
148	2048	11
164	4096	12
184	8192	13
208	16384	14

Margin Adjustment

A margin value may be configured for each cnBR to adjust the RxMER to the Bit loading mapping listed in the table. This configured value (in quarter-DB) is added to the RxMER values collected by cnBR before using the above mapping table. This gives you more control in selecting the recommended profiles.

Exempt Subcarrier Percentage

An exempt subcarrier percentage may be configured for each cnBR. When computing the recommended profile for a modem, this threshold percentage of subcarriers may be ignored when comparing the modem's desired bit loading values to those in each configured profile.

RxMER Poll Interval

cnBR uses OPT message with bit-0 option to collect RxMER data from CMs, after the initial modem registration and periodically thereafter. The collected RxMER data is used to compute the recommended profile for each modem.

Unfit Profile

The profile indicates that the CM-STATUS message is marked as *unfit profile* if the CMTS receives CM-STATUS Event 16 (DS OFDM Profile Failure).

A configurable maximum age is associated with each unfit profile for a given modem. If the unfit profile for a modem exceeds this age, it is no longer considered *Unfit* for that modem.

Profile Selection Parameter Configuration

The following table lists the parameter range for the profile selections:

This table shows parameter ranges for profile selections.

Table 32: Parameter Ranges for Profile Selections

Profile Selection Parameter	Minimum	Maximum	Default
rxmer-poll-interval	1 minute	1440 minutes	60 minutes
exempt-sc-pct	1	100	2
mer-margin-qdb	0 qDB	40 qDB	0
recm-prof-age	1 minute	1440 minutes	120 minutes
unfit-prof-age	1 minute	1440 minutes	120 minutes

An example of the parameter configuration is as follows:

```
"ofdmProfMgmt":
{
    "rxmer-poll-interval": 180,
    "exempt-sc-pct": 20,
    "mer-margin-qdb": 16,
    "recm-prof-age": 360,
    "unfit-prof-age": 360
}
```

View OFDM Channel and Profile Statistics

You can choose to view the OFDM channel and profile statistics information on the Cisco cnBR dashboard.

You can view the OFDM channel and profile statistics through the **Dashboard** page. You can choose to view the following:

• Downstream Channel Statistics

View the DS channel (SC QAM and OFDM channel) byte and packet counters for a given SG on the **DS Channel Rate** dashboard of the Cisco Operations Hub.

To load this dashboard, click the Cisco Operations Hub main menu button. Choose **Dashboard** to open the **Dashboard** page. Click **Find a Dashboard** to open the search pane. Enter **DS Channel Rate** in the **Search dashboards by name** field and click the **DS Channel Rate** row.

The **DS Channel Rate** dashboard also shows the historical data of the downstream channel (SC QAM and OFDM channel) bit and packet rates for a given SG, along with the historical data of the downstream channel (SC QAM and OFDM channel) utilizations.

• OFDM Modulation Profile Statistics

View the OFDM modulation per-channel-per-profile byte and packet counters on the **OFDM Channel Profile Stats** dashboard in the Cisco Operations Hub.

To load this dashboard, click the Cisco Operations Hub main menu button. Choose **Dashboard** to open the **Dashboard** page. Click **Find a Dashboard** to open the search pane. Enter **OFDM Channel Profile Stats** in the **Search dashboards by name** field and click the **OFDM Channel Profile Stats** row.

• OFDM OCD and DPD Information

View the OFDM channel OCD and DPD configuration sent through MAC Management Message to CMs on the **OFDM Channel OCD DPD Information** dashboard.

To load this dashboard, click the Cisco Operations Hub main menu button. Choose **Dashboard** to open the **Dashboard** page. Click **Find a Dashboard** to open the search pane. Enter **OFDM Channel OCD DPD Information** in the **Search dashboards by name** field and click the **OFDM Channel OCD DPD Information** row.

View DOCSIS 3.1 Modem Data

You can view the DOCSIS 3.1 modem data through the Cisco cnBR dashboard.

You can use the dashboard to view information on the following:

• **D3.1 Modem Information display**

On the Cisco Operations Hub, click the Cisco Operations Hub main menu button. Choose **Dashboard** to open the **Dashboard** page. Click **Find a Dashboard** to open the search pane. Enter **Cable Modem Verbose** in the **Search dashboards by name** field and click the **Cable Modem Verbose** row to open the **Cable Modem Verbose** dashboard.

The **Modem Other Info** and **Modem OFDM Info** tables display information specific to D3.1.

• **OFDM Profile Stats**

On the Cisco Operations Hub, click the Cisco Operations Hub main menu button. Choose **Dashboard** to open the **Dashboard** page. Click **Find a Dashboard** to open the search pane. Enter **Cable Modem OFDM Profile Stats** in the **Search dashboards by name** field and click the **Cable Modem OFDM Profile Stats** row to open the **Cable Modem OFDM Profile Stats** dashboard.

The profile stats information from each D3.1 modem is available.

DEPI Latency Measurement

DEPI Latency Measurement (DLM) measures the delay and latency of the packets traversing through the Converged Interconnect Network (CIN) from Cisco cnBR to the RPD.

DLM configuration has three parameters: staticDelay, interval, and updateMap. Without any DLM configuration, the network delay uses 500 microseconds (μs) as default value for the calculation of Map Advance Time. When you configure staticDelay with nonzero value, it replaces the default network delay in Map Advance Time. When you configure the interval with nonzero value, DLM starts to send the packets from Cisco cnBR to RPD and calculate the downstream path CIN delay. You can use the CIN delay measurements from DLM to display or debug. When you set updateMap to true, and statiDelay configuration is absent or 0, you can also use the CIN delay measurements to replace the network delay time and adjust the DOCSIS MAP Advance Time. When the DLM is disabled, the network delay restores to the default value of 500 μs.

The DLM calculated delay is valid if it falls in the range of 30 μs and 100 ms. The valid DLM delay replaces the network delay when it is enabled. Subsequent ongoing update to the network delay happens only when the difference between the old and new value is larger than 75 μs. The following table summarizes how the map advance time can be affected based on the parameters in the table.

This table summarizes how the map advance time can be affected based on the parameters in the table.

DLM staticDelay	DLM interval	DLM updateMap	DLM measuring CIN delay	Map Advance Network Delay
Absent or zero	Absent or zero	true or false	No	500 μs (default)
Nonzero	Absent or zero	true or false	No	staticDelay (configured)
Nonzero	Nonzero	true or false	Yes	staticDelay (configured)
Absent or zero	Nonzero	false (display only)	Yes	500 μs (default)
Absent or zero	Nonzero	true	Yes	DLM calculated delay

Configure DLM

DLM is configured in the Service Group configuration. Because DLM measures CIN delay to RPD, it is set for each RPD.

Configure DLM using AutoDeployer script

In the AutoDeployer script SG template file, you can add `netDelayCfg` block to `rpdCfg` block to enable DLM. The SG template configuration applies to all service groups on the Cisco cnBR. See Configure Cisco cnBR Using Autodeployer, on page 43 for additional information.

```
"rpdCfg": {
    "rfTopology": {
        ......
    },
    "netDelayCfg": {
        "staticDelay": 1000,
        "dlmCfg": {
            "interval": 10,
            "updateMap": true
        }
    }
}
```

Update the DLM Configuration using AutoDeployer Reconfigure (Preferred)

After the initial DLM configuration during the deployment using the AutoDeployer, you can update the configuration by modifying the `netDelayCfg` block in the SG template and running the AutoDeployer configuration script again.

Note The system first deletes all the RPDs/SGs and then adds them back when you rerun AutoDeployer configuration.

Update DLM configuration using cnBR Manager

After the initial DLM configuration during the deployment using the AutoDeployer, you can also update the configuration through the cnBR Manager **Core Management** window.

Step 1 On the Cisco Operations Hub, click the Cisco Operations Hub main menu button.

Step 2 Choose **cnBR Manager** > **cnBRs** to open the **cnBR Clusters** page.

Step 3 Click **Import & Export cnBR** to open the **Export/Import** page.

Step 4 In the **Export cnBR Configuration** section, from the drop-down list, choose the Cisco cnBR that manages the RPD.

Step 5 Click the **Export** button to retrieve the current SG configuration of the selected Cisco cnBR.

Step 6 Update one or more parameters in the `netDelayCfg` section of the SG configuration to the desired configuration.

Step 7 Save the updated file on the local disk.

Step 8 In the **Import cnBR Configuration File** pane, from the drop-down list, choose the Cisco cnBR to update.

Step 9 Click **Browse** to locate the file which you updated (saved at Step 5).

Step 10 Click **Import** to push the updated SG configuration to the RPD.

Step 11 Delete the RPD and add the RPD again for the updated SG configuration to take effect.

For more details, see RPD Operations, on page 300.

Configuration Parameters

This table lists and describes DLM configuration parameters.

Field Name	Description	Type	Enforcement
Interval	The interval of sending request packets to RPD and performing the delay calculation by DLM	Integer, 1 ~ 420, in second	Default is 0 and it means that DLM is disabled by default
UpdateMap	If the StaticDelay value is not set, determine if DLM calculated delay is used to update network delay portion of Map Advance.	Bool	Default is false and it means that DLM does not update Map Advance. Set it to true, and clear the StaticDelay, for DLM to update Map Advance after DLM delay calculation

Field Name	Description	Type	Enforcement
StaticDelay	Use static delay to set the network delay portion of the MAP advance. If set, the dynamically calculated delay value is not used even if the UpdateMap flag is set to true.	Integer, 30 ~ 100000, in µs	Default is 0 and it means that there is no static delay to update map advance

Monitor DLM Information

You can find the DLM summary and related plots in two DLM display panels in cnBR Manager.

This table lists and describes the fields in the DLM Summary table.

Field Name	Description	Type
cnBR Name	Cisco cnBR cluster name.	Name string
cnBR ID	Cisco cnBR cluster address.	IPv4/IPv6 address
SG Name	The name of the service group for the RPD.	Name string
SG ID	The Service Group identifier.	Integer
RPD ID	The MAC address of the RPD. This RPD is part of the Service Group with the preceding SG ID.	MAC address
Interval	Configured DLM interval.	Integer, in seconds
Channel	DS channel ID where DLM packet is sent.	Integer, index
Delay	The most recent time delay calculated by DLM.	Integer, in µs
Jitter	The most recent time jitter calculated by DLM.	Integer, in µs
Transaction	The transaction ID of the most recent DLM request packet sent from Cisco cnBR.	Integer, index
Refresh Count	The number of times the DLM updates Map Advance network delay.	Integer, Counter

Click RPD ID to enter the DLM verbose display panel.
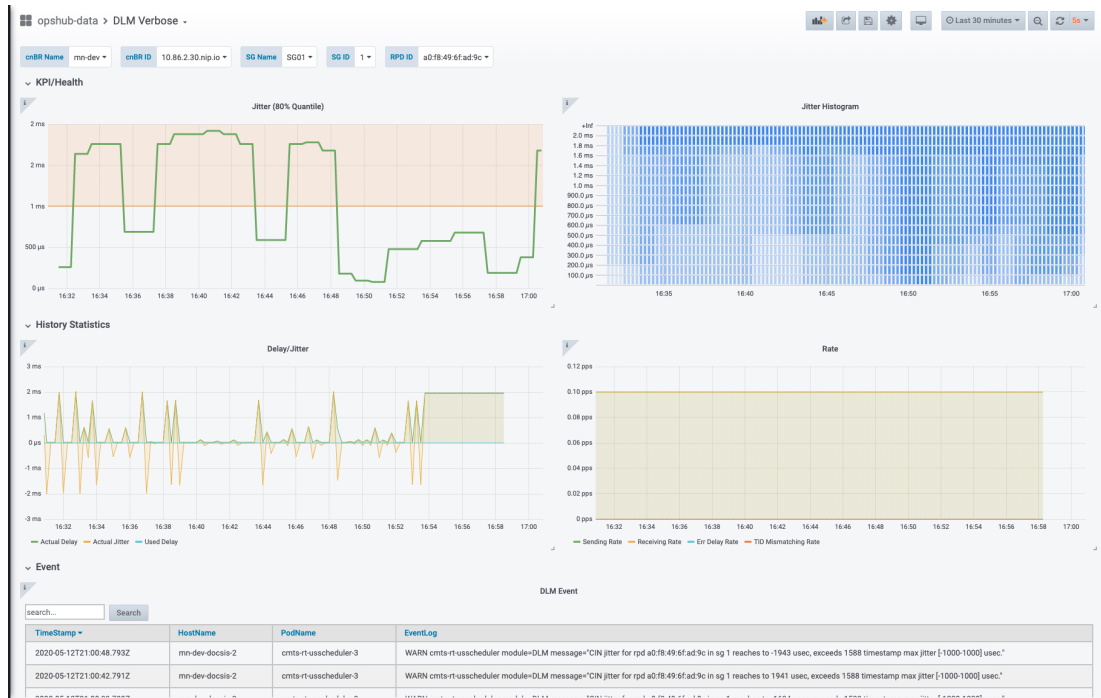
- Jitter Health: Jitter graph and histogram are in the top of the DLM verbose display panel.

- Latency History Statistics

  - Delay/Jitter

    This table lists and describes the fields in the Jitter section of DLM Verbose dashboard.

Field Name	Description	Type
Actual Delay	The actual delay calculated by DLM over time	Integer, in μs
Actual Jitter	The actual jitter calculated by DLM over time	Integer, in μs
Used Delay	The average delay used to update map advance	Integer, in μs

  - Rate

    This table lists and describes the fields in the Rate section of DLM Verbose dashboard.

Field Name	Description	Type
Sending Rate	Sending rate of the DLM request packets from cnBR	Rate, unit is pps.
Receiving Rate	Receiving rate of the DLM response packets from RPD	Rate, unit is pps.
Err Delay Rate	Receiving rate of the DLM response packets with abnormal timestamp from RPD	Rate, unit is pps.

Field Name	Description	Type
TID Mismatching Rate	Receiving rate of the DLM response packets with abnormal transaction id from RPD	Rate, unit is pps.

- DLM Event: The warning events from DLM are listed in the bottom of the DLM verbose display panel.

DOCSIS Set-Top Gateway

This table lists the features and the releases in which the feature was introduced and gives a small description of the feature.

Table 33: Feature History

Feature Name	Release Information	Feature Description
DOCSIS Set-Top Gateway	Cisco cnBR 20.3	DOCSIS Set-top Gateway (DSG) allows the configuration and transport of out-of-band (OOB) messaging. OOB messaging occurs between a set-top controller (or application server) and the customer premise equipment (CPE).

DOCSIS Set-top Gateway (DSG) allows the configuration and transport of **out-of-band (OOB) messaging**. OOB messaging takes place between a set-top controller (or application servers) and the customer premise equipment (CPE). DSG is not intended for the delivery of programming content.

The following figure depicts a typical DSG topology over a Cisco cnBR system.

Figure 29: Typical DSG Topology over a Cisco cnBR System
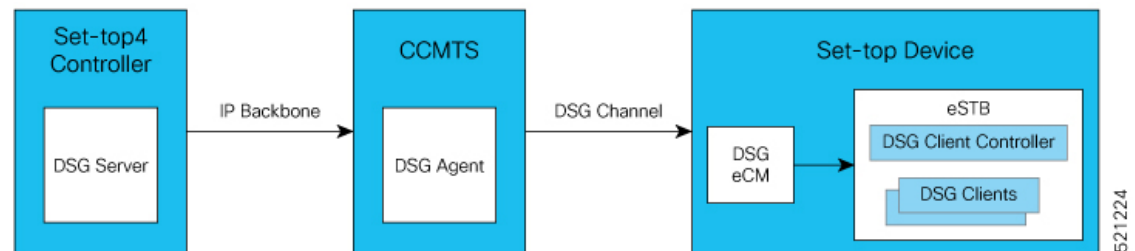
DSG has the following components:

- **DSG Server**: DSG Server is any server (such as an application server or other network attached device) that provides content that is transported through the DSG Tunnel to the DSG Client.

- **DSG Agent**: The DSG Agent is the implementation of the DSG protocol within the Cisco cnBR. DSG Agent creates the DSG Tunnel, places content from the DSG Server into the DSG Tunnel, and sends the DSG Tunnel to the DSG Client.

- **DSG eCM (Embedded Cable Modem)**: A DSG eCM is a DOCSIS cable modem that is embedded into a set-top device and includes DSG functionality.

- **DSG Client Controller**: DSG Client controller is the component of a set-top device that handles the processing of Downstream Channel Descriptor (DCD) messages and decides the forwarding of DSG tunnels within the set-top device.

- **DSG Client**: The DSG Client terminates the DSG Tunnel and receives content from the DSG Server. There may be more than one DSG client within a set-top device.

Configure DSG

You can configure DSG using the Day1 deploy script. You can also configure DSG by importing the Cisco cnBR configuration YAML file to the target Cisco cnBR using cnBR Manager. Using this configuration method overwrites the existing configuration and activates the new configuration. The following is an example configuration for DSG. Add separate DSG configuration entries in the MAC Domain (MD) configuration. See DSG Configuration in MAC Domain (MD), on page 175.

The following example is a sample DSG Configuration.

```
"dsg":
    {
        "cfr": [
            {
              "Id": 1,
              "enable": true,
              "DestIp": "203.0.113.10",
              "DestPortStart": 1,
              "DestPortEnd": 65530,
              "Priority": 1
            },
            {
              "Id": 2,
              "enable": true,
              "DestIp": "203.0.113.2",
              "Priority": 1
            }
        ],
        "chanList": [
            {
              "Id": 1,
              "Chans": [
                {
                  "Id": 1,
                  "Freq": 753000000
                },
                {
                  "Id": 2,
                  "Freq": 765000000
                }
              ]
            }
        ],
        "clientList": [
            {
              "Id": 1,
              "Clients": [
                {
                  "Id": 1,
                  "CaSystemId": "701"
                }
              ]
            },
            {
```

```
              "Id": 2,
              "Clients": [
                {
                  "Id": 1,
                  "Broadcast": "2"
                }
              ]
          },
      ],
      "dseh": true,
      "nameUpdateInterval": 0,
      "tg": [
          {
              "Id": 1,
              "Tunnel": [
                1
              ]
          },
          {
              "Id": 2,
              "Tunnel": [
                2
              ]
          }
      ],
      "tunnel": [
          {
              "Id": 1,
              "MacAddr": "00:53:00:00:00:01",
              "ClientList": 1,
              "Cfr": [
                1
              ]
          },
          {
              "Id": 2,
              "MacAddr": "00:53:00:00:00:02",
              "ClientList": 2,
              "Cfr": [
                2
              ]
          }
      ],
      "timer": [
          {
              "Id": 1,
              "Timeout": [
                2,
                30,
                35,
                60
              ]
          }
      ],
      "vendorParam": [
          {
              "Id": 1,
              "Vendor": [
                {
                  "Id": 1,
                  "Oui": "ce"
                }
              ]
          }
```

```
                ]
            }
```

Configure DSG from Autodeployer

In the Autodeployer script SG template file, the DSG configuration is in the "dsg" section. Some DSG configuration is also present in the "md" section. See example configurations in the preceding section. See Configure Cisco cnBR Using Autodeployer for additional information.

Update DSG Configuration Using Autodeployer Re-Configuration (Preferred)

You can update the DSG configuration by modifying the DSG-related blocks in the SG template and rerunning the autodeployer configuration script. Use this method to update the configuration after the initial configuration of DSG during the deployment using autodeployer.

Note Rerunning autodeployer configuration deletes and readds all the RPDs/SGs.

Update DSG Configuration Using cnBR Manager

After the initial configuration of DSG made during the deployment using autodeployer, you can update the configuration using the cnBR Manager **cnBRs** interface.

Step 1	On the Cisco Operations Hub, click the Cisco Operations Hub main menu button.
Step 2	Choose **cnBR Manager** > **cnBRs** to open the **cnBR Clusters** page.
Step 3	Click **Import & Export cnBR** to open the **Export/Import** page.
Step 4	In the **Export cnBR Configuration** section, from the drop-down list, choose the required Cisco cnBR to update.
Step 5	Click **Export** to get the current SG configuration of the selected Cisco cnBR.
Step 6	Update the parameters in the **dsg** and **md** sections of the SG configuration.
Step 7	Save the updated configuration file on the local disk.
Step 8	In the **Import cnBR Configuration File** pane, from the drop-down list, choose the Cisco cnBR to update.
Step 9	Click **Browse** to locate the file which you updated (saved at Step 5).
Step 10	Click **Import** to upload the updated SG configuration to the selected Cisco cnBR.

Configuration Parameters

All configurations of DSG are not mandatory. The mandatory configurations are dsg client-list, dsg classifier, dsg tunnel, and dsg tunnel-group. The optional configuration details include timer, vendor parameters, DSG channel lists, DSEH, and name-update-interval.

DSG Clients

Use dsg client-list to configure the DSG downstream channel list on a Cisco cnBR. This configuration is mandatory.

This table lists and describes the parameters in DSG `clientList` configuration.

Field Name	Description	Type	Enforcement
id	DSG client list ID	Integer	Required
clients	DSG client entry	Array	Required
clients.id	DSG client ID index for the client list	Integer	Required
clients.caSystemId	DSG client type CA system ID	String	Optional
clients.macAddr	DSG client type MAC address	string[]	Optional
clients.applicationId	DSG client type Application ID	String	Optional
clients.broadcast	DSG client type broadcast	String	Optional
clients.vendorParam	DSG vendor parameters group ID	Integer	Optional

```
"clientList": [
    {
        "id": 0,
        "clients": [
            {
                "id": 0,
                "caSystemId": "701",
                "macAddr": [
                    "00:53:00:00:00:02"
                ],
                "applicationId": "0",
                "broadcast": "2",
                "vendorParam": 0
            }
        ]
    }
]
```

DSG Classifier

Add the DSG classifiers, with optional support for the DCD parameter. This configuration is mandatory.

This table lists and describes the parameters in DSG `cfr` (DSG Classifier) configuration.

Field Name	Description	Type	Enforcement
id	DSG classifier ID	Integer	Required
enable	Enable DSG classifier	Boolean	Required
destIp	Destination IP address	String	Required
srcIp	Source IP address	String	Optional
srcIpMask	Source IP mask	String	Optional
destPortStart	Destination TCP/UDP port start	String	Optional
destPortEnd	Destination TCP/UDP port end	Integer	Optional
srcPortStart	Source TCP/UDP port start	String	Optional
srcPortEnd	Source TCP/UDP port end	Integer	Optional

Field Name	Description	Type	Enforcement
priority	Classifier priority	Integer	Optional

```
"cfr": [
        {
            "id": 0,
            "enable": true,
            "destIp": "203.0.113.2",
            "srcIp": "192.0.2.12",
            "srcIpMask": "255.255.255.0",
            "destPortStart": 0,
            "destPortEnd": 0,
            "srcPortStart": 0,
            "srcPortEnd": 0,
            "priority": 0
        }
    ]
```

Tunnel

Add DSG tunnel and associate a client-list ID to it. This configuration is mandatory.

This table lists and describes the parameters in DSG `tunnel` configuration.

Field Name	Description	Type	Enforcement
id	DSG tunnel ID	Integer	Required
macAddr	DSG tunnel MAC address	String	Required
clientList	DSG client list ID	Integer	Required
cfr	DSG classifier	integer[]	Required

```
"tunnel": [
    {
        "id": 0,
        "macAddr": "00:53:00:00:00:02",
        "clientList": 0,
        "cfr": [
            0
        ]
    }
]
```

Tunnel Group

Add a DSG tunnel group and associate a tunnel to it. This configuration is mandatory.

This table lists and describes the parameters in DSG `tg` (Tunnel Group) configuration.

Field Name	Description	Type	Enforcement
id	User-defined DSG tunnel group ID	Integer	Required

Field Name	Description	Type	Enforcement
tunnel	DSG tunnel IDs defined in the "tunnel group" API	integer[]	Required

```
"tg": [
    {
        "id": 0,
        "tunnel": [
            0
        ]
    }
]
```

Timer

Configure a DSG timer if necessary. Define different timeouts in seconds for Init, Operational, Two-Way, and One-Way. The timer configuration is optional. However, if you define a DSG timer, all the fields are mandatory.

This table lists and describes the parameters in DSG `timer` configuration.

Field Name	Description	Type	Enforcement
id	User-defined DSG timer ID	Integer	Required
timeout	DSG timeout in seconds[Init,Operational,Two-Way,One-Way]	integer[]	Required

```
"timer": [
    {
        "id": 0,
        "timeout": [
            2,
            30,
            35,
            60
        ]
    }
]
```

Vendor Parameters

Configure the DSG vendor-specific parameters if necessary. This configuration is optional. However, if you define vendor-specific parameters, all the fields are mandatory.

This table lists and describes the parameters in DSG `vendorParam` (Vendor Parameters) configuration.

Field Name	Description	Type	Enforcement
id	DSG vendor parameters ID	Integer	Required
vendor	DSG vendor parameters entry	Array	Required
vendor.id	DSG vendor parameters vendor index	Integer	Required
vendor.oui	DSG vendor parameters vendor OUI	String	Required

Field Name	Description	Type	Enforcement
vendor.value	DSG vendor parameters vendor value	String	Required

```
"vendorParam": [
  {
    "id": 0,
    "vendor": [
      {
        "id": 0,
        "oui": "ce",
        "value": "0"
      }
    ]
  }
]
```

DSG Channel List

Configure a DSG channel list if necessary. This configuration is optional. However, if you define a DSG channel list, all the fields are mandatory.

This table lists and describes the parameters in DSG `chanList` (DSG Channel List) configuration.

Field Name	Description	Type	Enforcement
id	DSG channel list ID	Integer	Required
chans	DSG channel frequency entry	Array	Required
chans.id	DSG channel frequency entry index	Integer	Required
chans.freq	DSG channel frequency	Integer	Required

```
"chanList": [
  {
    "id": 0,
    "chans": [
      {
        "id": 0,
        "freq": 0
      }
    ]
  }
]
```

Other Parameters

NameUpdateInterval: This parameter is the interval in minutes to update the fully-qualified domain name (FQDN) classifiers on a Cisco cnBR based on the DNS server record. The valid range is 1–60.

Dseh: Downstream Service Extended Header: This parameter is a boolean value indicating whether the DSG tunnels use DS-EH.

This table lists and describes other parameters in DSG configuration.

Field Name	Description	Type	Enforcement
NameUpdateInterval	Interval in minutes to check the DNS server for any FQDN classifier changes	Integer	Optional
Dseh	Boolean value indicating if DSG tunnels use the DS-EH (Downstream Service Extended Header)	Boolean	Optional

DSG Configuration in MAC Domain (MD)

Add DSG configuration to the MD configuration. The tunnel-group (tg) parameter is mandatory. Other values in the DSG field are optional. Associate the DSG tunnel group to the mac-domain.

This table lists and describes the parameters under `dsg` in MAC Domain configuration.

Field Name	Description	Type	Enforcement
channelList	DSG channel list ID defined in the 'channel list' API	Integer	Optional
dcdDisable	Disable DSG DCD	integer[]	Optional
tg	DSG tunnel groups in the 'tunnel group' API	integer[]	Required
timer	DSG timer ID in the 'DSG timer' API	Integer	Optional
vendorParam	DSG vendor parameters ID in the 'channel list' API	Integer	Optional

```
"dsg": {
    "channelList": 0,
    "dcdDisable": [
        0
    ],
    "tg": [
        0
    ],
    "timer": 0,
    "vendorParam": 0
}
```

SP Router Configuration

To set up an SP router, perform the following steps:

Step 1   Enable ip multicast-routing distributed.

Step 2   Enable **ip pim spare-dense-mode** and **ip igmp version 3** on the BVI Interface for Multinode cnBR.

Step 3   Configure static IGMP corresponding to DSG **cfr** groups and sources, on the BVI Interface for Multinode cnBR.

Example

The following example is a sample configuration. The actual configuration may vary depending on the type and version of the router.

```
multicast-routing
address-family ipv4
interface BVI1005
 enable
!
interface Loopback0
 enable
!
!
!
router igmp
interface BVI1005
static-group 233.1.1.1
version 3
!
!
router pim
address-family ipv4
interface BVI1005
 enable
!
interface Loopback0
 enable
!
!
!
```

Policy-based Load Balancing

This table lists the features and the releases in which the feature was introduced and gives a small description of the feature.

Table 34: Feature History

Feature Name	Release Information	Feature Description
Policy-based Load Balancing	Cisco cnBR 20.4	Enables each service group (SG) to manage traffic based on the weight assigned to the SG.

Policy-based load balancing enables each service group (SG) to manage traffic based on the weight assigned in the configuration file. Policy-based load balancing assigns a weight to the SG to determine how much network traffic it can handle.

By default, the service groups are given a static traffic rate for both downstream and upstream traffic. The weight is an integer between 1 and 4 with the default value of 1. An SG with weight 4 can handle 4 times the traffic of the default load. Each data-plane pod can hold up to 4 total weight.

Configure Policy-Based Load Balancing Using Operations Hub

Different SG templates are required for configuring different weights on SGs.

Step 1 To enable policy-based load balancing, add `sgWeight` key to a new or existing template in the Cisco Operations Hub.

```
"sgWeight": 2,
```

For information on how to add SG configuration, see Add Service Group Configuration to cnBR, on page 67.

Step 2   Create a new SG and apply the appropriate SG template.

When updating an existing SG, delete the existing SG first and then add the SG with the new template.

For information on how to add or delete SGs, see RPD Operations, on page 300.

Configure Policy-based Load Balancing Using AutoDeployer

To enable policy-based load balancing, add `sgWeight` key in the AutoDeployer script SG template file.

```
"sgWeight": 2,
```

Different SG templates are required for configuring different weights on SGs. When updating the weight for an existing SG, the AutoDeployer script deletes and adds the SG.

For more details, see Configure Cisco cnBR Using Autodeployer, on page 43.

Dynamic Load Balancing

This table lists the features, the releases in which each feature was introduced, and gives a small description of each feature.

Table 35: Feature History

Feature Name	Release Information	Feature Description
Dynamic Load Balancing	Cisco cnBR 21.3	Cisco cnBR supports downstream Dynamic Load Balancing (DLB). The purpose of DLB is to balance utilization of downstream channels within the SG using configurable thresholds. You can balance the load on downstream channels and optimize channel bandwidth usage.

Cisco cnBRCisco cnBR supports downstream Dynamic Load Balancing (DLB). The purpose of DLB is to balance utilization of downstream channels within the SG using configurable thresholds. The Cisco cnBR identifies the cable modems with the highest downstream throughput that are bonded to channels with the highest utilization. The Cisco cnBR then moves these cable modems to channels with lower utilization using the Dynamic Bonding Change (DBC) operation.

DLB operates for downstream SC-QAM channels only. The Cisco cnBR does not consider utilization of OFDM downstream channels in the DLB algorithm. For DOCSIS 3.1 cable modems, DLB uses throughput on SC-QAM channels only when determining the total throughput. This design allows balanced utilization of the SC-QAM channels, while fully utilizing OFDM channels. DLB moves only DOCSIS 3.0 and DOCSIS 3.1 cable modems. There are certain exclusion criteria that prevents moving cable modems—An in progress DSX/DBC transaction, active voice traffic, or L2vpn traffic.

DLB is disabled by default. You can enable DLB for each SG by updating the configuration in the dlb block at for each SG.

Dynamic Load Balancing: Configuration

Dynamic Load Balancing (DLB) is disabled by default. The configuration is in the dlb block at the SG level. Add the dlb configuration block to the SG Template for configuration.

```
"dlb":
{
  "enable": true,
  "interval": 60,
  "loadMaxThresh": 80,
  "loadMinThresh": 20,
  "cmSuccessHoldTime": 30,
  "cmFailureHoldTime": 120
},
```

The following table provides information about each configuration parameter:

This table lists information about each configuration parameter, the default values, minimum and maximum values, unit, and type of the parameter.

Table 36: DLB Parameters

Parameter	Default	Min	Max	Units/Type
enable	False	N/A	N/A	Boolean
interval	60	10	600	Seconds / Integer
loadMaxThresh	80	1	100	Percentage / Integer
loadMinThresh	20	1	100	Percentage / Integer
cmSuccessHoldTime	30	1	1440	Minutes / Integer
cmFailureHoldTime	120	1	1440	Minutes / Integer

The following list describes each parameter in the previous table.

- enable: Use this Boolean parameter to turn on DLB for this SG.

- interval: This parameter is the interval (in seconds) between each time DLB wakes up. DLB scans channel utilization and cable modem throughput to determine if any cable modems require a move.

- loadMaxThresh: This parameter defines the necessary channel utilization threshold for DLB to attempt to balance utilization. For example, assume loadMaxThresh is 80, but the channel with the highest utilization in the SG is below 80% utilization. In this case, DLB performs no action.

- loadMinThresh: This parameter defines the channel utilization threshold the Cisco cnBR uses to find an underutilized channel. The Cisco cnBR compares loadMinThresh to loadMaxThresh to calculate the loadVarianceThreshold (loadMaxThresh - loadMinThresh = loadVarianceThreshold). If the utilization difference between the most utilized channel and the least utilized channel is less than loadVarianceThreshold, DLB performs no action.

- cmSuccessHoldTime: This parameter defines the time (in minutes) before which DLB attempts a new DBC operation on a cable modem after the last successful DBC operation.

- cmFailureHoldTime: This parameter defines the time (in minutes) before which DLB attempts a new DBC operation on a cable modem after the last failed DBC operation.

There are some additional restrictions on the configuration of these parameters:

- loadMaxThresh must not be less than, or equal to, loadMinThresh.

- loadMaxThresh - loadMinThresh must not be less than five.

DLB handles any invalid configuration using default values for invalid parameters.

After the initial configuration during deployment using the Autodeployer, you can update the DLB configuration using the cnBR Manager.

Use the following procedure to update the configuration:

- Add Service Group Configuration to cnBR

- Edit RPDs

Dynamic Load Balancing: Channel Selection

Dynamic Load Balancing (DLB) runs at a fixed interval that you configure using the interval parameter. DLB starts collecting channel utilization data for all downstream channels in the Service Group (SG). DLB stores this information as a utilization percentage for each SC-QAM channel. DLB does not consider the utilization for OFDM channels. The list of all channels in the SG is then sorted by utilization percentage in descending order.

DLB then finds the difference in utilization between the channels with the highest and lowest utilizations. This difference is the utilization variance.

```
Utilization_Variance = Highest_Utilization - Lowest_Utilization
```

DLB compares the utilization variance to the utilization variance threshold. The utilization variance threshold is the difference between the configured loadMaxThresh and loadMinThresh for the SG.

If the utilization variance is greater than or equal to the utilization variance threshold, DLB acts on the SG. Otherwise DLB takes no action and waits until the next interval.

```
Utilization_Variance = Highest_Utilization - Lowest_Utilization
```

If DLB acts on the SG, it iterates through the sorted channels list. If a channel's utilization is above the configured loadMaxThresh, then DLC proceeds to select CMs that are bonded to that channel. If DLB tries to move a cable modem by DBC on this channel, DLB processes no further channels during this interval. DLB moves at most one cable modem per interval.

Dynamic Load Balancing: Cable Modem Selection

When Dynamic Load Balancing (DLB) acts on an SG, DLB finds the channel with the highest utilization in the SG. Next, DLB creates a list of cable modems that are bonded to this channel.

Then DLB calculates the Receive Channel Set (RCS) average utilization for each cable modem on the list. The cable modem list is then sorted by RCS average utilization in descending order. If two cable modems have the same RCS average utilization, DLB sorts the modems in descending order of the cable modem downstream throughput.

Now DLB iterates through the final sorted cable modem list. For candidate modems, DLB generates a Target RCS based on:

- The channel utilization of all channels in the SG

- Any restrictions the cable modem may have.

- There are several criteria that prevents the selection of cable modems for a DBC move. They are:

- If the previous successful DBC operation for the modem occurred within the cmSuccessHoldTime window.

- If the previous failed DBC operation for the modem occurred within the cmFailureHoldTime window.

- If the Target RCS average utilization of the cable modem is not a significant improvement over the current RCS average utilization.

- If the Target RCS of the cable modem fails cto pass the RCS Ping Pong check. For example, this check could fail due to the Target RCS matching the cable modem's previous Source RCS.

If a cable modem passes these criteria, DLB performs a DBC operation to the new Target RCS.

Dynamic Load Balancing: Dashboard

You can use the cnBR Manager to monitor DLB activity for each SG by opening the Dynamic Load Balance dashboard. The dashboard displays the following information:

- Current Channel Load: Real-time channel utilization percentage for all downstream channels in the SG.

- Channels Load Trend: Channel utilization percentage for all downstream channels in the SG over the last hour.

- Max and Min Load Difference: The utilization variance over the last hour.

- LB Movement History: A list of the most recent cable modems to have been moved by using DBC.

  - Cable Modem: MAC Address of the cable modem moved by DBC

  - Mac Domain: Mac Domain of this cable modem

  - Source RCS: The original RCS of this cable modem

  - Target RCS: The RCS selected by DLB to reduce average channel utilization

  - Result: Whether the DBC operation was successful or failed

  - Time: cnBR relative timestamp of when the DBC operation took place

Voice

Cisco cnBR provides voice communication capabilities over cable networks.
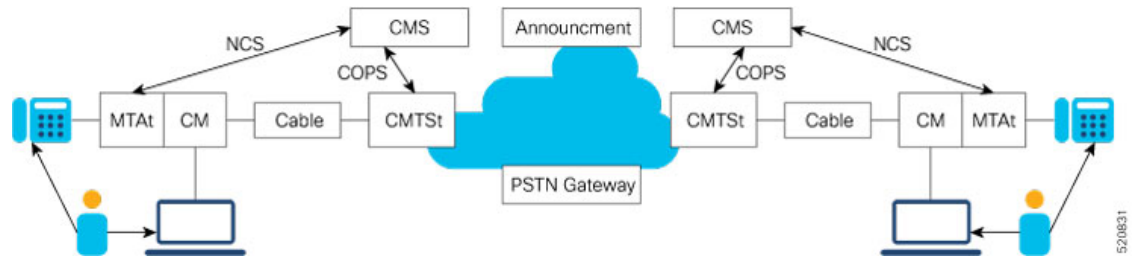
Packetcable

Packetcable is a set of protocols developed to deliver Quality of Service (QoS) enhanced communications services using packetized data transmission technology to your home over the cable network.

Packetcable 1.5 is an enhanced version of packetcable protocols from Packetcable 1.0. The following figure shows the basic network topology.

Figure 30: Topology for Packetcable 1.5

Packetcable Configuration Parameters

This table lists the Packetcable configuration parameters and the values the parameters can take.

Parameter	Values	Description	Default Value
pcEnable	True, False	True = Enabled, False = Disabled	True
pcMaxGate	Integer	Maximum gate number allowed in Cisco cnBR	51200
t0Timer	Integer in milliseconds	The period that an allocated gate exists without having the gate parameter set	30000
t1Timer	Integer in milliseconds	The period that an authorized gate exists without having the gate parameter set	200000
sendSubscriberEnable	True, False	If it is True, GateClose and GateSetAck messages include Subscriber ID	False
copsAddrIp	IP address	IP address of CMS	None
copsGwIp	IP address	First hop gateway IP to CMS	None

By default, Packetcable 1.5 is enabled. The following configuration is used to disable the feature or change the timers. Usually, the default configuration is sufficient. For more details of timer parameters, see DQoS1.5 SPEC.

You can configure the Packetcable 1.5 by using the Cisco cnBR Autodeployer YAML file.

```
packetcable :
    {enable:'true', 'max-gate':51200, 't0':30000, 't1':200000, 'subscriber':'false',
'ip':'5.230.205.10', 'gw':'5.230.205.1'}
```

You can also configure the Packetcable 1.5 by using the Configurator as depicted in the following figure:

Figure 31: Configure Packetcable 1.5 using cnBR Manager

cnBR Cluster Configuration

172.25.29.110.nip.io

Packet Cable

Select a node...
☐ ▼ Config {0}
☐   (empty object)

SAVE

Configuration Example   −

```
// packetcable 1.5
{
  "pcEnable": true,
  "pcMaxGate": 51200,
  "t0Timer": 30000,
  "t1Timer": 200000,
  "sendSubscriberEnable": false,
  "copsAddrIp": "80.2.0.9/28",
  "copsGwIp":   "80.2.0.1"
}
```

The **PC DQOS Enabled** field in the Cisco cnBR Manager **Voice Overview** dashboard indicates whether the voice is enabled as shown in the following figure:

Figure 32: PC DQOS Enabled in cnBR Manager

clusterIp   10.124.210.237 ▾   PC DQOS Enabled   true ▾   PC Multimedia Enabled   false ▾   Voice Logging Enabled   false ▾   520833

Cisco Operations Hub Voice Dashboard

The cnBR Manager Voice Dashboards monitor Cisco cnBR Packetcable 1.5 voice features.

Voice Main page

As shown in the following figure, the first part of Voice Main page displays the Packetcable feature enable/disable status, COPS connection status, established call status, and the alerts that are reported by system.

Figure 33: Voice Main Dashboard Part 1
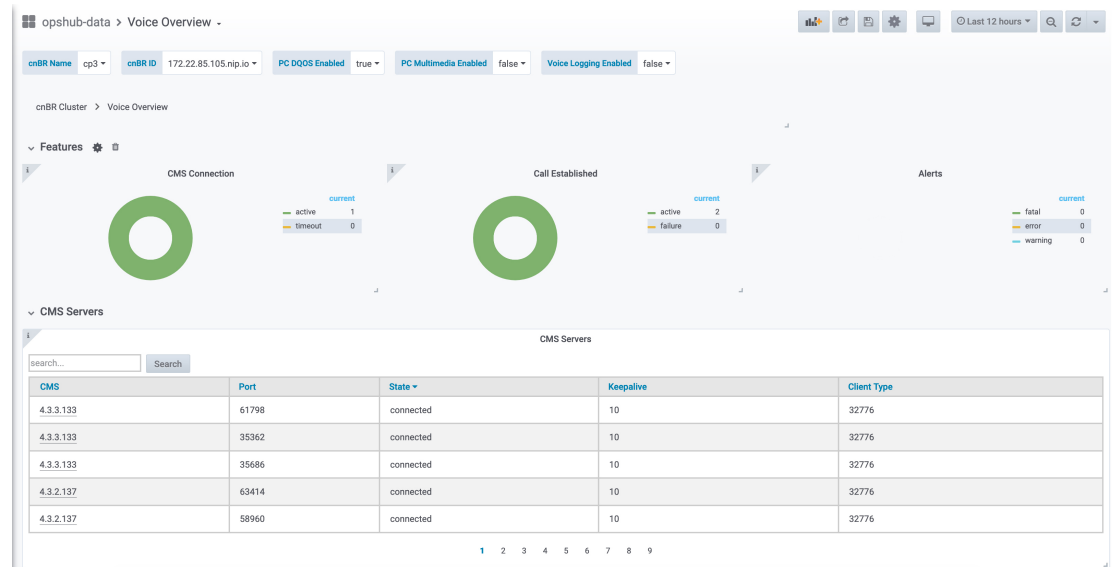
Detailed explanation for components in the preceding figure.

- Pie chart for CMS Connection.

    - active - The counter for CMS connections which are in active status.

    - timeout - The counter for CMS connections which are timeout.

- Pie chart for Call Established.

    - active - The counter for Established Calls which are in active status.

    - failure - The counter for Established Calls which are failure.

- Pie chart for Alert.

    - fatal - Fatal event counter.

    - error - Error event counter.

    - warning - Warning event counter.

- Table for CMS Servers.

    - CMS - Server IP address.

    - Port - Server port.

    - State - Server connection states.

    - Keepalive - Keepalive timer between CMS and Cisco cnBR.

    - Client Type - The client type value (32776 for Packetcable and 32778 for Packetcable Multimedia).

    - You can use **Search...** text box to do fuzzy search in the entire table.

As shown in the following figure, the second part of Voice Main page displays overall call statistics and error logs reported by cmts-app-packetcable container in Cisco cnBR side.

Figure 34: Voice Main Dashboard Part 2
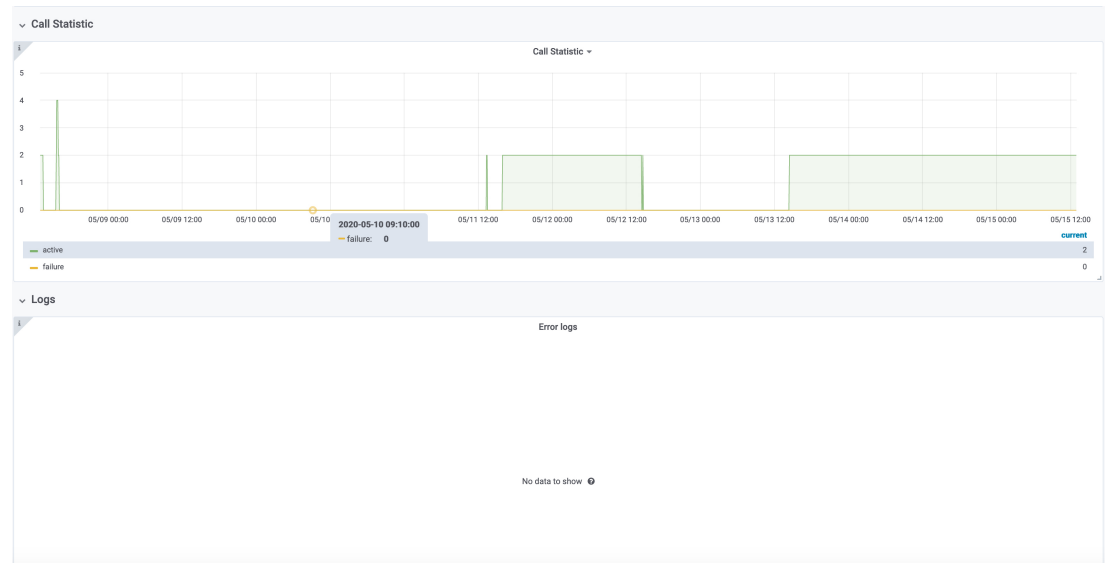
Legends for components in the preceding figure.

- Graph for Call Statistic
    - X-axis - Time.
    - Y-axis - Number of gates.

- Logs
    - Error messages from cmts-app-packetcable container.

Call Status Page

The Call Status page shows current and completed call status, as shown in the following figure:

Figure 35: Call Status Page

Legends for each column of tables in the preceding figure.

- Table for Ongoing Call Status

    - Modem - Modem MAC address.

    - Subscriber - Subscribe's MTA IP address.

    - Start time - The start time for the call.

    - Duration - Call duration.

    - CMS - Call Management Server IP address.

    - Gate ID - Gate identifier.

    - SFID(US) - Service flow ID for upstream.

    - SFID(DS) - Service flow ID for downstream.

- Table for Completed Call Status

    - Modem - Modem MAC address.

    - Subscriber - MTA IP address.

    - Start time - The start time for the call.

    - Stop time - The stop time for the call.

    - Duration - Call duration.

    - CMS - Call Management Server IP address.

    - Gate ID - Gate identifier.

    - SFID(US) - Service flow ID for upstream.

• SFID(DS) - Service flow ID for downstream.

COPS Status Page

The COPS Status page shows the COPS connection status as shown in the following figure:

Figure 36: COPS Status Page
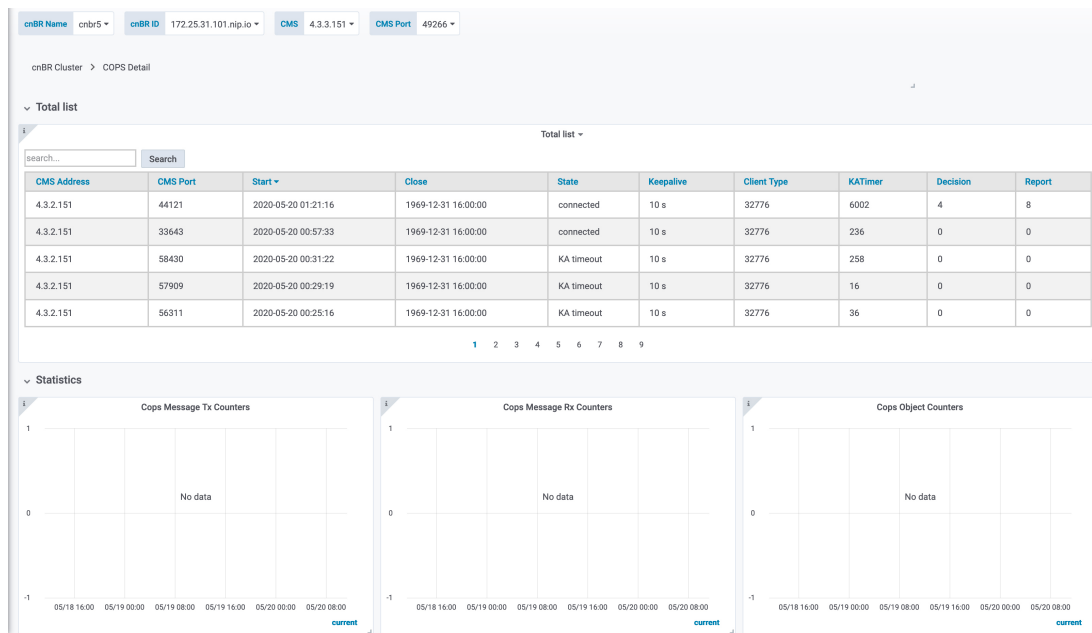
Legends for each table in the preceding figure.

- Table for Total list

    - CMS Address - Call Management Server IP address.

    - CMS Port - Port of the Call Management Server IP address.

    - Start - The start time for CMS connection.

    - Close - The close time for CMS connection.

    - State - The server connection states.

    - Keepalive - The keepalive time for CMS and Cisco cnBR.

    - Client Type - The client type (32776 for Packetcable and 32778 for Packetcable Multimedia).

    - KATimer - The counter for keepalive message.

    - Decision - The counter for COPS decision message.

    - Report - The counter for COPS report-type message.

    - You can use **Search...** text box to do fuzzy search in the entire table.

- COPS Message Tx Counters

• X-axis - Time.

• Y-axis - The counter for each type of COPS Tx Message.

• COPS Message Rx Counters

• X-axis - Time.

• Y-axis - The counter for each type of COPS Rx Message.

• COPS Object

• X-axis - Time.

• Y-axis - The counter for each type of COPS Object.

Service Flow Information

Four dynamic service flows are created to set up a voice path for each two-way call.

One upstream and one downstream service flow are created for each modem in the call.

You can find Service Flow Information for each modem in Downstream Service Flow List or Upstream Service Flow List dashboard.

The Downstream Service Flow List is used as an example in the following figure:

Figure 37: Service Flow List For Specific Modem
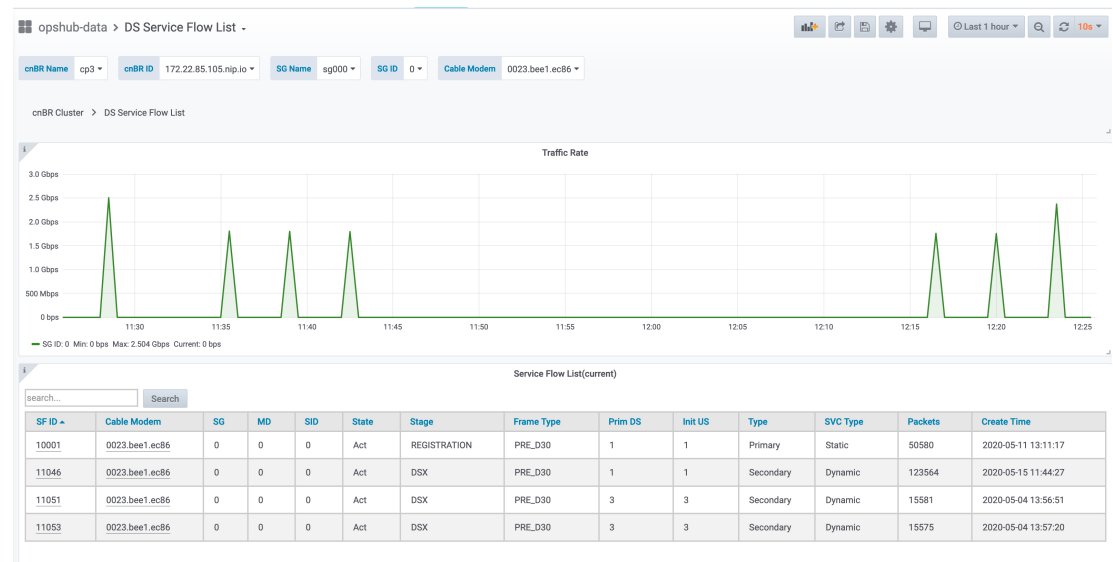
The downstream dynamic service flow created for voice call is listed under Service Flow List table.

Detailed explanations of each column in Downstream Service Flow List table in the preceding figure.

• Table for Downstream Service Flow List

• SF ID - Service Flow ID.

• Cable Modem - MAC Address of the modem.

- SG - Service Group of the modem.

- MD - MAC Domain of the modem.

- State - State of service flow [Prov, Adm, Act].

  - Prov - Service flow is in provision state.

  - Adm - Service flow is in admit state.

  - Active - Service flow is active state.

- Stage - Stage of service flow [PRE_REGISTRATION, REGISTRATION, DSX].

  - PRE_REGISTRATION - Service flow is provisioned before REGISTRATION.

  - REGISTRATION - Service flow is provisioned in REGISTRATION.

  - DSX - Service flow is dynamically provisioned for voice.

- Frame Type - [PRE_D30, CCF_ON, CCF_OFF].

  - PRE_D30 - Pre-3.0 DOCSIS concatenation and fragmentation.

  - CCF_ON - Continuous Concatenation and Fragmentation is enabled.

  - CCF_OFF - Continuous Concatenation and Fragmentation is disabled.

- Prim DS - Primary downstream channel ID.

- Init US - Init upstream channel ID.

- Type - [Primary, Secondary].

- SVC Type - [Dynamic, Static].

  - Dynamic - Service flow is dynamically provisioned.

  - Static - Service flow is statically provisioned.

- Packets - Number of packets.

- Create Timestamp - When the service flow created.

Clicking on the SFID of dynamic flow in above table to redirect to the Downstream Service Flow Verbose page.

The voice traffic throughput data is available in that page, as shown in the following figure:

Figure 38: Downstream Service Flow Verbose Page
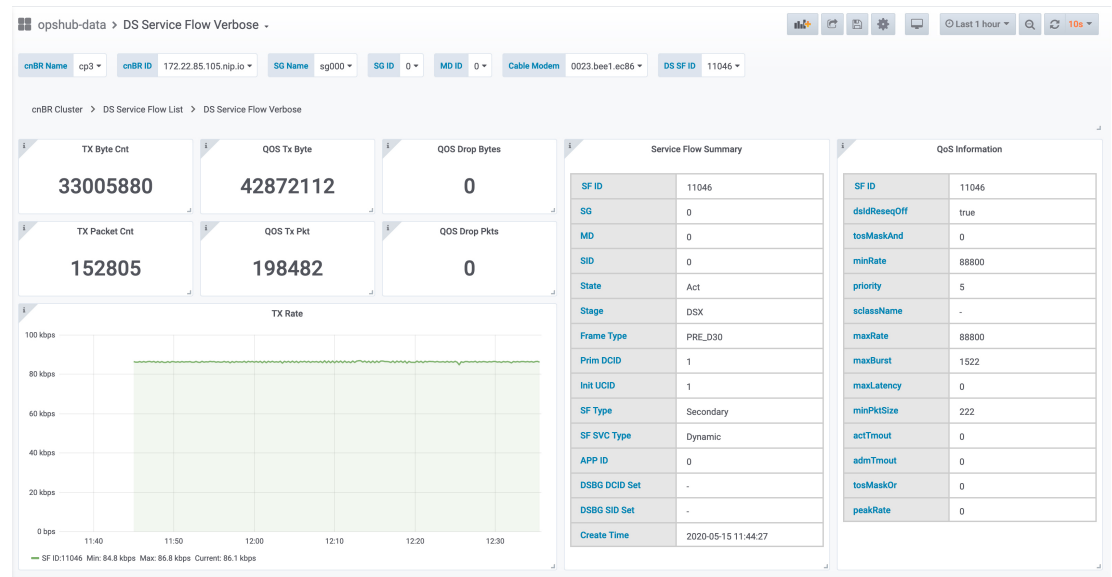
The TX Rate table in the preceding figure shows the downstream traffic throughout for voice.

Legends of relevant tables and counters in the preceding figure.

- Service Flow Traffic Rate

    - X-axis - Time

    - Y-axis - Throughput in kilobit per second

- TX byte cnt is the count of total bytes received by policer.

    - "TX Byte cnt" = "QOS Tx Byte" - "QOS Drop Bytes"

- TX packet cnt is the count of total packets received by policer.

    - "TX Packet Cnt" = "QOS Tx Pkt" - "QOS Drop Pkts"

- QOS TX byte is the count of total bytes sent to policer.

    - "QOS Tx Byte" = "TX Byte cnt" + "QOS Drop Bytes"

- QOS TX pkt is the count of total packets sent to policer.

    - "QOS Tx Pkt" = "TX Packet Cnt" + "QOS Drop Pkts"

- QOS drop bytes are the drop bytes count of policer, includes policer drops, queue full drops, and approximate Fair Drop drops.

    - "QOS Drop Bytes" = "QOS Tx Byte" - "TX Byte cnt"

- QOS drop pkts are the drop packets count of policer, includes policer drops, queue full drops, and approximate Fair Drop drops.

    - "QOS Drop Pkts" = "QOS Tx Pkt" - "TX Packet Cnt"

Video Services

Cisco cnBR provides the control plane to enable Video Services between RPDs and Traffic Engines. Traffic Engines are legacy devices that support only data plane functions. Traffic Engines do not support the L2TPv3 control plane protocol or the GCP protocol. The Cisco cnBR configures static L2TPv3 pseudowires on RPDs so that they can communicate with Traffic Engines. You must configure matching static pseudowires on the Traffic Engines. The Cisco cnBR does not configure the Traffic Engines.

To support Traffic Engines, Cisco cnBR supports the Downstream Video SC QAM channel and pseudowire configuration on RPD.

Video Downstream SC QAM

This table lists the features and the releases in which the feature was introduced and gives a small description of the feature.

Table 37: Feature History

Feature Name	Release Information	Feature Description
Video Downstream SC QAM	Cisco cnBR 21.1	You can configure RPD video QAM and OOB sources (multicast IPv4 or IPv6) without using a cBR-8 or other external video core. This feature allows deployments of Cisco cnBR with RPDs without any third-party devices.

The Cisco cnBR is the DOCSIS principal CCAP core for RPDs. It provides DOCSIS services, but it does not provide video services. There are two ways to support the video services:

- Use a Video Auxiliary CCAP core

- Use Video Traffic Engines

Figure 39: Video Downstream SC QAM Overview
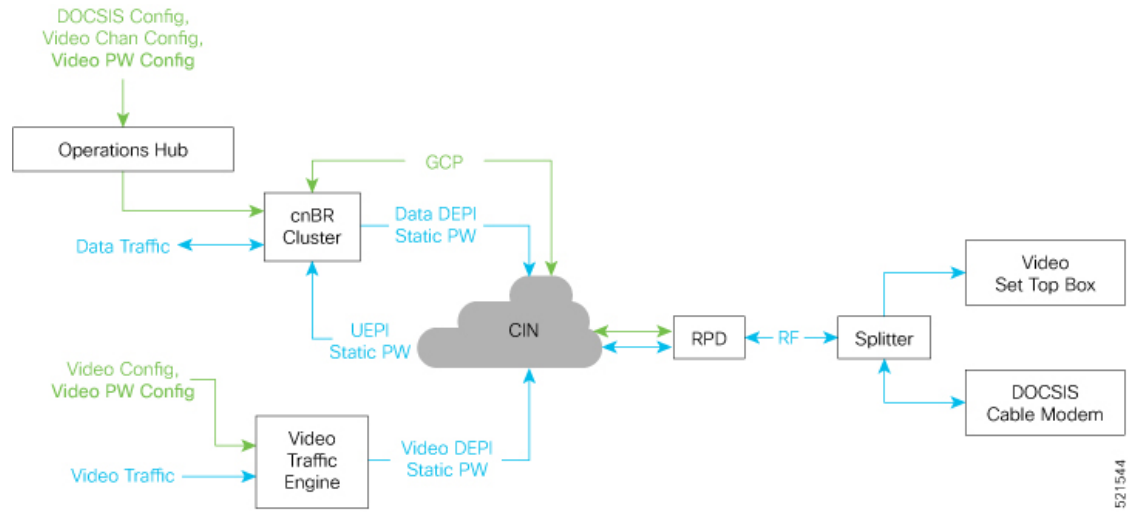
In the preceding diagram, the Video Traffic Engine provides the video service but only supports the data plane function. It encapsulates the downstream MPEG video traffic in a DEPI static pseudowire (PW). Video Traffic Engines do not support Generic Control Protocol (GCP) communication with RPDs.

To support Video Traffic Engines, the Cisco cnBR communicates with RPDs using GCP to configure video Downstream SC QAM channels and associated multicast forward static pseudowires. The Cisco cnBR communicates to the RPD about:

- The static pseudowires that carry a video stream

- The Downstream SC QAM channel that transmits the video stream

The cnBR RPD configuration must be consistent with the Video Traffic Engine configuration:

- The cnBR RPD static pseudowires configuration must match the source IP address, group IP address, and sessionID used by the Video Traffic Engine.

- The cnBR RPD Downstream SC QAM configuration (annex, modulation, and symbol-rate) must be consistent with the bit-rate of the associated video stream from the Video Traffic Engine.

- Configure the cnBR RPD Downstream SC QAM for asynchronous video if the Cisco cnBR and the video Traffic Engine are in different timing domains.

The Cisco cnBR supports the following video services:

- Narrowcast – set of channels that apply to one RPD downstream port or a small group of RPD downstream ports.

  - Video on Demand (VoD)

  - Switched Digital Video

- Broadcast – set of channels that apply to a large group of RPD downstream ports across a geographic area.

An explicit configuration of the type of service is not necessary. You can group a set of channels and assign them to groups of RPD downstream ports. You may have to set a broadcast channel group flag for channels that are associated with multiple downstream ports on an RPD node or shelf.

Configure Video Downstream SC QAM

Configure Video Downstream SC QAM using the cnBR Manager. The configuration involves instantiation of Video Downstream Profile, Video Channel Profile, and Video QAM Template from the cnBR Manager. After defining the Video QAM Template, use the template in the Add RPD or Edit RPD operations to configure the Cisco cnBR and RPDs.

Perform the following steps to configure Video Downstream SC QAM:

Step 1 On the Cisco Operations Hub main menu, click **cnBR Manager > Profiles and Templates**

Step 2 Click **Create** > **Video Downstream Profiles**.

Step 3 Enter a Name and description in the respective text boxes and click **Next**. Configure the values of the parameters as necessary and click **Create**.

Video DS Profile supports the following configuration parameters for DS SC QAM channels:

This table lists and describes the configuration parameters for downstream SC QAM channels that Video downstream profile supports.

Field Name	Description	Type
annex	RF Channel Annex Type. Possible values: AnnexA, AnnexB, or AnnexC	String
interleaver	Interleaver depth of a channel. Possible values: fecI8J16, fecI12J17, fecI16J8, fecI32J4, fecI64J2, fecI128J1, fecI128J2, fecI128J3, fecI128J4, fecI128J5, fecI128J6, fecI128J7, or fecI128J8	String
modulation	QAM modulation for the channel. Possible values: qam256, qam64	String
powerAdjust	Power level adjustment for the channel from base power of the RF downstream port. Value range: −8 to 6 in dB	Integer
channelWidth	RF Channel Width in Hz. Mandatory field for annex value: AnnexA Possible values: 6000000, 7000000, 8000000. Optional field for annex values: AnnexB and AnnexC. AnnexB and AnnexC default to and only support 6000000.	Integer
symbolRate	Number of symbol changes for each unit of time in kilo-symbols/second. Value range: 3500–7000. Mandatory for 'annex' values, AnnexA and AnnexC. Optional and ignored for AnnexB. AnnexB symbol rate is fixed based on QAM modulation.	Integer
spectrumInversion	RF signal spectrum inversion. True: Channel Spectrum is inverted False: Channel Spectrum is not inverted.	Boolean
rfChanType	Mode in which a QAM channel is operating. Possible values: sync, async. The value, sync indicates that channel operates as a synchronous MPEG video channel. The value async, indicates that channel operates as an asynchronous MPEG video channel. Configure the channel for asynchronous video if the cnBR and video Traffic Engine are in different timing domains.	String

Step 4 On the Cisco Operations Hub main menu, click **cnBR Manager > Profiles and Templates >**

Step 5 Click **Create** > **Video Channel Profiles**.

Step 6   Enter a Name and description in the respective text boxes and click **Next**. Configure the values of the parameters as necessary and click **Create**.

Video Channel Profile represents a group of channels that are connected to specific Video Traffic Engine. Video Channel Profile supports following configuration parameters for downstream SC QAM channels.

This table lists and describes the configuration parameters for downstream SC QAM channels that Video Channel Profile supports.

Field Name	Description	Type
broadCastChanGroup	Instruct RPD to include the channel in a Broadcast Channel Group (BCG). When true, RPD adds the channels to a BCG. BCGs group downstream SC-QAM channels from all Downstream RF Ports identified by the same ID in an SG that has broadcastChanGroup set to true. In this case, the channel is associated with multiple downstream ports on an RPD node or shelf. The same content goes to the same channel on each Downstream port for the BCG.	Boolean
idInSGRange	IDs of channels specified as a range. For example: 30–40. Value of channel IDs should be in range 0–157.	String
startSessionId	Unique PW Session Identifier represented in Hexadecimal or Decimal. The startSessionId value is used as SessionId of first channel in idInSGRange. For subsequent channels, SessionId is incremented by 1. Value range: **0x80000001 to 0x8000FFFF**	String
startFrequency	The startFrequency is the center frequency of the first channel in idInSGRange. For subsequent channels, frequency value is incremented based on value of annex and channelWidth of channel.	Integer
groupAddress	Group Address of Video Traffic Engine in IPv4 or IPv6	String
sourceAddress	Source Address of Video Traffic Engine in IPv4 or IPv6	String

Step 7   On the Cisco Operations Hub main menu, click **cnBR Manager > Profile and Templates**

Step 8   Click **Templates** to go to the Templates tab.

Step 9   Click **Create** > **Video DS QAM Templates**.

Step 10   Enter a Name and description in the respective text boxes and click **Next**.

Step 11   Select the **Video DS Profile** and the **Video Channel Profile** created in the previous steps and click **Create**.

Step 12   Perform the Add RPDs operation using Video QAM Template created in the previous step.

Note   You can configure nonconsecutive channel ranges(for example, 0-10,50-60,100) in a single **Video Channel Profile** and use them in a **Video QAM Template**. This ability allows you to configure entire video services in one attempt.

Configure Video Downstream SC QAM Using Autodeployer Script

You can also configure Video Downstream SC QAM using Autodeployer script. See Configure Cisco cnBR Using Autodeployer, on page 43 for additional information.

Out-of-Band Services

The following table provides description of the various Out-of-Band Service features and their release information

Table 38: Feature History

Feature Name	Release Information	Feature Description
Support for OOB Services	Cisco cnBR 21.2	This release of Cisco cnBR supports passing OOB signals through an RPD using the SCTE 55-1 and SCTE 55-2 standards. It also supports NDF and NDR protocols for the same purpose.

The following three approaches are used to pass out-of-band (OOB) signals through a Remote PHY Device (RPD):

- SCTE 55-1 Remote PHY solution

- SCTE 55-2 Remote PHY solution

- Narrowband Digital Forward (NDF) and Narrowband Digital Return (NDR)

The SCTE 55-1 and SCTE 55-2 standards specify two different out-of-band signaling systems for two-way communication with the legacy set-top boxes (STB). They provide localization, video control or enablement, data delivery, code upgrade, and interactive applications. The DOCSIS set-top gateway (DSG) standard provides this same data-delivery in newer STBs. However, SCTE 55-1 and SCTE 55-2 OOB are necessary to support MPEG video transport with millions of legacy STBs.

NDF and NDR are protocols introduced for RPD telemetry signaling. It digitizes an analog portion of the spectrum and encapsulates it in DEPI or UEPI.

As a principal core, the Cisco cnBR plays a role in the SCTE 55-1 OOB, NDF, and NDR. A separate auxiliary core, such as the Cisco D9485 or Vecima Entra Interactive Video Controller, handles SCTE 55-2 OOB.
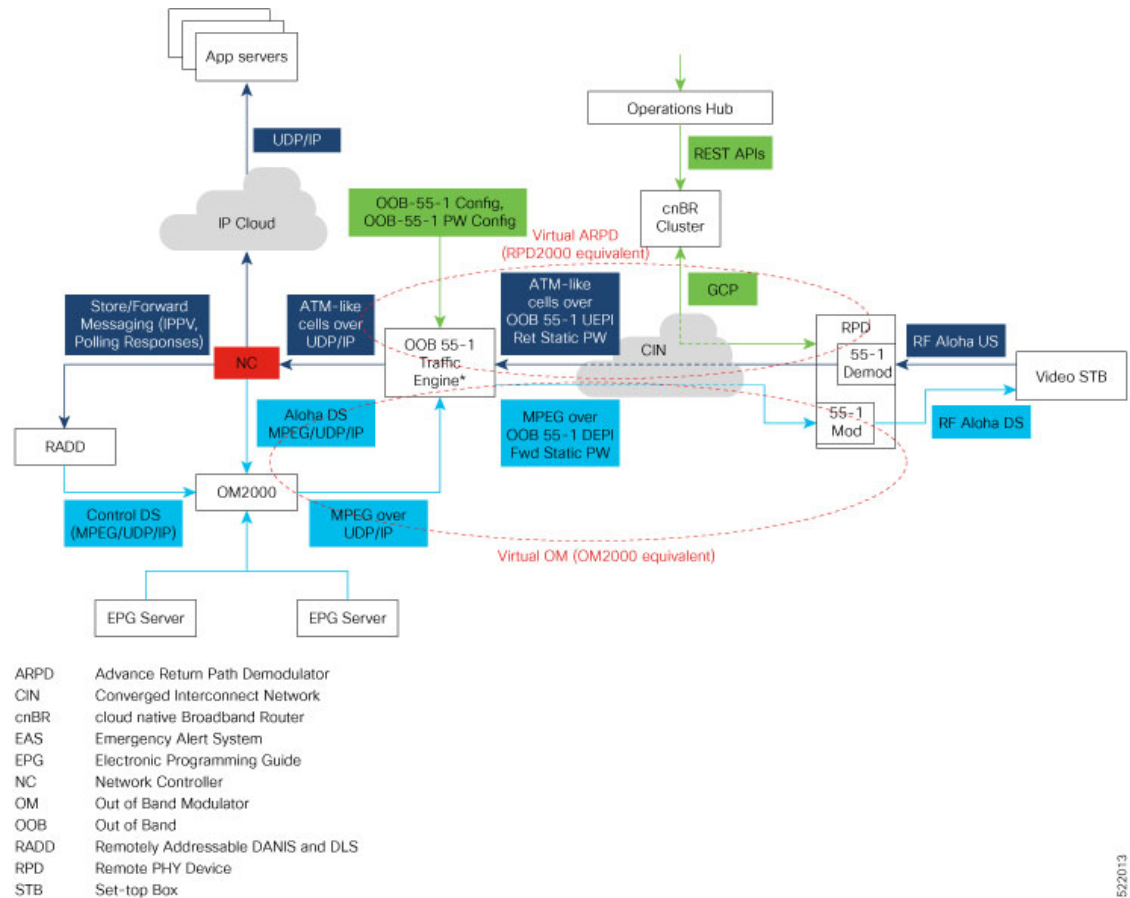
SCTE 55–1 OOB

The SCTE 55–1 OOB service enables two-way communication with legacy set-top boxes (STB). Cisco cnBR supports this service in the following two ways by:

- using OOB auxiliary CCAP core such as Cisco cBR-8.

- using OOB traffic engine.

SCTE 55–1 OOB Traffic Engine Support

The following figure shows Cisco cnBR with an SCTE 55–1 OOB traffic engine.

Figure 40: cnBR with the SCTE 55–1 OOB Traffic Engine Support

ARPD	Advance Return Path Demodulator
CIN	Converged Interconnect Network
cnBR	cloud native Broadband Router
EAS	Emergency Alert System
EPG	Electronic Programming Guide
NC	Network Controller
OM	Out of Band Modulator
OOB	Out of Band
RADD	Remotely Addressable DANIS and DLS
RPD	Remote PHY Device
STB	Set-top Box

The OOB traffic engine provides a bidirectional data plane for the OOB services, using static pseudowires. Cisco cnBR provides RPD control, using GCP to configure the OOB downstream and upstream channels and associated forward and return static pseudowires.

The network controller (NC) manages and controls STBs. It supports two-way communication between STBs and application servers, and enables services such as video-on-demand (VoD) and switched digital video (SDV). In a traditional HFC network, for the downstream traffic, an OM-2000 out-of-band modulator (OM) processes source streams per SCTE 55–1 and performs the RF modulation; for the upstream traffic, an RPD-2000 Advanced Return Path Demodulator (ARPD) demodulates the RF OOB signals and forwards them through UDP/IP to the NC.

The OM-2000 multiplexes OOB MPEG streams from the following sources:

- Network controller (NC)

- Remotely addressable DANIS and DLS (RADD): provides MPEG data necessary for video operation (For example, EMM, NIT, CDL, PAT/PMT)

- Electronic Program Guide (EPG) server

- Emergency Alert Service (EAS) server

The RPHY solution uses a virtual OM (VOM) in the downstream path:

- The OM-2000 multiplexes OOB source MPEG streams, but it does not perform RF modulation. Instead, it sends the streams to the traffic engine over UDP/IP.

- The traffic engine DEPI encapsulates the OOB source streams and sends them to the RPD on forward-static pseudowires.

- RPD performs the QPSK RF modulation.

The RPHY solution uses a virtual ARPD (VARPD) in the upstream path:

- The RPD demodulates the upstream OOB RF signals and encapsulates data UEPI, and sends it upstream on the return-static pseudowires.

- The traffic engine UDP/IP encapsulates the OOB upstream data and sends it to the NC.

You can configure the SCTE-55 OOB service on the RPD using the Cisco Operations Hub UI. The Cisco Operations Hub uses REST APIs to command Cisco cnBR to configure the RPD through GCP.

Configure Upstream SCTE 55–1 OOB

An RPD supports up to three SCTE 55–1 OOB upstream (US) channels. Typically, the US channels are one 3.2 MHz channel or three 192 kHz channels.

Limitations of Cisco 1x2 RPD

Cisco 1x2 RPD has the following limitations:

- SCTE 55–1 OOB shares US resources with NDR channels.

- Supports one NDR channel on the US port 0, only if two SCTE 55–1 OOB channels are configured on the US port 0.

- Uses same session ID or pseudowire for all OOB 55–1 upstream channels of both ports. If different session IDs are configured, the RPD uses the last configured session ID.

Configurable Parameters

The following table shows the configurable parameters for each SCTE 55–1 OOB upstream channel:

The table depicts the configurable parameters for each SCTE 55–1 OOB upstream channel

Field Name	Type	Description
sessionId	String	Unique session identifier for return-static pseudowire (PW) in hexadecimal. Range: 0x1 to 0xFFFFFFFF. Recommended range: 0x01200000 to 0x012FFFFF. 0x12 is MPT-55-1 PW subtype.
channel	Integer	Index of SCTE 55–1 OOB upstream channel. Range: 0–2.

Field Name	Type	Description
pwDestIpAddr	String	Destination IPv4 or IPv6 address to which the RPD sends data on a return-static PW.
idInSG	Integer	Unique ID of upstream channel in RPD. Range: 16 to 39.
frequency	Integer	Center frequency of the SCTE 55–1 upstream channel in hertz. Range: 8.096 MHz to 40.160 MHz in 192-kHz steps. Cisco cBR-8 range: 5.216 to 64.736 MHz in 1-kHz steps
varpdDeviceId	Integer	32-bit identifier used in the virtual ARPD protocol. No range limit.
varpdPortId	Integer	8-bit RF port identifier used in virtual ARPD protocol. Range: 0–255. Cisco cBR-8 range: 1–6.
varpdDemodId	Integer	8-bit demodulator identifier used in virtual ARPD protocol. Range: 0–23. Cisco cBR-8 range: 0–2.
targetRxPowerAdjust	Integer	Target-receive power level adjustment for upstream channel relative to the base power level specified for the corresponding US RF port in step of 0.1 dBmV/1.6MHz. The default value is 0.0. No range limit. Cisco cBR-8 range: –10.0 to 5.0.

Configure Downstream SCTE 55-1 OOB

An RPD supports one or two SCTE 55-1 OOB downstream (DS) frequencies or channels. However, both downstream channels carry the same data from a single pseudowire.

Limitations of Cisco 1x2 RPD

Cisco 1x2 RPD has the following limitations:

- It supports only one NDF channel if SCTE 55-1 OOB DS is configured.
- SCTE 55-1 OOB shares DS resources with NDF channels.

Configurable Parameters

The following table shows the configurable parameters for SCTE 55-1 OOB downstream:

The table depicts the configurable parameters for SCTE 55-1 OOB downstream

Field Name	Type	Description
sessionId	String	Unique session identifier for multicast forward-static pseudowire (PW) in hexadecimal. Range: 0x1 to 0xFFFFFFFF. Multicast range: 0x80000001 to 0x8000FFFF
sourceAddress	String	For multicast forward-static PW and source specific (SSM) operation, source IPv4 or IPv6 address of the multicast group that the RPD needs for joining and receiving data on this PW. Use NULL IP address for any-source multicast operation.
groupAddress	String	For multicast forward-static PW, group (destination) IPv4 or IPv6 address of the multicast group that the RPD needs for joining and receiving data on this PW.
idInSG	Integer	Unique ID of the downstream channel in the RPD. Range: 0 to 157, 163.
frequency	Integer	Center frequency of the SCTE 55-1 downstream channel in hertz. Range: 71 to 129 MHz in steps of 50 kHz. The default value is 75250000 Hz.
powerAdjust	Integer	Power level adjustment for SCTE 55-1 downstream channel, relative to the base power level configured for the corresponding DS RF port in steps of 0.1 dB. No range limit. (Cisco cBR-8 range: -7.0 to 0.0)

Field Name	Type	Description
secondFrequency	Integer	Center frequency of the second SCTE 55-1 downstream channel in hertz, which carries the same content as the first channel. Range: 0 or 71 to 129 MHz in steps of 50 kHz. The default value is 0 Hz (for no second frequency).
sfPowerAdjust	Integer	Power level adjustment for the second SCTE 55-1 downstream channel, relative to the base power level configured for corresponding DS RF port in steps of 0.1 dB. No range limit. (Cisco cBR-8 range: -7.0 to 0.0)

Narrowband Digital Forward and Narrowband Digital Return

The following table provides description of the various NDF and NDR features and their release information

Table 39: Feature History

Feature Name	Release Information	Feature Description
Support for Narrowband Digital Forward and Narrowband Digital Return	Cisco cnBR 21.2	The Narrowband Digital Forward (NDF) supports FM broadcast, DAB+ broadcast, and OOB signals. NDF digitizes the analog portion of the DS and sends it to the RPD, where it recreates the original analog portion. Narrowband Digital Return (NDR) digitizes the analog portion of the US and sends it to the CMTS, where it recreates the original analog portion at the headend. It supports legacy OOB signals.

Narrowband Digital Forward (NDF) and Narrowband Digital Return (NDR) are protocols that are introduced for RPD telemetry signaling.

NDF refers to the digitizing of the analog portion of the downstream spectrum at the headend, sending the digital samples as payload in [DEPI] packets to the RPD, and then re-creating the original analog stream at the RPD. NDF supports services such as FM broadcast, DAB+ broadcast, and OOB signals for forward sweep, DS leakage, and element management.

NDR refers to the digitizing of an analog portion of the upstream spectrum at the RPD, sending the digital samples as payload in [R-UEPI] packets to the CMTS, and then re-creating the original analog stream at the

headend. NDR supports legacy OOB signals for reverse sweep, return path monitoring, FSK-based HMS, and other FSK-based telemetry signals.

The following figure shows the role of Cisco Operations Hub and Cisco cnBR with NDF and NDR applications:

Figure 41: Cisco Operations Hub and cnBR interacting with NDF and NDR
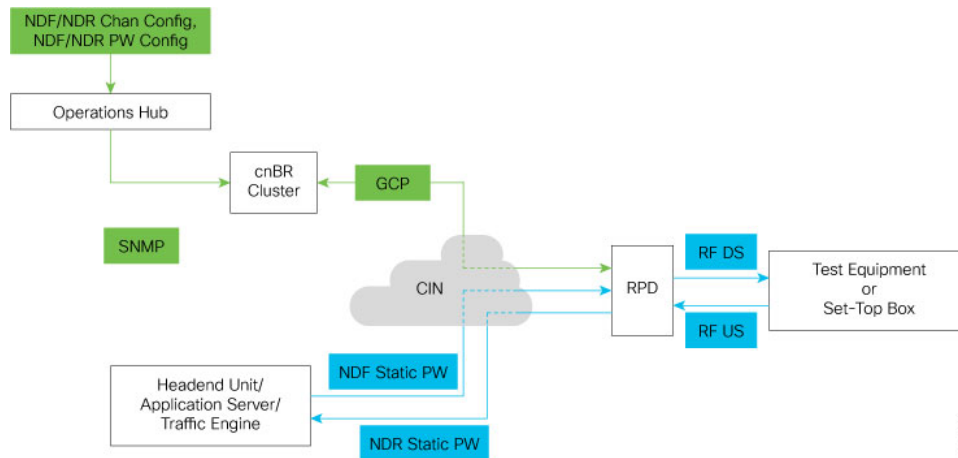
You can configure the NDF and NDR services on the RPD using the Cisco Operations Hub user interface. The Cisco Operations Hub uses REST APIs to command Cisco cnBR to configure the RPD through GCP. Cisco cnBR configures the RPD's NDF and NDR channels, and the associated forward and return-static pseudowires.

These forward and return-static pseudowires carry the digitized analog data between the headend application server or the traffic engine and the RPD. The RPD RF modulates and demodulates these signals, connecting to the tester equipment or set-top boxes (STB) on the RF plant.

By using NDR and NDF, Cisco cnBR can support the NDR and NDF Viavi Sweep Application, on page 200.

NDR and NDF Viavi Sweep Application

The following figure shows the role of Cisco Operations Hub and Cisco cnBR in the Viavi Sweep application:

The Viavi reverse (upstream) sweep solution requires a headend unit and a field meter. The headend unit and the field meter communicate through a forward (downstream) frequency-shift keying (FSK) telemetry burst (headend unit to the field meter) and a return (upstream) FSK telemetry burst (field meter to the headend).

These telemetry signals provide the control necessary to allow multiple meters to sweep on the same node simultaneously. When a field meter is actively sweeping, the field meter waits for a downstream telemetry burst showing the meter which frequencies to sweep. After receiving the downstream telemetry, the field meter sends a burst of upstream telemetry followed by a series of RF signals at each of the frequencies that are indicated in the downstream telemetry. The headend unit measures the sweep frequencies and returns the measured levels to the meter on the next downstream telemetry burst.

For the Viavi sweep application, enable the Cisco Operations Hub SNMP agent and configure the community string with both read and write permissions. The Viavi headend unit must be able to enable and disable the NDF and NDR channels to perform the sweep operation; it must control the channel's administrative up and down states. The channels must be set to `down` in the initial configuration.

For the Viavi sweep application, configure the NDF parameters as follows:

NDF Parameter	Configuration
sourceAddress	IP address of the RCI agent interface that is streaming NDF.
unicast	Set to `true`.
groupAddress	Not used for unicast. It can be set to null: `::` for IPv6 or `0.0.0.0` for IPv4.
adminState	Initially set to `down`.

For the Viavi sweep application, configure the NDR parameters as follows:

NDR Parameter	Configuration
destAddress	IP address for the RCI agent interface (server IP address) that is receiving NDR.
adminState	Initially set to `down`.

Configure Narrowband Digital Forward

An RPD supports up to three NDF channels in the downstream traffic. NDF channels are defined by the channel width and the center frequency. Cisco cnBR supports the following NDF modes (channel widths):

NDF modes supported by cnBR

Table 40: NDF modes supported by cnBR

NDF Mode	Bandwidth	Band
0	80 KHz	Narrowband
1	160 KHz	Narrowband
2	320 KHz	Narrowband
3	640 KHz	Narrowband
4	1.28 MHz	Narrowband
5	2.56 MHz	Narrowband
6	5.12 MHz	Narrowband
7	25.6 MHz	Wideband Supports FM radio.

Limitations of Cisco 1x2 RPD

Cisco 1x2 RPD has the following limitations:

- Supports up to three narrowband NDF channels or one wideband channel.

- Supports NDF sharing of downstream resources with OOB.

- Supports only one NDF channel if OOB 55-1 is configured.

- Supports two NDF channels if OOB 55-2 configured.

Configurable Parameters

The following table shows the configurable parameters for each NDF downstream channel:

Configurable parameters for each NDF downstream channel

Table 41: Configurable parameters for each NDF downstream channel

Field Name	Type	Description
sessionId	String	Unique session identifier for forward static pseudowire (PW) in hexadecimal.
		Full range: 0x1 to 0xFFFFFFFF. Multicast range: 0x80000001 to 0x8000FFFF.
		Recommended range for unicast: 0x01500000 to 0x015FFFFF
		0x15 is PSP-NDF PW subtype.
channel	Integer	Index of NDF channel. Range: 0–2
sourceAddress	String	For multicast forward-static PW and source-specific (SSM) operation, the source IPv4 or IPv6 address of the multicast group that the RPD needs for joining and receiving data on this PW.
		Use NULL IP address for any-source multicast operation.
		Use the IP address of the remote peer for unicast PW.
groupAddress	String	For multicast forward-static PW, group (destination) IPv4 or IPv6 address of the multicast group that the RPD needs for joining and receiving data on this PW.
		Not used for unicast PW.
idInSG	Integer	Unique ID of the downstream channel in RPD.
		Range: 0–157.

Field Name	Type	Description
frequency	Integer	Center frequency of the NDF channel in hertz. Range: 50 MHz to 1 GHz (Cisco cBR-8 router).
channelWidth	Integer	Width of the NDF channel in hertz. Values: 80 KHz, 160 KHz, 320 KHz, 640 KHz, 1.28 MHz, 2.56. MHz, 5.12 MHz, 25.6 MHz.
powerAdjust	Integer	Power level adjustment for the NDF channel, relative to the base power level configured for a corresponding DS RF port in steps of 0.1 dB. Range: –12.0 to 3.0 (Cisco cBR-8: –30.0 to –3.0; CM-SP-R-OOB: –12.0 to 3.0)
adminState	String	Administrative state of the NDF channel. Values: 1 – other; 2 – up; 3 – down; 4 – testing. The default value is up (2).
unicast	Boolean	Indicates whether the forward static PW is unicast. • True: Unicast • False: Multicast The default value is `false`.

Configure Narrowband Digital Return

An RPD supports up to three NDR channels for the upstream traffic. NDR channels are defined by channel width and center frequency. Cisco cnBR supports the following NDR modes (channel widths):

The table displays the NDR modes supported by Cisco cnBR, and their bandwidth

NDR Mode	Bandwidth
0	80 kHz
1	160 kHz
2	320 kHz
3	640 kHz

NDR Mode	Bandwidth
4	1.28 MHz
5	2.56 MHz
6	5.12 MHz

Limitations of Cisco 1x2 RPD

Cisco 1x2 RPD has the following limitations:

- NDR shares the upstream (US) resources with OOB 55–1 and OOB 55–2.

- Supports one NDR channel on the US port, only if the US port is configured with two OOB 55–1 channels.

- Supports either one NDR-mode 6 or two NDR-mode 1–5 channels if OOB 55–2 is configured on the US port.

- Does not support NDR mode 0 (80 kHz).

Configurable Parameters

The following table shows the configurable parameters for each NDR upstream channel:

The table displays the parameters for NDR upstream channels

Field Name	Description	Type
sessionId	Unique session identifier for return-static pseudowire (PW) in hexadecimal. Range: 0x1 to 0xFFFFFFFF. Recommended range: 0x01600000 to 0x016FFFFF 0x16 is the PSP-NDR PW subtype.	String
channel	Index of the NDR channel. Range: 0–2.	Integer
destAddress	Destination IPv4 or IPv6 address to which the RPD sends data on a return-static PW. Cisco cBR-8 calls this server IP.	String
idInSG	Unique ID of the upstream channel in RPD. Range: 16 to 39.	Integer

Field Name	Description	Type
frequency	Center frequency of the NDR channel in hertz. Range: 5 to 26.5 MHz (Cisco cBR-8 and CM-SP-R-OOB).	Integer
channelWidth	Width of the NDR channel in hertz. Values: 80 kHz, 160 kHz, 320 kHz, 640 kHz, 1.28 MHz, 2.56. MHz, 5.12 MHz.	Integer
targetRxPowerAdjust	Target-receive power-level adjustment for upstream channel, relative to the base power-level specified for the corresponding US RF port in steps of 0.1 dBmV/1.6MHz. Default value: 0.0. Range: –12.0 to 5.0 (Cisco cBR-8: –12.0 to 5.0; CM-SP-R-OOB: –12.0 to 3.0)	Integer
adminState	Administrative state of the NDR channel: 1 – other; 2 – up; 3 –down; 4 – testing The default value is up (2).	String

Traffic Management

Cisco cnBR provides traffic management functionalities to prevent data loss in important business applications, and to ensure that mission-critical applications take priority over other traffic.

DOCSIS Downstream QoS

DOCSIS downstream QoS consists of classifying packets into service flows for downstream and providing QoS at the service flow level.

Packet Classification

The packet classification supports the following packet header fields, as specified in the DOCSIS specification.

IPv4 fields:

- IPv4 TOS values
- IP protocol

Downstream Service Flow

- IP source address and mask

- IP destination address and mask

IPv6 fields:

- IPv6 traffic class values

- IPv6 flow label

- IPv6 next header type

- IPv6 source address and prefix length (bits)

- IPv6 destination address and prefix length (bits)

TCP or UDP fields:

- TCP/UDP source port start and end

- TCP/UDP destination port start and end

The packet classifiers are specified in cable modem configuration files. These configuration files are sent to Cisco cnBR either when registering the modem (for static service flows) or later through DSX messages (for dynamic service flows).

Downstream Service Flow

The basic unit of downstream QoS is the downstream service flow, which is a unidirectional sequence of packets transported across RF channels between Cisco cnBR and cable modems. The following parameters define the QoS of service flows in DOCSIS:

- Maximum sustained traffic rate

- Minimum sustained traffic rate

- Peak traffic rate

- DOCSIS traffic priority

- Maximum traffic burst size

- Maximum DS latency, used to indicate only the absolute priority

A service flow can be in one of the following three states:

- Provisioned

- Admitted

- Active

Only active flows are used to carry traffic and subject to the QoS treatment.

You can specify the service flow parameters directly in the individual modem configuration files or indirectly through the service classes on Cisco cnBR.

206

Service Class

Service providers can use service classes to manage QoS parameters. For example, the provider can add QoS parameters to each tier of service it offers in a service class. Use the service class names to match a modem's service flows to a service class, as defined by DOCSIS.

Downstream QoS Configuration

You can configure all packet classification parameters and the downstream service flow QoS parameters in the modem configuration files. If you want to use the service class feature, configure Cisco cnBR accordingly.

When you use a service class, the modem configuration files should have the service class names that match the ones configured in the service class.

Note QoS parameters for a service flow are decided when creating the service flow, either during modem registration or its dynamic creation.

Initial Configuration from Autodeployer Script

Configure service classes in the `svcds` block in the SG configuration `json` file. The following traffic parameters are supported.

Note The maximum values provided in the following table indicate the valid parameter range. Provide the actual parametric values that are based on the actual system capacity and traffic planning.

Traffic Parameters Supported

Parameter Name	Description	Minimum	Maximum	Unit
maxSustTrafRate	Maximum Sustained Traffic Rate	0	4G	bps
minRsvdTrafRate	Minimum Reserved Traffic Rate	0	4G	bps
peakTrafRate	Peak Traffic Rate	0	4G	bps
trafPrio	Traffic priority used to indicate traffic ratio under congestion	0	7	N/A
maxTrafBurst	Maximum traffic burst	1522	4G	Byte
maxDsLatcy	Indication for High Priority	0	>0	N/A
servClassName	Service Class Name	N/A	N/A	a string

Example

```
"svcds": [
    {
        "maxSustTrafRate": 3000000,
        "servClassName": "DS_3M",
        "qoSParaSetType": 7
    },
    {
        "maxSustTrafRate": 4000000,
        "servClassName": "DS_4M",
        "qoSParaSetType": 7
    },
    {
        "maxSustTrafRate": 5000000,
        "servClassName": "DS_5M",
        "qoSParaSetType": 7
    },
    {
        "maxSustTrafRate": 10000000,
        "servClassName": "DS_MST_10M"
    },
    {
        "maxTrafBurst": 300000000,
        "servClassName": "DS_MTB_300M"
    },
    {
        "peakTrafRate": 12000000,
        "servClassName": "DS_PTR_12M"
    },
    {
        "minRsvdTrafRate": 2000000,
        "servClassName": "DS_CIR_2M"
    },
    {
        "maxSustTrafRate": 20000000,
        "maxTrafBurst": 200000000,
        "servClassName": "ds_level2_sf1"
    },
    {
        "maxSustTrafRate": 10000000,
        "peakTrafRate": 12000000,
        "servClassName": "ds_level2_sf2"
    },
    {
        "maxSustTrafRate": 15000000,
        "minRsvdTrafRate": 2000000,
        "servClassName": "ds_level2_sf3"
    },
    {
        "maxTrafBurst": 100000000,
        "peakTrafRate": 8000000,
        "servClassName": "ds_level2_sf4"
    },
    {
        "maxTrafBurst": 80000000,
        "minRsvdTrafRate": 26000000,
        "servClassName": "ds_level2_sf5"
    },
    {
        "minRsvdTrafRate": 26000000,
        "peakTrafRate": 12000000,
        "servClassName": "ds_level2_sf6"
    },
```

```
{
    "maxSustTrafRate": 10000000,
    "maxTrafBurst": 100000000,
    "peakTrafRate": 26000000,
    "servClassName": "ds_level3_sf1"
},
{
    "maxSustTrafRate": 20000000,
    "maxTrafBurst": 300000000,
    "minRsvdTrafRate": 26000000,
    "servClassName": "ds_level3_sf2"
},
{
    "maxSustTrafRate": 25000000,
    "minRsvdTrafRate": 22000000,
    "peakTrafRate": 18000000,
    "servClassName": "ds_level3_sf3"
},
{
    "maxTrafBurst": 200000000,
    "minRsvdTrafRate": 3000000,
    "peakTrafRate": 26000000,
    "servClassName": "ds_level3_sf4"
},
{
    "maxSustTrafRate": 20000000,
    "maxTrafBurst": 300000000,
    "minRsvdTrafRate": 26000000,
    "peakTrafRate": 8000000,
    "servClassName": "ds_level4_sf"
}
```

View Downstream QoS Configuration

Step 1 On the Cisco Operations Hub, click the Cisco Operations Hub main menu button.

Step 2 Choose **cnBR Manager** > **cnBRs** to open the **cnBR Clusters** page.

Step 3 Click **Import & Export cnBR** from the vertical navigation tab to access the **Export/Import** page.

Step 4 In the **Export cnBR Configuration** section, select the target Cisco cnBR from the drop-down list.

Step 5 Click **Export** to retrieve the SG configuration of the selected Cisco cnBR.

A `.json` file containing the full configuration is saved to your machine. Service class settings are available in the `svcds` block.

Update Downstream QoS Configuration

You can update the configuration using the following two methods:

• cnBR Manager

• Autodeployer re-configuration

In both these options, the full configuration is sent to the CMTS. The existing configuration is overwritten and the new configuration is activated. For more details, see Autodeployer Limitations, on page 61.

Using Operations Hub Configurator

Step 1   On the Cisco Operations Hub, click the Cisco Operations Hub main menu button.

Step 2   Choose **cnBR Manager** > **cnBRs** to open the **cnBR Clusters** page.

Step 3   Click **Import & Export cnBR** to open the **Export/Import** page.

Step 4   In the **Export cnBR Configuration** section, choose the Cisco cnBR router address from the drop-down list.

Step 5   Click **Export** to retrieve the current SG configuration of the selected Cisco cnBR.

Step 6   Open the file and update the configuration in the `svcds` block of the SG configuration.

Step 7   Save the updated file on the local disk.

Step 8   In the **Import cnBR Configuration File** pane, choose the Cisco cnBR address from the drop-down list.

Step 9   Click **Browse** to locate the saved configuration file.

Step 10   Click **Import** to upload the updated SG configuration.

This updated file overwrites the existing configuration file and activates the new configuration.

Using Autodeployer Reconfiguration

After the initial configuration of the Source-Verify using the Autodeployer, update the configuration by modifying the appropriate blocks and rerunning the Autodeployer. This process overwrites the existing configuration and activates the new configuration.

For more details on the Autodeployer, see Configure Cisco cnBR Using Autodeployer, on page 43.

Default Configuration

If the service class configuration does not exist, specify the service flow QoS parameters in the cable modem configuration file.

Downstream QoS Statistics

In cnBR Manager, under **opshub-data** menu, you can see the following service flow details:

- Downstream Service Flow List

- Downstream Service Flow Verbose

- Downstream Service Flows for a Modem

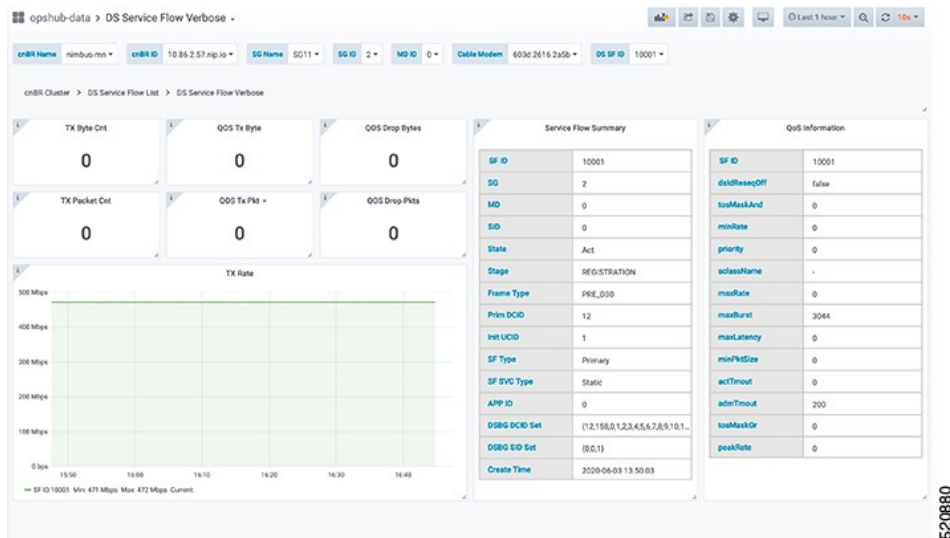### Downstream Service Flow List

The **Downstream Service Flow List** window provides the details of downstream service flows for each service group. The window displays a live graph of the traffic rate and a table listing all service flows of the selected service group.
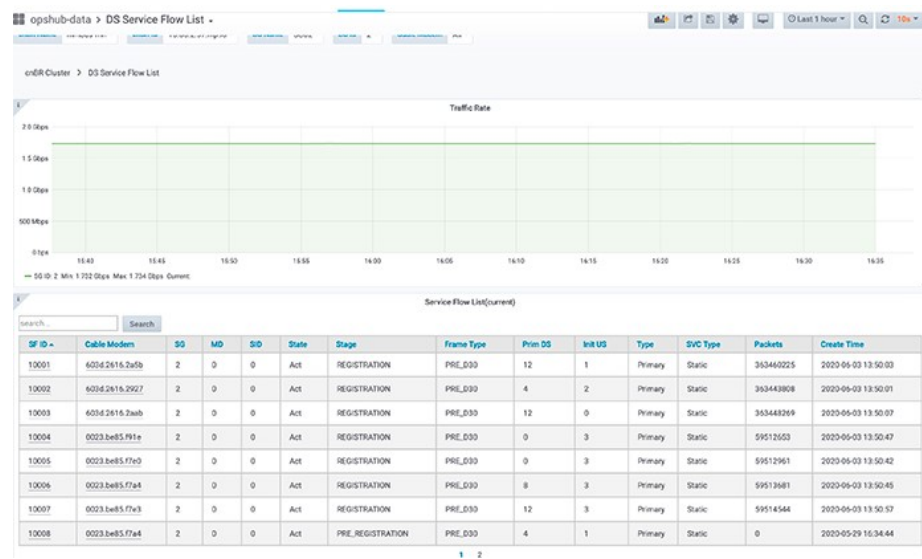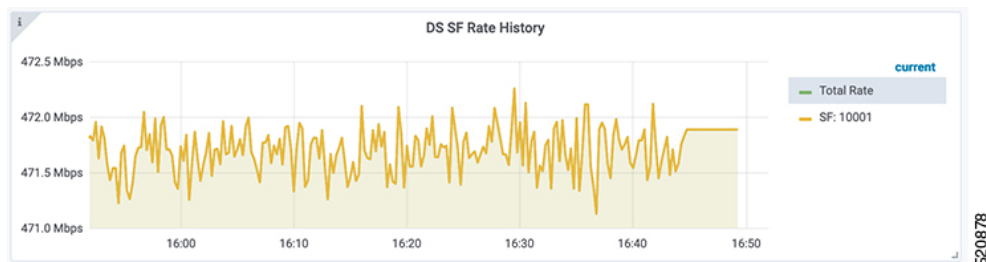

Downstream Service Flow Verbose

This window provides detailed information of an individual downstream service flow, including its transmission rate.

Downstream Service Flows for Cable Modem

The **Cable Modem Verbose** window provides the downstream service flow rate for all the flows on that modem.

Punt Path Rate Limiting in Data Plane

The Cisco cnBR *punts* packets that the Data Plane (DP) cannot process to application services (for example, DHCP relay service) through **to-app-svc** queues. For example, ARP packets, DHCP packets, IP packets destined to unresolved adjacency, and so on.

The *DP punt-path* assigns a punt-cause to each punted packet, and prepares the packet for entry into **to-app-svc** queues.

Figure 42: Punt path rate-limiting
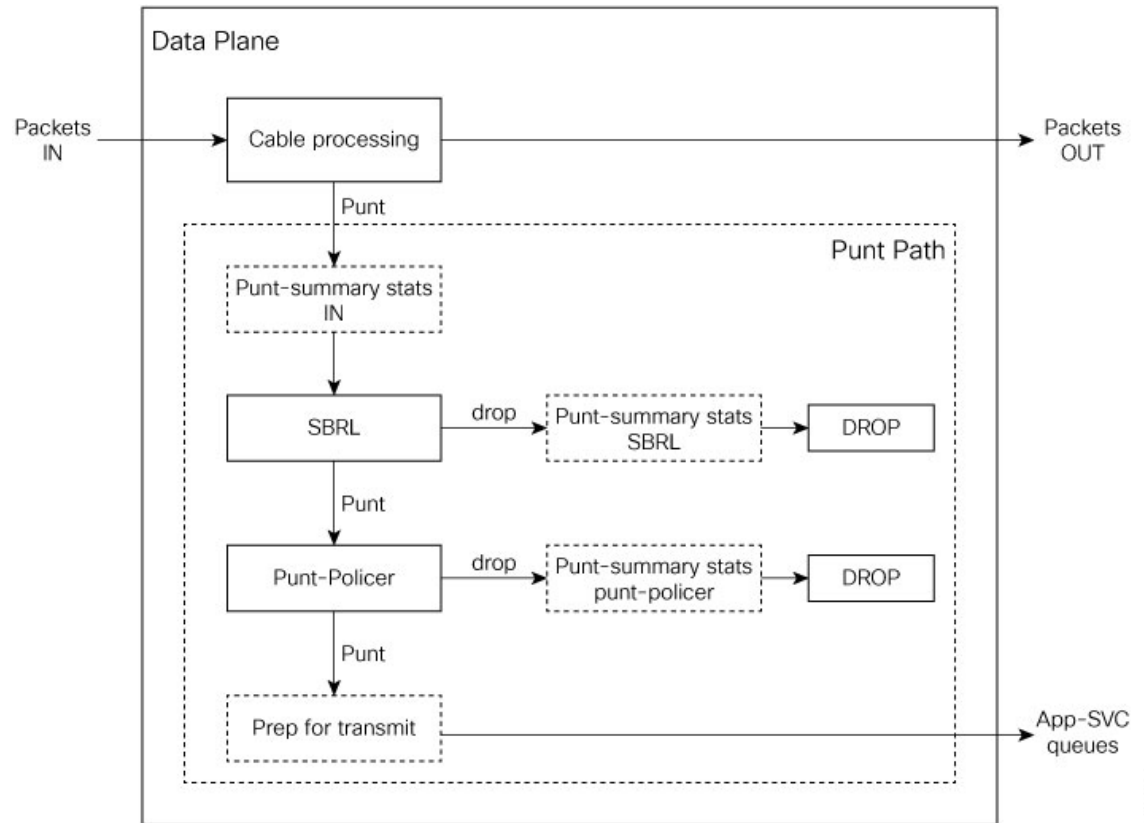
Denial of Service occurs when a service starts tail-dropping legitimate packets as a result of the queues becoming congested. To prevent this congestion, punt-path rate limiting (PPRL) operates in the punt-path to drop packets selectively. The Cisco cnBR identifies malicious actors and drops corresponding packets, while punting legitimate packets.

Cisco cnBR rate limiting operates on two levels:

- Source-Based Rate Limiting (SBRL) combines the subscriber MAC-address and the punt-cause to create an index for rate-limiting.

- Punt-Policer uses the punt-cause as the index for rate-limiting.

SBRL operates first. The Cisco cnBR combines MAC-address and punt-cause to create an index for rate-limiting. The Cisco cnBR rate-limits this MAC/punt stream according to the configured rate. The Cisco cnBR drops nonconforming packets. SBRL uses the source MAC address in the upstream direction and the destination MAC address in the downstream direction.

Next, the Punt-Policer aggregates packets with the same punt-cause, and rate-limits each punt-cause according to the configured rate. The Cisco cnBR drops nonconforming packets.

The following table lists the supported punt-causes:

Supported Punt-causes

Cause Id	Cause Name	Cause Description
6	dhcpv4_us	DHCP IPv4 upstream

Cause Id	Cause Name	Cause Description
14	dhcpv6_us	DHCP IPv6 upstream
10	cable_arp	ARP request and reply
11	ndp	Neighbor discovery protocol
20	svfy_v4	Source-verify IPv4
21	svfy_v6	Source-verify IPv6
22	ds_lq_v4	Lease query downstream IPv4
23	ds_lq_v6	Lease query downstream IPv6
25	mobility_v4	IPv4 CPE mobility
26	mobility_v6	IPv6 CPE mobility
7	tftp_req	TFTP request
32	ds_no_adj_v4	No adjacency downstream IPv4
33	ds_no_adj_v6	No adjacency downstream IPv6

Configure Punt Path Rate Limiting

Both SBRL and Punt-Policer configurations are on a per-punt-cause basis.

Initial Configuration of Punt Path Rate Limiting From Autodeployer Script

In the Autodeployer script SG template file, the PPRL configuration is in the *punt* block. Configure SBRL using the *subMacAddrSbrlList* block. Configure Punt-Policer using the *icpiPerCausePuntCfgList* block.

```
"sgs": [
    ...
    "sg-config": {
        ...
        "punt": {
            "subMacAddrSbrlList": [
                {
                    "PuntCause":cable_arp,
                    "RateLimitCfg": {
                    "RatePer4Sec":1000,
                    "BurstTimeMs":7000
              }
                },
                {
                    "PuntCause":ndp,
                    "RateLimitCfg": {
                "RatePer4Sec":6000,
                "BurstTimeMs":6000
          }
        }
    ]
            "icpiPerCausePuntCfgList": [
              {
                "CauseId": 20,
                "icpiPerCausePuntCfg": {
                    "MaxRate": 20
                }
```

```
                },
                {
                  "CauseId": 21,
                  "icpiPerCausePuntCfg": {
                      "MaxRate": 20
                  }
                },
                {
                  "CauseId": 22,
                  "icpiPerCausePuntCfg": {
                      "MaxRate": 20
                  }
                },
                {
                  "CauseId": 23,
                  "icpiPerCausePuntCfg": {
                      "MaxRate": 20
                  }
                }
              ]
          }
          ...
        }
      ]
```

View Punt Path Rate Limiting Configuration

Step 1 On the Cisco Operations Hub, click the Cisco Operations Hub main menu button.

Step 2 Choose **cnBR Manager** > **cnBRs** to open the **cnBR Clusters** page.

Step 3 Click **Import & Export cnBR** from the vertical navigation tab to access the **Export/Import** page.

Step 4 In the **Export cnBR Configuration** section, select the target Cisco cnBR from the drop-down list.

Step 5 Click **Export** to retrieve the SG configuration of the selected Cisco cnBR.

A .json file containing the full configuration is saved to your machine. PPRL settings are available in the *punt* block.

Update Punt Path Rate Limiting Configuration

You can update the configuration using the following methods:

- cnBR Manager

- Autodeployer reconfiguration

Both options send the full configuration to the CMTS. The Cisco cnBR overwrites the existing configuration and activates the new configuration. For more details, see Autodeployer Limitations, on page 61.

Update Configuration Using cnBR Manager

Step 1 On the Cisco Operations Hub, click the Cisco Operations Hub main menu button.

Step 2 Choose **cnBR Manager** > **cnBRs** to open the **cnBR Clusters** page.

Step 3 Click **Import & Export cnBR** to open the **Export/Import** page.

Step 4   In the **Export cnBR Configuration** section, select the target Cisco cnBR from the drop down list.

Step 5   Click **Export** to retrieve the SG configuration of the selected Cisco cnBR.

Step 6   Update the configuration in the *punt* block of the SG configuration and save the file.

Step 7   In the **Import cnBR Configuration File** section, select the target Cisco cnBR from the drop down list.

Step 8   Click **Browse** and select the saved configuration file.

Step 9   Click **Import** to push the updated SG configuration.

This import overwrites the existing configuration and activates the new configuration.

Update Configuration Using Autodeployer Reconfiguration

After the initial configuration of SBRL and Punt-Policer using the Autodeployer, update the configuration by modifying the corresponding blocks in the Autodeployer script and rerunning the Autodeployer. This process overwrites the existing configuration and activates the new configuration.

Configuration Parameters

SBRL Configuration Parameters

Table 42: SBRL Configuration Parameters

Field Name	Description	Type	Units	Value	Enforcement
PuntCause	Punt cause ID to be rate limited	string	—	dhcpv4_us, dhcpv6_us, cable_arp, ndp, svfy_v4, svfy_v6, ds_lq_v4, ds_lq_v6, mobility_v4, mobility_v6, tftp_req, ds_no_adj_v4, ds_no_adj_v6	Required
RatePer4Sec	Max rate in pkts-per-4-sec	integer	pkts-per-4-sec	1-255	Required
BurstTimeMs	For burst packets handling	integer	microseconds	1000-8000	Optional

Punt-Policer Configuration Parameters

Table 43: Punt-Policer Configuration Parameters

Field Name	Description	Type	Units	Value	Enforcement
CauseId	Punt cause ID to be rate limited	integer	—	6, 14, 10, 11, 20-23, 25, 26, 7, 32, 33	Required

Field Name	Description	Type	Units	Value	Enforcement
MaxRate	Max rate in pkts-per-sec	integer	pkts-per-sec	10-300000	Required

Default Configuration of Punt Path Rate Limiting

SBRL Default Configuration

Table 44: SBRL Default Configuration

PuntCause	RatePer4Sec(pkts/4-sec)	BurstTime(msec)
dhcpv4_us	16	4000
dhcpv6_us	16	4000
cable_arp	16	4000
ndp	16	4000
svfy_v4	4	4000
svfy_v6	4	4000
ds_lq_v4	4	4000
ds_lq_v6	4	4000
mobility_v4	16	4000
mobility_v6	16	4000
tftp_req	16	4000
ds_no_adj_v4	4	4000
ds_no_adj_v6	4	4000

Punt-Policer Default Configuration

Table 45: Punt-Policer Default Configuration

CauseId	Cause Description	MaxRate(pkts/sec)
6	DHCP IPv4 upstream	1200
14	DHCP IPv6 upstream	1200
10	ARP request and reply	1200
11	Neighbor Discovery Protocol	1200
20	Source-verify IPv4	1200
21	Source-verify IPv6	1200
22	Lease query downstream IPv4	400
23	Lease query downstream IPv6	400
25	IPv4 CPE mobility	1200

CauseId	Cause Description	MaxRate(pkts/sec)
26	IPv6 CPE mobility	1200
7	TFTP request	1200
32	No adjacency downstream IPv4	400
33	No adjacency downstream IPv6	400

Monitor Punt Path Rate Limiting

On the Cisco Operations Hub, click the Cisco Operations Hub main menu button. Choose **Dashboard** to open the **Dashboard** page. Click **Find a Dashboard** to open the search pane. Enter **Punt Inject Stats** in the **Search dashboards by name** field and click the **Punt Inject Stats** row to open the **Punt Inject Stats** dashboard.

Punt Inject Stats dashboard contains the PPRL statistics. Overall punt statistics are also available, along with SBRL and Punt-Policer statistics.
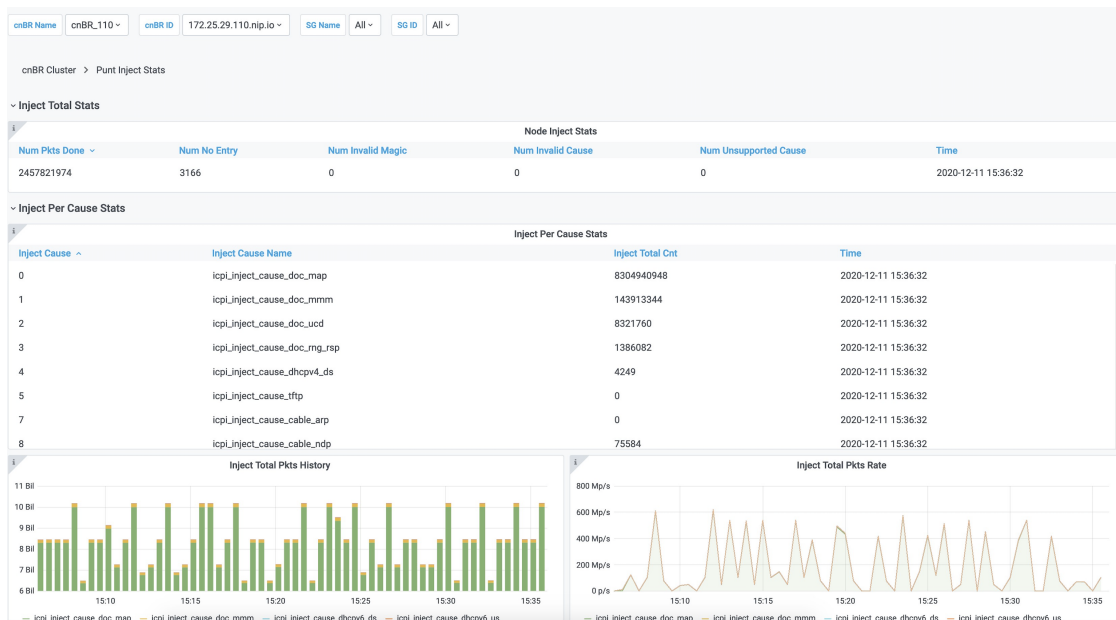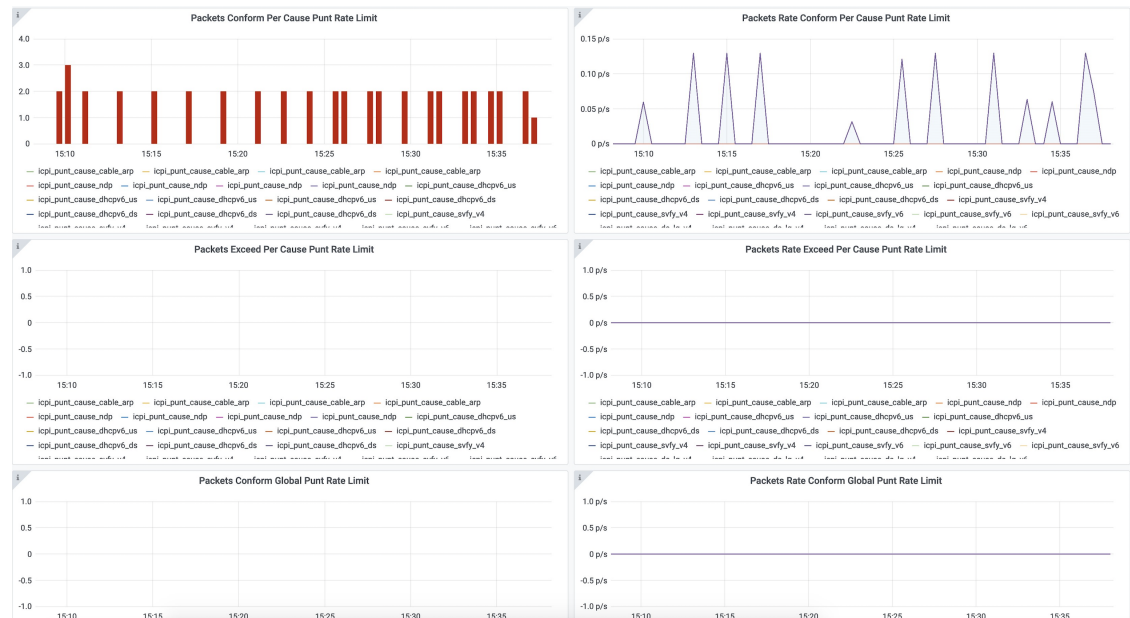
Figure 43: Overall Punt Statistics

Figure 44: SBRL Statistics

Figure 45: Punt-Policer Statistics

Upstream Type-of-Service (ToS) Overwrite

The Cisco cnBR can overwrite the DSCP/ToS field of packets associated with the DOCSIS Service Flow.

Configure ToS

Currently, you can configure ToS Overwrite through only the DOCSIS configuration file.

DOCSIS Configuration File

The DOCSIS service flow parameter *IP Type of Service (DSCP) Overwrite* contains two bytes, one for the **tos-and-mask** and one for the **tos-or-mask**. According to DOCSIS requirements, when you configure a

Service Flow with an *IP Type of Service (DSCP) Overwrite* parameter, the CMTS overwrites the DSCP/ToS value in the IP packets as follows:

```
new-ip-tos = ((orig-ip-tos AND tos-and-mask) OR tos-or-mask)
```

DOCSIS cable-modem configuration file uses *IP Type of Service Flow* under *Upstream Service Flow Encodings* to configure the upstream service flow parameter *IP Type of Service (DSCP) Overwrite*.

ToS Overwrite TLV

SubType	Length	Value
23	2	[and-mask, or-mask]

A configuration example is following:

```
24 (Upstream Service Flow Encoding)
   S01 (Service Flow Reference)        = 4
    S06 (QoS Parameter Set Type)       = 7
    S023 (IpTosOverwrite)              = 00 FF
```

More information on the DOCSIS parameters is available in DOCSIS 3.0 MAC and Upper Layer Protocols Interface Specification.

Default Configuration of ToS

By default ToS Overwrite is disabled; so the Cisco cnBR does not overwrite the DSCP/ToS field in the packet.

Enabling Security

Cisco cnBR provides security functionalities to defend against outside attacks.

Packet Filtering

Packet Filtering provides the ability to configure device-specific filters in the upstream and downstream directions.

- Devices are assigned with upstream and downstream filter groups through the DOCSIS configuration file.

- Different groups can be assigned for the upstream and downstream directions.

- If no filter group is specified in the DOCSIS configuration file, devices receive the default group configured on Cisco cnBR.

- If no default filter group is specified on Cisco cnBR, then no filtering is applied and the default action is FORWARD.

The rules for filter groups are configured on Cisco cnBR. Matching rules and actions (FORWARD or DROP) are specified in priority order. Rules are based on layer 2, layer 3, and layer 4 packet fields.

By default, Packet Filtering is disabled.

Configure Packet Filtering

Note Cable modems use the settings that are active during CM registration. If the default Packet Filtering groups are changed, you must reset cable modems to use the updated settings.

Initial Configuration using AutoDeployer Script

- In the Optional Configuration section of Packet Filtering configuration is in the `pfgActive` and `pfgGroup` blocks.

- Default Packet Filtering groups are specified in the `pfgActive` block.

- Rules for the groups are specified in the `pfgGroup` block.

The following is a sample configuration along with some explanation.

- The default filter group for downstream packets to a cable modem (cm_ds) is Group 10.

- Group 1 defines a filter that permits 90.90.90.2 ICMP packets, while denying other 90.90.90.0/24 ICMP packets. Groups 1 and 2 are not default groups. Therefore assign devices to these groups via the DOCSIS configuration file.

```
"global": {
    ...
    "pfgActive": {
        "cm_ds"  : 10,
        "cm_us"  : 11,
        "host_ds": 20,
        "host_us": 21,
        "mta_ds" : 30,
        "mta_us" : 31,
        "ps_ds"  : 40,
        "ps_us"  : 41,
        "stb_ds" : 50,
        "stb_us" : 51
    },
    "pfgGroup": {
        "grpList": [
          {
            "id" : 1,
            "ruleList": [
              {
                "isPermit": 1,
                "isIpv6": 0,
                "srcIp": "0.0.0.0",
                "srcIpPrefixLen": 0,
                "dstIp": "90.90.90.2",
                "dstIpPrefixLen": 32,
                "proto": 1,
                "srcportOrIcmptypeFirst": 0,
                "srcportOrIcmptypeLast": 65535,
                "dstportOrIcmptypeFirst": 0,
                "dstportOrIcmptypeLast": 65535,
                "tcpFlagsMask": 0,
                "tcpFlagsValue": 0,
                "tosMask": 0,
                "tosValue": 0
              },
```

```
                          {
                            "isPermit": 0,
                            "isIpv6": 0,
                            "srcIp": "0.0.0.0",
                            "srcIpPrefixLen": 0,
                            "dstIp": "90.90.90.0",
                            "dstIpPrefixLen": 24,
                            "proto": 1,
                            "srcportOrIcmptypeFirst": 0,
                            "srcportOrIcmptypeLast": 65535,
                            "dstportOrIcmptypeFirst": 0,
                            "dstportOrIcmptypeLast": 65535,
                            "tcpFlagsMask": 0,
                            "tcpFlagsValue": 0,
                            "tosMask": 0,
                            "tosValue": 0
                          }
                        ],
                      },
                      {
                        "id" : 2,
                        "ruleList": [
                          {
                            ...
                          },
                          ...
                          {
                            ...
                          }
                        ],
                      },
                      {
                        "id" : 10,
                        "ruleList": [
                          {
                            ...
                          },
                          ...
                          {
                            ...
                          }
                        ],
                      },
                      ...

                      {
                        "id" : 51
                        "ruleList": [
                          {
                            ...
                          },
                          ...
                          {
                            ...
                          }
                        ]
                      }
                    ]
                  },

                  ...

                },
                ...
```
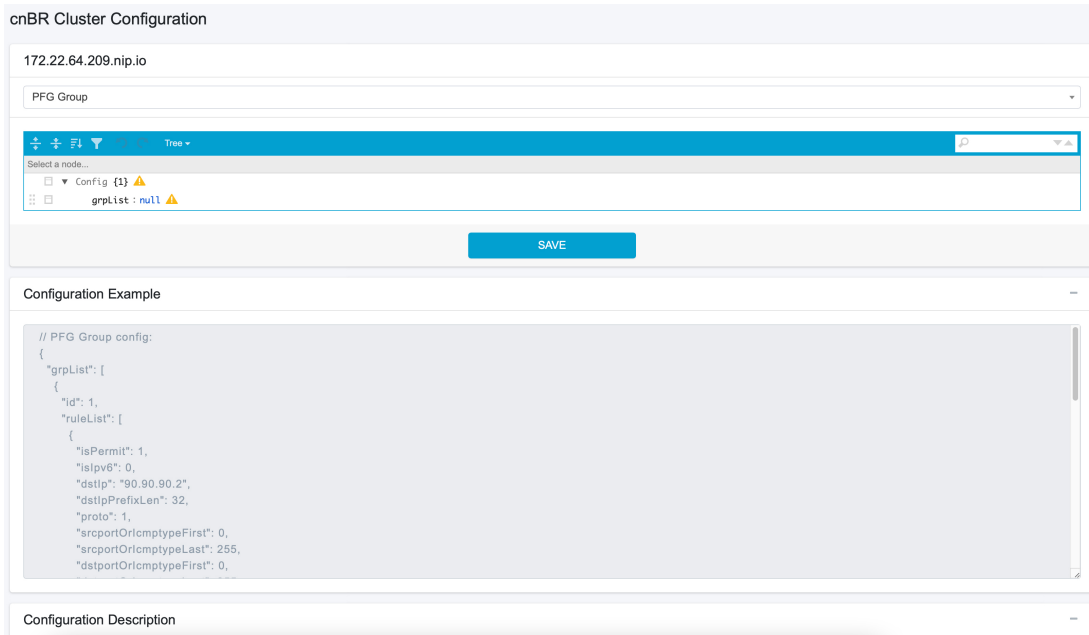
Display Current Configuration using cnBR Manager

Step 1   On the Cisco Operations Hub, click the Cisco Operations Hub main menu button.

Step 2   Choose **cnBR Manager** > **cnBRs** to open the **cnBR Clusters** page.

Step 3   Click the name of the Cisco cnBR to open the **cnBR Cluster Configuration** page.

Step 4   Click on drop-down menu and select **PFG Active** or **PFG Group** to display the corresponding configuration.

Figure 46: PFG Active Configuration

Figure 47: PFG Group Configuration

Update Configuration using cnBR Manager

Step 1   On the Cisco Operations Hub, click the Cisco Operations Hub main menu button.

Step 2   Choose **cnBR Manager** > **cnBRs** to open the **cnBR Clusters** page.

Step 3   Click the name of the Cisco cnBR to open the **cnBR Cluster Configuration** page.

Step 4   Click on drop-down menu and select **PFG Active** or **PFG Group** to display the corresponding configuration.

Step 5   Modify the configuration.

Step 6   Click **SAVE** to push the updated configuration to the Cisco cnBR.

Update Configuration using Autodeployer Reconfiguration

After the initial configuration of Packet Filtering following the Configure Cisco cnBR Using Autodeployer, on page 43, you can update the configuration by modifying the appropriate blocks and rerunning the AutoDeployer. It fully overwrites the existing configuration and activates the new configuration. See Autodeployer Limitations, on page 61.

Configuration Parameters

- A group can have multiple rules. Rules are processed in the listed order.

- If a packet matches a rule, the specified action is performed and filtering is complete.

- If a packet does not match any rule in the group, the packet is forwarded.

The table displays the PFG Active: Default Packet Filtering Groups

Table 46: PFG Active: Default Packet Filtering Groups

Field Name	Description	Type	Range	Enforcement
cm_ds	Cable Modem downstream default group	integer	-1 means no group, otherwise [1, 254]	required
cm_us	Cable Modem upstream default group	integer	-1 means no group, otherwise [1, 254]	required
host_ds	Host (ie. CPE) downstream default group	integer	-1 means no group, otherwise [1, 254]	required
host_us	Host (ie. CPE) upstream default group	integer	-1 means no group, otherwise [1, 254]	required
mta_ds	Multimedia Terminal Adaptor downstream default group	integer	-1 means no group, otherwise [1, 254]	required
mta_us	Multimedia Terminal Adaptor upstream default group	integer	-1 means no group, otherwise [1, 254]	required
ps_ds	Portal Server downstream default group	integer	-1 means no group, otherwise [1, 254]	required
ps_us	Portal Server upstream default group	integer	-1 means no group, otherwise [1, 254]	required
stb_ds	Set-Top Box downstream default group	integer	-1 means no group, otherwise [1, 254]	required
stb_us	Set-Top Box upstream default group	integer	-1 means no group, otherwise [1, 254]	required

The table displays the PFG Group: Rule Definition

Table 47: PFG Group: Rule Definition

Field Name	Description	Type	Enforcement
isPermit	0 means deny, 1 means permit	Integer	required
isIpv6	0 means IPv4, 1 means IPv6	Integer	required
srcIp	Source IP value	IPv4 or IPv6	required
srcIpPrefixLen	Source IP prefix length	Integer	required
dstIp	Destination IP value	IPv4 or IPv6	required
dstIpPrefixLen	Destination IP prefix length	Integer	required
tosValue	ToS/traffic class value	Integer	required
tosMask	ToS/traffic class mask	Integer	required

Field Name	Description	Type	Enforcement
proto	Layer 4 protocol	Integer	required
srcportOrIcmptypeFirst	Start of source port or ICMP4/6 type range	Integer	required
srcportOrIcmptypeLast	End of source port or ICMP4/6 type range	Integer	required
dstportOrIcmpcodeFirst	Start of destination port or ICMP4/6 code range	Integer	required
dstportOrIcmpcodeLast	End of destination port or ICMP4/6 code range	Integer	required
tcpFlagsValue	TCP flags value	Integer	required
tcpFlagsMask	TCP flags mask	Integer	required

Source-Verify

Source-Verify inhibits certain types of Denial of Service attacks based on IP address spoofing and IP address theft. When you enable Source-Verify, Cisco cnBR verifies the validity of IP packets received from CMs and CPEs. This verification is based on layer 2 and layer 3 addresses known to Cisco cnBR. Cisco cnBR learns the layer 2 and layer 3 addresses when DHCP assigns IP addresses to CM and CPE clients. If Cisco cnBR cannot determine the validity of a packet, it generates a lease-query in order to verify the packet. Source-Verify supports CPE IPv6 Prefix Delegation.

Source-Verify Logic

The following flowchart describes the Source-Verify logic in Cisco cnBR.

Figure 48: Source-verify logic
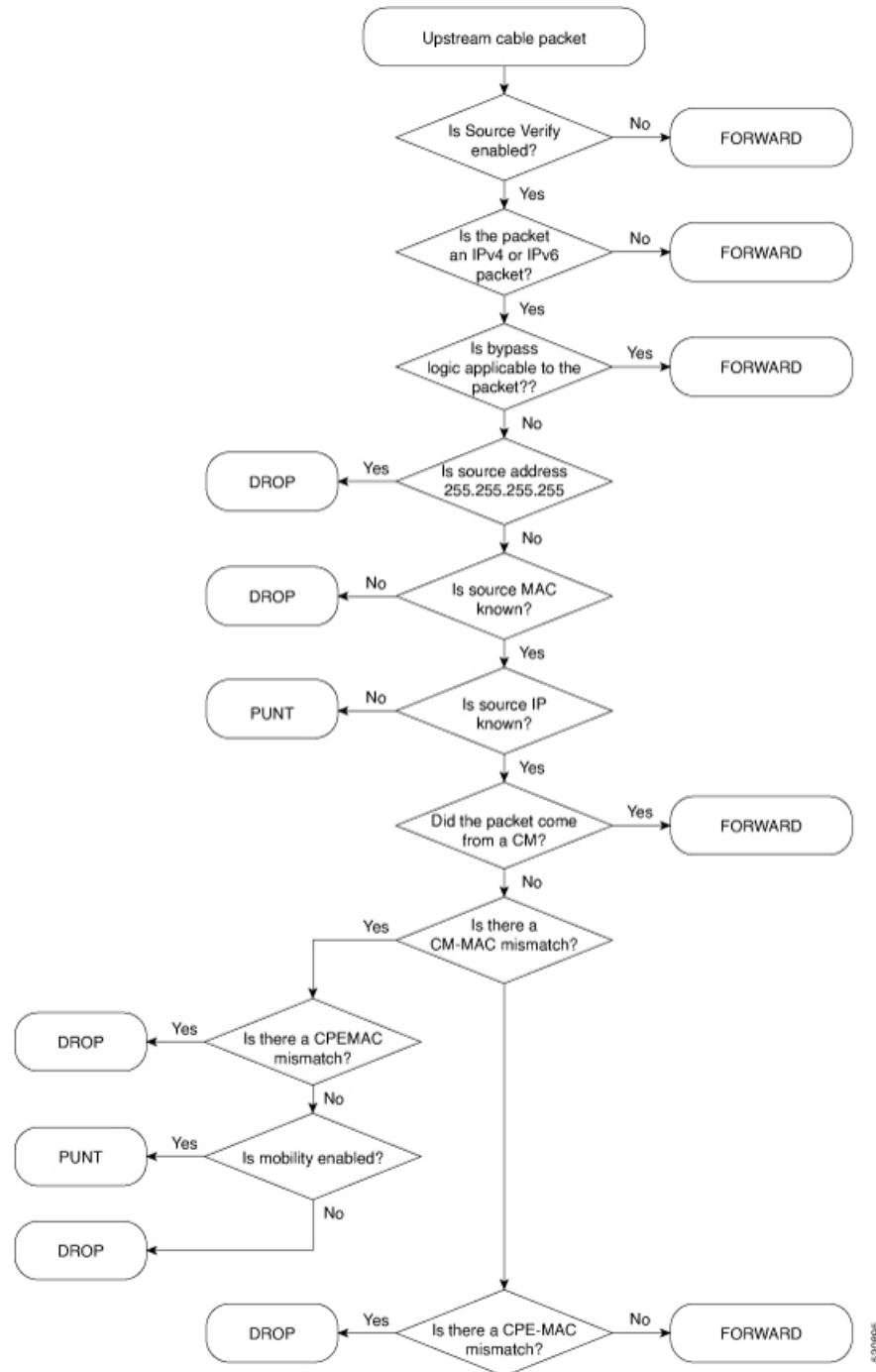
Bypass Logic

Cisco cnBR forwards packets that match any of the following criteria. These packets pass Source-Verify.

- IPv4 packets with src address 0.0.0.0

- IPv6 packets with multicast link local destination address

• IPv6 packets with unicast link local source or destination address

• IPv6 packets with unspecified source address

Invalid src Logic

Cisco cnBR drops packets that match the following criteria. These packets fail Source-Verify.

• IPv4 packets with source address 255.255.255.255

Configure Source-Verify

Initial Configuration of Source Verify From Autodeployer Script

In the Autodeployer script L3 template file, the Source-Verify configuration is in the *dhcp* block. To enable IPv4 Source-Verify, set *ipv4Lq* to true. To enable IPv6 Source-Verify, set *ipv6Lq* to true. To enable mobility, align CM/CPE scope with *mobilityScopes*.

```
"sgs": [
    ...
    "sg-config": {
        ...
        "dhcp": {
            "arpGlean": true,
            "arpProxy": true,
            "dhcpIfname": "cnr",
            "dhcpServers": [
                "10.2.2.91"
            ],
            "ipv4Lq": true,
            "ipv6Lq": true,
            "mobilityScopes": [
                "10.1.1.1/24",
                "2001::a/88"
            ],
            "ndProxy": true,
            "relayModeV4": 0,
            "relayModeV6": 0,
            "relayPolicies": [
                {
                    "deviceClass": "HOST",
                    "giAddr": "24.44.9.2",
                    "linkAddr": "2010::1",
                    "v4ServerIp": "1.2.2.91"
                }
            ],
            "v4Nets": [
                "9.44.9.2/24",
                "24.44.9.2/24"
            ],
            "v6Nets": null
        },
        ...
```

View Source Verify Configuration

Step 1   On the Cisco Operations Hub, click the Cisco Operations Hub main menu button.

Step 2 Choose **cnBR Manager** > **cnBRs** to open the **cnBR Clusters** page.

Step 3 Click **Import & Export cnBR** from the vertical navigation tab to access the **Export/Import** page.

Step 4 In the **Export cnBR Configuration** section, select the target Cisco cnBR from the drop-down list.

Step 5 Click **Export** to retrieve the SG configuration of the selected Cisco cnBR.

A .json file containing the full configuration is saved to your machine. Source-Verify settings are available in the *dhcp* block.

Update Source-Verify Configuration

You can update the configuration using the following methods:

- cnBR Manager Configurator

- Autodeployer reconfiguration

Both options send the full configuration to the CMTS. Cisco cnBR overwrites the existing configuration and activates the new configuration. For more details, see Autodeployer Limitations, on page 61.

Update Configuration using cnBR Manager

Step 1 On the Cisco Operations Hub, click the Cisco Operations Hub main menu button.

Step 2 Choose **cnBR Manager** > **cnBRs** to open the **cnBR Clusters** page.

Step 3 Click **Import & Export cnBR** to open the **Export/Import** page.

Step 4 On the **Export cnBR Configuration** pane, choose the Cisco cnBR that you want to update.

Step 5 Click **Export** to retrieve the SG configuration of the selected Cisco cnBR.

Step 6 Update the configuration in the *dhcp* block of the SG configuration and save the file.

Step 7 In the **Import cnBR Configuration File** section, select the target Cisco cnBR from the drop down list.

Step 8 Click **Browse** and select the saved configuration file.

Step 9 Click **Import** to push the updated SG configuration.

This import overwrites the existing configuration and activates the new configuration.

Update Configuration Using Autodeployer Reconfiguration

After the initial configuration of Source-Verify using the Autodeployer, update the configuration by modifying the corresponding blocks in the Autodeployer script and rerunning the Autodeployer. This process overwrites the existing configuration and activates the new configuration.

Default Source-Verify Configuration

By default, Source-Verify for both IPv4 and IPv6 is disabled.

Monitor Source-Verify

When the Cisco cnBR is unable to determine packet validity in the dataplane, it punts the packet for lease-query generation. Only punt statistics are available for Source-Verify.

- Mobility packets get the *mobility_v4* or *mobility_v6* punt-cause.

- All other Source-Verify punts get the *svfy_v4* or *svfy_v6* punt-cause.

On the Cisco Operations Hub, click the Cisco Operations Hub main menu button. Choose **Dashboard** to open the **Dashboard** page. Click **Find a Dashboard** to open the search pane. Enter **Punt Inject Stats** in the **Search dashboards by name** field and click the **Punt Inject Stats** row to open the **Punt Inject Stats** dashboard.

The Punt Inject Stats dashboard contains the punt statistics for Source-Verify and Mobility. Punted packets are subject to Punt-Rate-Limit processing. See for more information on these statistics.

Figure 49: Punt Inject Stats Page
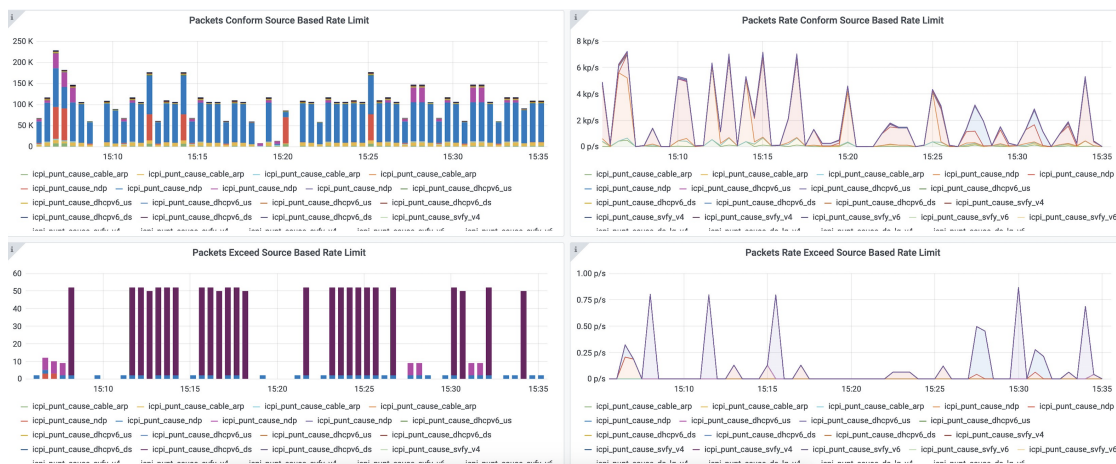
Cisco Cloud Native Broadband Router Maintenance

Cisco cnBR enables you to perform software upgrades seamlessly, and without disrupting any of the services. You can continuously deploy new services and features with minimal downtime.

RPD Secure Software Download

The cnBR Manager provides automated ways to securely download and activate software images to RPDs.

The secure software download (SSD) feature helps you to authenticate the source of a file and verify the integrity of the downloaded code before you use it in your system. The SSD feature is applicable to Remote PHY (R-PHY) devices installed in unsecure locations.

Prerequisites

To use SSD, the following prerequisites must be met:

- For Non-Express mode: The RPD software image is available at an external TFTP or HTTP image server. The image server is where the software image is stored, and can be accessed by RPD.

- For Express mode: The RPD software image is available in the Cisco Operations Hub. Ensure that RPD has connectivity to the management IP of Cisco Operations Hub.

- Ensure that code validation certificates are available. For more information, go through the Add Code Validation Certificates topic.

Upload Software Image for RPD

For Express-mode of SSD, upload the software image to the cnBR Manager. Complete the following steps:

Step 1 Enter the Cisco Operations Hub URL `https://{Hostname}` in the web browser.

Step 2   On the Cisco Operations Hub, click the Cisco Operations Hub main menu button.

Step 3   Choose **cnBR Manager** > **Remote PHY Devices** to open **Remote PHY Devices** page.

Step 4   Click **Image Management** to open **RPD Image** pane.

Step 5   Click **Choose file** to select the RPD software image file that you want to upload.

Step 6   Click **Upload**.

To delete any of the listed software image files, click the **X** icon that appears against the image name.

Download Software Image for RPD

Download the software image from the specified server. The software image is available on an external TFTP or HTTP image server.

To download an RPD software image using SSD, complete the following steps:

Step 1   Manually upload the software image to the external image server.

Step 2   Add code validation certificates.

Step 3   Upgrade the software image.

Note   You need to download the software image for RPD only for Non-Express mode. For Express mode, the image is available in the Operations Hub.

Add Code Validation Certificates

To authenticate the source and verify the integrity of the software image, Cisco cnBR uses the following two types of RPD code validation certificates (CVC).

• M-CVC: The type of CVC released along with the Cisco RPD software image. Contact Cisco Support to get the M-CVC.

• C-CVC: The type of CVC created and signed through Manufacturer's Statement of Origin (MSO). When CVCs are available, upload them using the following procedure:

Step 1   Enter the Cisco Operations Hub URL `https://{Hostname}` in the web browser.

Step 2   On the Cisco Operations Hub, click the Cisco Operations Hub main menu button.

Step 3   Choose **cnBR Manager** > **Remote PHY Devices** to open **Remote PHY Devices** page.

Step 4   Click **Code Validation Check** to open **RPD Code Validation Check** pane.

Step 5   Copy the contents from the CVC file to the appropriate text box and click **Add**.

Upgrade the Software Image

To upgrade the software, complete the following steps:

Step 1   Enter the Cisco Operations Hub URL `https://{Hostname}` in the web browser.

Step 2   On the Cisco Operations Hub, click the Cisco Operations Hub main menu button.

Step 3   Choose **cnBR Manager** > **Remote PHY Devices** to open **Remote PHY Devices** page.

Step 4   Click **Secure Software Download** to open **RPD Secure Software Download** pane.

Step 5   Scroll down the page and use the toggle button to choose to upgrade using either of the following options:

- Express Mode

- Non-Express Mode

Upgrade RPD in Express Mode

Complete the following steps to upgrade the RPD software in Express mode:

Note	Express mode works only with HTTP on PORT 80.

Step 1   In the **RPD Secure Software Download** pane, click **On** in the toggle button to choose the Express Mode option.
This step enables the Express mode, and the corresponding text fields are visible.

Step 2   Enter the following details in the appropriate text fields:

Field	Description
RPD Image	Choose the image from the list of available images in the drop-down list.

Ensure that the RPD is able to reach the Cisco Operations Hub management IP.

Step 3   Filter out the required RPDs by using the search field in the **RPD Summary** section. The list depicts the target RPDs for upgrade.

Step 4   Click **Upgrade Now** to upgrade the image without a reboot. Alternatively, you can also choose to upgrade during the next reboot by clicking **Save Configuration**.

Upgrade RPD in Non-Express Mode

Complete the following steps to upgrade the RPD software in Non-Express mode:

Step 1   In the **RPD Secure Software Download** pane, click **Off** in the Express Mode toggle button to choose the non-Express Mode option.

This step enables the Non-Express mode.

Step 2 Enter the following details in the appropriate text fields:

Field	Description
Image Server	Address of the server that stores the software image, and from where RPDs can access the software images.
Image Path	The relative path of the RPD software image on the server. The file is available in the default directory of the image server.
Method	HTTP or TFTP for RPD download SSD image.
M-CVC	Indicator showing whether the certificate is valid or not.
C-CVC	Indicator showing whether the certificate is valid or not.

Ensure that the RPD is able to reach the Cisco Operations Hub management IP.

Step 3 Filter out the target RPDs by using the search field in the **RPD Summary** section. The RPDs in this list of RPDs are the target RPDs for upgrade.

Step 4 Click **Upgrade Now** to upgrade the image without a reboot. Alternatively, you can also choose to upgrade during the next reboot, by clicking **Save Configuration**.

Monitor RPD and SSD State

The RPD SSD window provides options to monitor and trigger SSD operations. A dashboard, displaying three pie charts, provides details of the RPD status and metrics. Access this dashboard under the **Cisco Operations Hub** > **cnBR Manager** > **Remote PHY Devices** > **Secure Software Download**.

- RPD State: Displays the states of RPDs that are upgraded. During the upgrade process, the RPD becomes offline and then returns online.

- Software Version: Shows the number of RPDs for each RPD software version.

- SSD State: Shows various phases of the SSD progress of RPDs.

RPD Summary

The **RPD Summary** table provides details of RPDs which can be upgraded. You can also search for a specific RPD or set of RPDs that can be upgraded. The following table explains the fields in the **RPD Summary** pane.

This table explains the fields in the RPD Summary pane.

Field	Description
Name	Name of the RPD.
MAC Address	MAC address of the RPD.
Service Group	Service group ID of the RPD.

Field	Description
IPv4 Address	IPv4 address of the RPD.
IPv6 Address	IPv6 address of the RPD.
State	Status of the RPD: • online • offline
CCMTS ID	Host name of the Cisco cnBR application. Example: `cnbr1.cisco.com`
SSD State	Phase of the SSD progress.
Software Version	Version of the software running on the RPD.
Online Timestamp	Time when the RPD became online.

Service Group Operations

This table lists the features and the releases in which the feature was introduced and gives a small description of the feature.

Table 48: Feature History

Feature Name	Release Information	Feature Description
Service Group Operations	Cisco cnBR 21.1	You can view the worker-node each service group is running on and move service groups from one worker-node to another. This allows you to balance workloads across worker-nodes. You have better visibility and management on the service groups and the worker-nodes that they are running on.

Cisco cnBR enables you to move Data-over-Cable Systems Interface Standard (DOCSIS) service group workloads to other Cisco cnBR nodes during maintenance and troubleshooting activities. The Service Group related operations help avoid service interruptions during maintenance activities and help balance workloads across nodes.

Move Service Groups

You can move DOCSIS service groups across nodes. Moving Service Groups allows nodes to balance the Service Group workloads effectively. You can move one or multiple Service Groups using the cnBR Manager.

Perform the following steps to move Service Groups.

Step 1   On the Cisco Operations Hub, click **cnBR Manager** > **cnBRs**.

Step 2   On the navigation panel, click **Service Group Operations**.

Step 3   Select an available Cisco cnBR cluster from the drop-down list.
The table displays the nodes for the selected cluster.

Step 4   Select a node and click **Move Service Groups**.
The right panel lists down the available Service Groups for that node.

Step 5   Click the plus icon next to the Service Group to select a target Service Group.

Step 6   Select the destination node from the drop-down list.

Step 7   Click **Move** to trigger the move operation.
The status of the host and destination nodes changes to **SG Moving**. On completion of the operation, the Cisco Operations Hub updates Service Group information in the table.

Drain the Node

You can drain a node by moving all the DOCSIS service group workloads from the node. Draining allows you to safely remove the node from the cluster, allowing other nodes to take up workloads.

Perform the following steps to drain a node.

Step 1   Click Cisco Operations Hub > **cnBR Manager** > **cnBRs** > **Service Group Operations**.

Step 2   On the Service Group Operations panel, select an available Cisco cnBR cluster from the drop-down list. The table displays the nodes for the selected cluster.

Step 3   Select a node, click **Drain & Deactivate**, and confirm the drain operation.
On confirmation, the status of the node changes to *SG Moving*. On completion, the status changes to *Inactive*. A drained node has no associated Service Groups.

Activate the Node

A drained node appears as Inactive in the **Service Group Operations** pane (**cnBR Manager > cnBRs > Service Group Operations**). To move a drained node back to the working pool after maintenance, complete the steps:

Step 1   Select an available Cisco cnBR cluster from the drop-down list. The table displays nodes for the selected cluster.

Step 2   Select an inactive node and click **Activate**.
On successful activation, the selected node appears as *Active* in the Service Group Operations dashboard.

Audit of Service Group Operations

The Cisco Operations Hub records all Service Group related moves in the cnBR Manager for auditing.

To view the service group move, drain or activation history, perform the following step:

Navigate to **cnBR Manager > cnBRs > Service Group Operations** and click **Operations History**.
The **Operations History** table provides the following information:

- Action undertaken
- Status of the operation
- cnBR name
- Source and Destination Node
- Service Groups that moved successfully
- Service Groups that failed during movement (if any)
- Failure details (if any)
- The initiation time of the operation

Service Group Operations Errors and Warnings

Service Group Operations have the following errors and warnings:

Error

Error: Failed to drain node *<node-name>*, reason: job failed. Please try again later.

Diagnosis: The common cause for a draining job failure is a timeout occurring while waiting for responses from other microservices.

Solution: Attempt the operation later and see whether the issue is resolved.

Warning

Warning: Unable to drain *<node-name>*, reason: Insufficient SG capacity in other worker node.

Diagnosis: When draining a DOCSIS node, the Cisco cnBR moves the service groups to other DOCSIS nodes to keep the services running. Sometimes, the other DOCSIS nodes do not have the capacity to hold all service groups. In such cases, an error-dialog warns of the insufficient capacity.

Solution: To resolve the issue, click **Cancel** and stop the drain operation.

Export and Import Configuration

The system administrator performs the import and export of Cisco Operations Hub configurations using the Cisco Operations Hub UI or RESTful APIs. The system administrator can store the exported configuration

at a secure location. For Disaster Recovery, the system administrator performs the import operation to restore the Cisco Operations Hub to their original configurations.

From Cisco Operations Hub cluster, you can import and export:

- User Management data
- LDAP configuration
- Tag information
- Login Banner content
- User created Grafana and Kibana dashboards

Export Cisco cnBR Configuration using cnBR Manager

To export the Cisco cnBR configuration, complete the following steps:

Step 1 Click **Cisco Operations Hub** > **cnBR Manager** > **cnBRs**

Step 2 On the navigation panel, click **Import & Export cnBR**.

Step 3 Select the target Cisco cnBR from the drop-down list in the **Export cnBR Configuration** section.

Step 4 Click **Export**

Step 5 Rename the file and save it at a secure location.

Export Cisco cnBR Configuration using RESTful API

Run the following command in a UNIX shell to export the Cisco cnBR configuration:

```
curl -k -X GET 'https://{opsHUBHost}/api/configurator/v1/cmts/config/{cmts-id}' -H 'Accept:
application/json' -H 'Authorization: Bearer <token>' | tee path/to/backup/config
```

Example

```
hostname#curl -k -X GET
'https://opshub1.cisco.com/api/configurator/v1/cmts/config/cnbr1.cisco.com' -H 'Accept:
application/json' -H 'Authorization: Bearer <token>' | tee
cnbr-10.79.193.236-configuration.json
```

Export Cisco Operations Hub Configuration using Cisco Operations Hub

To export the Cisco Operations Hub configuration, complete the following steps:

Step 1 Click the Cisco Operations Hub main menu button > **System** > **Import & Export** to open the Cisco Operations Hub Export/Import pane.

Step 2 Click **Export** in the **Export Configuration** section to download the file containing the configuration.

Step 3 Rename the file and save it to a secure location.

Export Cisco Operations Hub Configuration using RESTful API

Run the following command in a UNIX shell to export the Cisco Operations Hub configuration:

```
curl -k -X GET 'https://{opsHUBHost}/configurator/opshub/export' -H 'Accept: application/json' -H
'Authorization: Bearer <token>' | tee path/to/backup/config
```

Example

```
hostname#curl -k -X GET 'https://opshub1.cisco.com/configurator/opshub/expor' -H 'Accept:
application/json' -H 'Authorization: Bearer <token>' | tee
opshub-172.22.29.221-configuration.json
```

Import Cisco cnBR Configuration using cnBR Manager

To import the Cisco cnBR configuration, complete the following steps:

Step 1 Click **Cisco Operations Hub** > **cnBR Manager** > **cnBRs**

Step 2 On the navigation panel, click **Import & Export cnBR**.

Step 3 Select the target Cisco cnBR from the drop-down list in the **Import cnBR Configuration** section.

Step 4 Click **Browse** and choose a cnBR Configuration file.

Step 5 Click **Import**.

Import Cisco cnBR Configuration using RESTful API

Run the following command in a UNIX shell to import the Cisco cnBR configuration:

```
curl -k -X PUT 'https://{opsHUBHost}/api/configurator/v1/cmts/config/{cmts-id}' -H 'Accept:
application/json' -H 'Content-Type: application/json' -H 'Authorization: Bearer <token>' -d
'@path/to/backed/up/config
```

Example

```
hostname#curl -k -X PUT
'https://opshub1.cisco.com/api/configurator/v1/cmts/config/cnbr1.cisco.com' -H 'Accept:
application/json' -H 'Content-Type: application/json' -H 'Authorization: Bearer <token>'
-d '@cnbr-10.79.193.236-configuration.json
```

Import Cisco Operations Hub Configuration using Cisco Operations Hub

To import the Cisco Operations Hub configuration, complete the following steps:

Step 1   Click the Cisco Operations Hub main menu button > **System** > **Import & Export** to open the Cisco Operations Hub Export/Import pane.

Step 2   On the **Import Configuration** section, browse and choose an Operations Hub configuration file in tar.gz format.

Step 3   Click **Import**.

Import Cisco Operations Hub Configuration using RESTful API

Run the following command in a UNIX shell to import the Cisco Operations Hub configuration:

```
curl -k -X PUT "https://{opsHUBHost}/configurator/opshub/import" -H "accept: application/json" -H
"Content-Type: application/json" -H 'Authorization: Bearer <token>' -d "@path/to/backed/up/config
```

Example

```
hostname#curl -k -X PUT 'https://opshub1.cisco.com/configurator/opshub/import' -H 'Accept:
 application/json' -H 'Content-Type: application/json' -H 'Authorization: Bearer <token>'
-d '@opshub-172.22.29.221-configuration.json
```

CHAPTER 5

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 Cisco Operations Hub dashboard. On-Demand diagnosis does not require any configuration changes.

Complete the following steps to enable On-Demand Diagnosis:

Step 1   Enter the Cisco Operations Hub URL `https://{Hostname}` in the web browser.

Step 2   On the Cisco Operations Hub, click the Cisco Operations Hub main menu button.

Step 3   Choose **Dashboard** to open the **Dashboard** page.

Step 4   Click **Find a Dashboard** to open the search pane.

Step 5   Enter **Cable Modem Verbose** in the **Search dashboards by name** field and click the **Cable Modem Verbose** row to open the **Cable Modem Verbose** dashboard.

Step 6   Select the Cisco cnBR name and modem that you want to debug from the **cnBR Name** and **Cable Modem** drop-down lists.

Step 7   Click **Cable Modem Log From cnBR** pane.

Step 8   Click **Debug**.

Step 9   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   Enter the Cisco Operations Hub URL `https://{Hostname}` in the web browser.

Step 2   On the Cisco Operations Hub, click the Cisco Operations Hub main menu button.

Step 3   Choose **Dashboard** to open the **Dashboard** page.

Step 4   Click **Find a Dashboard** to open the search pane.

Step 5   Enter **diagnosis** in the **Search dashboards by name** field and click the **Diagnosis** row to open the **Diagnosis** dashboard.

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

Step 6   To view detailed information about these tables, expand the tables and click the **i** icon at the top-left corner.

Cable Modem Troubleshooting

The table lists the features, the Cisco cnBR version in which it was introduced, and also gives a short description of the feature.

Table 49: 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   Enter the Cisco Operations Hub URL `https://{Hostname}` in the web browser.

Step 2   On the Cisco Operations Hub, click the Cisco Operations Hub main menu button.

Step 3   Choose **Dashboard** to open the **Dashboard** page.

Step 4   Click **Find a Dashboard** to open the search pane.

Step 5   Enter **Cable Modem Verbose** in the **Search dashboards by name** field and click the **Cable Modem Verbose** row to open the **Cable Modem Verbose** dashboard.

Step 6   Click **Troubleshoot**.

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

Step 7   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_MTN_Q\",\"RngTxchState\":\"TXCH_ST_STA_MTN\",


\"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 Enter the Cisco Operations Hub URL `https://{Hostname}` in the web browser.

Step 2 On the Cisco Operations Hub, click the Cisco Operations Hub main menu button.

Step 3 Choose **Dashboard** to open the **Dashboard** page.

Step 4 Click **Find a Dashboard** to open the search pane.

Step 5 Enter **Cable Modem Verbose** in the **Search dashboards by name** field and click the **Cable Modem Verbose** row to open the **Cable Modem Verbose** dashboard.

Step 6 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.

Cable Modem IP Ping-Loss History		
Time ▼	RTT	IP Loss
2021-06-22 11:52:03	-	100.0%
2021-06-22 11:51:03	-	100.0%
2021-06-22 11:50:03	-	100.0%
2021-06-22 11:49:03	-	100.0%

1 2 3 4 5 6 7 8 9

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.

Step 7 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 8   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 50: 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 Dashboards

The **Dashboards** menu in the Cisco Operations Hub allows you to monitor the status of the Cisco cnBR router. Cisco Operations Hub 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 dashboards later retrieve and display the data.

The following illustration shows the Dashboards framework.

Cisco cnBR Dashboards

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

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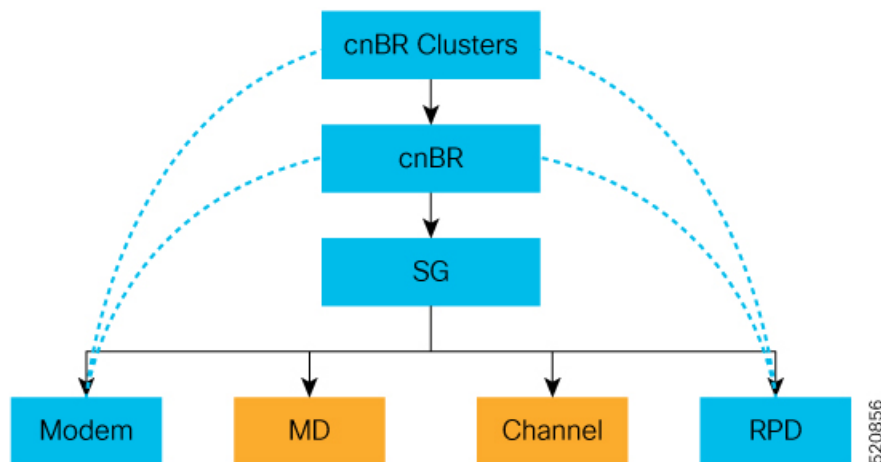
The Dashboard user interface (UI) has the following components:

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.
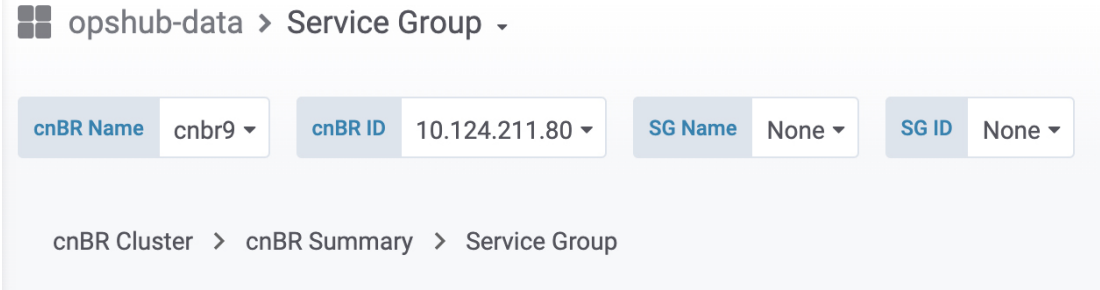
Links

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.
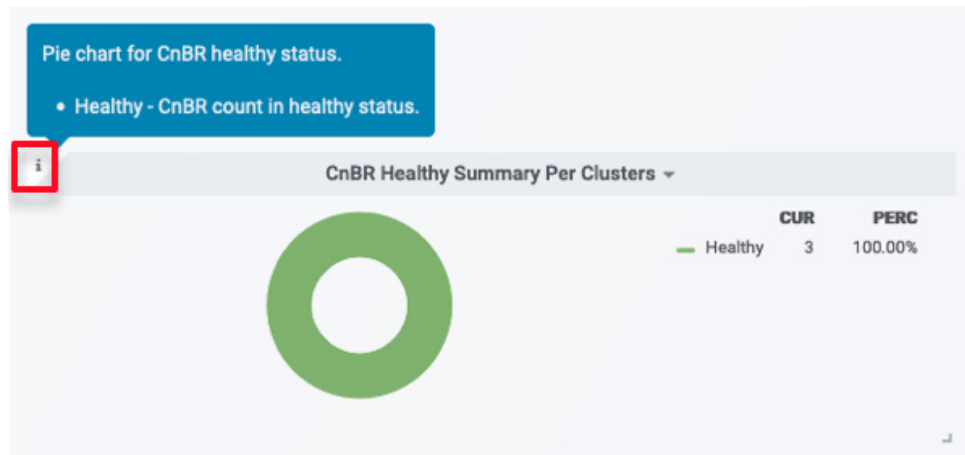
Dashboard Refresh and Time Range

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.
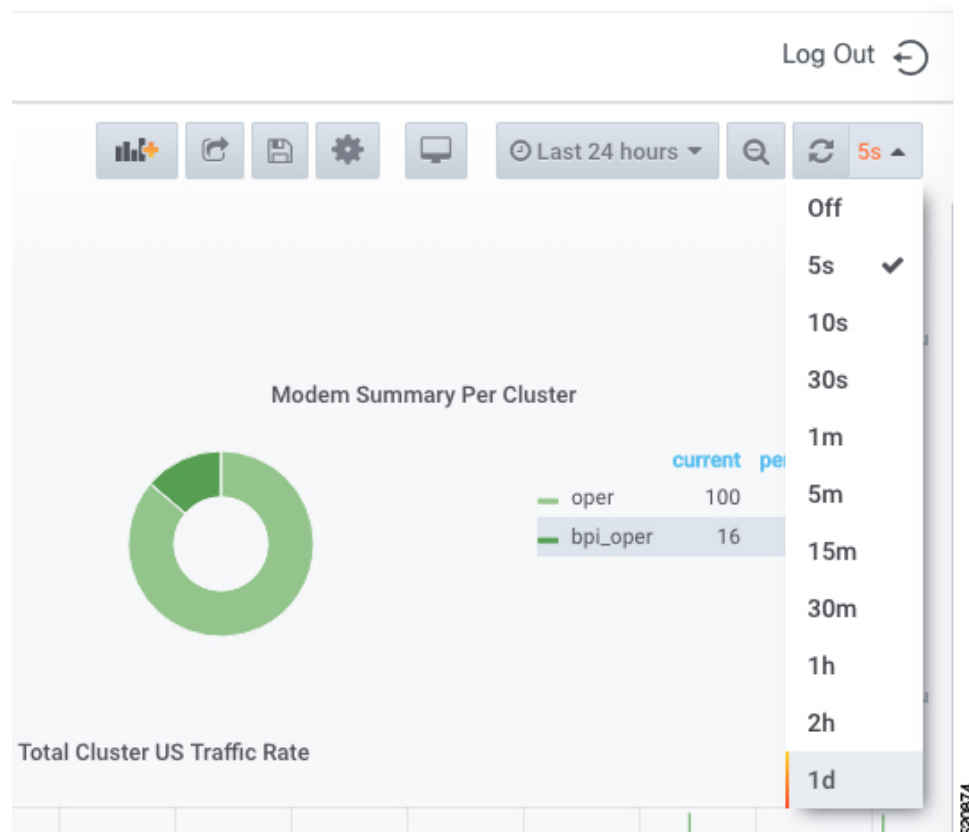
If data is retrieved from the Prometheus database, choose the required value from the **Custom time range** drop-down list as shown in the following image.
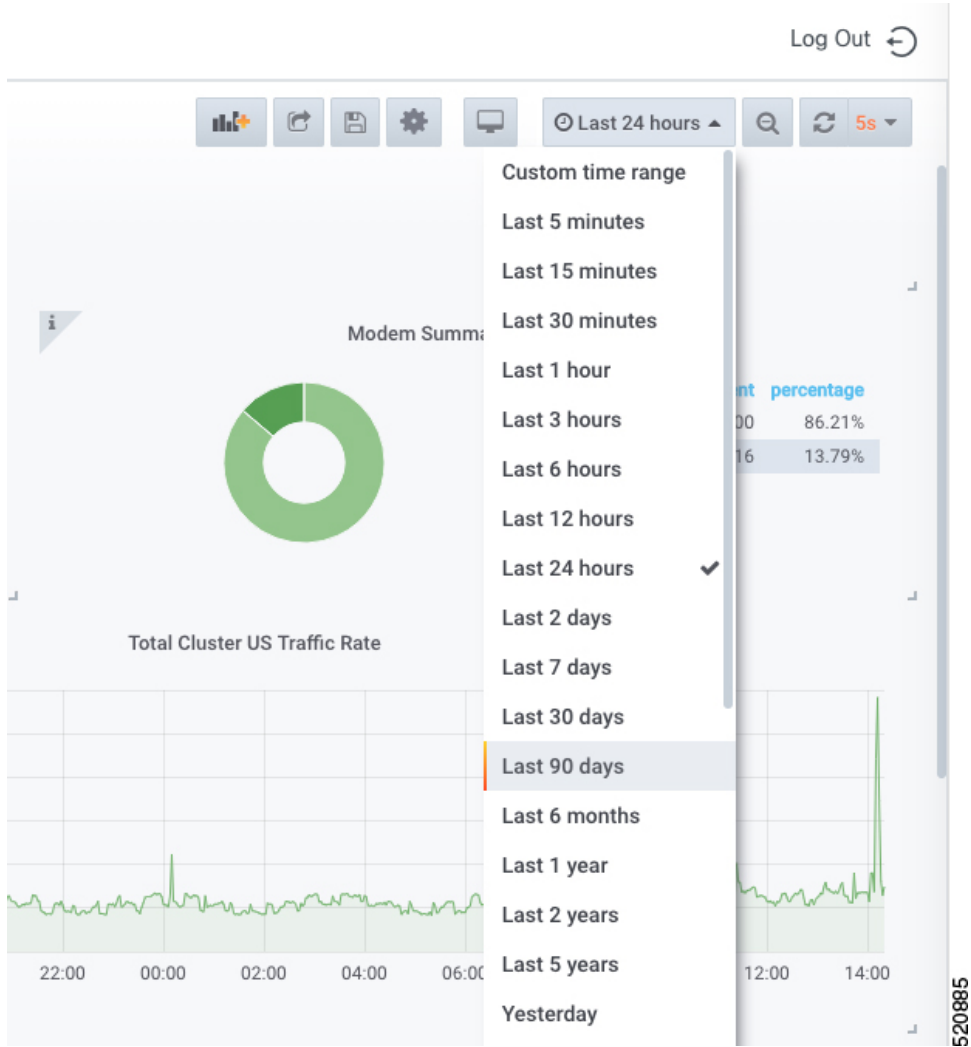
Data Display on Dashboard

The table lists the features, the Cisco cnBR version in which it was introduced, and also gives a short description of the feature.

Table 50: Feature History

Feature Name	Release Information	Feature Description
Downstream and upstream channel utilization live graphs	Cisco cnBR 21.2	Downstream and upstream channel utilization live graphs are added in the traffic throughput section of the service group dashboard. You can view the utilization of the downstream and upstream channels under the service group in these live graphs.

Feature Name	Release Information	Feature Description
Modem type column	Cisco cnBR 21.2	A modem type column is added in the Cable Modem List table of the Cable Modem List dashboard. It shows the DOCSIS version of the cable modem.

The Dashboard panel provides a list of commonly used dashboards. The dashboard includes the cnBR Manager Overview, cnBR Summary, RPD List Summary, Service Group Summary, Service Groups List, Cable Modem Table List, and other recently used dashboards.

To access the Dashboard, click **Cisco Operations Hub** > **Dashbboard**.

You can alternatively search for dashboards by clicking **Find a 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:

Describes each panel in the cnBR Cluster dashboard

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

Panel Name	Description
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.
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:

Describes each panel in the cnBR Summary dashboard

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.

Note   Use the **Actions** drop-down option in this dashlet to reset or delete all offline cable modems for the selected Cisco cnBR cluster.
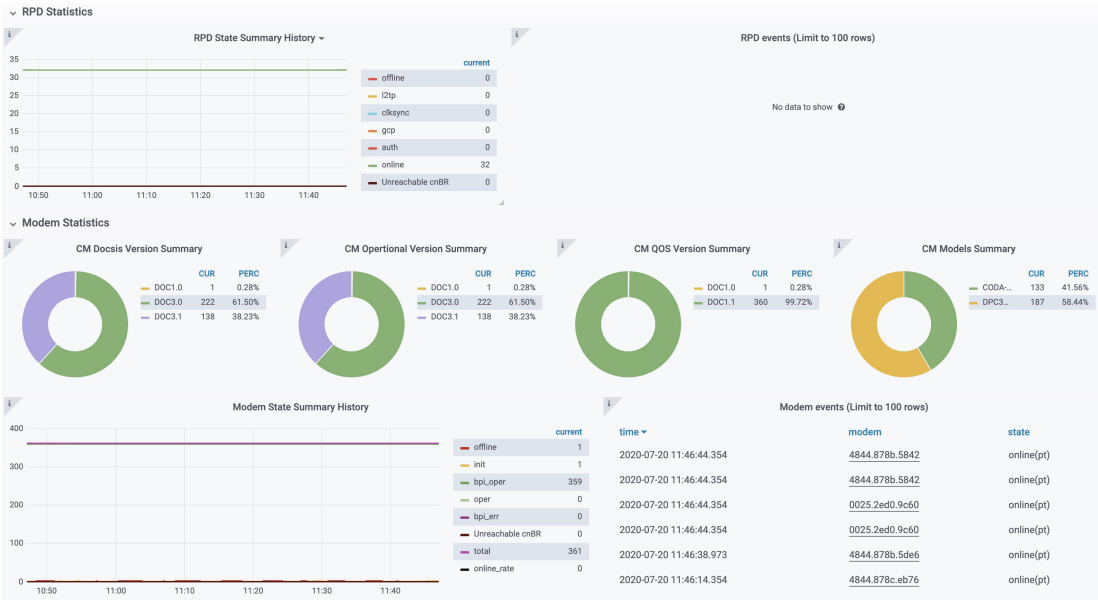
Service Group

The Dashboard displays the following information:

Describes each panel in the Service Group dashboard

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	Shows the traffic throughput for a selected service group. Provides following live graphs: • DS Traffic Throughput • DS Channel Frequency & Utilization • US Traffic Throughput • US Channel Frequency & Utilization.

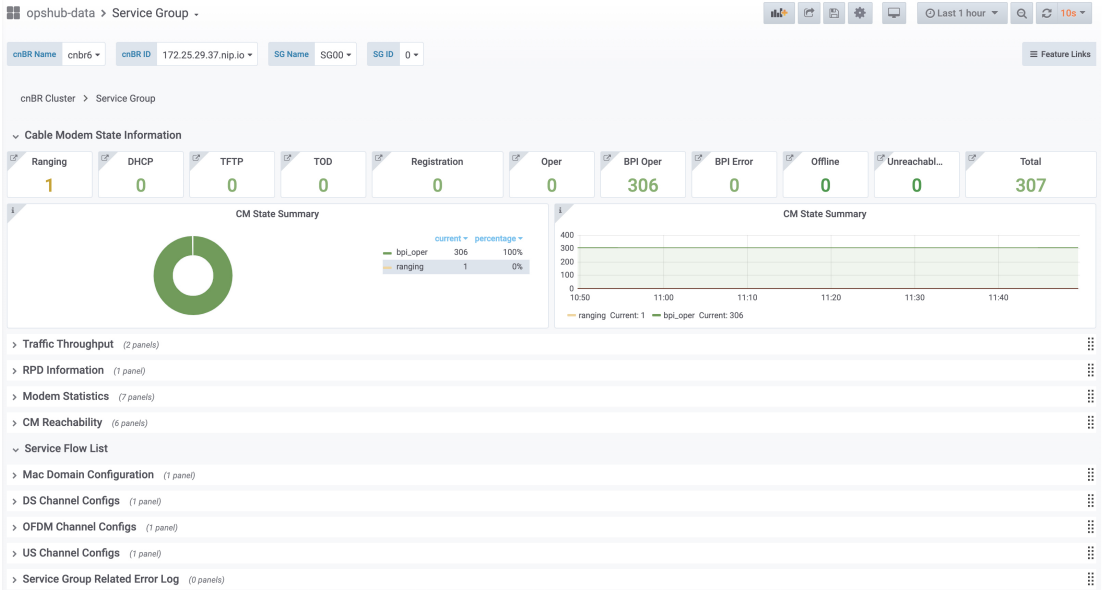| Panel Name	Description

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
Cable 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 operations on cable modems for a selected Cisco cnBR and the service group from the **Actions** drop-down option. • Reset All Offline Modems • Reset All Searched Modems • Delete All Offline Modems • Delete All Searched Modems
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.

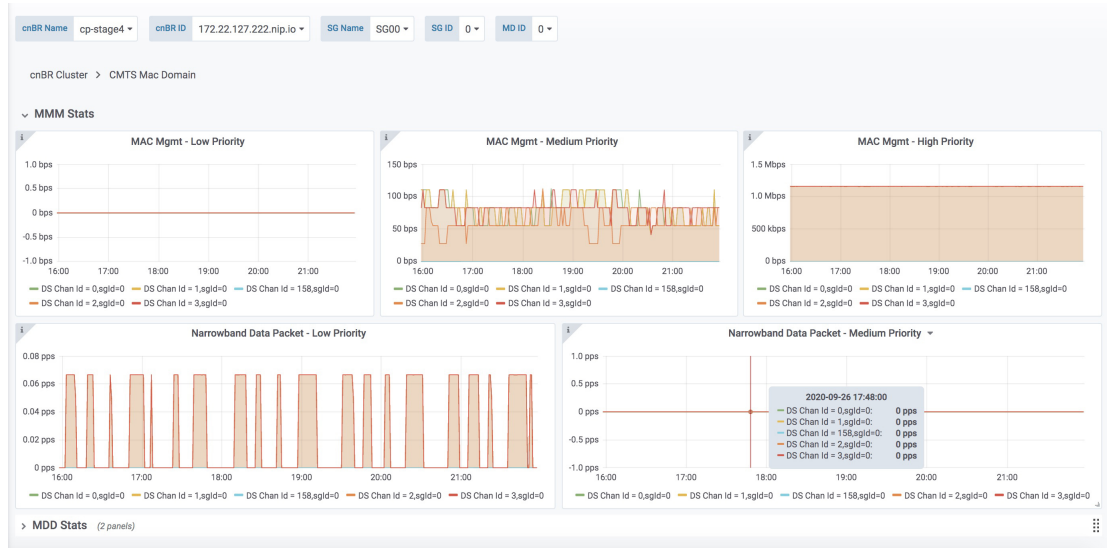| Panel Name	Description
US channel configs	Upstream channel configuration. • upstream channel id: Upstream channel ID • slotsize: Minislot size • frequency: Frequency • docsismode: DOCSIS Mode • modulation: Modulation profile • powerlevel: Power level • channelwidth: Channel width • sgid: Service group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

CMTS MAC Domain

The Dashboard displays the following information:

Describes each panel in the CMTS MAC Domain dashboard

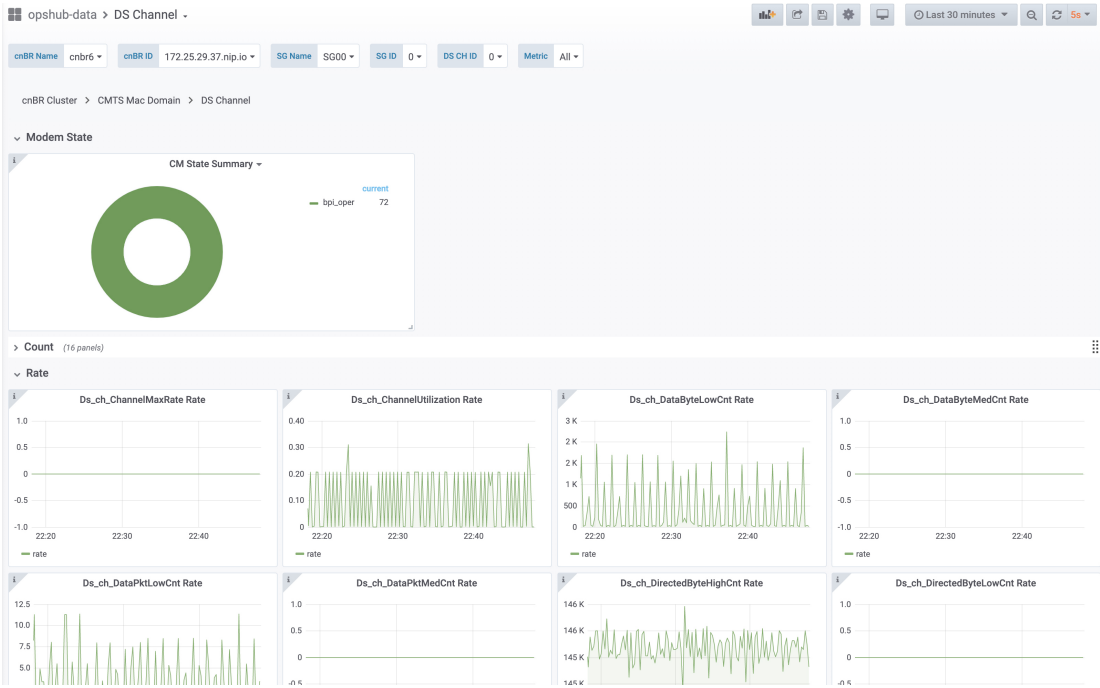| Panel Name	Description
MMM stats	Rate history of MAC management messages.
MDD stats	Rate history of MDD.

DS Channel

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

Describes each panel in the DS Channel dashboard

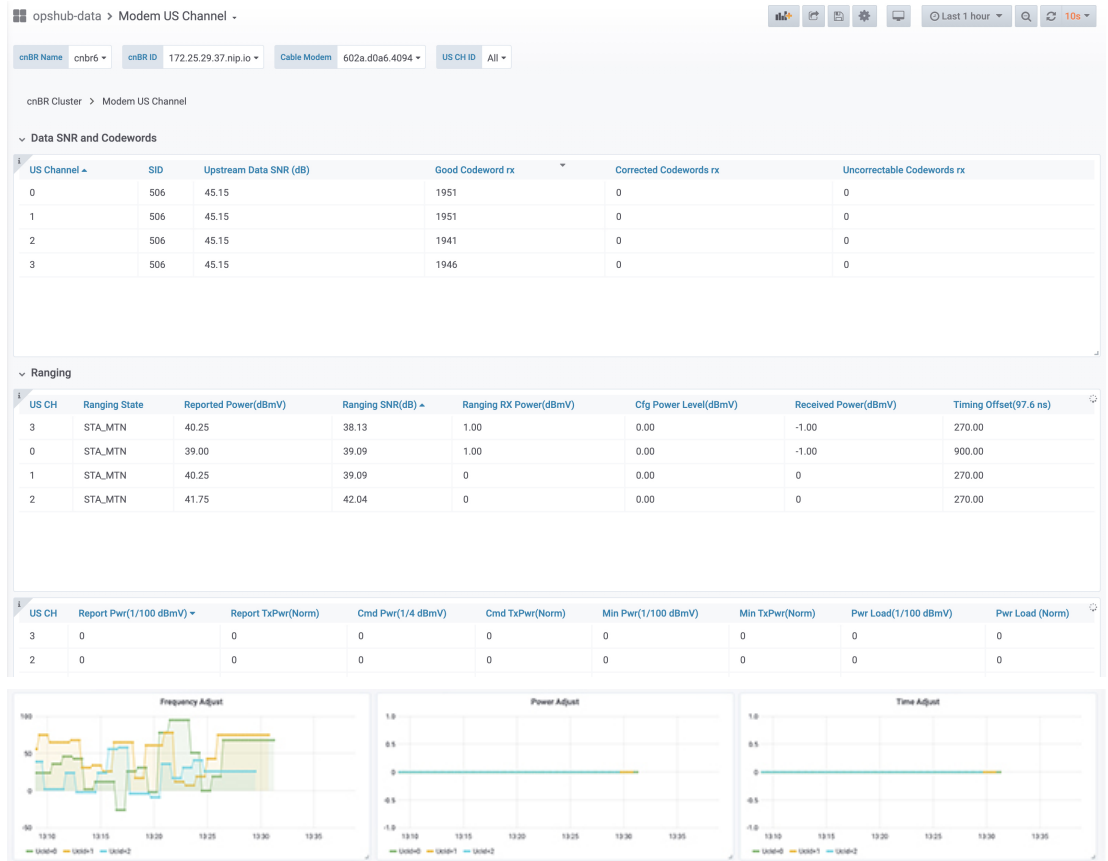| Panel Name	Description
Modem state	Summary of modems in different states for the specific Cisco cnBR cluster.
Count	Downstream channel count of the cable modem.
Rate	Downstream traffic rate for the Cisco cnBR cluster.

Modem US Channel

The Dashboard displays the following information:

Describes each panel in the Modem US Channel dashboard

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.

opshub-data > Modem US Channel

Last 1 hour   10s

cnBR Name cnbr6   cnBR ID 172.25.29.37.nip.io   Cable Modem 602a.d0a6.4094   US CH ID All

cnBR Cluster > Modem US Channel

Data SNR and Codewords

US Channel ▲	SID	Upstream Data SNR (dB)	Good Codeword rx ▼	Corrected Codewords rx	Uncorrectable Codewords rx
0	506	45.15	1951	0	0
1	506	45.15	1951	0	0
2	506	45.15	1941	0	0
3	506	45.15	1946	0	0

Ranging

US CH	Ranging State	Reported Power(dBmV)	Ranging SNR(dB) ▲	Ranging RX Power(dBmV)	Cfg Power Level(dBmV)	Received Power(dBmV)	Timing Offset(97.6 ns)
3	STA_MTN	40.25	38.13	1.00	0.00	-1.00	270.00
0	STA_MTN	39.00	39.09	1.00	0.00	-1.00	900.00
1	STA_MTN	40.25	39.09	0	0.00	0	270.00
2	STA_MTN	41.75	42.04	0	0.00	0	270.00

US CH	Report Pwr(1/100 dBmV) ▼	Report TxPwr(Norm)	Cmd Pwr(1/4 dBmV)	Cmd TxPwr(Norm)	Min Pwr(1/100 dBmV)	Min TxPwr(Norm)	Pwr Load(1/100 dBmV)	Pwr Load (Norm)
3	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0

Frequency Adjust

Power Adjust

Time Adjust

520887

520888

Cable Modem List

The Dashboard displays all Cable Modems in a list, based on the cluster, Service Group, Mac Domain, CM state and CM type.

Describes each panel in the Cable Modem List dashboard.

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. The parameter `Total` denotes 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 • Modem Type: DOCSIS version of cable modem, that is D3.1, D2.0, D1.0 • 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: cnBR Identifier • 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: Time stamp when the cable modem became offline • Last Update: Time stamp of the last entry

The **Download CSV** option allows you to download information for online and offline cable modems. However, the download option is limited to one Cisco cnBR cluster at a time. You can use the Cable Modem State History dashboard for historical information.

Cable Modem Verbose

The Dashboard displays the following information:

Describes each panel in the Cable Modem Verbose dashboard.

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

Cable System Description Summary

The dashboard displays the Cable Modem versions and system summary. The following table lists the panel names and their descriptions.

The table contains information about the dashboard, and displays the Cable Modem versions and system summary.

Panel Name	Description
Vendor	The pie chart shows Cable Modem Vendor distribution.
HW Version	The pie chart shows Cable Modem Hardware Version distribution.
SW Version	The pie chart shows Cable Modem Software Version distribution.
Cable system Description	The table shows Cable Modem system information along with Power level and SNR

The Cisco cnBR Manager periodically queries Cable Modems to retrieve Cable Modem system information using SNMP. The default polling interval for a query is 15 minutes, and the default SNMP read-only community

string is *public*. You can change the default polling interval and community string by using Kubernetes ConfigMap APIs.

```
ConfigMap Name: cmts-hm-conf
NameSpace: cnbrmanager-data
Key:
  remote_query:
      interval: 900
      snmp:
          community : public
```

RPD List Summary
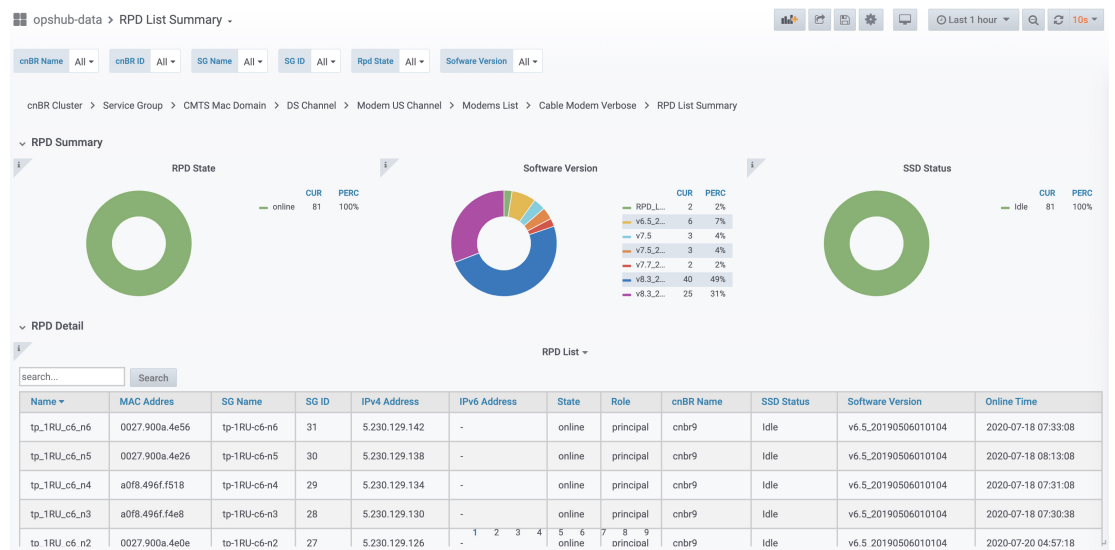
The Dashboard displays the following information:

Describes each panel in the RPD List Summary dashboard.

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:

Describes each panel in the RPD Verbose dashboard.

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 Preconfiguration. • 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
	• Bidirection RF Ports: bidirectional 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 timings 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: time stamp

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
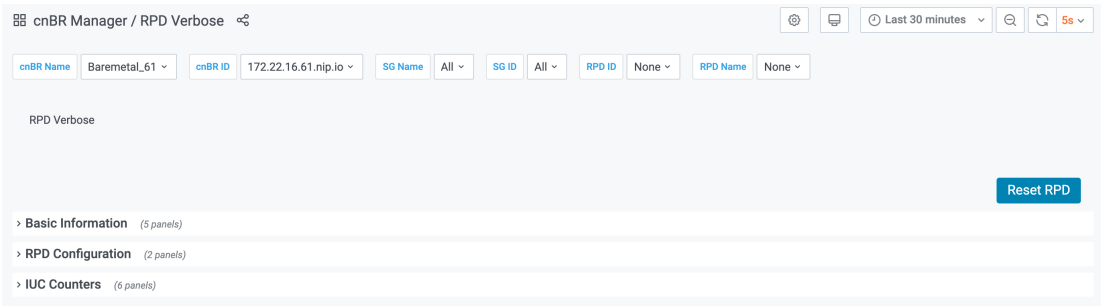
You can use the **Reset RPD** button to reboot all operations on the RPD.

> ✎
>
> **Note** Resetting the RPD would affect all existing services.

Search for Dashboards

Follow this procedure to search for dashboards:

Step 1 Click **Cisco Operations Hub** > **Dashboards**.

Step 2 On the navigation panel, click **Find a Dashboard**.

Step 3 Enter the dashboard name in the **Search dashboards by name** field and select the target dashboard.

Alternatively, you can also click *Infrastructure*, *cnBR Manager*, or *Operations Hub* folders and browse for a specific dashboard.

Customize Dashboards

This table lists the features and the releases in which the feature was introduced and gives a small description of the feature.

Table 51: Feature History

Feature Name	Release Information	Feature Description
Customize Dashboards	Cisco cnBR 21.2	You can customize Cisco cnBR and Cisco Operations Hub dashboards to analyze and visualize your data the way you want to. You can use the real-time data or the historical data for this purpose.

Cisco Operations Hub and Cisco cnBR Manager include numerous prebuilt data-visualization dashboards.

Dashboards in cnBR Manager show information about the Cisco cnBR and the RPDs they serve. The dashboards provide the following information:

- A real-time look at the health and metrics (updated every 10 sec)

- Historical data for visualizing trends over longer intervals

Cisco Operations Hub dashboards show information on the infrastructure and cloud software that powers Cisco cnBR and the Operations Hub.

The prebuilt dashboards are designed to meet the needs of most cable service providers. However, according to your requirement, you may customize the existing dashboards or create new dashboards. This section explains how to customize and create new dashboards.

Plan and Organize New Dashboards

You can create or customize dashboards based on your familiarity with Grafana and its data sources.

- If you are new to Grafana, you can create new dashboards using existing dashboards.

- If you are familiar with Grafana, you can create dashboards from scratch or export existing dashboards, modify them, and import them back into the Cisco Operations Hub.

Before customizing or creating new dashboards, you must do the following:

- Identify data sources

- Identify visualization panels

- Plan the layout

Create a New Dashboard

Step 1   From the Cisco Operations Hub main menu, click **Dashboards**.

Step 2   Click **Advanced** > **Manage** in the left navigation menu of the **Dashboards** page.

Step 3   Click the **New Dashboard** button under the **Manage** tab.

Step 4   Click **Add new panel**.

Step 5   Configure the panel with the required data sources and visualization type.

Step 6   Click **Save**.

You can rearrange the panel location within the dashboard by dragging the panel header to the correct location. You can also resize the panels by dragging the bottom-right corner of the panel.

Create a New Dashboard from an Existing Dashboard

Step 1   Open the dashboard which you want to customize.

Step 2   Click the **Dashboard settings** gear icon at the top of the dashboard page.

Step 3   Click **Save As…** on the left side of the dashboard **Settings** page.

Step 4   Enter a new dashboard name and choose a folder in the **Save dashboard as...** pop-up window.

Step 5   Click **Save**.

Step 6   Open this new dashboard, click the **Panel Title**, and click **Edit** to edit the panel properties.

On the **Edit Panel** page, edit the panel properties in the three tabs: **Panel**, **Field**, and **Overrides**. You can also create a query, and set the transformations and alerts for the dashboard.

Step 7   Click **Save** at the top of the **Edit Panel** page.

You can rearrange the panel location within the dashboard by holding and dragging the panel title to the required location. You can also resize the panels by dragging the bottom-right corner of the panel.

Create New Dashboard Using Export and Import

The following process is recommended only for advanced users.

Step 1   Open the dashboard that you want to export.

Step 2   Click the share icon at the top of the page to the right of the dashboard name.

Step 3   Click the **Export** tab.

Step 4   Click **Save to file**.

Step 5   Edit the JSON file.

Step 6   From the Cisco Operations Hub main menu, click **Dashboards** > **Advanced** > **Manage**.

Step 7   Click **Import**.

Use one of the following options to import the dashboard file:

- Click **Upload JSON file** and choose the dashboard file.

- Enter a dashboard URL or ID in the **Import via grafana.com** text box and click **Load**.

- Enter a valid dashboard JSON model in the **Import via panel json** text area and click **Load**.

On the next page, add the required data and click **Import**.

What to do next

After you import a dashboard, you can customize it. For more details, see .

Customize Dashboard Panels

You can add new panels to a newly created dashboard.

- When you create a dashboard from an existing one, click the **Add panel** icon to open the **Edit Panel** page to add more panels.

- When you create a new dashboard using the **New Dashboard** option, click the **Add new panel** button to open the **Edit Panel** page.

The following tabs are available on the **Edit Panel** page using which you can edit all panel properties.

The table describes each tab in the Edit Panel

Tab	Description
Query	Allows you to create new queries, configure, and update existing data sources.
Transform	Allows you to calculate, reorder, and rename your query results before visualizing them.
Alert	Allows you to create rules, conditions, and notifications on the supported data sources.
Panel	Allows you to configure the visual properties of the panel. You can choose from the available visualization plug-ins.
Fields	Allows you to rename and configure fields appearing in the visualizations. In addition, you can link the current panel to other panels and dashboards using the **Data Links** option.
Overrides	Allows you to add rules for field overrides, which provide fine-grained control over how your data appears in the dashboard.

KPI Alert Management

The table lists the features, the Cisco cnBR version in which it was introduced, and also gives a short description of the feature.

Table 52: 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 dashboard:

Step 1 Enter the Cisco Operations Hub URL `https://{Hostname}` in the web browser.

Step 2 On the Cisco Operations Hub, click the Cisco Operations Hub main menu button.

Step 3 Choose **Dashboard** to open the **Dashboard** page.

Step 4 Click **Find a Dashboard** to open the search pane.

Step 5 Enter **KPI Alert Management** in the **Search dashboards by name** field and click the **KPI Alert Management** row to open the **KPI Alert Management** dashboard.

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.

Alert groups and alerts for each group

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

To view the KPI Alert Summary Dashboard, complete the following steps:

1. On the Cisco Operations Hub, click the Cisco Operations Hub main menu button.

2. Click **Dashboards** > **DAA Overview**.

KPI Alert Information

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

The table describes attribute in the KPI Alert Information pane

Attribute Name	Description
Firing Time	Alert fired time.
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.

Configure Alerts - Global Configuration pane

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

| 1 alert for |

View In AlertManager

[1] Firing

Labels
alertname = NodeNotHealthy
cluster = jiancheng-0
cnbr = 10.124.211.230
group = Infra
instance = cmts-hm-clusterkpi-service.opshub-data.svc:3000
job = kubernetes-probe-honor-labels-services
monitor = prometheus
namespace = cee-data
path = /health/kube/node/cpu/
pod = node-exporter-49vp6
replica = jiancheng-0
severity = critical
Annotations
description = On cnBR: 10.124.211.230, node is not healthy for more than 10 minutes, and KPI path: /health/kube/node/cpu/.
summary = Node not Healthy
type = Quality Of Service Alarm
Source

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.

Customize Kibana Queries and Data Visualization

The table lists the features, the Cisco cnBR version in which it was introduced, and also gives a short description of the feature.

Table 53: Feature History

Feature Name	Release Information	Feature Description
Customize Kibana Queries and Data Visualization	Cisco cnBR 21.2	You can create Kibana queries, retrieve data, and then customize how you want to present the queried data in Cisco cnBR.

To customize Kibana queries and data visualizations, use the following procedure:

- Create index patterns

- Discover data and save the query

- Visualize data from the query

Create Index Patterns

Define the data for which you want to create the panel. Data is always generated from Elasticsearch indices. You can use an existing index or create a new one by providing a pattern.

Step 1   From the Cisco Operations Hub main menu, click **System** > **Logs**.

Step 2   Click **Advanced** > **Manage** in the left navigation menu.

Step 3   Click **Index Patterns** link in the Kibana **Management** panel.

You can search and create a new pattern based on your requirement.

Step 4   Click **Create index pattern**.

Follow the index pattern creation window.

Discover Data

After you identify or create an Index pattern, discover the relevant data and clean it.

Step 1   From the Cisco Operations Hub main menu, click **System** > **Logs**.

Step 2   Click **Advanced** > **Discover** in the left navigation menu.

The data query panel appears.

Step 3   Create search, add filters, and choose required data columns.

Step 4   Set up refresh intervals using the option in the top-right corner.

Step 5   After the data discovery, save the query with a valid name.

Next time when you view **Advanced** > **Discover**, this saved query appears.

Visualize Data from Query

After data discovery, you can present your data in different ways.

Step 1   From the Cisco Operations Hub main menu, click **System** > **Logs**.

Step 2   Click **Advanced** > **Visualize** in the left navigation menu.

Step 3   Click **Create visualization** or search for an existing configuration.

Step 4   In the **New Visualization** window, choose a visualization type, and then configure and save them.

Next time when you view the **Visualizations** window, the saved visualizations appear in the **Visualization** window.

Log Aggregation and Management

The table lists the features, the Cisco cnBR version in which it was introduced, and also gives a short description of the feature.

Table 54: 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 collect logs from all the components. However, to send the logs to Cisco Operations Hub, you must manually configure Cisco cnBR.

To manually configure the Cisco cnBR to send the logs to Cisco Operations Hub, complete the following steps:

Step 1 Log in to Cisco cnBR 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 Enter the Cisco Operations Hub URL `https://{Hostname}` in the web browser.

Step 2 On the Cisco Operations Hub, click the Cisco Operations Hub main menu button.

Step 3 Choose **System** > **Logs** to open **Logs** page.

Step 4 Click **Advanced** > **Discover** from the left navigation menu.

Step 5 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   Enter the Cisco Operations Hub URL `https://{Hostname}` in the web browser.

Step 2   On the Cisco Operations Hub, click the Cisco Operations Hub main menu button.

Step 3   Choose **System** > **Logs** to open **Logs** page.

Step 4   Click **Advanced** > **Visualize** from the left navigation menu.

Step 5   Click **Create visualisation**.

Step 6   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 7   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 297.

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.

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   Enter the Cisco Operations Hub URL `https://{Hostname}` in the web browser.

Step 2   On the Cisco Operations Hub, click the Cisco Operations Hub main menu button.

Step 3   Choose **System** > **Logs** to open **Logs** page.

Step 4   Click **Advanced** > **Manage** from the left navigation menu.

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.

Operations of Cisco Cloud Native Broadband Router

Cisco cnBR supports day-to-day operations of the Data-over-Cable Service Interface Specifications (DOCSIS) system from the deployment to the monitoring for optimal operations. This chapter describes utilities to facilitate typical workflows during such operations.

RPD Cutover

Cisco cnBR Manager supports the Remote PHY Device (RPD) Cutover process through a GUI-based step-by-step wizard to move the RPDs from an existing cBR-8 system to a Cisco cnBR. RPD cutover assumes the Cisco cnBR is operational and the related service group (SG) configuration is ready before running this wizard. The wizard focuses on step-by-step instructions, preparation, and post verification including cable modem, CPE, and RF signal.

Prerequisites for RPD Cutover

- Target RPD is online and connected to cBR-8 system.

- Cisco cnBR is operational and healthy.

- Target SG is configured and verified on Cisco cnBR.

- SG configuration has the correct Secure Software Download (SSD) configuration.

- The SSD Image is in the TFTP or HTTP server.

- Network connectivity between Cisco cnBR and target cutover RPD is available.

Perform RPD Cutover from cBR-8 to Cisco cnBR

Choose **cnBR Manager** > **Remote PHY Devices** from the Cisco Operations Hub main menu and click **Cutover RPD** to start RPD Cutover. The wizard presents fields for entry in sets on a progressive series of interface pages.

Step 1 Set target details at the Connection page.

a) Select or input original cBR-8 Access Protocol, IP Address, Username, Password, and Enable Password.

b) Click **Connect to cBR-8** to see all RPDs on the cBR-8 available for selection.

c) Select the target RPD to cutover and target Cisco cnBR.

d) Fill in expected values for the `CM online ratio threshold after cutover:` (for example: 95) and `Max wait-time after cutover init:` (for example: 40) fields.

e) Click **Next Step**.

Step 2 Get prechecks done at the Pre-Check page.

a) This step automatically performs prechecks. If a check fails, correct the failure, and click the rerun icon to rerun the precheck.

b) After all prechecks are complete, manually update the RPD CCAP-CORE-List from cBR-8 to Cisco cnBR at the DHCP server.

c) If the same CM/CPE IP scopes must move from the original cBR-8 to Cisco cnBR on DHCP server, move it.

d) Check the confirm check box when it is complete.

e) Click **Start Cutover** to start the RPD cutover process.

Step 3 View progress and summary information at the Cutover page.

a) Click **Next Step** when the RPD successfully comes online on Cisco cnBR and the target Cable Modem comes online within the time that is specified in the MAX wait-time field.

Step 4 Get postchecks done at the Post-Check page.

a) After these checks are complete, click **Next Step**.

Step 5 View the Summary Report at the Report page. If there is any issue during this task, click **View Details** to get more information. Rollback tips are available in case you want to rollback when the cutover is not successful.

RPD Operations

cnBR Manager allows you to add, edit, delete, and replace RPDs serviced by a Cisco cnBR using the Configurator interface. This section provides step-by-step instructions to add, edit, delete, and replace RPDs.

Add RPDs

This table lists the features and the releases in which the feature was introduced and gives a small description of the feature.

Table 55: Feature History

Feature Name	Release Information	Feature Description
Out-of-band Services Configuration	Cisco cnBR 21.2	You can create and update OOB configuration templates, and save them to each RPD when you add or edit an RPD.

Before you begin

- Use an existing template or create new SG and L3 templates. For information on how to create new SG templates and L3 templates, see Configure cnBR using cnBR Manager, on page 61.

- Note the MAC address of the target RPD.

Step 1   Log into Cisco Operations Hub.

Step 2   Click **Cisco Operations Hub** > **cnBR Manager** > **Remote PHY Devices** > **Add RPD**.

Step 3   Select the Cisco cnBR and enter the required RPD details.

cnBR Cluster, RPD MAC, RPD Name, Service Group Name, Service Group Template, and L3 Template are mandatory fields.

Step 4   To create a configuration template for video services, check the **Configure Video and Out-of-band Services** check box.

You can create multiple video QAM templates and OOB services templates.

You can also add multiple video QAM templates per downstream port.

Step 5   Enter the following details for the template that you are creating:

This table explains the fields you have to populate in the Configure Video and Out-of-band Services screen to configure Video QAM and Out-of-band Services.

Field	Video QAM Template	OOB Services
Port	Choose only a downstream port.	Choose an upstream or a downstream port.
Template	Choose a video template.	Choose an OOB template.
Start Session ID	Default value is auto-populated. You can edit the value.	Default value is auto-populated. You can edit the value. This field is grayed out for upstream ports as it is not applicable.

Field	Video QAM Template	OOB Services
Group ID	Default value is auto-populated. You can edit the value.	Default value is auto-populated. You can edit the value. This field is grayed out for upstream ports as it is not applicable.
Source ID	Default value is auto-populated. You can edit the value.	Default value is auto-populated. You can edit the value. This field is grayed out for upstream ports as it is not applicable.
Channel ID Range	Default value is auto-populated. You can edit the value.	Default value is auto-populated. You can edit the value. This field is grayed out for upstream ports as it is not applicable.
Action	Click the Save icon. To delete a template, you can click the delete icon.	Click the Save icon. To delete a template, you can click the delete icon.

Step 6   Click **Next Step**.

Wait for the cnBR Manager to complete the automated prechecks.

Step 7   Check the **Please confirm RPD has been connected physically and start RPD config adding.** check box at the bottom of the checklist to confirm that the RPD is physically connected. Click **Next Step**.
The cnBR Manager starts to add the RPD. Progress is displayed on this page.

Step 8   If the operation is successful, click **Next Step**.

If the operation fails, the cnBR Manager displays a failure message.

Wait for the cnBR Manager to perform the automated postchecks.

Step 9   Click **Next Step**.
The cnBR Manager displays a summary report showing the results of the operation.

What to do next

If adding the RPD fails during Steps 6 or 7, the cnBR Manager displays an error message. Use this information to diagnose and correct the problem. After you fix the problem, redo the **Add RPD** operation from Step 1. If the problem resolution requires a change in configuration, delete and add the RPD again with the updated configuration.

Edit RPDs

This table lists the features and the releases in which the feature was introduced and gives a small description of the feature.

Table 56: Feature History

Feature Name	Release Information	Feature Description
Simplified RPD Parameter Editing	Cisco cnBR 21.1	You can edit SG/L3 template and other parameters of online RPDs instead of deleting and readding the RPD with new parameters.

Before you begin

Note the MAC address of the target RPD.

Step 1	Log in to the Cisco Operations Hub.
Step 2	Choose **cnBR Manager** > **Remote PHY Devices** from the Cisco Operations Hub main menu and click **Edit RPD**.
Step 3	Choose the Cisco cnBR Cluster and the RPD MAC address.
	For the chosen RPD, you can edit the RPD Name, SG Template, SG Name, L3 Template, and RPD Location attributes. If video, OOB, NDF, or NDR services are also configured for the RPD, you can update the parameters in the template table or add a new template. For more details, see Add RPDs, on page 300.
Step 4	After updating, click **Next Step**.
	If you updated the parameters of an existing template or added a new template, the new parameters are applied after the RPD edit operation is successful.
	Wait for the cnBR Manager to complete the RPD edit operation. This may take a few minutes.
Step 5	Click **Next Step**.
	Wait for the cnBR Manager to perform the automated post checks.
Step 6	Click **Next Step**.
	If an error appears in the previous step, this step is skipped.
	The cnBR Manager displays a detailed summary report at the end of the RPD edit operation.

Delete RPDs

Before you begin

• Have the MAC address of the target RPD at hand.

Step 1	Log in to the Cisco Operations Hub.

Step 2 Click **Cisco Operations Hub** > **cnBR Manager** > **Remote PHY Devices** > **Delete RPD**.

Step 3 Select the **cnBR Cluster** and the target RPD and click **Next Step**.

Step 4 Wait for the cnBR Manager to check if the target cnBR is ready. Check the box to confirm you want to delete the RPD and click **Start Delete**.
The cnBR Manager starts to delete RPD. The progress is displayed in this page.

Step 5 If the operation is successful, click **Next Step**. If it fails, the cnBR Manager displays a message to inform you that this step has failed; skip to Step 8.

Step 6 Wait for the cnBR Manager to perform the automated postchecks. Click **Next Step**. (If Step 6 fails, the cnBR Manager skips this step.)

Step 7 The cnBR Manager displays a summary report that has the results of the operation.

What to do next

If deleting the RPD fails at Steps 6 or 7, the cnBR Manager displays the error information. Use this information to diagnose and correct the problem. After you fix the problem, restart the **Delete RPD** operation from Step 1.

Replace RPDs

Before you begin

- Have the MAC addresses of the target RPD and the new RPD at hand.

Step 1 Log in to the Cisco Operations Hub.

Step 2 Click **Cisco Operations Hub** > **cnBR Manager** > **Remote PHY Devices** > **Replace RPD**.

Step 3 Select the Cisco cnBR and the existing RPD you want to replace. Enter the MAC address of the new RPD and the maximum wait time for the new RPD to be online. Click **Next Step**.

> **Note** New RPDs need at least 12 minutes to come online.

Step 4 Wait for the cnBR Manager to complete automated prechecks. Check the box at the bottom of the checklist to confirm that the RPD is physically connected. Click **Start Replace**.
The cnBR Manager starts to replace RPD. The progress is displayed in this page.

Step 5 If the operation is successful, click **Next Step**. If it fails, the cnBR Manager displays a message to inform you that this step has failed; skip to Step 8.

Step 6 Wait for the cnBR Manager to perform the automated postchecks. Click **Next Step**. (If Step 6 fails, the cnBR Manager skips this step.)

Step 7 The cnBR Manager displays a summary report that has the results of the operation.

What to do next

If replacing the RPD failed at Steps 6 or 7, the cnBR Manager displays the error information. Use this information to diagnose and correct the problem. After you fix the problem, restart the **Replace RPD** operation from Step 1.

Monitor RPDs

After you add or replace an RPD serviced by Cisco cnBR, you can use the **Inventory** to monitor the status of the RPD.

To view the RPD inventory, click **Cisco Operations Hub** > **cnBR Manager** > **Remote PHY Devices** > **Inventory**.

The **RPD List Summary** dashboard also has the same information.

Figure 51: RPD List Summary Dashboard

RPD Overview

| RPD State | Software Version | SSD state |

RPD Summary

Show 10 entries   Search:

Name	MAC Address	Service Group	SG Template	IPv4 Address	IPv6 Address	State	CCMTS ID	SSD State	Software Version	Online Timestamp
RPD0	c4b2.3997.a2d2	5		10.40.108.44		online	172.22.16.81.nip.io	Idle	v9.5	2021-06-17T05:38:49.822Z
RPD0	c4b2.3997.a332	2		10.40.98.34		online	172.22.16.61.nip.io	Idle		2021-06-21T22:15:45.543Z
RPD00	0027.900b.0166	0		166.111.50.100		init(gcp)	172.22.64.209.nip.io			1970-01-01T00:00:00Z
RPD01	c4b2.3997.a2f0	1		166.111.50.103		init(clksync)	172.22.64.209.nip.io			1970-01-01T00:00:00Z
RPD02	683b.7810.02ec	2		166.111.50.104		online	172.22.64.209.nip.io			2021-06-22T01:45:00.559Z
RPD1	c4b2.3997.a284	4		10.40.108.42		online	172.22.16.81.nip.io	Idle	v9.5	2021-06-16T22:49:54.297Z
RPD1	c4b2.3997.a32c	1		10.40.98.36		online	172.22.16.61.nip.io	Idle		2021-06-21T22:15:54.518Z
RPD2	c4b2.3997.a2a8	3		10.40.108.40		online	172.22.16.81.nip.io	Idle	v9.5	2021-06-16T22:49:50.595Z
RPD2	c4b2.3997.a2f6	0		10.40.98.38		online	172.22.16.61.nip.io	Idle		2021-06-21T22:13:43.92Z
RPD3	c4b2.3997.a28a	2		10.40.108.38		online	172.22.16.81.nip.io	Idle	v9.5	2021-06-16T22:49:40.655Z

Showing 1 to 10 of 12 entries

521900

External Interfaces Support for Cisco Cloud Native Broadband Router

Cisco cnBR supports legacy interface translation, general network management, and monitoring information.

Cisco cnBR supports the following external interfaces:

- IP Detail Record Service, on page 307
- Simple Network Management Protocol, on page 315

IP Detail Record Service

The Cisco Operations Hub hosted IP Detail Record (IPDR) service provides the mechanisms to export IP detailed records to IPDR collectors and the ability to configure the IPDR service.
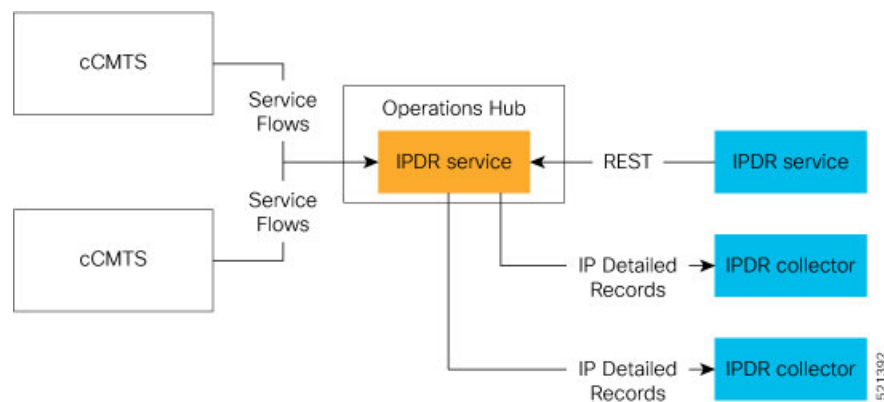
The Cisco Operations Hub IPDR service operates in a similar way as other Cisco Cable Modem Termination Systems (CMTS) products. You can configure it through the REST interface. See IPDR Streaming Protocol on the Cisco CMTS Routers for reference.

The URL `https://{Hostname}/api/ipdr` is created for the IPDR service, which is used for the REST configuration and status requests. The collector connects to the IPDR service on default port 4737 to establish a TCP session. Then, IPDR records are streamed from the IPDR service to the collector over this TCP session.

For the IPDR service to deliver records, the IP address of the collector that receives the records is required. An ordered list of collectors is contained in a session. Only one collector in a session receives the records, the

others are available as backup. The session describes the delivery mechanism and record format. You can define multiple sessions so that more than one collector can receive IPDR records from Operations Hub.

Terminology

This table lists and describes the IPDR terminology.

Term	Description
Collector	The host that receives (collects) the IPDR records.
Exporter	The IPDR service includes an exporter service that generates the IPDR records.
Session	Describes the set of collectors and templates that are used to send IPDR records. At a time, only one collector in a session gets IPDR data at a time based on a priority order. If a collector is unavailable, the collector with the next highest priority gets the records.
Template	Identifies the record format for sending the records.

Configure IPDR Service

To configure the IPDR service, use a single command to set all configuration parameters in JSON format in one single action. This configuration method overwrites the existing configuration and activates the new configuration.

```
/v1/config
```

Note `/ipdr/config` is deprecated but usable.

To set the configuration, use the **PUT** HTTP method as shown in the following example.

```
curl -k -X PUT -H "Content-Type: application/json" -d @- << EOF
https://{Hostname}/api/ipdr/v1/config
{json_string}
EOF
```

Note Parameter -k allows insecure server connections when using SSL.

Example: Add or change IPDR configuration.

```
curl -k -X PUT -H "Content-Type: application/json" -d @- << EOF
https://opshub1.cisco.com/api/ipdr/v1/config
{
    "sessions": [
        {
            "id": 1,
            "name": "session_1",
            "description": "IPDR Session 1",
            "type": {
                "type": "time-interval",
                "interval": 15
            },
            "templates": [
```

```
                {
                    "template-type": "SAMIS-TYPE1"
                }
            ],
            "associated-collectors": [
                {
                    "collector-name": "Collector1",
                    "priority": 1
                }
            ]
        },
        {
            "id": 2,
            "name": "session_2",
            "description": "IPDR Session 2",
            "type": {
                "type": "event",
                "interval": 0
            },
            "templates": [
                {
                    "template-type": "DS-UTIL"
                }
            ],
            "associated-collectors": [
                {
                    "collector-name": "Collector1",
                    "priority": 1
                }
            ]
        },
        {
            "id": 3,
            "name": "session_3",
            "description": "IPDR Session 3",
            "type": {
                "type": "event",
                "interval": 0
            },
            "templates": [
                {
                    "template-type": "US-UTIL"
                }
            ],
            "associated-collectors": [
                {
                    "collector-name": "Collector1",
                    "priority": 1
                }
            ]
        }
    ],
    "collectors": [
        {
            "name": "Collector1",
            "address": "10.0.0.1",
            "nat-address": "0.0.0.0",
            "port": 0
        }
    ],
    "exporter": {
        "ack-timeout": 60,
        "keep-alive": 300,
        "max-unacked": 200,
```

```
        "started": true
    },
    "utilization": {
        "interval": 300
    }
}
EOF
```

After setting the configuration, you can use the **GET** HTTP method as shown in the following example to display the consolidated configuration:

```
curl -H 'Content-Type: application/json' -X GET https://{Hostname}/api/ipdr/v1/config
```

Example: Display the existing IPDR configuration

```
curl -k -H 'Content-Type: application/json' -X GET
https://opshub1.cisco.com/api/ipdr/v1/config
{
    "sessions": [
        {
            "id": 1,
            "name": "session_1",
            "description": "IPDR Session 1",
            "type": {
                "type": "time-interval",
                "interval": 2
            },
            "templates": [
                {
                    "template-type": "SAMIS-TYPE1"
                }
            ],
            "associated-collectors": [
                {
                    "collector-name": "Collector1",
                    "priority": 1
                }
            ]
        },
        {
            "id": 2,
            "name": "session_2",
            "description": "IPDR Session 2",
            "type": {
                "type": "event",
                "interval": 0
            },
            "templates": [
                {
                    "template-type": "DS-UTIL"
                }
            ],
            "associated-collectors": [
                {
                    "collector-name": "Collector1",
                    "priority": 1
                }
            ]
        },
        {
            "id": 3,
            "name": "session_3",
            "description": "IPDR Session 3",
            "type": {
                "type": "event",
```

```
                        "interval": 0
                    },
                    "templates": [
                        {
                            "template-type": "US-UTIL"
                        }
                    ],
                    "associated-collectors": [
                        {
                            "collector-name": "Collector1",
                            "priority": 1
                        }
                    ]
                }
            ],
            "collectors": [
                {
                    "name": "Collector1",
                    "address": "10.0.0.1",
                    "nat-address": "0.0.0.0",
                    "port": 0
                }
            ],
            "exporter": {
                "ack-timeout": 60,
                "keep-alive": 300,
                "max-unacked": 200,
                "started": true
            },
            "utilization": {
                "interval": 240
            }
        }
```

Example: Remove IPDR configuration

```
curl -X PUT -H "Content-Type: application/json" https://opshub1.cisco.com/api/ipdr/v1/config
```

Note   The `opshub1.cisco.com` is only for illustrative purposes. Use the Fully Qualified Domain Name (FQDN) of the Cisco Operations Hub deployed at your site.

Fields In JSON

This table lists the fields used in JSON and their description.

This table lists the fields used in JSON and their description.

Field Name	Description	Type	Enforcement
ack-timeout	Exporter timeout, after which an acknowledgement is received from the collector before retry.	Number. 5–60 seconds; the default value is 60.	Optional
address	The IP address of the collector, which is used to receive the IPDR records.	IP Address	Required
collector-name	A specific collector definition for collectors.	String	Required

Field Name	Description	Type	Enforcement
collectors:name	Unique name used to identify a collector.	String	Required
description	Long descriptive text.	String	Required
id	A unique session number for the purpose of reference.	Number	Required
interval	The interval used to send DS-UTIL and US-UTIL data.	Number in seconds, **0** means disabled.	Optional
keep-alive	The keepalive time after which the collector is considered unavailable.	Number. 5–300 seconds; the default value is 300.	Optional
max-unacked	The maximum number of unacknowledged records.	Number. 5–200; the default value is 200.	Optional
name	Descriptive name for reference purposes.	String	Required
nat-address	The NAT IP address of the collector.	IP Address	Optional
port	The port of the collector.	Number	Optional
priority	The order to use the collector. Use the collector with the lowest priority number first.	> 0	Required
started	Start the IPDR service or not.	Boolean	Required
type:type	The method used to request data from the service.	String. Possible values: adhoc, event, time-interval	Required
type:interval	The frequency of sending the data for a session.	2–1440 minutes.	Required only if "type:type" field is set to "time-interval".
template-type	Identifies the records format.	String. Possible values: SAMIS-TYPE1, US-UTIL, DS-UTIL, TOPOLOGY	Required

REST Return Codes

You can use the status codes listed in the following table to convey the results of a request.

This table lists the REST Return codes, descriptions, response text, and actions.

Code	Short Description	Response Text	Actions
400	HTTP_BAD_REQUEST	• Failure: request format error. • Failed to configure session when exporter starts, stop it at first.	Confirm that the format of the request is valid or restart the IPDR service to apply new sessions.

Code	Short Description	Response Text	Actions
404	HTTP_NOT_FOUND	• Failure: collector doesn't exist.	Return this code when adding a session referring to a collector that does not exist. If it is a consolidated configuration request, correct the request to include a valid collector.
500	HTTP_BAD_REQUEST	• Failed to add new session to cache. • Failed to apply IPDR configuration. • Failed to config ipdr session to exporter. • Failed to get ipdr sessions with internal error. • Failed to recover configurations. • Failed to remove session in cache. • Failed to revert session in cache when db failed. • Failed to update IPDR configuration. • Failure: allocate JSON object error. • Failure: get ipdr config information error. • Failure: not enough memory. • Failure: save global cfg error. • IPDR configuration not updated, restored to original.	Internal error that requires engineering team engagement.
503	HTTP_SER_UNAVAIL	• not ready	Use this code only in response to readiness check. If the service is not ready, confirm that the Cassandra database is ready. Otherwise, get the database ready. If the Cassandra database is ready and operational, ask for customer support.

Monitor

Use the **GET** HTTP method of the following REST APIs to monitor the status of the IPDR session, collector, and exporter.

Monitor Session Status

- Get the status of all sessions.

  ```
  /v1/sessions
  ```

- Get the status of a specific session.

  ```
  /v1/sessions/{id}
  ```

> **Note** `/ipdr/session/status` is deprecated but usable.

Example:

```
curl -k -H 'Content-Type: application/json' -X GET
https://opshub1.cisco.com/api/ipdr/v1/sessions
Session ID: 1, Name: samis, Descr: samis, Started: True
Session Type: Time Interval (15 minutes).
Expires in 81 seconds.
Exporting not started.
2019-05-29T05:08:14 Statistics:
 Transmitted 0 Acknowledged 0 Enqueued 0 Lost 0
 queuedOutstanding 0 queuedUnacknowledged 0
1 Collectors in the session:
 Name: collector1, IPAddr: 10.0.0.1, Port: N/A, Priority: 1[DISCONNECTED]
Templates in the session:
 Template ID: 2, Name:
http://www.cablelabs.com/namespaces/DOCSIS/3.0/xsd/ipdr/DOCSIS-SAMIS-TYPE-1/DOCSIS-SAMIS-TYPE-1_3.5.1-A.1.xsd,
 Type: SAMIS-TYPE-1, KeyNumber: 28
Session 1 has a total of 1 templates.
Session ID: 2, Name: cmts-ds-util-stats, Descr: cmts-ds-util-stats, Started: True
Session Type: Event Based.
2019-05-29T05:08:14 Statistics:
 Transmitted 0 Acknowledged 0 Enqueued 0 Lost 0
 queuedOutstanding 0 queuedUnacknowledged 0
1 Collectors in the session:
 Name: collector1, IPAddr: 10.0.0.1, Port: N/A, Priority: 0[DISCONNECTED]
Templates in the session:
 Template ID: 13, Name:
http://www.cablelabs.com/namespaces/DOCSIS/3.0/xsd/ipdr/DOCSIS-CMTS-DS-UTIL-STATS-TYPE/DOCSIS-CMTS-DS-UTIL-STATS-TYPE_3.5.1-A.3.xsd,
 Type:
http://www.cablelabs.com/namespaces/DOCSIS/3.0/xsd/ipdr/DOCSIS-CMTS-DS-UTIL-STATS-TYPE/DOCSIS-CMTS-DS-UTIL-STATS-TYPE_3.5.1-A.3.xsd,
 KeyNumber: 11
Session 2 has a total of 1 templates.
Session ID: 3, Name: cm-status, Descr: cm-status, Started: True
Session Type: Ad-hoc.
Exporting not started.
2019-05-29T05:08:14 Statistics:
 Transmitted 0 Acknowledged 0 Enqueued 0 Lost 0
 queuedOutstanding 0 queuedUnacknowledged 0
1 Collectors in the session:
 Name: collector1, IPAddr: 10.0.0.1, Port: N/A, Priority: 1[DISCONNECTED]
Templates in the session:
 Template ID: 8, Name:
http://www.cablelabs.com/namespaces/DOCSIS/3.0/xsd/ipdr/DOCSIS-CMTS-CM-REG-STATUS-TYPE/DOCSIS-CMTS-CM-REG-STATUS-TYPE_3.5.1-A.1.xsd,
 Type:
http://www.cablelabs.com/namespaces/DOCSIS/3.0/xsd/ipdr/DOCSIS-CMTS-CM-REG-STATUS-TYPE/DOCSIS-CMTS-CM-REG-STATUS-TYPE_3.5.1-A.1.xsd,
 KeyNumber: 18
Session 3 has a total of 1 templates.

curl -k -H 'Content-Type: application/json' -X GET
https://opshub1.cisco.com/api/ipdr/v1/sessions/1
```

```
Session ID: 1, Name: samis, Descr: samis, Started: True
Session Type: Time Interval (15 minutes).
Expires in 81 seconds.
Exporting not started.
2019-05-29T05:08:14 Statistics:
 Transmitted 0 Acknowledged 0 Enqueued 0 Lost 0
 queuedOutstanding 0 queuedUnacknowledged 0
1 Collectors in the session:
 Name: collector1, IPAddr: 10.0.0.1, Port: N/A, Priority: 1[DISCONNECTED]
Templates in the session:
 Template ID: 2, Name:
http://www.cablelabs.com/namespaces/DOCSIS/3.0/xsd/ipdr/DOCSIS-SAMIS-TYPE-1/DOCSIS-SAMIS-TYPE-1_3.5.1-A.1.xsd,
 Type: SAMIS-TYPE-1, KeyNumber: 28
Session 1 has a total of 1 templates.
```

Monitor Collector Status

```
/v1/collectors
```

Note `/ipdr/collectors/status` is deprecated but usable.

Example:

```
curl -k -H 'Content-Type: application/json' -X GET
https://opshub1.cisco.com/api/ipdr/v1/collectors
Collector name collector1, ip addr 10.0.0.1, port 0
```

Monitor Exporter Status

```
/v1/exporter
```

Note `/ipdr/exporter/status` is deprecated but usable.

Example:

```
curl -k -H 'Content-Type: application/json' -X GET
https://opshub1.cisco.com/api/ipdr/v1/exporter
IPDR exporter is started.
Current parameters:
    KeepAliveInterval:  300
      AckTimeInterval:   60
  AckSequenceInterval:  200
```

Simple Network Management Protocol

The Simple Network Management Protocol (SNMP) allows you to monitor the DOCSIS elements of Cisco cnBR.

The REST API is the recommended method to configure and operate Cisco cnBR. However, partial SNMP functionality is provided for compatibility with legacy SNMP applications. The Cisco cnBR SNMP Agent is located on the Cisco Operations Hub, and not on individual Cisco cnBRs.

SNMP aggregates information from multiple Cisco cnBR cores that are managed by Cisco Operations Hub.

From an application perspective, you must consider the Cisco Operations Hub as a *large* Cisco cnBR.

The following image provides you an overview of how the SNMP works in the Cisco cnBR.
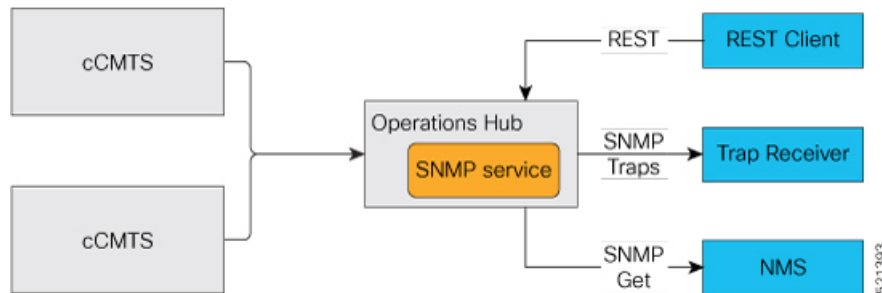
Configure SNMP

Follow these steps to configure SNMP for Cisco cnBR:

Use the REST API to configure the SNMPv2 community string or Trap Receivers.

```
curl -X {GET|PUT|DELETE} https://{hostname}/api/snmp/v1/config
```

Use one of the following options:

- **SNMPv2 Community**

  To configure SNMPv2 Community, replace `<opshub-ip>` with the Cisco Operations Hub IP. The following example is only indicative. See the *Cisco Cloud Native Broadband Router Operations Hub REST API Guide* for the authentication and encryption format.

```
curl -X GET https://{hostname}/api/snmp/v1/config
{"community-list":[],"v3user-list":[],"trap-receivers":[],"trap-enabled-list":[]}

curl -X PUT -d @- << EOF https://{hostname}/api/snmp/v1/config
{
  "community-list": [
    {
      "community": "public",
      "access": "ro",
      "source": "",
      "oid": ""
    }
  ]
}
EOF

curl -X GET https://{hostname}/api/snmp/v1/config
{"community-list":[{"community":"public","access":"ro","source":"","oid":""}],
"v3user-list":[],"trap-receivers":[],"trap-enabled-list":[]}

curl -X DELETE -d @- << EOF https://{hostname}/api/snmp/v1/config
{
  "community-list": [
    {
      "community": "public",
      "access": "ro",
      "source": "",
      "oid": ""
```

```
      }
    ]
  }
  EOF
```

- **SNMPv1/v2 Trap**

  The Trap Receiver is a server listening to a specific UDP port for SNMP Trap events. Use the following REST API to configure the Trap Receiver IP address, port, and other information in the Cisco cnBR SNMP agent. The REST API enables the agent to send traps to the trap receiver.

```
curl -X PUT -d @- << EOF https://{hostname}/api/snmp/v1/config
{
  "trap-receivers": [
    {
      "host": "10.1.1.2",
      "port": 12348,
      "version": 2,
      "community": "private"
    }
  ]
}
EOF

curl -X GET https://{hostname}/api/snmp/v1/config
{"community-list":[],"v3user-list":[],"trap-receivers":
[{"host":"1.1.2.2","port":12345,"version":1,"community":"public"},
{"host":"10.1.1.2","port":12348,"version":2,"community":"private"}]}

curl -X DELETE -d @- << EOF https://{hostname}/api/snmp/v1/config
{
  "trap-receivers": [
    {
      "host": "1.1.2.2"
    }
  ]
}
EOF
```

Note	
	• `host`: Trap Receiver's IP address. For DELETE action, *host* is the key, and the other fields are not necessary.
	• `port`: Trap Receiver listens on this port. The Trap Receiver uses the default port **162**, if the *port* is not specified.
	• `version`: 1 for SNMPv1, 2 for SNMPv2.
	• `community`: Specify the community string to send or receive trap. At the receiver side, there is a configuration file to specify the *community*.

SNMP Support

MIBs

Cisco cnBR supports the following tables:

```
docsIf31CmtsDsOfdmChanTable
docsIf31DocsisBaseCapability
docsIf3CmtsCmRegStatusTable
docsIf3CmtsCmUsStatusTable
docsIf3DsChSetTable
docsIf3MdChCfgTable
docsIf3MdDsSgStatusTable
docsIf3MdNodeStatusTable
docsIf3MdUsSgStatusTable
docsIf3UsChSetTable
docsIfCmtsChannelUtilizationInterval
docsIfCmtsChannelUtilizationTable
docsIfCmtsCmStatusTable
docsIfCmtsDownChannelCounterTable
docsIfCmtsModulationTable
docsIfCmtsUpChannelCounterTable
docsIfDocsisBaseCapability
docsIfDownstreamChannelTable
docsIfUpstreamChannelTable
docsPnmBulkDestIpAddr
docsPnmBulkDestIpAddrType
docsPnmCmtsUtscCfgTable
docsPnmCmtsUtscCtrlTable
docsQos3CmtsMacToSrvFlowTable
docsQos3ServiceFlowStatsTable
docsQos3ServiceFlowTable
docsRphyCmtsCmRegStatusTable
docsRphyRpdDevIdentificationTable
docsRphyRpdDevNdfCfgTable
docsRphyRpdDevNdrCfgTable
docsRphyRpdIfCoreToRpdMapTable
docsRphyRpdIfRpdToCoreMapTable
docsRphyStatsRpdUsOfdmaChanPerfStatsTable
docsRphyStatsRpdUsScQamChanPerfStatsTable
ifTable
```

Note
- Cisco cnBR supports only a subset of the OIDs required for the third-party tools integration.

- Following MIBs support SNMP Write:

  ```
  docsPnmBulkDestIpAddr
  docsPnmBulkDestIpAddrType
  docsPnmCmtsUtscCfgTable
  docsPnmCmtsUtscCtrlTable
  ```

-
  ```
  docsRphyRpdDevNdfCfgTable
  docsRphyRpdDevNdrCfgTable
  ```

- For the following MIB, the table returns value zero (0) for all rows until Cisco cnBR supports OFDMA.

  ```
  docsRphyStatsRpdUsOfdmaChanPerfStatsTable
  ```

Trap

Cisco cnBR manager supports online and offline events of cable modems (CM).

SNMP Limitations

Cisco cnBR SNMP has the following limitations:

- SNMP write is supported only for the MIB object or table that is listed in the MIB section. For more information, see OIDs of MIB tables supported by Cisco Operations Hub.

- Only a limited set of DOCSIS MIB OIDs and traps is supported. For more information, see OIDs of MIB tables supported by Cisco Operations Hub.

MIBs for NDF and NDR

This table lists the features and the releases in which the feature was introduced and gives a small description of the feature.

Table 57: Feature History

Feature Name	Release Information	Feature Description
SNMP support for NDF and NDR	Cisco cnBR 21.2	From this release, Cisco cnBR provides SNMP support for NDF and NDR.

SNMP builds the NDF and NDR MIB tables based on the service group configuration in Cisco cnBR.

- NDF MIB: OID 1.3.6.1.4.1.9.9.857.1.1

- NDR MIB: OID 1.3.6.1.4.1.9.9.857.1.2

NDF SNMP Table

This table lists and describes the NDF SNMP fields.

Field	Description
UniqueID	RPD MAC address
RF Port	RPD NDR channel
RF Channel	RPD NDR channel
Enable	Enable or disable the NDR stream.
Dst Address	IP address of the receiver of the NDR L2TP stream.
Src Address	IP address of the transmitter of the L2TP stream.
Session ID	L2TP session ID of the NDF stream.
Frequency	Center frequency of the NDF channel.

Field	Description
Bandwidth	Bandwidth of the NDR channel.
RPD Status	Status of the RPD: online or offline.

Sample Output for NDF Table

```
show
snmpwalk -v 2c -c public 172.22.127.185 1.3.6.1.4.1.9.9.857.1.1
iso.3.6.1.4.1.9.9.857.1.1.1.4.196.178.57.151.162.108.0.80 = INTEGER: 1
iso.3.6.1.4.1.9.9.857.1.1.1.4.196.178.57.151.162.108.0.81 = INTEGER: 1
iso.3.6.1.4.1.9.9.857.1.1.1.4.196.178.57.151.162.108.0.82 = INTEGER: 1
iso.3.6.1.4.1.9.9.857.1.1.1.5.196.178.57.151.162.108.0.80 = Hex-STRING: 0A 28 13 21
iso.3.6.1.4.1.9.9.857.1.1.1.5.196.178.57.151.162.108.0.81 = Hex-STRING: 0A 28 13 21
iso.3.6.1.4.1.9.9.857.1.1.1.5.196.178.57.151.162.108.0.82 = Hex-STRING: 0A 28 13 21
iso.3.6.1.4.1.9.9.857.1.1.1.6.196.178.57.151.162.108.0.80 = Hex-STRING: FC FC FC 7A
iso.3.6.1.4.1.9.9.857.1.1.1.6.196.178.57.151.162.108.0.81 = Hex-STRING: FC FC FC 7A
iso.3.6.1.4.1.9.9.857.1.1.1.6.196.178.57.151.162.108.0.82 = Hex-STRING: FC FC FC 7A
iso.3.6.1.4.1.9.9.857.1.1.1.7.196.178.57.151.162.108.0.80 = Gauge32: 2415919361
iso.3.6.1.4.1.9.9.857.1.1.1.7.196.178.57.151.162.108.0.81 = Gauge32: 2415919362
iso.3.6.1.4.1.9.9.857.1.1.1.7.196.178.57.151.162.108.0.82 = Gauge32: 2415919363
iso.3.6.1.4.1.9.9.857.1.1.1.8.196.178.57.151.162.108.0.80 = Gauge32: 78000000
iso.3.6.1.4.1.9.9.857.1.1.1.8.196.178.57.151.162.108.0.81 = Gauge32: 78000000
iso.3.6.1.4.1.9.9.857.1.1.1.8.196.178.57.151.162.108.0.82 = Gauge32: 78000000
iso.3.6.1.4.1.9.9.857.1.1.1.9.196.178.57.151.162.108.0.80 = Gauge32: 160000
iso.3.6.1.4.1.9.9.857.1.1.1.9.196.178.57.151.162.108.0.81 = Gauge32: 160000
iso.3.6.1.4.1.9.9.857.1.1.1.9.196.178.57.151.162.108.0.82 = Gauge32: 160000
iso.3.6.1.4.1.9.9.857.1.1.1.10.196.178.57.151.162.108.0.80 = INTEGER: 0
iso.3.6.1.4.1.9.9.857.1.1.1.10.196.178.57.151.162.108.0.81 = INTEGER: 0
iso.3.6.1.4.1.9.9.857.1.1.1.10.196.178.57.151.162.108.0.82 = INTEGER: 0
iso.3.6.1.4.1.9.9.857.1.1.1.11.196.178.57.151.162.108.0.80 = INTEGER: 0
iso.3.6.1.4.1.9.9.857.1.1.1.11.196.178.57.151.162.108.0.81 = INTEGER: 0
iso.3.6.1.4.1.9.9.857.1.1.1.11.196.178.57.151.162.108.0.82 = INTEGER: 0
iso.3.6.1.4.1.9.9.857.1.1.1.12.196.178.57.151.162.108.0.80 = INTEGER: 0
iso.3.6.1.4.1.9.9.857.1.1.1.12.196.178.57.151.162.108.0.81 = INTEGER: 0
iso.3.6.1.4.1.9.9.857.1.1.1.12.196.178.57.151.162.108.0.82 = INTEGER: 0
iso.3.6.1.4.1.9.9.857.1.1.1.13.196.178.57.151.162.108.0.80 = STRING: "Active"
iso.3.6.1.4.1.9.9.857.1.1.1.13.196.178.57.151.162.108.0.81 = STRING: "Active"
iso.3.6.1.4.1.9.9.857.1.1.1.13.196.178.57.151.162.108.0.82 = STRING: "Active"
iso.3.6.1.4.1.9.9.857.1.1.1.14.196.178.57.151.162.108.0.80 = Counter64: 0
iso.3.6.1.4.1.9.9.857.1.1.1.14.196.178.57.151.162.108.0.81 = Counter64: 0
iso.3.6.1.4.1.9.9.857.1.1.1.14.196.178.57.151.162.108.0.82 = Counter64: 0
iso.3.6.1.4.1.9.9.857.1.1.1.15.196.178.57.151.162.108.0.80 = Counter64: 0
iso.3.6.1.4.1.9.9.857.1.1.1.15.196.178.57.151.162.108.0.81 = Counter64: 0
iso.3.6.1.4.1.9.9.857.1.1.1.15.196.178.57.151.162.108.0.82 = Counter64: 0
```

Sample Output for NDR Table

```
sh
snmpwalk -v 2c -c public 172.22.127.185 1.3.6.1.4.1.9.9.857.1.2
iso.3.6.1.4.1.9.9.857.1.2.1.4.196.178.57.151.162.108.0.24 = INTEGER: 1
iso.3.6.1.4.1.9.9.857.1.2.1.4.196.178.57.151.162.108.0.25 = INTEGER: 1
iso.3.6.1.4.1.9.9.857.1.2.1.4.196.178.57.151.162.108.0.26 = INTEGER: 1
iso.3.6.1.4.1.9.9.857.1.2.1.5.196.178.57.151.162.108.0.24 = Hex-STRING: FC FC FC 7A
iso.3.6.1.4.1.9.9.857.1.2.1.5.196.178.57.151.162.108.0.25 = Hex-STRING: FC FC FC 7A
iso.3.6.1.4.1.9.9.857.1.2.1.5.196.178.57.151.162.108.0.26 = Hex-STRING: FC FC FC 7A
iso.3.6.1.4.1.9.9.857.1.2.1.6.196.178.57.151.162.108.0.24 = Hex-STRING: 0A 28 13 21
iso.3.6.1.4.1.9.9.857.1.2.1.6.196.178.57.151.162.108.0.25 = Hex-STRING: 0A 28 13 21
iso.3.6.1.4.1.9.9.857.1.2.1.6.196.178.57.151.162.108.0.26 = Hex-STRING: 0A 28 13 21
iso.3.6.1.4.1.9.9.857.1.2.1.7.196.178.57.151.162.108.0.24 = Gauge32: 2533359617
iso.3.6.1.4.1.9.9.857.1.2.1.7.196.178.57.151.162.108.0.25 = Gauge32: 2533359618
```

```
iso.3.6.1.4.1.9.9.857.1.2.1.7.196.178.57.151.162.108.0.26 = Gauge32: 2533359619
iso.3.6.1.4.1.9.9.857.1.2.1.8.196.178.57.151.162.108.0.24 = Gauge32: 8000000
iso.3.6.1.4.1.9.9.857.1.2.1.8.196.178.57.151.162.108.0.25 = Gauge32: 8000000
iso.3.6.1.4.1.9.9.857.1.2.1.8.196.178.57.151.162.108.0.26 = Gauge32: 8000000
iso.3.6.1.4.1.9.9.857.1.2.1.9.196.178.57.151.162.108.0.24 = Gauge32: 160000
iso.3.6.1.4.1.9.9.857.1.2.1.9.196.178.57.151.162.108.0.25 = Gauge32: 160000
iso.3.6.1.4.1.9.9.857.1.2.1.9.196.178.57.151.162.108.0.26 = Gauge32: 160000
iso.3.6.1.4.1.9.9.857.1.2.1.10.196.178.57.151.162.108.0.24 = INTEGER: 0
iso.3.6.1.4.1.9.9.857.1.2.1.10.196.178.57.151.162.108.0.25 = INTEGER: 0
iso.3.6.1.4.1.9.9.857.1.2.1.10.196.178.57.151.162.108.0.26 = INTEGER: 0
iso.3.6.1.4.1.9.9.857.1.2.1.11.196.178.57.151.162.108.0.24 = INTEGER: 0
iso.3.6.1.4.1.9.9.857.1.2.1.11.196.178.57.151.162.108.0.25 = INTEGER: 0
iso.3.6.1.4.1.9.9.857.1.2.1.11.196.178.57.151.162.108.0.26 = INTEGER: 0
iso.3.6.1.4.1.9.9.857.1.2.1.12.196.178.57.151.162.108.0.24 = INTEGER: 0
iso.3.6.1.4.1.9.9.857.1.2.1.12.196.178.57.151.162.108.0.25 = INTEGER: 0
iso.3.6.1.4.1.9.9.857.1.2.1.12.196.178.57.151.162.108.0.26 = INTEGER: 0
iso.3.6.1.4.1.9.9.857.1.2.1.13.196.178.57.151.162.108.0.24 = STRING: "Active"
iso.3.6.1.4.1.9.9.857.1.2.1.13.196.178.57.151.162.108.0.25 = STRING: "Active"
iso.3.6.1.4.1.9.9.857.1.2.1.13.196.178.57.151.162.108.0.26 = STRING: "Active"
iso.3.6.1.4.1.9.9.857.1.2.1.14.196.178.57.151.162.108.0.24 = Counter64: 0
iso.3.6.1.4.1.9.9.857.1.2.1.14.196.178.57.151.162.108.0.25 = Counter64: 0
iso.3.6.1.4.1.9.9.857.1.2.1.14.196.178.57.151.162.108.0.26 = Counter64: 0
iso.3.6.1.4.1.9.9.857.1.2.1.15.196.178.57.151.162.108.0.24 = Counter64: 0
iso.3.6.1.4.1.9.9.857.1.2.1.15.196.178.57.151.162.108.0.25 = Counter64: 0
iso.3.6.1.4.1.9.9.857.1.2.1.15.196.178.57.151.162.108.0.26 = Counter64: 0
```

SNMPSET to Enable or Disable NDF

```
sh
snmpset -v 2c -c sweep 172.22.10.202 1.3.6.1.4.1.9.9.857.1.1.1.4.104.59.120.16.2.236.0.0 i
 1
snmpset -v 2c -c sweep 172.22.10.202 1.3.6.1.4.1.9.9.857.1.1.1.4.104.59.120.16.2.236.0.0 i
 0
```

SNMPSET to Enable or Disable NDR

```
sh
snmpset -v 2c -c sweep 172.22.10.202 1.3.6.1.4.1.9.9.857.1.2.1.4.104.59.120.16.2.236.0.0 i
 1
snmpset -v 2c -c sweep 172.22.10.202 1.3.6.1.4.1.9.9.857.1.2.1.4.104.59.120.16.2.236.0.0 i
 0
```