Figure 136: *Rotating the latch*

Optical

Copper

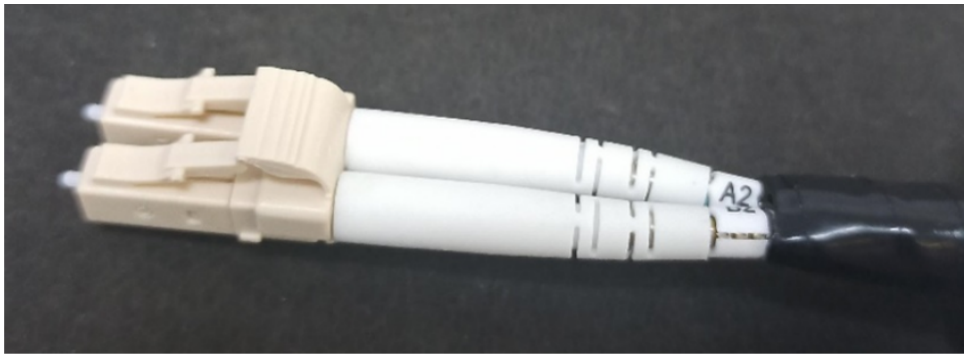
Connecting the cable

Attention

The Fiber optic cable assembly is very delicate. To avoid damage, handle it with extreme care. Ensure that the fiber optic cable does not twist during assembly, especially when fitting and tightening the weatherproofing gland. Do not insert the power over Ethernet drop cable from the PSU into the copper SFP module, as this will damage the module.

1. Remove the LC connector dust caps from the ODU end (optical cable only).

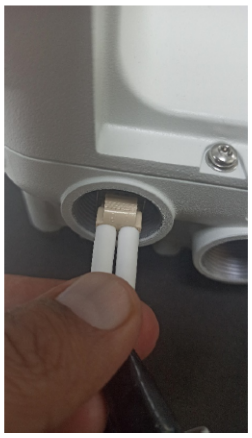
   Figure 137: *Removing the LC connector dust caps*



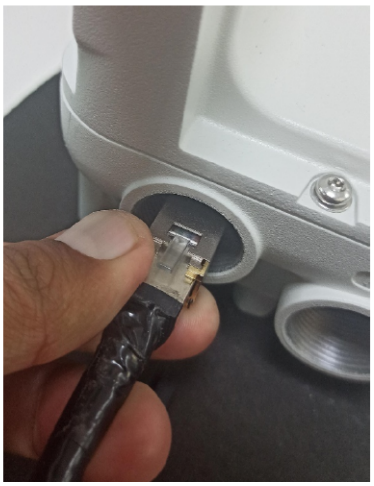
2. Plug the connector into the SFP module, ensuring that it snaps home.

Figure 138: *Plugging the connector into the SFP module*

Optical



Copper



Fitting the gland

1. Fit the gland body to the SFP port and tighten it to a torque of 5.5 Nm (4.3 lb-ft).

   Figure 139: *Fitting the land body*

2. Fit the gland nut and tighten until the rubber seal closes on the cable. Do not over-tighten the gland nut, as there is a risk of damage to its internal components.

Figure 140: *Fitting the gland nut*

3. Fit the gland nut to the rubble seal on the gland body and tighten it to a torque of 5.5 Nm (4.3 lb-ft).

Figure 141: *Fitting the gland nut to the rubble seal*

Removing the cable and SFP module

Do not attempt to remove the module without disconnecting the cable, otherwise, the locking mechanism in the ODU will be damaged.

1. Remove the cable connector by pressing its release tab before pulling it out.

   Figure 142: *Removing the cable connector*

   Optical

   Copper

2. Pull the bale clasp (latch) to the unlocked position. Extract the module by using a screwdriver.

   Figure 143: *Pulling the bale clasp (latch)*

   Optical

   Copper

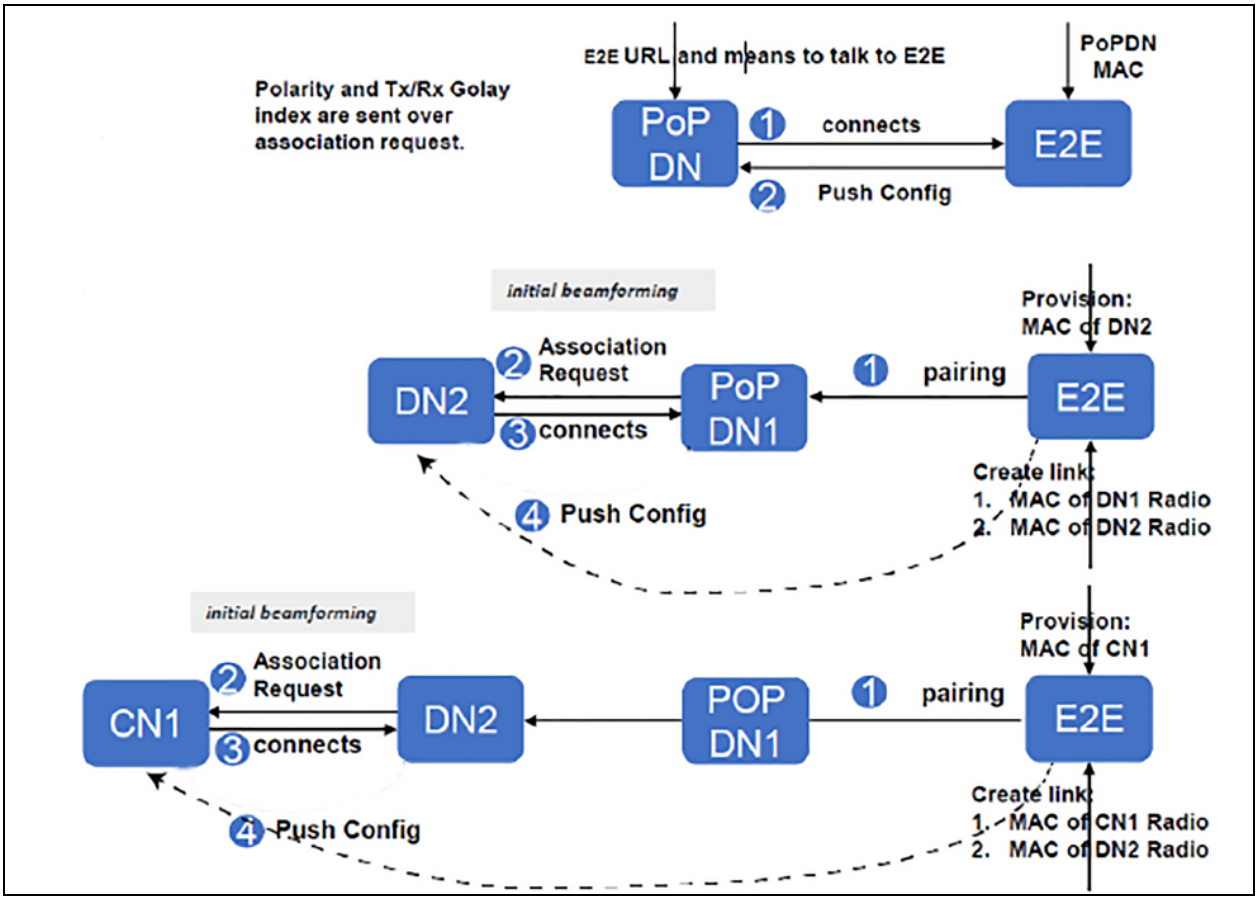
   

Configuring 60 GHz cnWave™

Nodes deployment

The configuration of cnWave nodes is handled automatically by the E2E service. However, the first PoP node must be configured manually since connectivity to the E2E controller has not yet been established. After establishing communication with the E2E controller, the nodes report a hash of their local configuration file and the controller automatically pushes configuration changes to the nodes upon seeing any mismatches. Centralized configuration management architecture implemented in which the E2E controller, serves as the single point of truth for configurations in the network.

Figure 144: *Nodes deployment*



More details on deployment of the 60 GHz series of products are available here.

Connecting to the unit

This section describes how to connect the unit to a management PC and power it up.

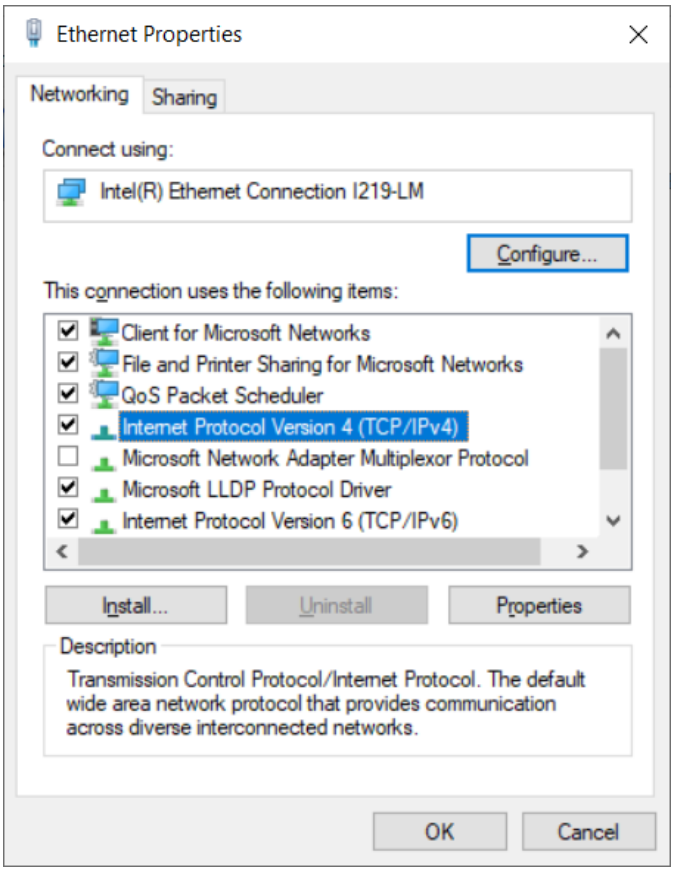
Configuring the management PC

Use this procedure to configure the local management PC to communicate with the 60 GHz cnWave devices.

Procedure:

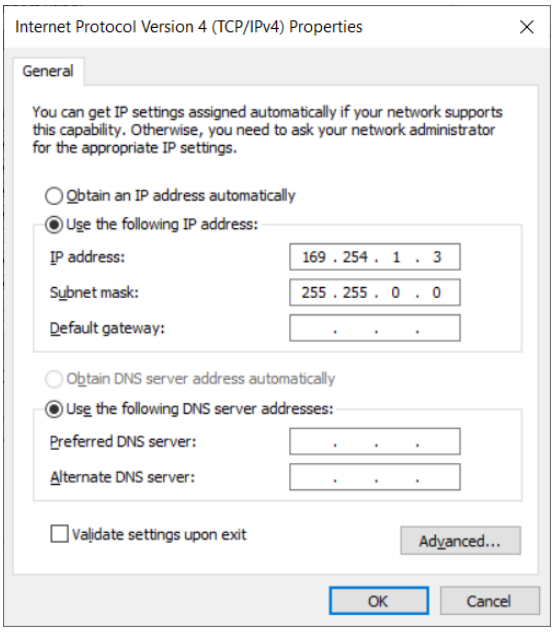
1. Select **Properties** for the Ethernet port. In Windows 7 this is found in **Control Panel** > **Network and Internet** > **Network Connections** > **Local Area Connection**.
2. Select **Internet Protocol Version 4 (TCP/IPv4)**.

   Figure 145: *The Ethernet Properties dialog box*



3. Click **Properties**.
4. Enter an IP address that is valid for the 169.254.X.X/16 network, avoiding 169.254.1.1 (eg: 169.254.1.3).

Figure 146: *The Internet Protocol Version 4 (TCP/IPv4) dialog box*



5. Enter a subnet mask of 255.255.0.0. Leave the default gateway blank.

Connecting to the PC and powering up

Use this procedure to connect a management PC and power up the 60 GHz cnWave devices.

Procedure:

1. Check that the ODU is connected to the power supply (AC/DC according to the configuration).
2. Connect the PC Ethernet port to the LAN port of the PSU or AUX port (according to device configuration).
3. Open a web browser and type: **169.254.1.1**.
4. When prompted, enter **admin/admin** to login to the GUI and complete the configuration.

Using the web interface

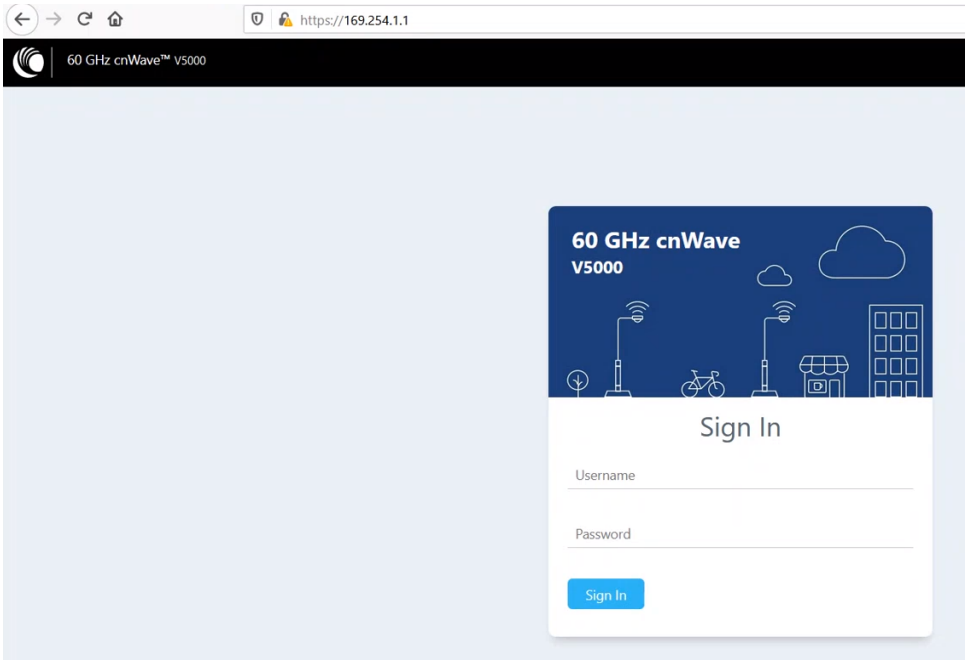
This section describes how to log into the 60 GHz cnWave web interface and use its menus.

Logging into the web interface

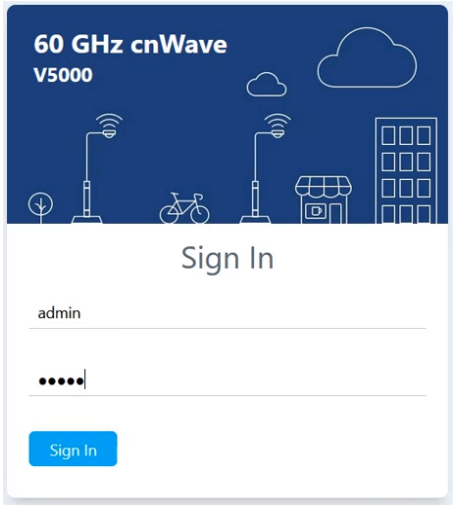
Use this procedure to log into the web interface as a system administrator.

Procedure:

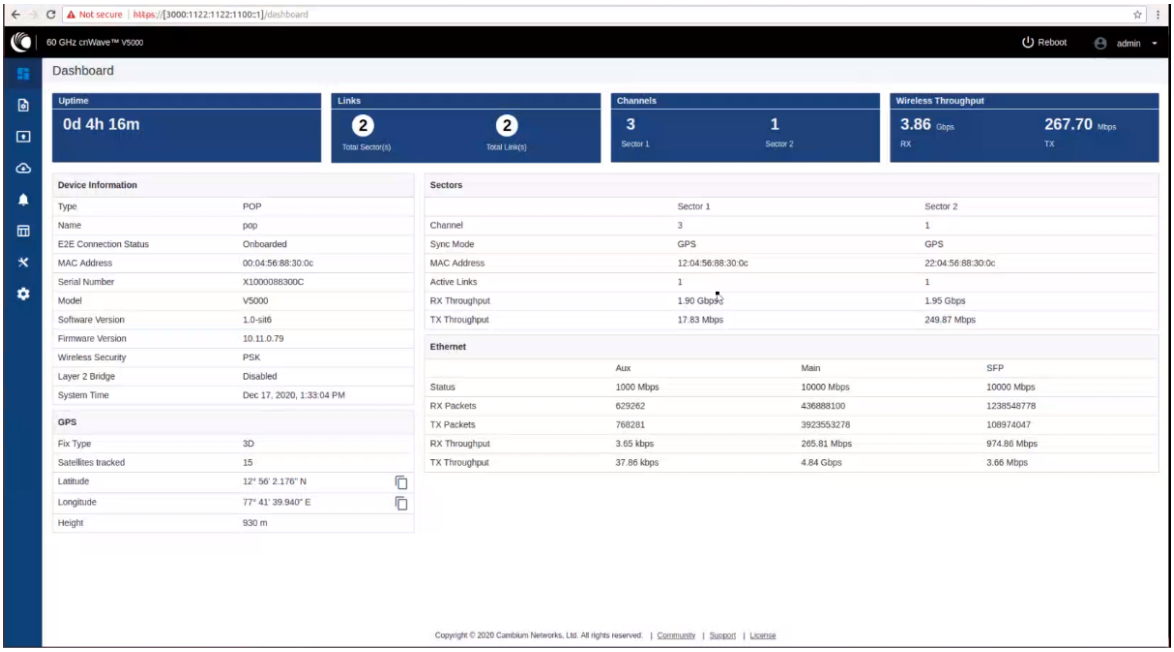
1. Start the web browser from the management PC.
2. Type the IP address of the unit into the address bar. The factory default IP address is **169.254.1.1** and press **Enter**.



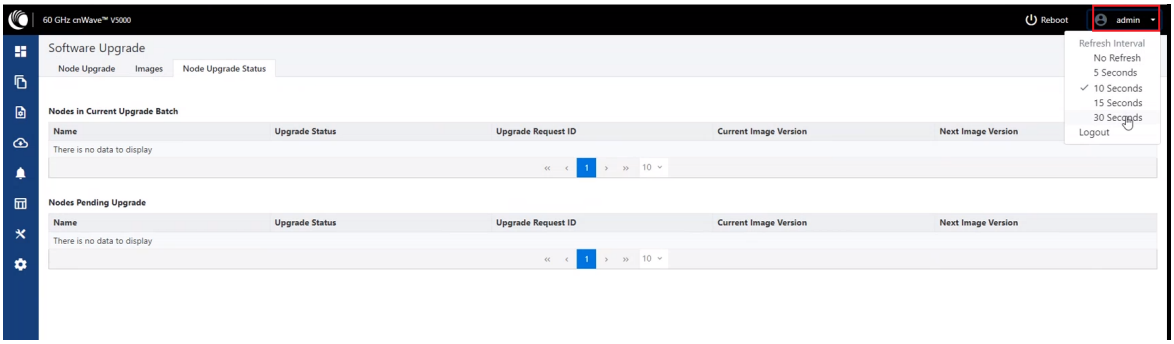
3. Type the username and password as **admin** and **admin**. Click **Sign In**.



The **Dashboard** page appears.



Users can select the refresh time interval. Click **admin** at the top-right and select the **Refresh Interval** from the drop-down.



The Dashboard contains the following options at the top:

- Uptime
- Links
- Channels
- Wireless Throughput

Uptime

Displays the total running time of the device.

Links

Displays the total number of active links which are connected to the 60 GHz cnWave™ device.

Channels

Displays the total number of channels (Sector 1, Sector 2, etc.,) which are connected to the 60 GHz cnWave™ device.

Wireless Throughput

Displays the transmitting and receiving throughput values.

Dashboard elements

Dashboard home page consist of the below elements:

- Device Information
- GPS
- Sectors
- Ethernet

Figure 147: *Dashboard - Device Information*

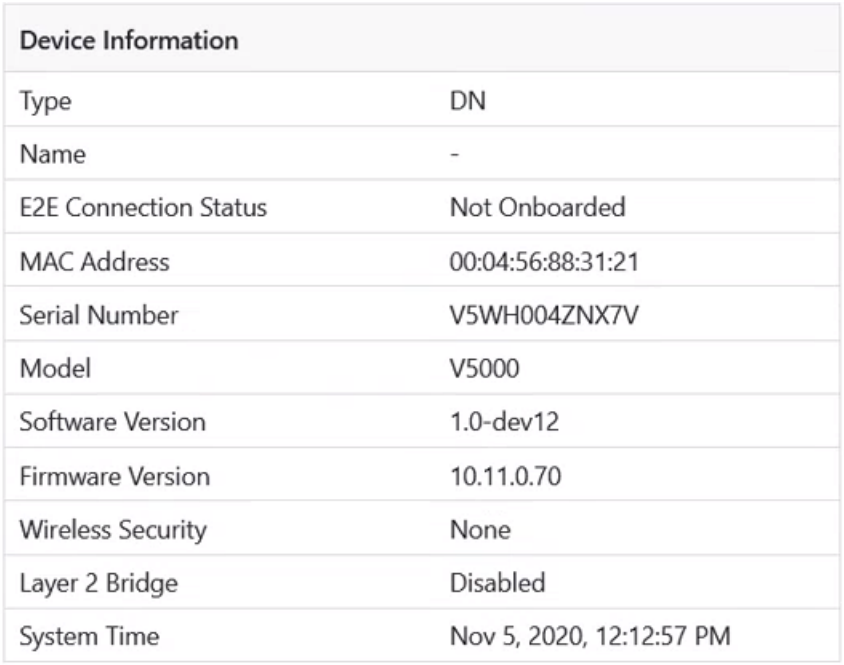


Table 35: Elements in the Device Information section

Element	Description
Type	Displays type of the device. The device types are: • DN • PoP DN • CN
Name	Displays name of the device.
E2E Connection Status	Displays the connection status of the E2E controller.
MAC address	Displays the MAC address of the 60 GHz cnWave device.
Serial Number	Displays the serial number of the 60 GHz cnWave device
Model	Displays the model of the 60 GHz cnWave device. The models are:

Element	Description
	• V1000 • V3000 • V5000
Software version	Displays the software version used in 60 GHz cnWave device.
Firmware version	Displays the Firmware version used in 60 GHz cnWave device.
Wireless security	Displays the security type. The types are: • Disabled • PSK • 802.1X
Layer 2 Bridge	Displays bridge status.
System Time	Displays current time.

GPS

GPS table displays the positioning information of the site.

Figure 148: *Dashboard - GPS*

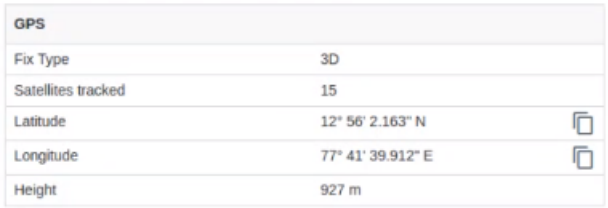


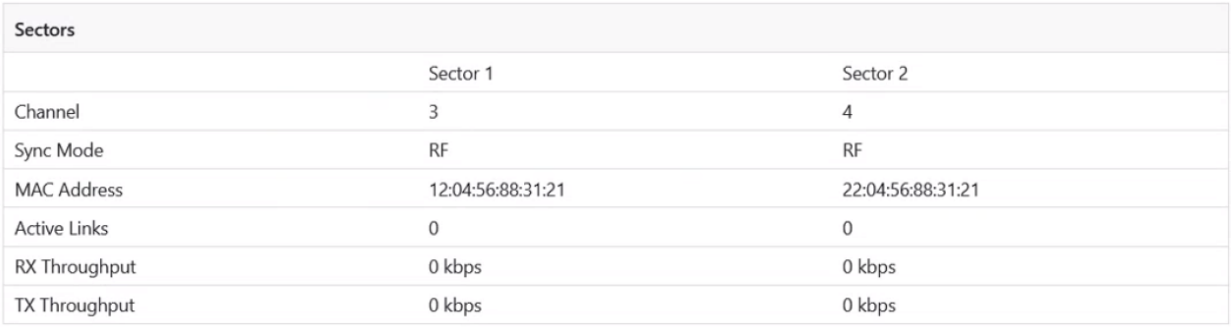
Table 36: Elements in the GPS section

Element	Description
Fix Type	Fix Type
Satellites tracked	Number of registered satellites
Latitude	Displays latitude of the site
Longitude	Displays longitude of the site
Height	Displays height of the device

Sectors

Sectors table displays the number of nodes added to the device and its information.

Figure 149: *Dashboard - Sectors*



Sectors		
	Sector 1	Sector 2
Channel	3	4
Sync Mode	RF	RF
MAC Address	12:04:56:88:31:21	22:04:56:88:31:21
Active Links	0	0
RX Throughput	0 kbps	0 kbps
TX Throughput	0 kbps	0 kbps

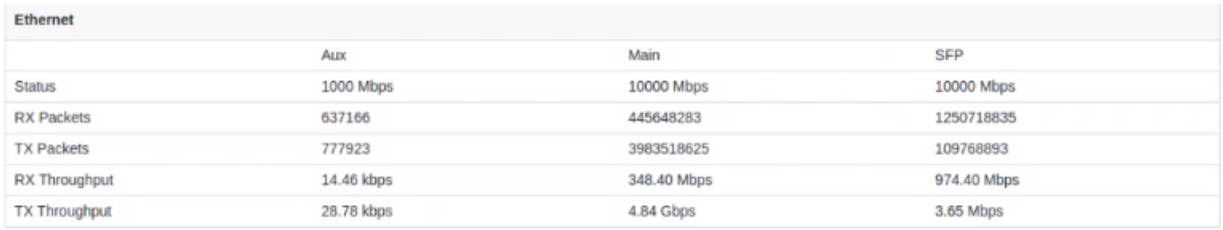
Table 37: Elements in the Sectors section

Element	Description
Channel	Displays the channel information used by the sector
Sync mode	Displays the sync mode of the sectors
MAC address	Displays the MAC address of the sectors
Active links	Displays the number of active links in connected sectors
RX Throughput	Displays RX Throughput of the individual sectors
TX Throughput	Displays TX Throughput of the individual sectors

Ethernet

Ethernet table displays the information about Aux, Main, and SFP ports.

Figure 150: *Dashboard - Ethernet*



Ethernet			
	Aux	Main	SFP
Status	1000 Mbps	10000 Mbps	10000 Mbps
RX Packets	637166	445648283	1250718835
TX Packets	777923	3983518625	109768893
RX Throughput	14.46 kbps	348.40 Mbps	974.40 Mbps
TX Throughput	28.78 kbps	4.84 Gbps	3.65 Mbps

Table 38: Elements in the Ethernet section

Element	Description
Status	Displays the speed of Ethernet ports
RX Packets	Number of packets received
TX Packets	Number of packets transmitted
RX Throughput	Displays the RX Throughput of the Ethernet
TX Throughput	Displays the TX Throughput of the Ethernet

Enabling internal E2E Controller

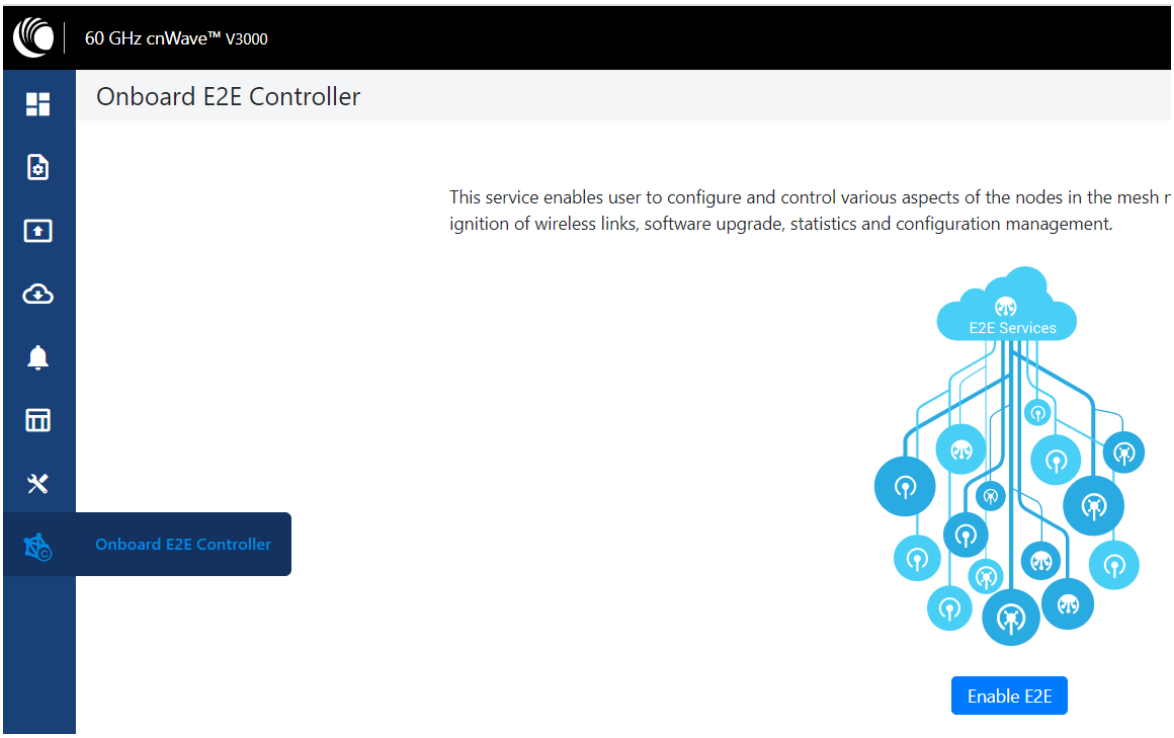
E2E Controller handles important management functions such as link bring-up, software upgrades and configuration management, etc. Enable E2E Controller to configure and establish the connection. To enable E2E Controller, perform the following steps:

Note

The internal E2E controller is not required if you intend to tun the E2E controller On-Premise (refer *E2E User Guide*) .

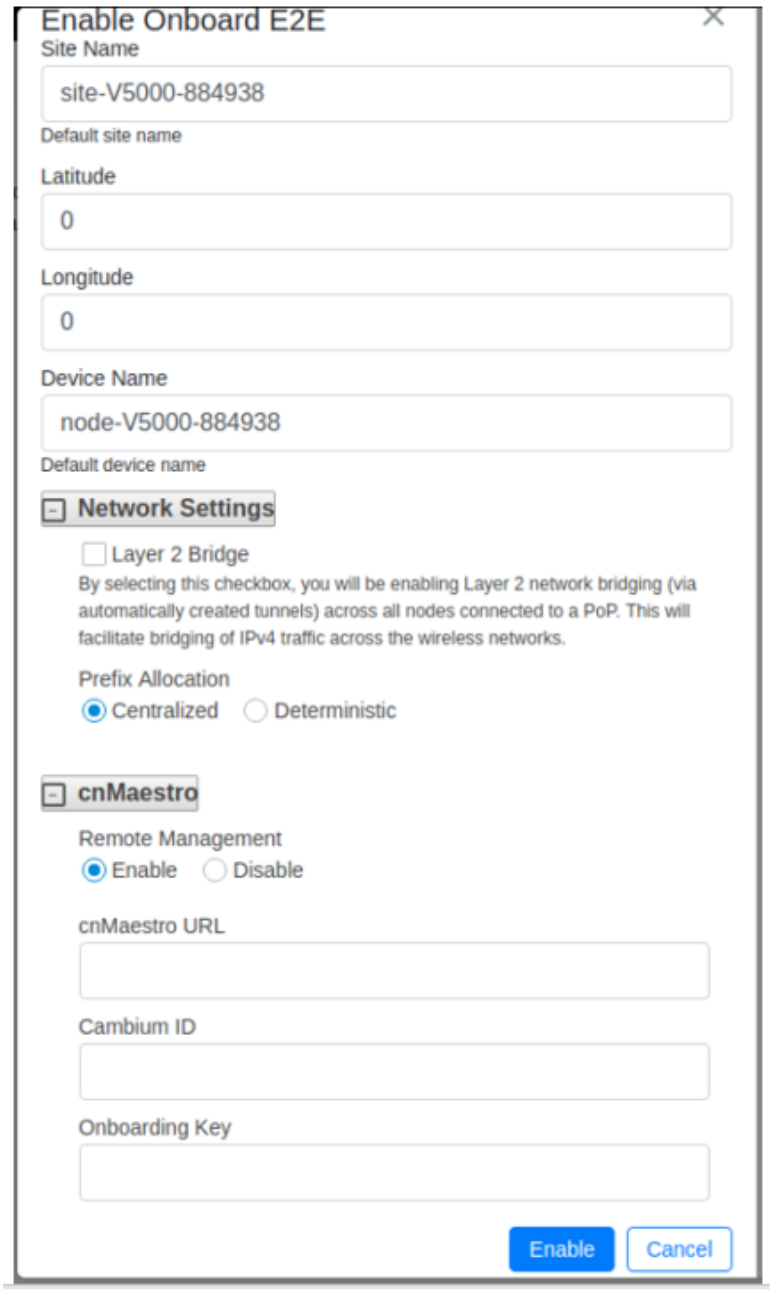
Currently, the internal E2E controller is restricted to 31 nodes.

1. Click the **E2E Controller** option on the left pane of the Dashboard.



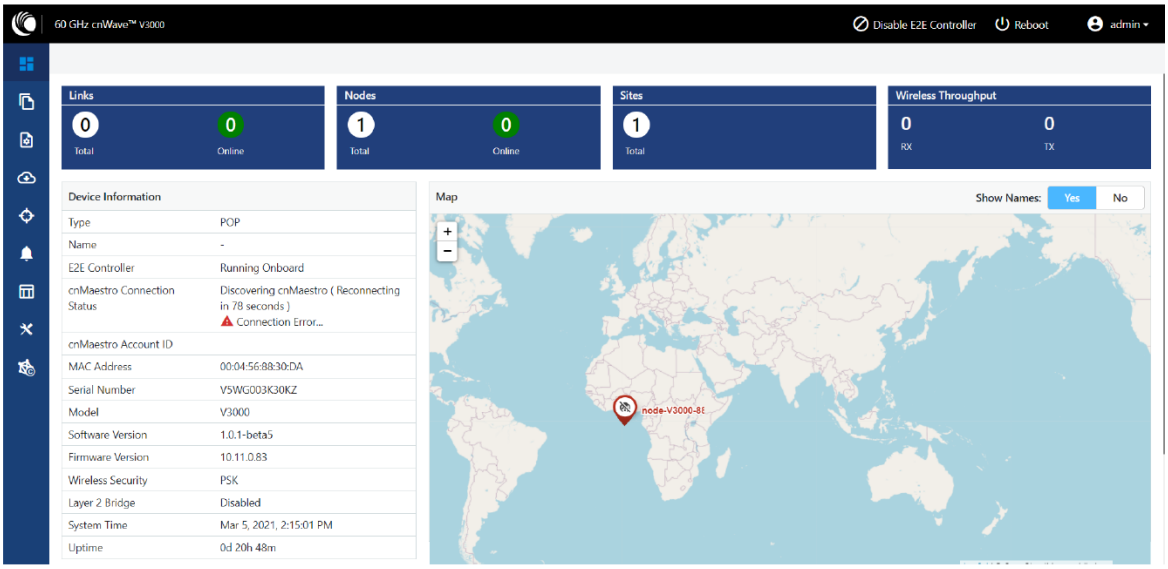
2. Click **Enable E2E**.

   The **Enable Onboard E2E** dialog box appears.

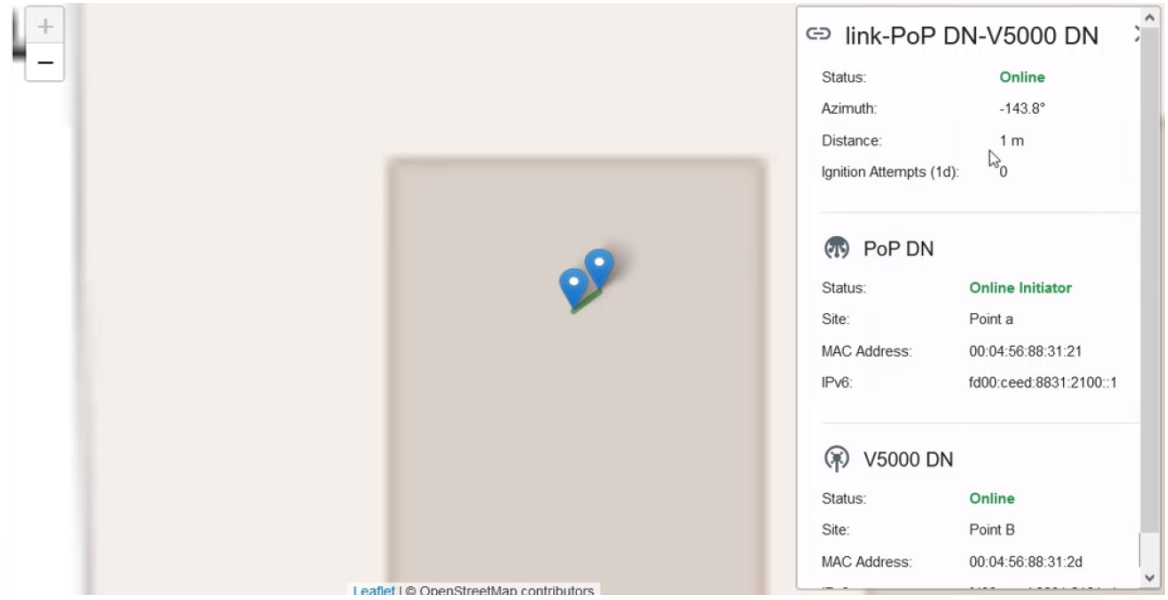


3. Enter the required details and click **Enable**.
4. After enabling E2E Controller, the dashboard displays the links which are connected to the device.

Figure 151: *Dashboard*



You must right-click on the site pin to see more information about the site, as shown below:



Topology

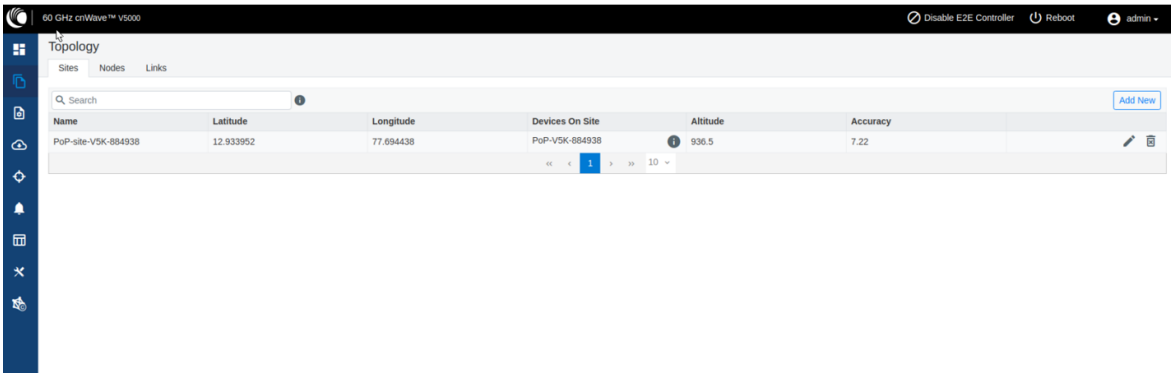
After enabling the E2E Controller, add Sites, Nodes and Links to establish the connection.

To add sites, nodes and links, perform the following steps:

1. In the main dashboard page, click **Topology** on the left navigation pane.

   The **Topology** page appears. By default, the **Sites** tab is selected, as shown below:

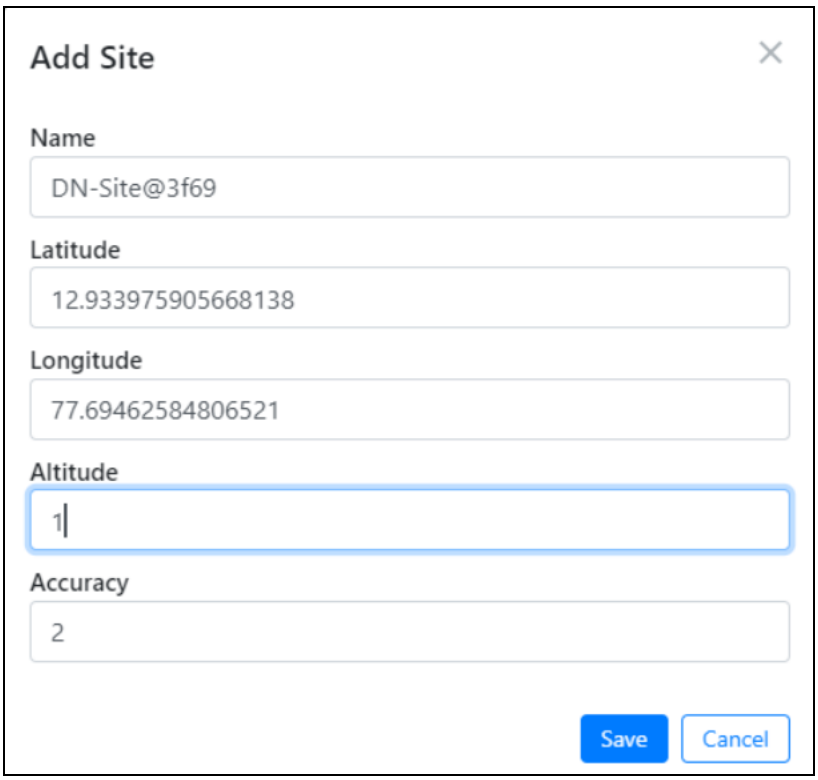
Figure 152: *The Sites page*



2. To add a DN site, click **Add New**.

   The **Add Site** dialog box appears, as shown below:

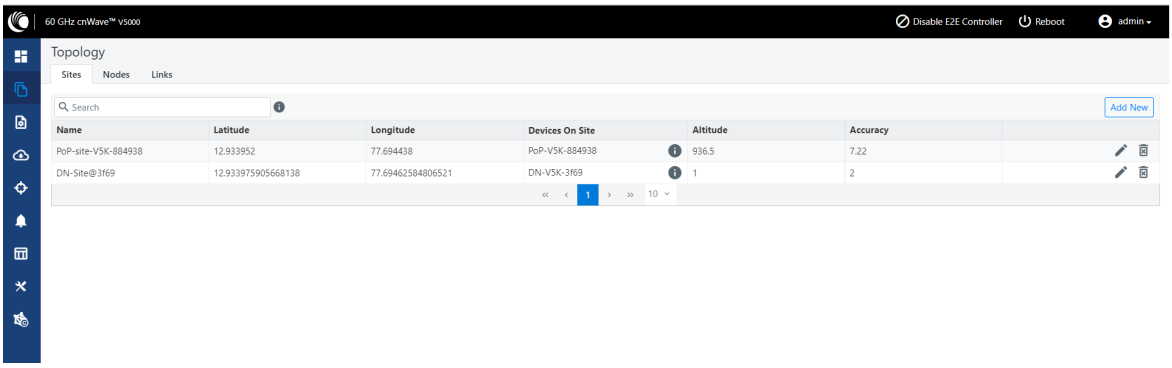
   Figure 153: *The Add Site dialog box*



3. Enter the Name, Latitude, Longitude, Altitude, Accuracy information, and click **Save**.

   The new DN site information gets added to to the topology, as shown below:

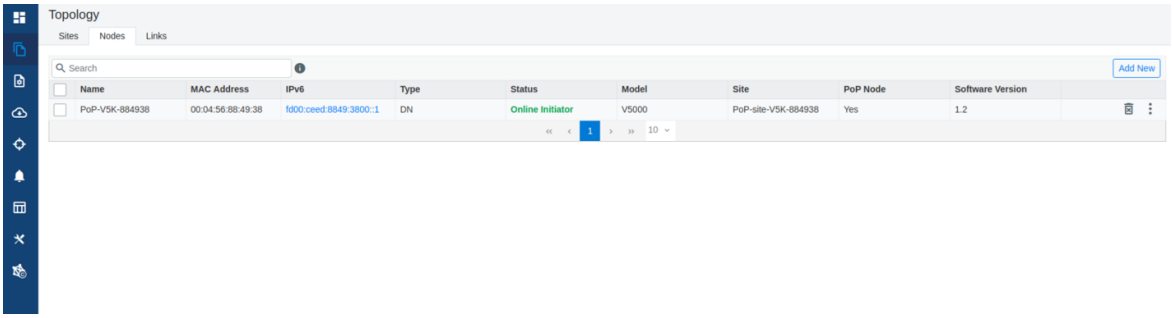
Figure 154: *The updated Sites page with new site details*



4. To add a DN node, click on the **Nodes** tab in the **Topology** page.

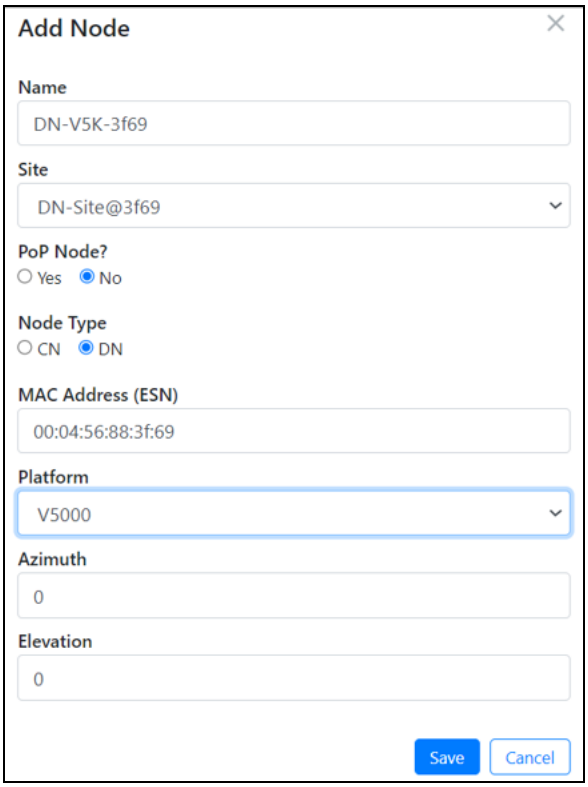
   The **Nodes** page appears, as shown below:

   Figure 155: *The Nodes page*



5. Click **Add New** and provide values in the **Add Node** dialog box, as shown below:

Figure 156: *The Add Node dialog box*



6. Click **Save**.

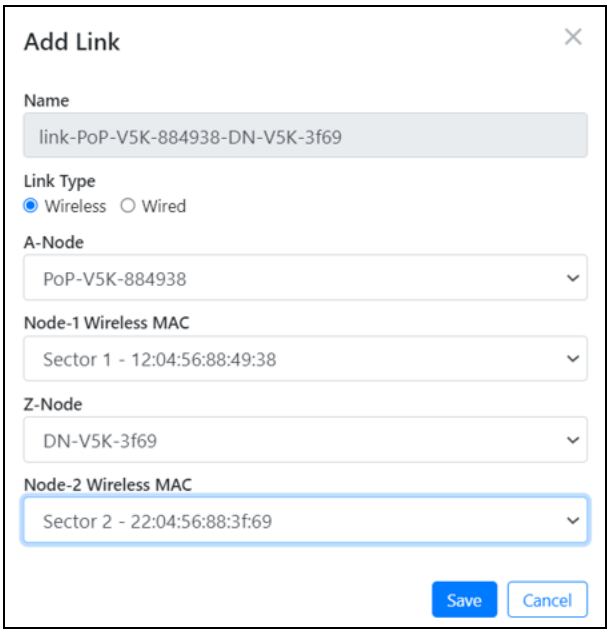
   The DN node gets added to the topology.

7. To add a link, click on the **Links** tab in the **Topology** page.

   The **Links** page appears.

8. Click **Add New** and provide values in the **Add Link** dialog box, as shown below:

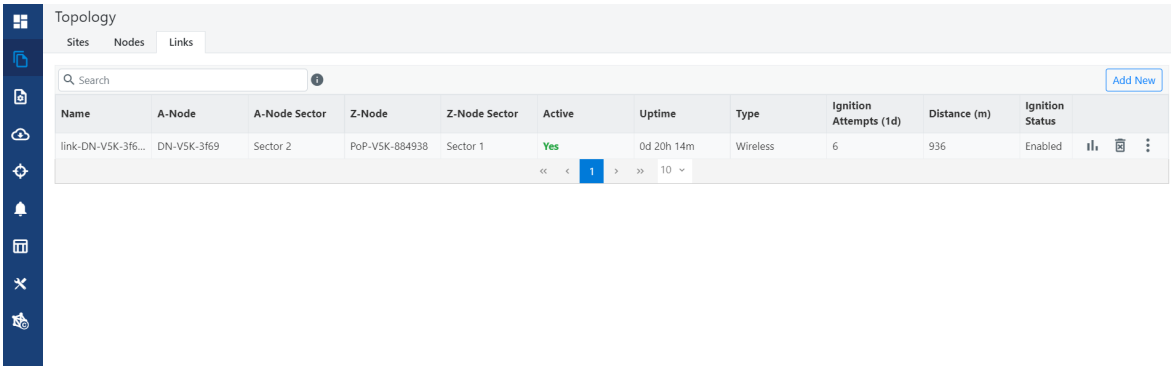
Figure 157: *The Add Link dialog box*



9. Click **Save**.

   The new link gets added to the topology, as shown below:

   Figure 158: *The updated Links page with the new link details*



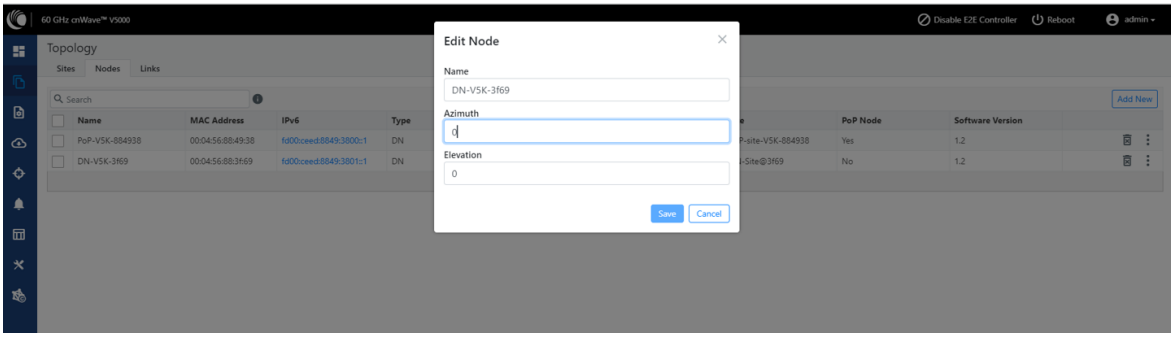
Support for renaming nodes

A node can be renamed in the topology. To rename the node, perform the following steps:

1. From the dashboard page, navigate to **Topology** > **Nodes**.
2. Select the required node and click in the corresponding row. Then, select **Edit Node**.

   The **Edit Node** dialog box appears with information for the selected node.
3. Rename the node, as shown below:

Figure 159: *The Edit Node dialog box*



4. Click **Save**.

Configuration

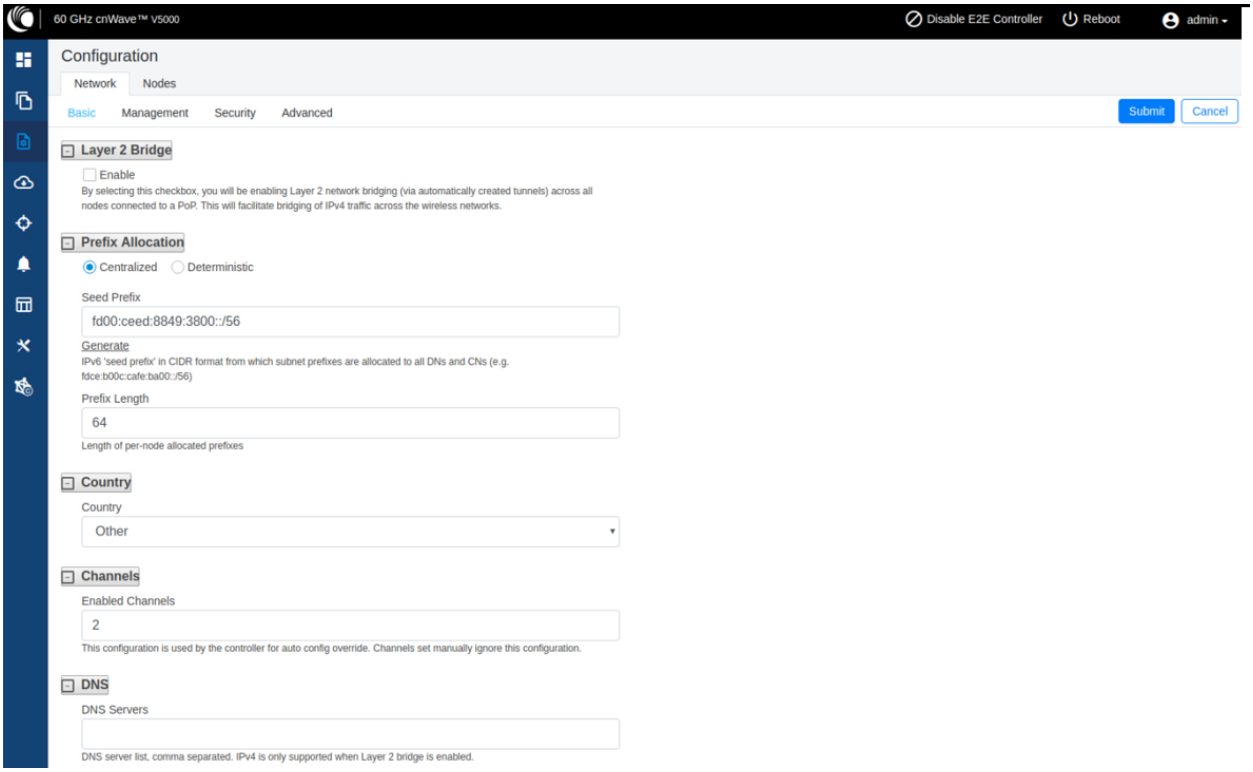
The **configuration** page contains the following two configuration options:

- Network configuration
- Node configuration

Network configuration

Network configuration is used to configure the network. User can modify the network settings. It has **Basic, Management, Security** and **Advanced** options for the configuration. Settings under **Network** apply to all the nodes in the network. Some apply to the **E2E Controller**. Enter the required information and click **Submit** to configure the network.

Figure 160: *The Network page with multiple tabs*



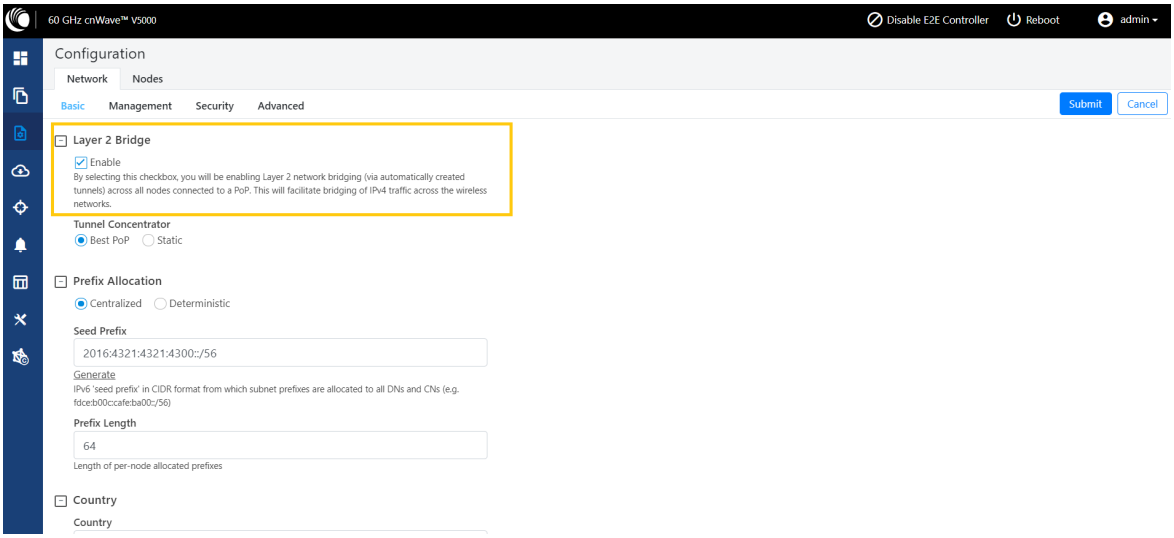
The **Network** page contains the following tabs:

- Basic tab
- Management tab
- Security tab
- Advanced tab

Basic tab

1. By default, cnWave is an IPv6-only network. By selecting this checkbox, Layer 2 network bridging is enabled (via automatically created tunnels) across all nodes connected to a PoP. This facilitates the bridging of IPv4 traffic across the wireless networks.

   Figure 161: *The Layer 2 Bridge section in the Basic page*



   The **Tunnel Concentrator** does encapsulation and de-encapsulation of GRE packets. If **Best PoP** is selected, then the node selects the best PoP as a Concentrator. If **Static** is selected, then the user can configure the external Concentrator that can be Linux machine/router/PoP.

2. Click **Generate** under **Prefix Allocation** to generate a unique local seed prefix automatically.

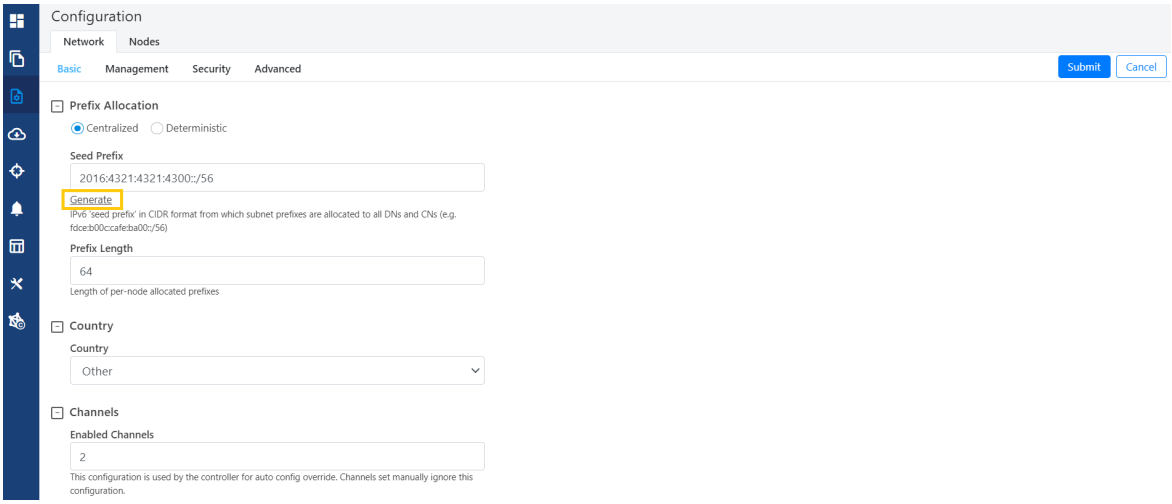
   cnWave networks are given an IPv6 **seed prefix** (e.g. face:b00c:cafe:ba00::/56) from which subnet prefixes are allocated to all DNs and CNs. There are two methods for allocating node prefixes with Open/R.

   Note

   PoP interface IPv6 address and seed prefix should not be in the same /64 prefix range to avoid the address conflict.

   - **Centralized (default)** - Centralized prefix allocation is handled by the E2E controller. The controller performs all prefix allocations, which prevents collisions and enables more sophisticated allocation algorithms. This is recommended for single PoP networks
   - **Deterministic** - Deterministic prefix allocation is also handled by the E2E controller. The controller assigns prefixes to nodes based on the network topology to allow PoP nodes to take advantage of route summarization and help load balance ingress traffic. This is recommended for multi-PoP networks.

Figure 162: *The Prefix Allocation section*



- **Seed Prefix**

  The prefix of the entire cnWave network, is given in CIDR notation.

3. Select **Prefix Length, Country, Channels, DNS Servers**, and **Time zone** from the drop-down.

   Prefix Length

   Specifies the bit-length of prefixes allocated to each node.

   Country

   Country for regulatory settings like the EIRP limit, allowed channels, and other elements.

   Channels

   The comma separates the list of channels given to the controller for auto-configuration. Manual settings in **Node > Radio** page do not depend on this setting. This setting is useful especially for PTP and small meshes that use a single channel for the entire network. In such cases, set the required channel here and do not override in the **node > Radio** page. Changing this setting alone does the channel change, .

   DNS Servers

   DNS server list is used for :

   - Resolution of NTP Server host name (can be IPv4 when Layer 2 bridge is enabled)
   - Given to IPv6 CPE as part of router advertisement

   Time Zone

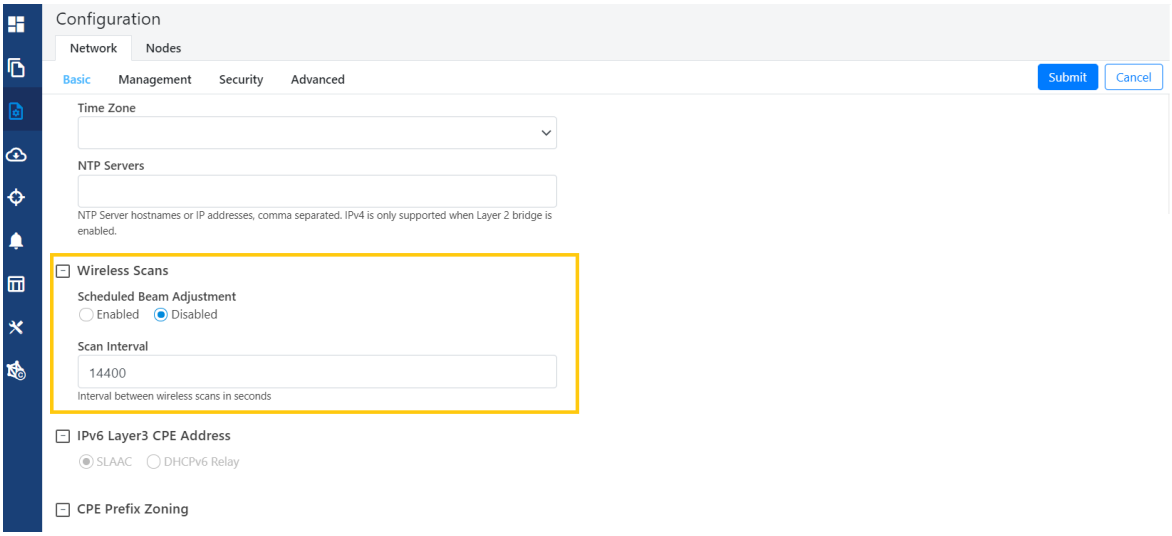
   Time zone for all the nodes. System time in the dashboard, time field in the Events section, Log files use this timezone.

   NTP Servers

   This is NTP Server FQDN or IP Address. All nodes use this NTP Server to set the time. Node time is important when 802.1X radius authentication is used as it requires certificate validation. The time is reflected in the dashboard, time field in the Events section, and Log files .

4. **Wireless Scans (Scheduled Beam Adjustment)** - This feature runs a PBF scan at every defined Scan Interval. Navigate to **Configuration** > **Network** > **Basic** > **Wireless Scans** to run a PBF scan, as shown below:

Figure 163: *The Wireless Scans section*



The 60 GHz cnWave products can align the wireless link within an azimuth/elevation range by selecting from a number of fixed beams.

A normal scan without Scheduled Beam Adjustment does the following operations:

- Beam selection occurs only on wireless link acquisition.
- Disassociating and re-associating the link or otherwise causing the link to drop and re-acquire is needed to perform a new beam selection.
- Any degradation in the wireless conditions does not trigger a new beam selection unless the link drops and reacquires.

The advantages of the Scheduled Beam Adjustment scan are:

- If the link is to acquire during heavy rain, then the optimal beam at that time may be suboptimal when the weather changes.
- If snow accumulation is present on the unit during acquisition, the optimally selected beam may be different when the snow has melted.
- Network-wide ignition in a dense deployment can cause interference when multiple nodes are acquiring. This interference can cause sub-optimal beam selection.
- Any physical change to alignment that is not severe enough to cause a link drop and subsequent beam scan can be corrected for.

The cost of Scheduled Beam Adjustment is:

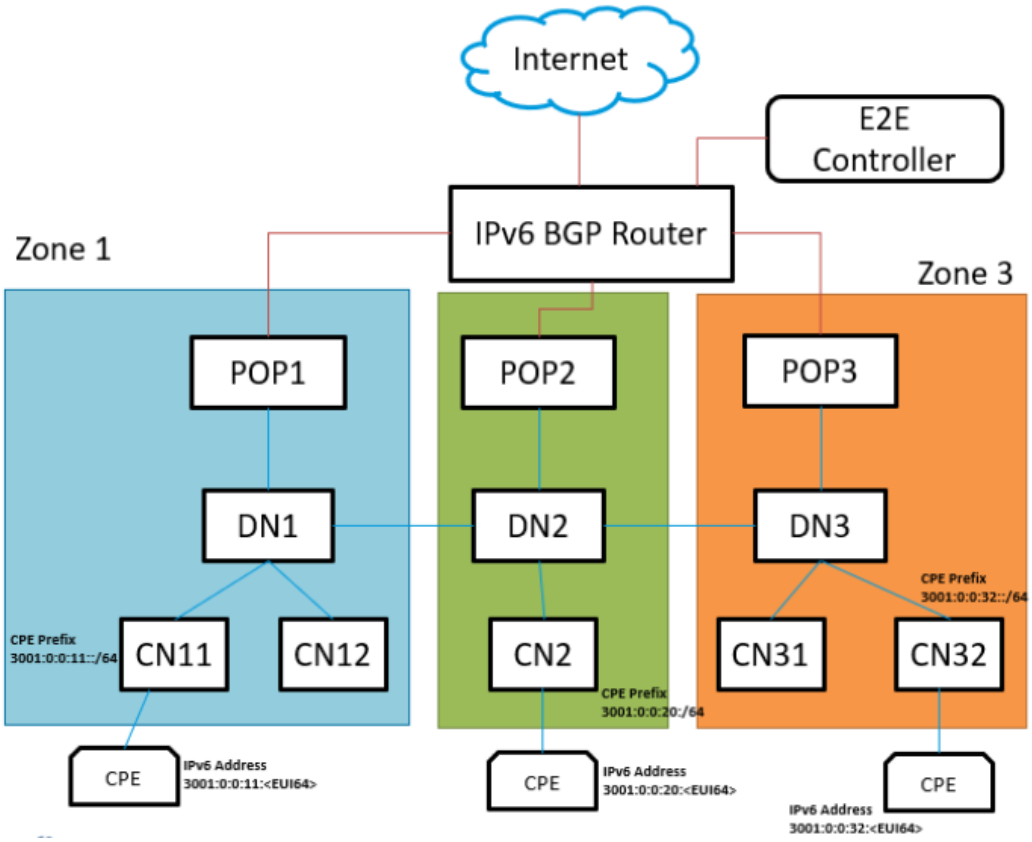
- This feature causes a network-wide outage of approximately **two minutes**. For this reason, unless there is a specific issue being addressed, it is recommended to either disable this feature or configure an interval of >=24 hours.

- Simple deployments (especially PTP links) without significant external factors such as snow may not benefit from regular beam adjustment.

CPE Prefix Zoning

This feature restricts a PoP to advertise the IPv6 CPE prefixes of its zone alone, thereby allowing an upstream BGP router to select an optimal PoP for downstream traffic. Figure 164 is an example of multi-PoP Layer 3 IPv6 topology, which is used to explain the feature in detail.

Figure 164: *Multi-PoP Layer 3 IPv6 topology*



In Figure 164 (which is an example), consider the following points:

- Seed Prefix is 2001::/56.
- Deterministic Prefix Allocation (DPA) is enabled and has three zones.
- An operator wants CPE Address to be in different ranges than Seed Prefix. Therefore, the user traffic can be distinguished from the traffic generated by the cnWave nodes.
- Customized CPE prefix is used with the range 3001:0:0:00XY::/64, where X contains values from 1 to 3.
- IPv6 addresses of CPEs that fall in the range of 3001:0:0:00XY::/64 prefix.

Prior to the introduction of this feature, all PoP BGP Peers advertised all the customized prefixes.

In this example (as shown in Figure 164), PoP1 BGP advertises 3001:0:0:11::/64, 3001:0:0:20::/64, and 3001:0:0:32::/64 prefixes. Similarly, PoP2 and PoP3 advertise all the three prefixes. The upstream BGP router is not able to route the packets to the best PoP. With this feature, PoP advertises the prefix of its zone alone. In the example:

- PoP1 BGP is advertising 3001:0:0:11::/64.
- PoP2 BGP is advertising 3001:0:0:20::/64.
- PoP3 is advertising 3001:0:0:32::/64.

A summarized prefix (shorter prefix) comprising of all the customized prefixes must be configured. When a PoP is down, traffic flows through another PoP. In this example, the summarized prefix is 3001::/58 (six bits from 11 to 30).

The same concept is applicable when the DHCPv6 relay is used. In that scenario, CPEs obtain IPv6 address or delegated prefix directly from the DHCPv6 server.

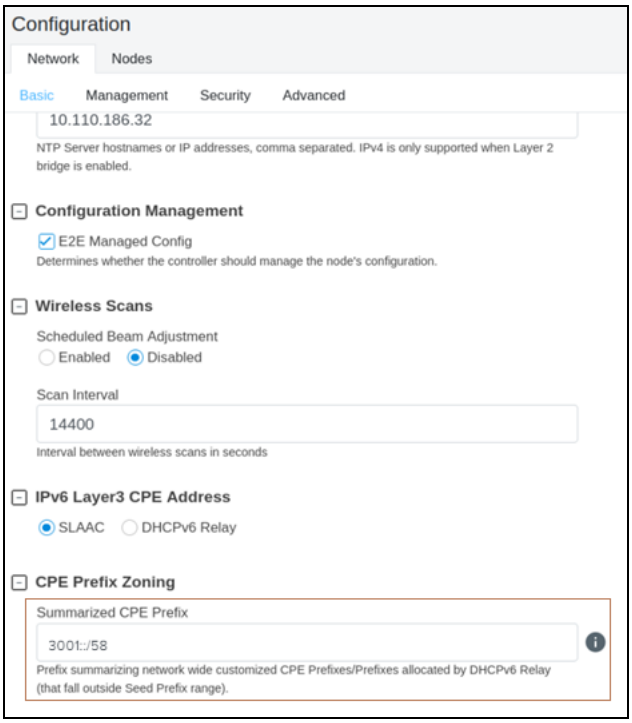
Configuring Summarized CPE Prefix

To configure the **Summarized CPE Prefix** feature, perform the following steps:

1. Navigate to **Network** > **Basic** from the home page.

   The **Basic** page appears. The **Summarized CPE Prefix** text box is available in the CPE Prefix Zoning section, as shown in Figure 165.

   Figure 165: *The Summarized CPE Prefix text box*



2. Type an appropriate value in the **Summarized CPE Prefix** text box.

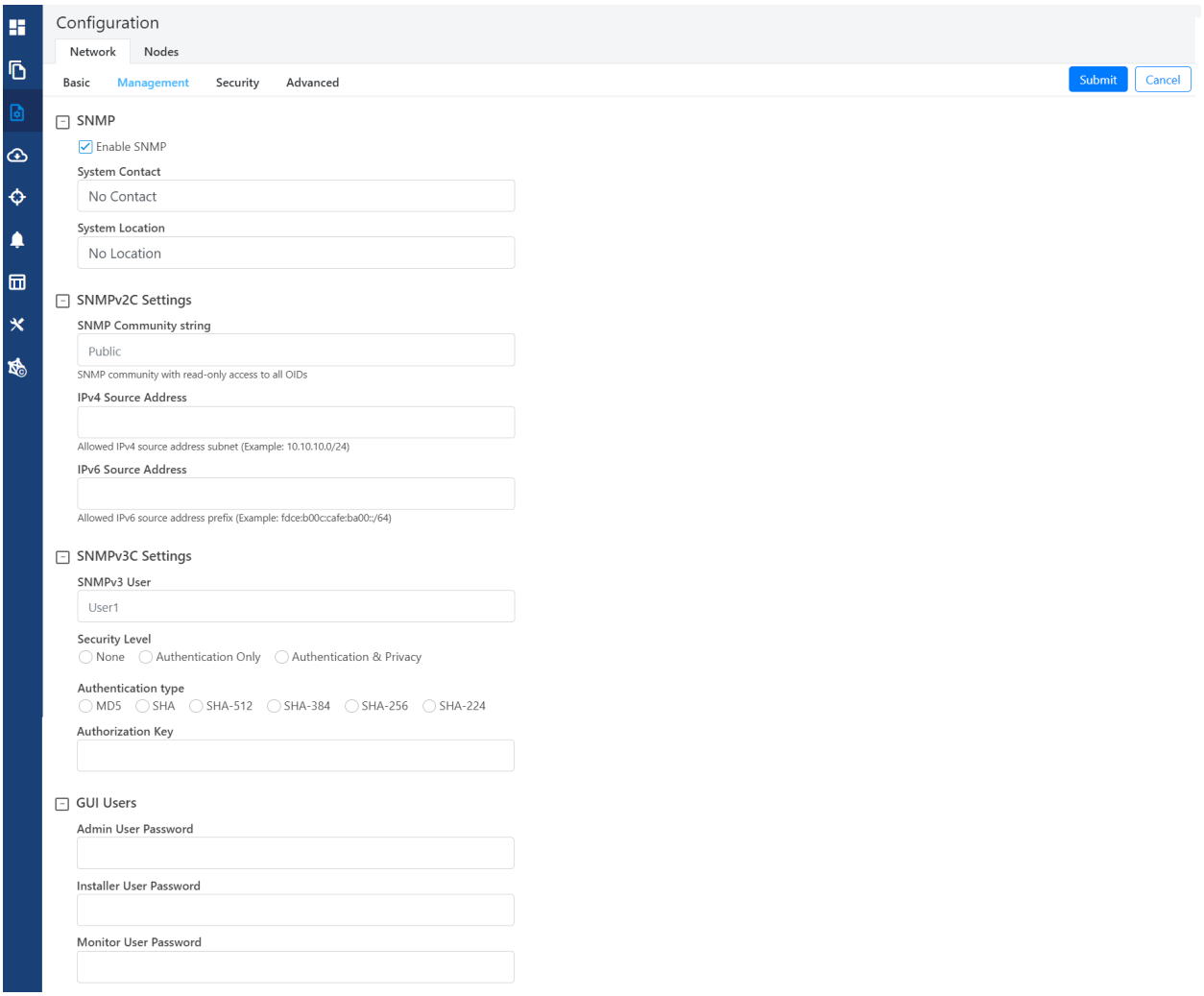
Note

Using a customized CPE prefix and not configuring the summarized CPE prefix can result in routing loops.

Management tab

Click **Management** and select SNMP, SNMPv2 Settings, SNMPv3 Settings, GUI Username and password.

Figure 166: *The Management page*



- **Enable SNMP** - Statistics can be read from the nodes using SNMP. This setting enables SNMP.
- **System Contact** - Sets the contact name as the System.sysContact.0 MIB-II variable.
- **System Location** - Sets the location name as the System.sysLocation.0 MIB-II variable.
- **SNMPv2c Settings**:

- SNMP Community string - Supports read-only access to all OIDs.
- IPV4 Source address - Specified, SNMP queries are allowed from the hosts belonging to this IPv4 address subnet.
- IPV6 Source Address - Specified, SNMP queries are allowed from the hosts belonging to this IPv6 address prefix.

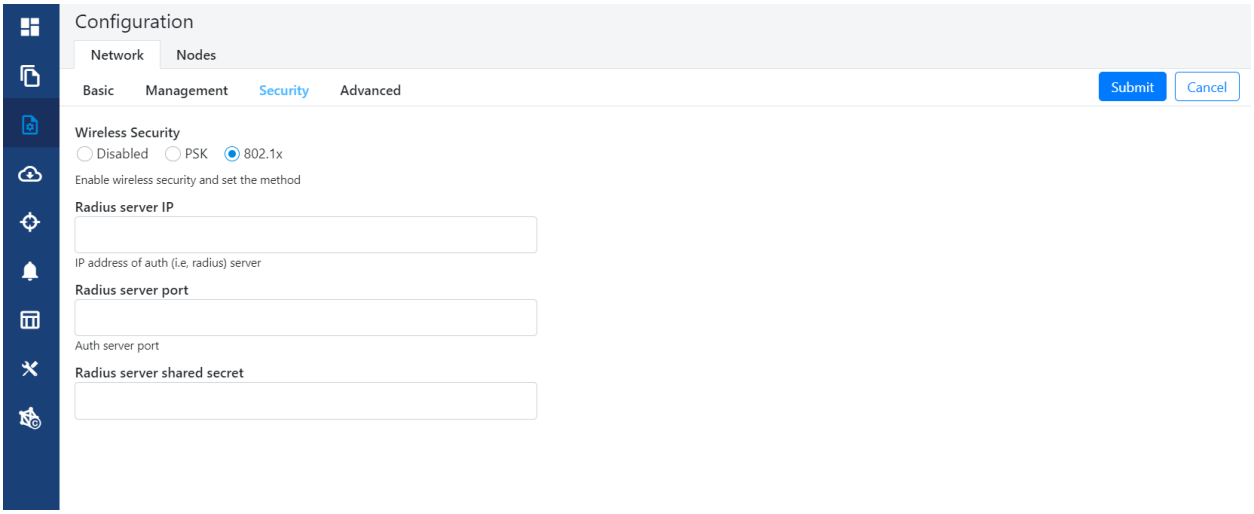
- **SNMPv3c Settings**:
  - **SNMPv3 User** - Name of the SNMPv3c user responsible for managing the system and networks.
  - **Security Level** - Following security levels are supported for the network communication:
    - None - Implies that there is communication without authentication and privacy.
    - Authentication Only - Implies that there is communication with authentication only (without privacy).
    - Authentication & Privacy - Implies that there is communication with authentication and privacy.
  - **Authentication Type** - Type of protocol used for the security of the network communication. Example: MD5 and Secure Hash Algorithm) (SHA) are used for authentication.
  - Authentication Key - A password for the authentication user.

- **GUI Users**:
  - Admin User Password - A password that you can set for GUI management.
  - Installer User Password - A password that you can set for the required installers.
  - Monitor User Password - A read-only password that you set for the monitoring purposes.

Security tab

Security tab contains **Disabled**, **PSK**, and **RADIUS Server** options for Wireless Security. Select the required option.

Figure 167: *The Security page*



Wireless Security

- **Disabled** - there is no wireless security.
- **PSK** – WPA2 pre-shared key can be configurable. A default key is used if this configuration is not present. AES-128 encryption is used for data encryption.
- **802.1X** – Nodes are authenticated using radius server and use EAP-TLS. Encryption is based on the negotiated scheme in EAP TLS.

RADIUS Server IP - IPv4/IPv6 address of the Radius authentication server.

RADIUS Server port - Radius authentication server port.

RADIUS server shared secret - The shared secret of a radius server.

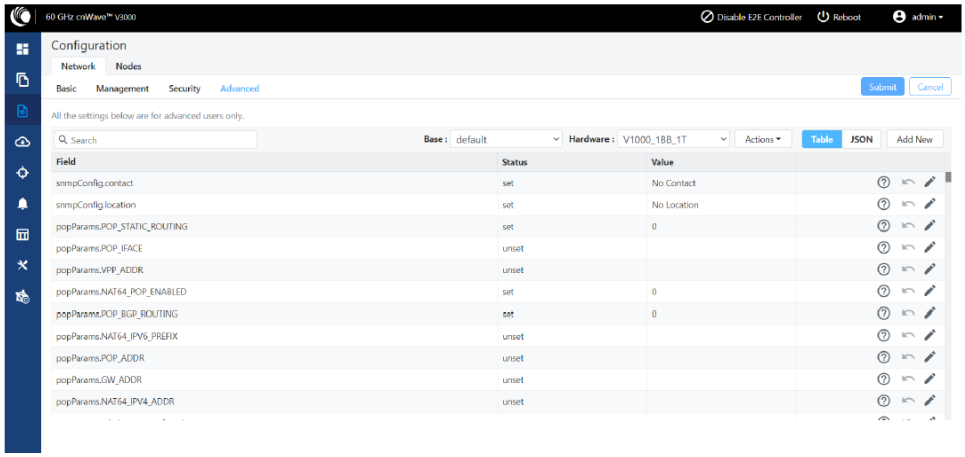
Advanced tab

These settings are for advanced users only. Displays the merged configuration off all layers for a particular node.

Caution

The users are not recommended to do these settings.

Figure 168: *The Advanced page*



Node configuration

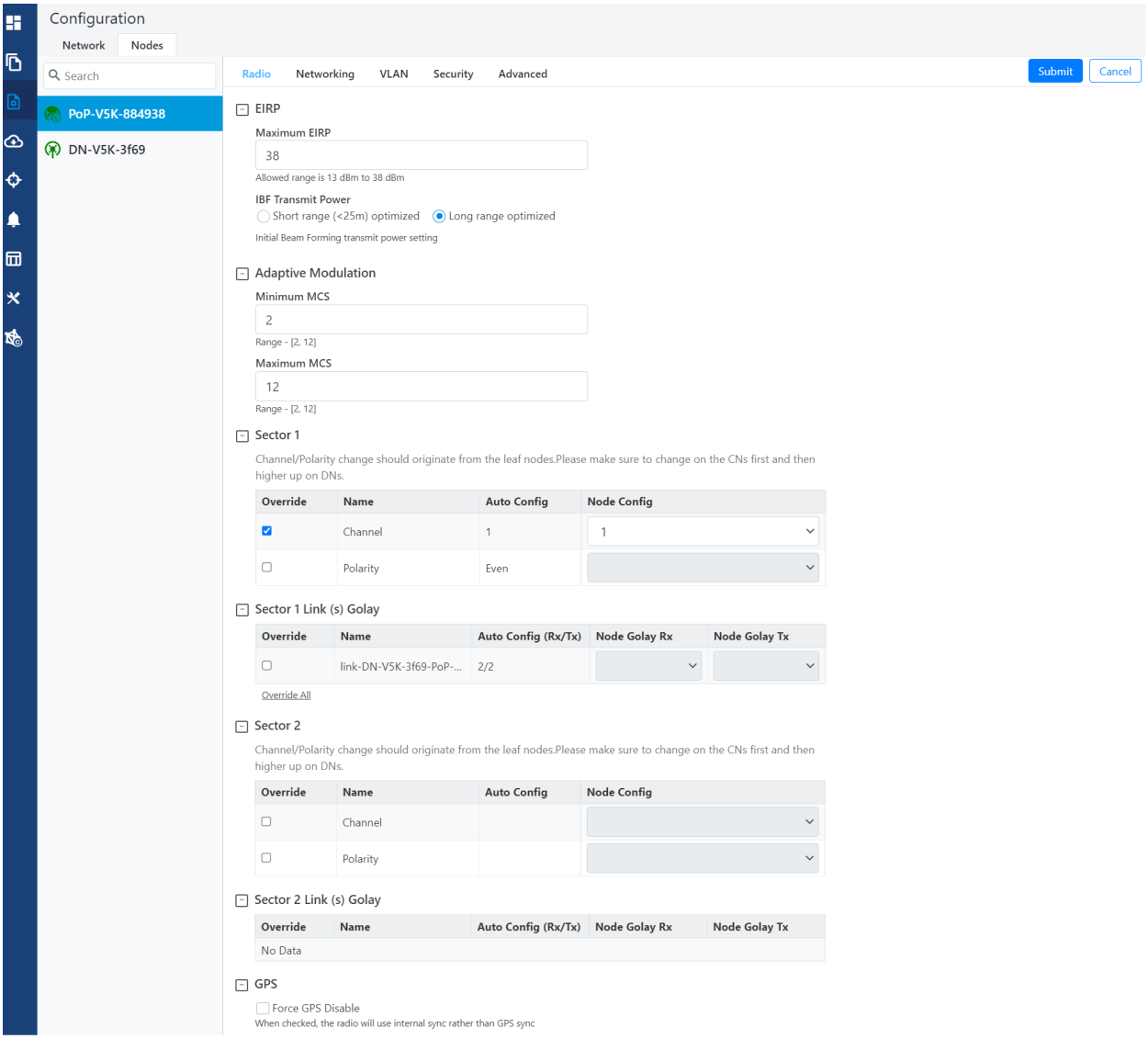
Node configuration is used to configure the nodes via E2E Controller. E2E Controller can modify the node settings. Select the node(Radio) on the left pane to modify the settings. Node configuration contains the following tabs:

- Radio tab
- Networking tab
- VLAN tab
- Security tab
- Advanced tab

Radio tab

These settings apply to individual nodes selected in the left side panel. Select the required options for Transmit Power, Adaptive Modulation, Sector 1, Sector 2 from the drop-down. Enable **Force GPS Disable** to establish the link between indoor nodes.

Figure 169: *The Radio page*



The **Radio** page contains the following elements:

Table 39: Elements in the Radio page

Elements	Description
EIRP	Transmit power of the radio • **Maximum EIRP** - The maximum EIRP transmitted by the radio. Range differs based on the platform and country selected (in the Network page). • **IBF Transmit power** - Transmit power using during initial beam forming. When all the links are in short-range, high transmit power can cause interference. Selecting short-range optimized will prevent this. Post beam forming, automatic power control will make sure the radio transmits at optimal power.

Elements	Description
Adaptive Modulation	Select minimum and maximum coding scheme ranging from 2 to 12.
Sector 1	• Select the frequency channel and polarity. • **Channel and Polarity** - When link is created in topology, the controller automatically sets the sector's channel and polarity. To manually override, click the check box and select the channel in the node configuration. Note that changing channel/polarity breaks the link. It is important to change for leaf nodes first and then higher up on DNs.
Sector 1 Link (s) Golay	Golay codes help in avoiding inter-sector interference. In rare scenarios, individual links might require separate Golay codes. In most scenarios, all the links belonging to a sector are configured same Golay code. The controller automatically sets the Golay code. To manually override, select the check box and set the Golay from the drop-down. **Override All** button helps in setting the same Golay code for all the links. **Note** Golay codes and frequency on both ends of the link should match.
Sector 2	Select the frequency channel and polarity.
Sector 2 Link (s) Golay	Golay code.
GPS	If enabled then, the radio uses internal sync rather than the GPS sync. In some scenarios like lab setups, it may be necessary to disable GPS.

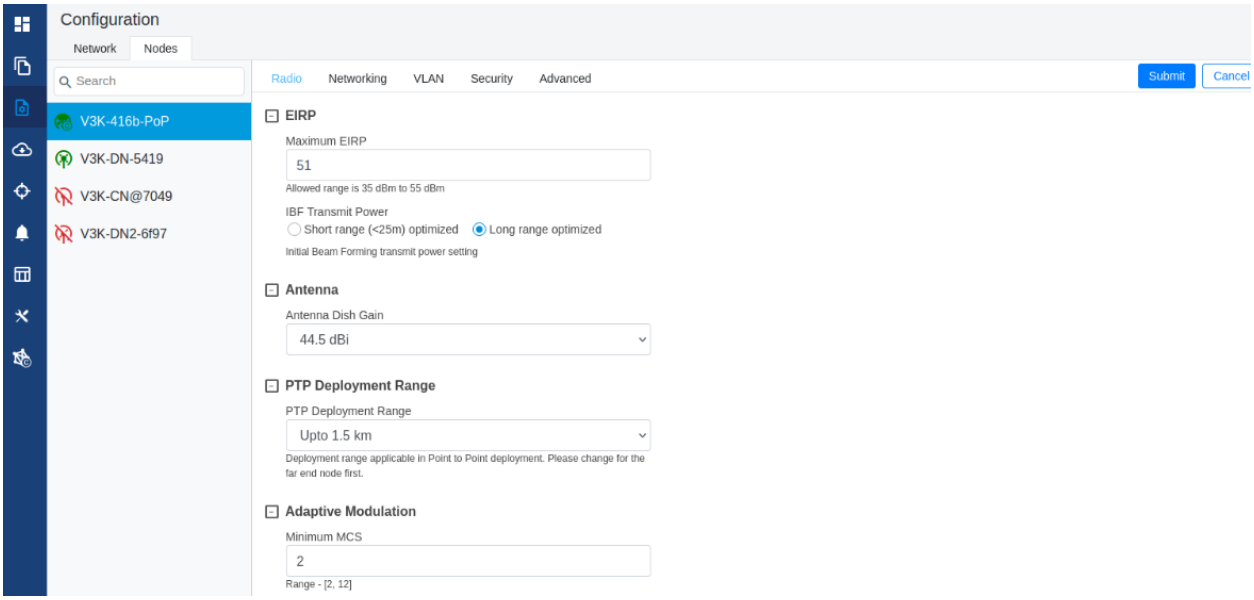
Caution

60 GHz cnWave V1000 and V3000 devices has only **Sector 1**.

V3000 Small dish support

The software allows the selection of smaller 40.5 dBi antenna dish. To select V3000 small dish, navigate to **Configuration** > **Nodes** > **Radio**. The **Antenna** section is available in the Radio page.

Figure 170: *The Antenna section*



Caution

Small dish is supported only for 60 GHz cnWave V3000.

Networking tab

When you navigate to **Nodes** > **Networking** from the home page, the **Networking** page appears.

In the **Networking** page, perform the following steps:

1. Enter the local IPv4 address.

   Figure 171: *The IPv4 Management section in the Networking page*

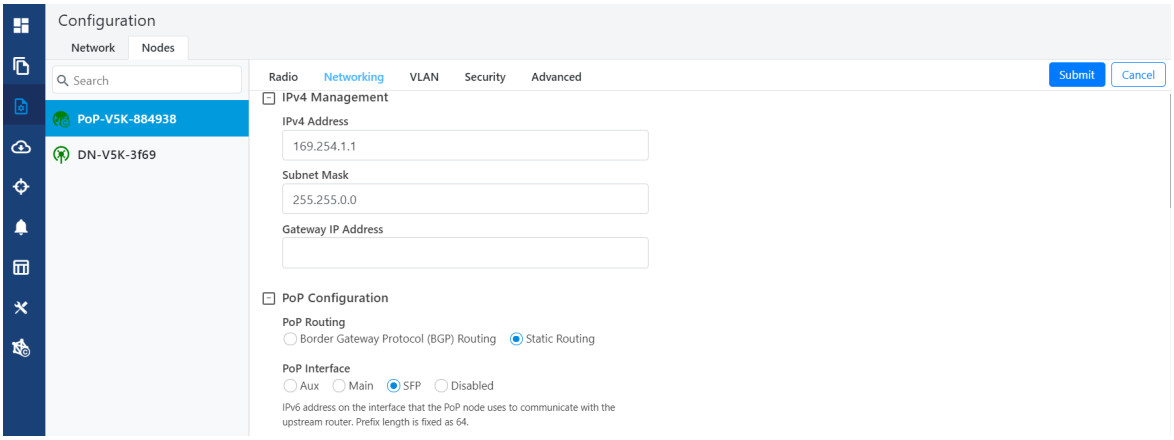


Table 40: Elements in the IPv4 Management section

Elements	Description
IPv4 Address	Static IPv4 address of the individual node. Node's GUI /CLI can be opened using this IP address when directly connected over Ethernet. For Over the air access, L2 Bridge should be enabled. Its predominantly used on PoP nodes with the onboard controller.
Subnet Mask	Subnet mask for the IPv4 address.
Gateway IP Address	IPv4 Gateway address.

2. Under **PoP Configuration**, select the options for **PoP Routing**, **PoP Interface**, and click **Generate** to generate **PoP Interface IP Address**.

Figure 172: *The PoP Configuration section in the Networking page*

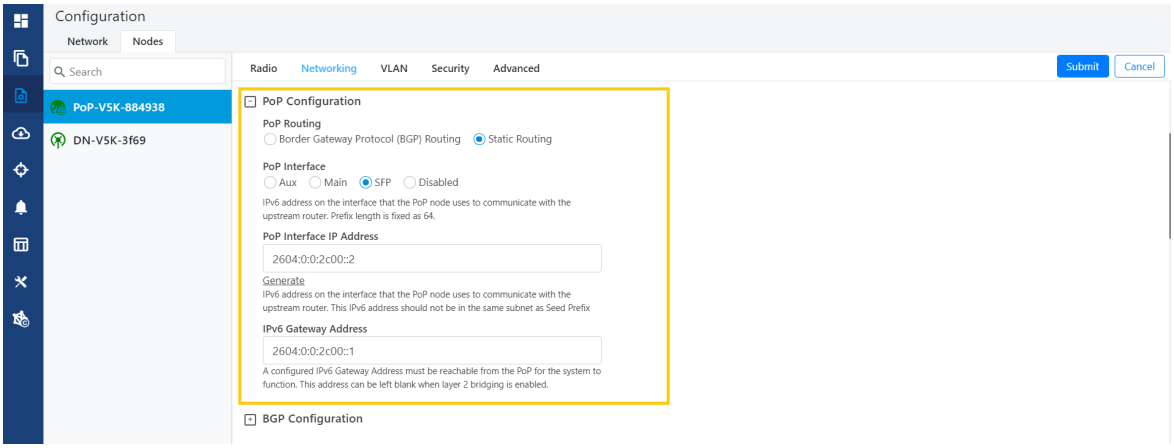


Table 41: Elements in the PoP Configuration section

Elements	Description
PoP Routing	PoP nodes connect to the upstream IPv6 router in one of two ways: • **Border Gateway Protocol (BGP) Routing** – PoP acts as a BGP peer • **Static routing** – IP gateway address should be specified on the PoP and static route should be added on the upstream router. When the system is targeted for L2 traffic (Layer 2 bridge enabled) and an onboard controller is used, this configuration is of not much significance, recommended to set to static routing.
PoP Interface	The wired interface on which PoP communicates to an upstream router or switch when the L2 bridge is enabled.
PoP Interface IP Address	IPv6 address on the interface that the PoP node uses to communicate with the upstream router.

Elements	Description
IPv6 Gateway Address	Gateway address. Can be left empty when the L2 bridge is enabled and no IPV6 services like NTP /Radius are used.

3. Under **E2E Controller Configuration**, enter E2E IPV6 Address (Address of E2E Controller). When using the onboard controller on the same node, can be left empty and GUI automatically fills the POP IPv6 address.

Note

If PoP DN is V5000/V3000 then, IPv6 both address is same.

Table 42: Elements in the E2E Controller Configuration section

Elements	Description
E2E IPv6 Address	Address of E2E Controller. When using the onboard controller on the same node, can be left empty and GUI automatically fills the POP IPv6 address.
E2E Network Prefix	Seed Prefix in the CIDR format followed by a comma and the prefix length. Should be specified when BGP is used. Otherwise, optional.
IPv6 CPE Interface	IPv6 SLAAC provides IP prefix to downstream CPE devices. Keep it disabled when L2 Bridge is active.

4. Select the required BGP configuration.

Figure 173: *The BGP Configuration section*

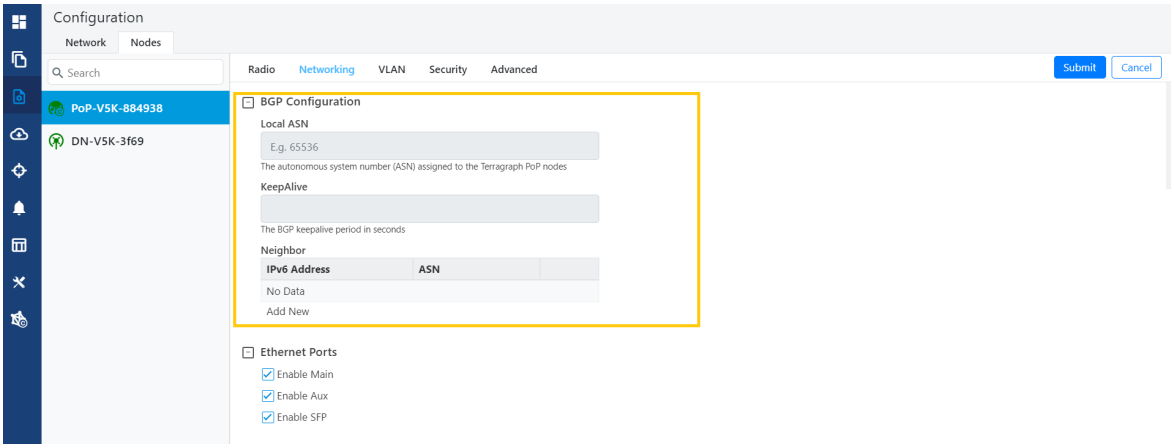
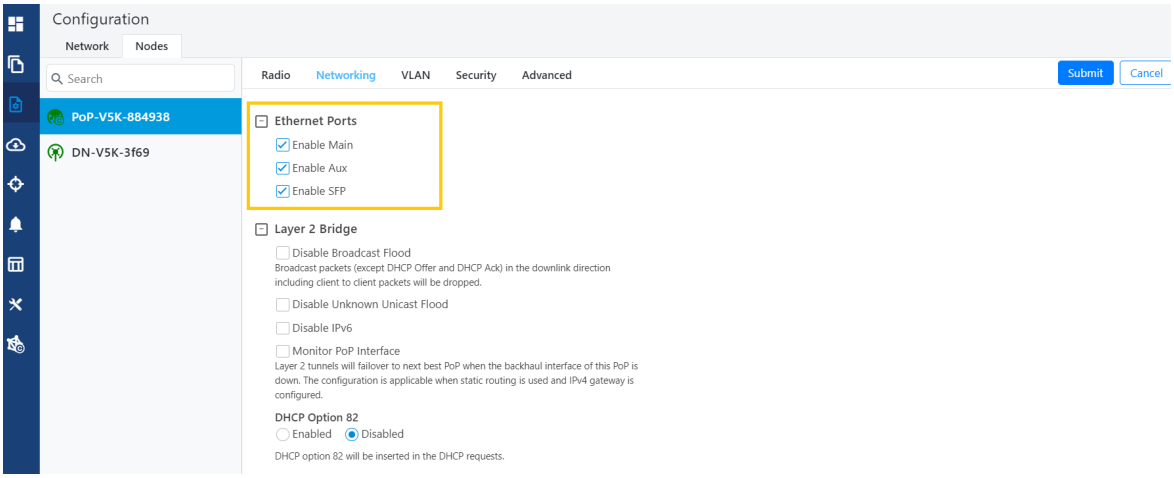


Table 43: Elements in the BGP Configuration section

Elements	Description
Local ASN	Local ASN
KeepAlive	The BGP keepalive period in seconds.
Neighbour ASN	Upstream router's ASN
Neighbour IPv6	Upstream router's IPv6 address
Specific Network prefixes	Specifically allocated network prefixes to be advertised via BGP

5. Enable the required Ethernet ports. Individual Ethernet ports can be turned off with this configuration.

   Figure 174: *The Ethernet Ports section*



6. Select the required options for **Layer 2 Bridge**, **IPv6 Layer 3 CPE**, **AuX PoE** (enable to power on AuX port), and **Multi-PoP / Relay Port**. By default, this option is disabled and PoP floods any unknown unicast ingress packets on all the L2GRE tunnels. When the option is enabled, PoP drops such packets.

Figure 175: *The Layer 2 Bridge section in the Networking page*

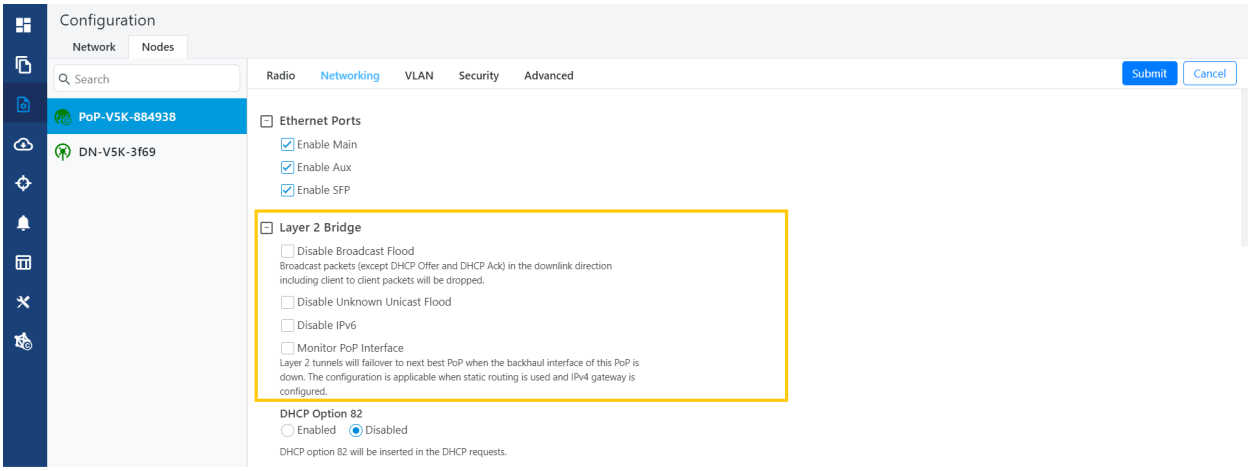


Table 44: Elements in the Layer 2 Bridge section

Elements	Description
Layer 2 Bridge	It has three options: • Disable Broadcast Flood • Disable Unknown Unicast Flood • Disable IPv6 • Monitor PoP Interface For information on **Monitor PoP Interface**, refer to Configuring Monitor PoP Interface,
Aux PoE	Enable PoE out (25 W) on V5000/V3000 aux port. 802.3af and 802.3at compliant devices could be powered up, passive PoE devices cannot be powered up. Note that the aux port cannot power another V5000/V3000.
Multi-PoP / Relay Port	Indicates the wired interfaces (or Ethernet) on which OpenR is running. This element must be used: • When DNs are connected back-to-back. • When multiple PoPs are in the network. This allows PoP nodes to forward traffic to other PoP nodes via a wired connection when the routing path of the other PoP node is closer to the traffic destination Following options are supported: • Aux • Main • SFP • Disabled