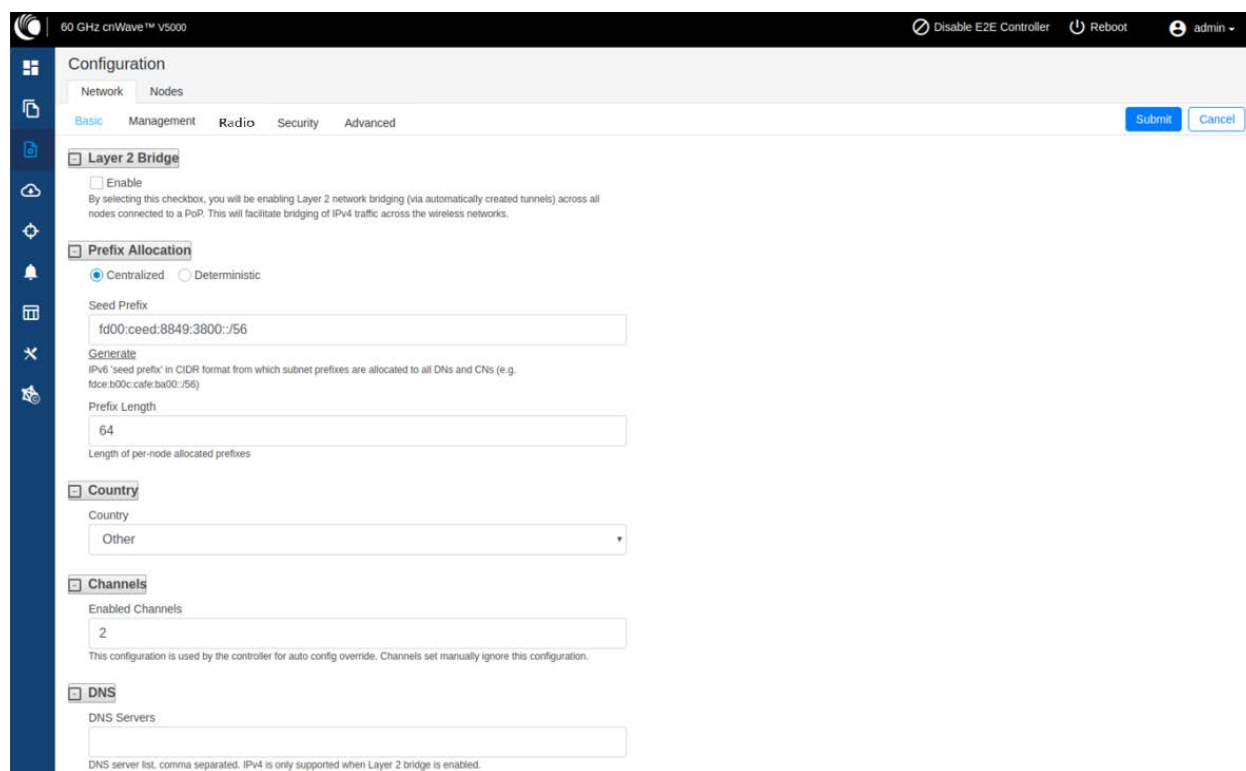


Figure 167: The Network page with multiple tabs



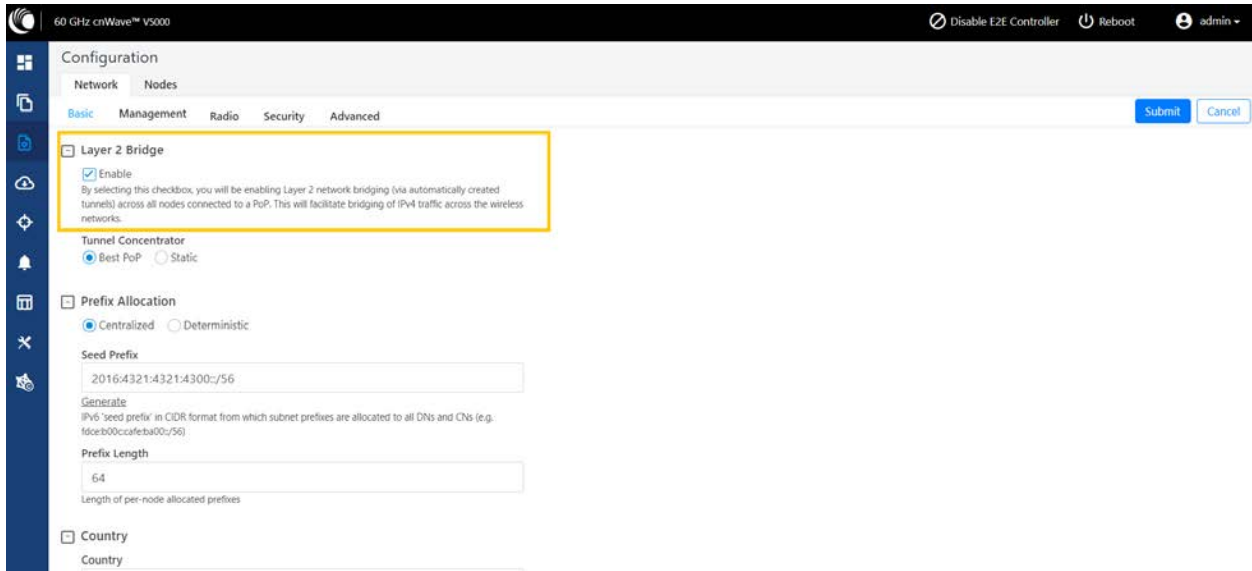
The **Network** page contains the following tabs:

- [Basic](#)
- [Management](#)
- [Radio](#)
- [Security](#)
- [Advanced](#)

Basic

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 168: 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.

To configure the parameters on the Basic page, perform the following steps:

1. 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 169: The Prefix Allocation section

The screenshot shows the 'Configuration' page for 'Network Nodes'. The 'Prefix Allocation' section is expanded, showing the following settings:

- Prefix Allocation:** Centralized, Deterministic
- Seed Prefix:** 2016:4321:4321:4300::/56 (highlighted with a yellow box)
- Generate:** IPv6 'seed prefix' in CIDR format from which subnet prefixes are allocated to all DNs and CHs (e.g. fdce80ccaf6ba00::/56)
- Prefix Length:** 64 (Length of per-node allocated prefixes)
- Country:** Other (dropdown menu)
- Channels:** 2 (Enabled Channels)

Below the Channels field, there is a note: "This configuration is used by the controller for auto config override. Channels set manually ignore this configuration."

- **Seed Prefix**

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

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

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

Indicates the channel number required for forming a link through an onboard E2E Controller or an external E2E Controller (if deployed).

By default, Channel 2 is supported. This parameter also supports a comma-separated list of channel numbers (for example: 2,3, 4,5), which you can give to a controller for auto configuration. Manual settings (which are made using the **Node > Radio** page) do not depend on this channel setting. This channel setting is useful, especially for PTP and small meshes that use a single channel for the entire network. In such a case, set the required channel number in this field and do not override the value that you set on the **Node > Radio** page. Modifying this **Channels** parameter is sufficient for 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

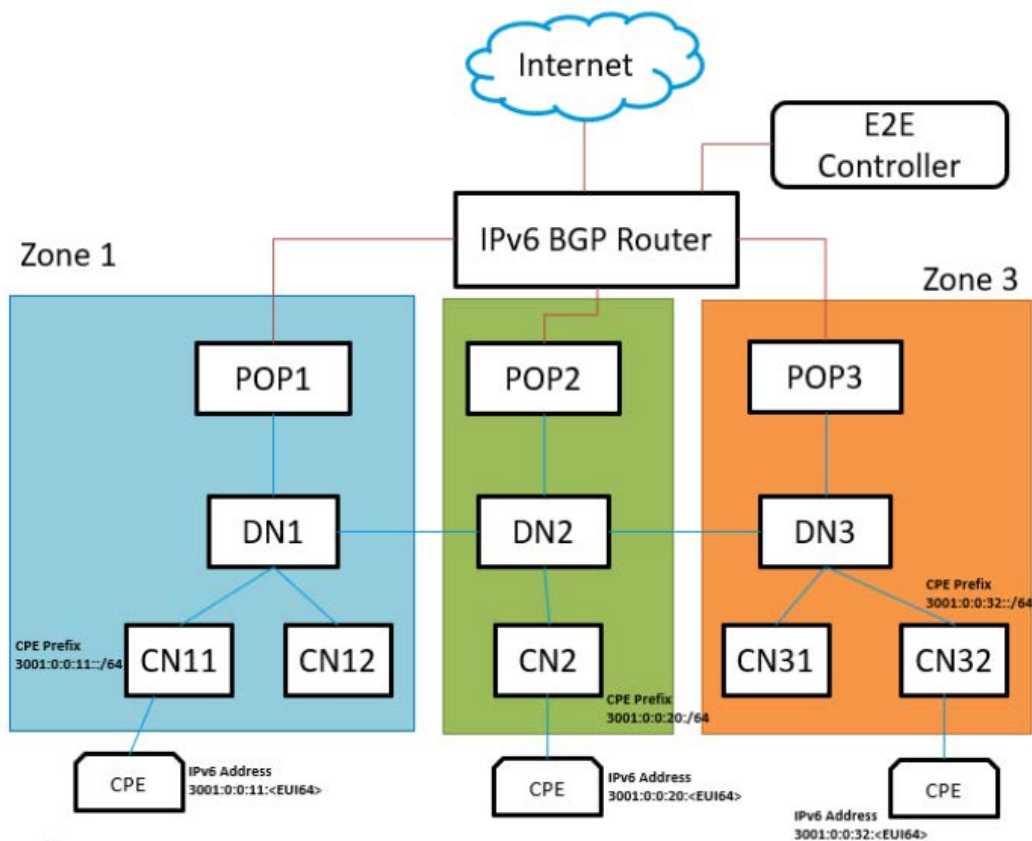
This is NTP Server FQDN or IP Address. All nodes use this NTP Server to set the time. Node time is important when 802.1X radius authentication is used as it requires certificate validation. The time is reflected in the dashboard, time field in the Events section, and Log files .

CPE Prefix Zoning

You can configure the **Summarized CPE Prefix** parameter using the **Basic** page.

The **Summarized CPE Prefix** 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 170](#) is an example of multi-PoP Layer 3 IPv6 topology, which is used to explain the feature in detail.

[Figure 170](#): Multi-PoP Layer 3 IPv6 topology



In [Figure 170](#) (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 170](#)), 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 171](#).

Figure 171: *The Summarized CPE Prefix text box*

The screenshot shows the 'Configuration' page for a network node. The 'Network' tab is selected, and the 'Basic' sub-tab is active. The 'Summarized CPE Prefix' field is highlighted with a red box. The field contains the value '3001::/58'. Below the field, there is a small information icon (i) and a tooltip that reads: 'Prefix summarizing network wide customized CPE Prefixes/Prefixes allocated by DHCPv6 Relay (that fall outside Seed Prefix range)'. Other sections visible include 'Configuration Management' (with 'E2E Managed Config' checked), 'Wireless Scans' (with 'Scheduled Beam Adjustment' set to 'Disabled' and 'Scan Interval' set to '14400'), and 'IPv6 Layer3 CPE Address' (with 'SLAAC' selected).

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

On the **Configuration > Network** page, click **Management** and select SNMP, SNMPv2 Settings, SNMPv3 Settings, GUI Username and password.

Figure 172: The Management page

The screenshot shows the 'Configuration' page with the 'Network' tab selected and the 'Management' sub-tab active. The page contains several configuration sections:

- SNMP**: Includes a checked 'Enable SNMP' checkbox, 'System Contact' (No Contact), and 'System Location' (No Location) text boxes.
- SNMPv2C Settings**: Includes 'SNMP Community string' (Public), 'SNMP community with read-only access to all OIDs', 'IPv4 Source Address', and 'IPv6 Source Address' text boxes.
- SNMPv3C Settings**: Includes 'SNMPv3 User' (User1), 'Security Level' (None selected), 'Authentication type' (MDS selected), and 'Authorization Key' text boxes.
- GUI Users**: Includes 'Admin User Password', 'Installer User Password', and 'Monitor User Password' text boxes.

- **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 network communication. Example: MD5 and Secure Hash Algorithm) (SHA) are used for authentication.
 - Authentication Key - A password for the authentication user.
- **For UI 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.

Radio

The **Radio** page allows you to configure the wireless scan settings, the CN channel scanning options, and other parameters.

Wireless Scan scheduling for beam adjustment

The **Scheduled Beam Adjustment** parameter, when enabled, allows you to make small adjustments to the selected fixed beam for optimal RF alignment in azimuth and elevation. You can select this schedule option using the **Scan Schedule Type** parameter (Day/Time or Interval schedule type).

To configure the **Scheduled Beam Adjustment** parameter, navigate to the **Wireless Scans** section on the **Configuration > Network > Radio** page (as shown in [Figure 173](#)).

A normal scan without the **Scheduled Beam Adjustment** setting 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:

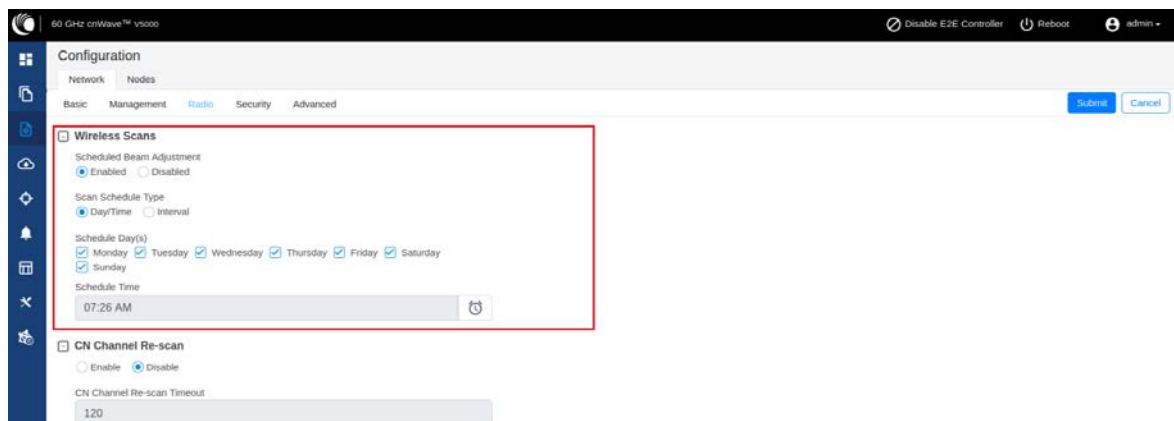
- This feature causes a 50% throughput reduction for about 20 minutes, depending on the size of the network.
- Simple deployments (especially PTP links) without significant external factors such as snow may not benefit from regular beam adjustment.

To configure the wireless scan scheduling options using the device UI, perform the following steps:

1. From the home page of the device UI, navigate to **Configuration > Network > Radio**.


The **Radio** page appears with the **Wireless Scans** section, as shown in [Figure 173](#).

[Figure 173](#): *The Wireless Scans section*



[Table 45](#) lists the parameters in the **Wireless Scans** section of the **Radio** page.

Table 45: Parameters in the Wireless Scans section

Parameter	Description
Scheduled Beam Adjustment	<p>Allows you to enable or disable the scheduled beam adjustment feature.</p> <p>This parameter, when enabled, allows you to make small adjustments to the selected fixed beam for optimal RF alignment in azimuth and elevation. You can select this schedule option using the Scan Schedule Type parameter.</p>
Scan Schedule Type	<p>Allows you to select the scan scheduling option for beam adjustment.</p> <p>This parameter supports the following scan scheduling options:</p> <ul style="list-style-type: none"> • Day/Time: This schedule option allows you to select any day (or all days) of the week and time of the day. <p>When you select the Day/Time option, following parameters are applicable:</p> <ul style="list-style-type: none"> • Schedule Day(s): Select the check boxes to choose the day(s). • Schedule Time: Use the  icon to set the time of the day. <p>Apart from the interval scans, you are allowed to select any day (or all days) of the week and time of the day. This setting enables you to schedule the scan during maintenance activities.</p> • Interval: This scan schedule option allows you to set an interval (in seconds) for wireless scans. The default value is 3600 seconds.

2. Set the parameters based on your requirements, as shown in [Figure 173](#).
3. Click **Submit** to save the changes.

Configuring CN Channel scanning options

When a CN loses its wireless connection, it initially scans the previously configured channel. This process speeds up the link acquisition in cases where the corresponding DN has not changed its channel. However, if the DN has switched channels, the CN scans all available channels, after a timeout period, to re-establish the connection.



Note

The advantages of CN channel rescan are:

- Moving the connected DN to a different channel is automatically detected by the CN when the configured timeout period expires.
- There is more flexibility in the topology as CNs can easily be reassigned to a different DN on a different channel without CN specific channel overrides.

The main reason to disable the CN channel rescan is to have the fastest possible network recovery following an event (for example, a software upgrade or network wide power cut). In networks, which have been fully deployed and where the configuration is not being changed, there may not be a requirement for channel rescan.

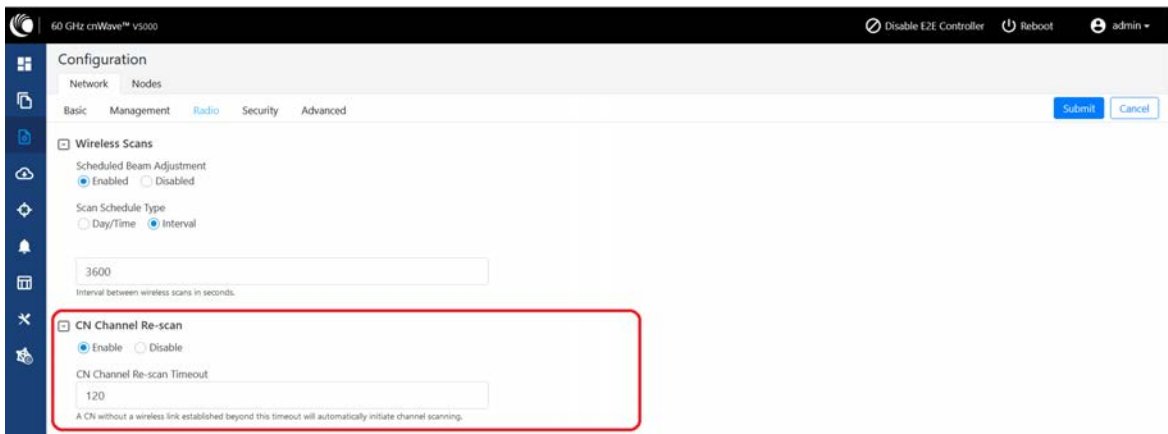
Using the device UI or the cnMaestro UI, you can configure the CN channel scanning options. These configurable options enhance the adaptability and responsiveness of your cnWave network, allowing it to better accommodate varying network conditions and configurations.

Using the device UI, perform the following steps:

1. From the home page of the device UI, navigate to **Configuration > Network > Radio**.

The **Radio** page appears with the **CN Channel Re-scan** section, as shown in [Figure 174](#).

Figure 174: The CN Channel Re-scan section - Device UI



[Table 46](#) lists the parameters in the **CN Channel Re-scan** section.

Table 46: CN Channel Re-scan specific parameters

Parameter	Description
Enable	By default, the Enable option is selected (enabled), as shown in Figure 174 . This option allows you to disable the full channel rescan feature. When this option is selected, the CN scans only the configured channel while attempting to re-establish a lost connection. This option can be beneficial in stable environments where DNs are unlikely to switch channels frequently, thereby accelerating the reconnection process.

Parameter	Description
CN Channel Re-scan Timeout	<p>When the rescan feature (Enable CN Channel Re-scan) is not disabled, you can set a custom timeout value (in seconds) for the CN before it initiates a full channel scan. This capability allows you to adjust the balance between quicker reconnection times (by scanning the configured channel) and broader network coverage (by scanning all channels after the timeout).</p> <p>By default, the value of this timeout option is set to 120 seconds. This option allows the value ranging from 120 to 3600 seconds</p>

2. Set the CN channel re-scan functionality using **Enable** or **Disable** check boxes, as described in [Table 46](#).
By default, this parameter is enabled.
3. Set the required value (in seconds) in the **CN Channel Re-Scan Timeout** text box.
4. Click **Submit** to save the changes.

Security

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

Figure 175: 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

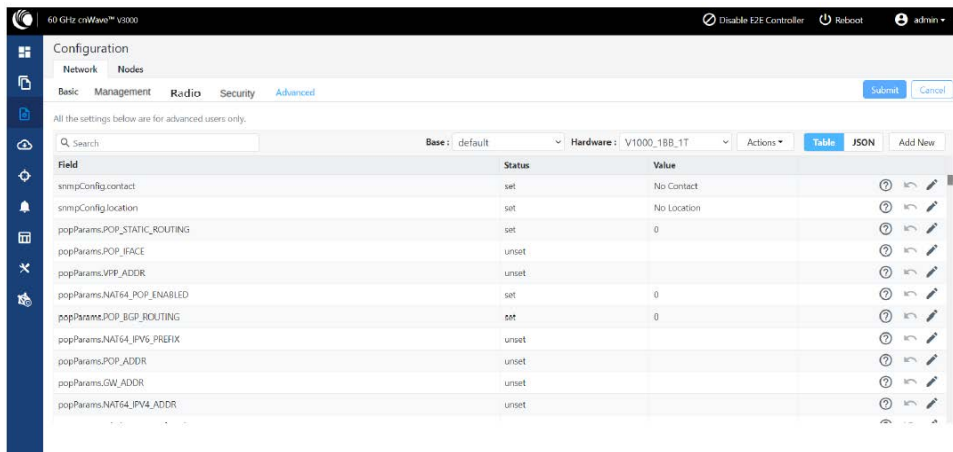
The **Advanced** page settings are for advanced users only. This page displays the merged configuration of all layers for a particular node.



Caution

The users are not recommended to modify or change settings on the **Advanced** page.

Figure 176: The Advanced page



The **Network > Advanced** page supports the configuration of the following feature:

DN Channel Rescan

The DN Rescan feature optimizes the deployment and management of temporary network structures in settings such as concerts, recreational vehicle (RV) parks, and others. The feature also enables a seamless reconnection of DNs that have moved within new network environments.

How this feature works?

The DN Rescan feature comes into action when a DN loses a DN-DN link, consequently leading to a Point of Presence (PoP) being unreachable.

In a normal operation, the DN remains on the same channel and does not perform a rescan. This is due to the lost link that might be in the downstream direction where rescan does not apply or the affected sector might be serving other active links. However, the DN Rescan feature changes this behaviour under specific circumstances.

How to configure the feature?

To enable the DN Rescan feature, configure the `envParams.CAMBIUM_ENABLE_DN_CHANNEL_RESCAN` parameter using the **Configuration > Advanced** page of the device UI. By default, the value of this parameter is `false` (disabled). To enable the DN Rescan feature, set the value of this parameter to `true`.

If you set the value of this parameter to `true` and the DN is unable to detect a PoP for a certain duration (which is configurable using the `envParams.CAMBIUM_DN_CHANNEL_RESCAN_TIMEOUT` parameter), the DN resets the channel, Golay, and polarity on all its sectors by proceeding to scan all channels. This scan process facilitates the DN to form new links with an upstream PoP or DN without any manual intervention, achieving a true zero-touch experience.



Note

To set the timeout duration (in minutes) for different environments, configure the `envParams.CAMBIUM_DN_CHANNEL_RESCAN_TIMEOUT` parameter using the **Configuration > Advanced** page of the device UI. The default value of this parameter is 20 minutes, and the minimum allowed value is 10 minutes.

Use cases

The DN Rescan feature supports the movement of DNs in temporary deployments with zero touch (main use case). In addition, the feature supports the modification of the channel on the near end DN first.

The correct method is to change the far end DN channel first and then the near end. However, this feature can serve as a fail-safe in case if the near end DN channel is modified first. Note that both the ends must match, otherwise the controller does not ignite the link.

Frequently asked questions (FAQs)

Following table lists the FAQs specific to the **DN Rescan** feature.

FAQ	Answer
How the feature detects the DN-DN link loss?	The DN Rescan feature does not detect the link loss, directly. It helps in monitoring the visibility of the POP, periodically.
What happens if the DN fails to detect a PoP even after the channel, golay, and polarity reset and rescan process?	The DN continues to scan until it reaches the timeout period (configured using the <code>CAMBIUM_POP_UNREACHABLE_REBOOT_TIMEOUT_INTERVAL</code> parameter), after which it reboots. Note: The <code>CAMBIUM_POP_UNREACHABLE_REBOOT_TIMEOUT_INTERVAL</code> parameter is available on the Configuration > Advanced page of the device UI.
Are there any impacts or disruptions to other active links in the same sector when the feature initiates a rescan process?	Yes. All the active links within the same sector goes down.
What are the prerequisites or requirements for the feature to work properly?	The DN Rescan feature does not require any specific prerequisites.
Can this feature be enabled or disabled on each DN or is it a global setting?	The DN Rescan feature can be enabled either at the node level or the network level. There are no restrictions.
Are there any caveats (cautions) when using the feature?	Yes. You must consider the following: <ul style="list-style-type: none"> 1. The DN will lose all its links and recovery will be slower, necessitating careful usage of this feature.

FAQ	Answer
	<ol style="list-style-type: none"> <li data-bbox="716 260 1409 380">2. If the channel is modified via the local GUI (for instance, to run Antenna Alignment), it is recommended to disable the feature first. Otherwise, the timeout might kick in and erase the set channel. <li data-bbox="716 415 1344 468">3. Scanning of CB1 and CB2 channels at a time is not supported.

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.

The **Node** configuration contains the following tabs:

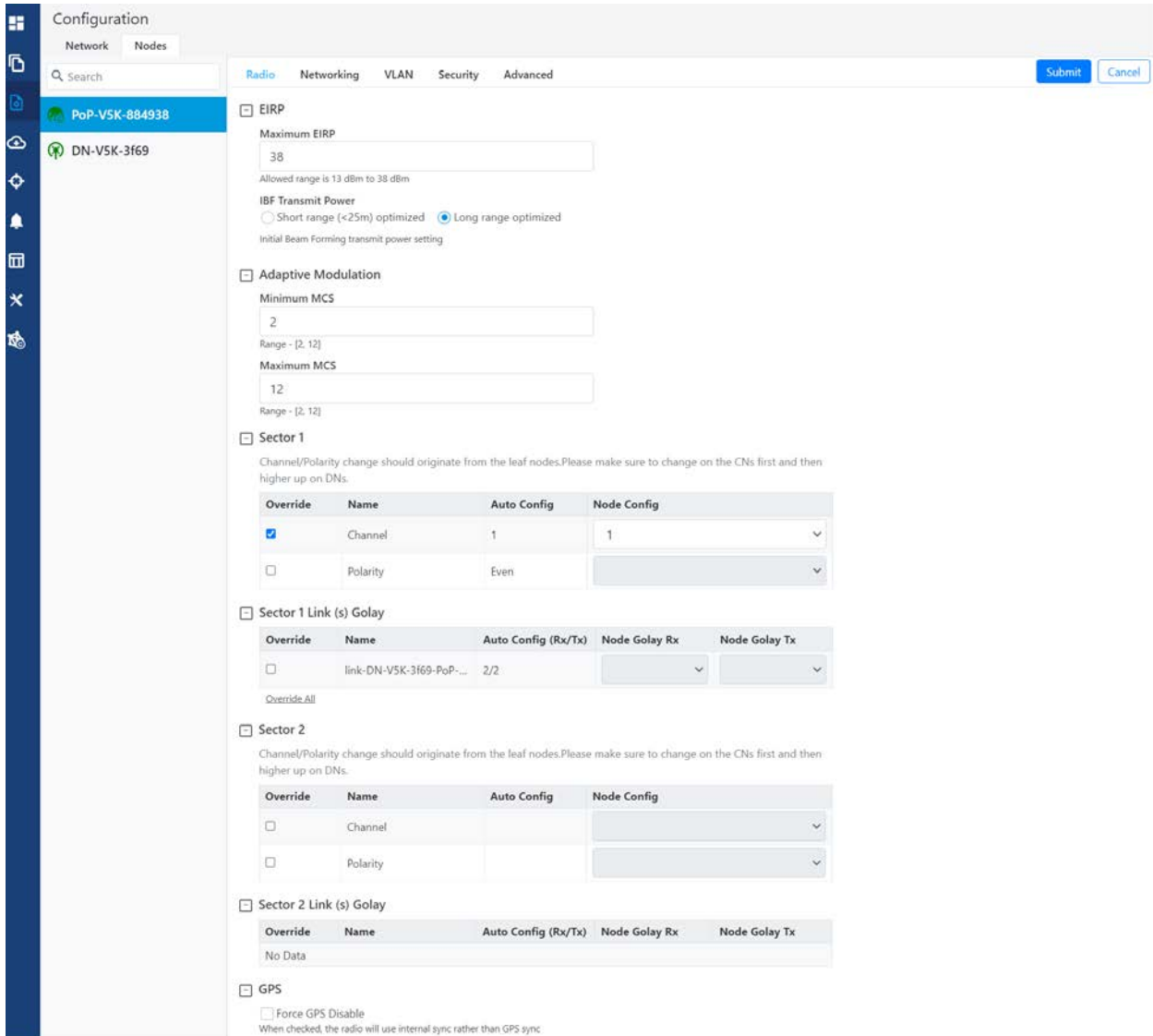
- [Radio](#)
- [Networking](#)
- [VLAN](#)
- [Security](#)
- [Advanced](#)

Radio

To configure the Radio page, navigate to **Nodes > Radio** page from the **Configuration** page.

The **Radio** page 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 177: The Radio page



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

Table 47: Elements in the Radio page

Elements	Description
EIRP	<p>Transmit power of the radio</p> <ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> Select the frequency channel and polarity. Channel and Polarity - When a 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	<p>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.</p> <div style="display: flex; align-items: center;">  <div style="border: 1px solid black; background-color: #e6f2ff; padding: 5px;"> <p>Note Golay codes and frequency on both ends of the link should match.</p> </div> </div>
Sector 2	Select the frequency channel and polarity.
Sector 2 Link (s) Golay	Golay code.
GPS	If enabled, the radio uses internal sync rather than GPS sync. In some scenarios like lab setups, it may be necessary to disable GPS.



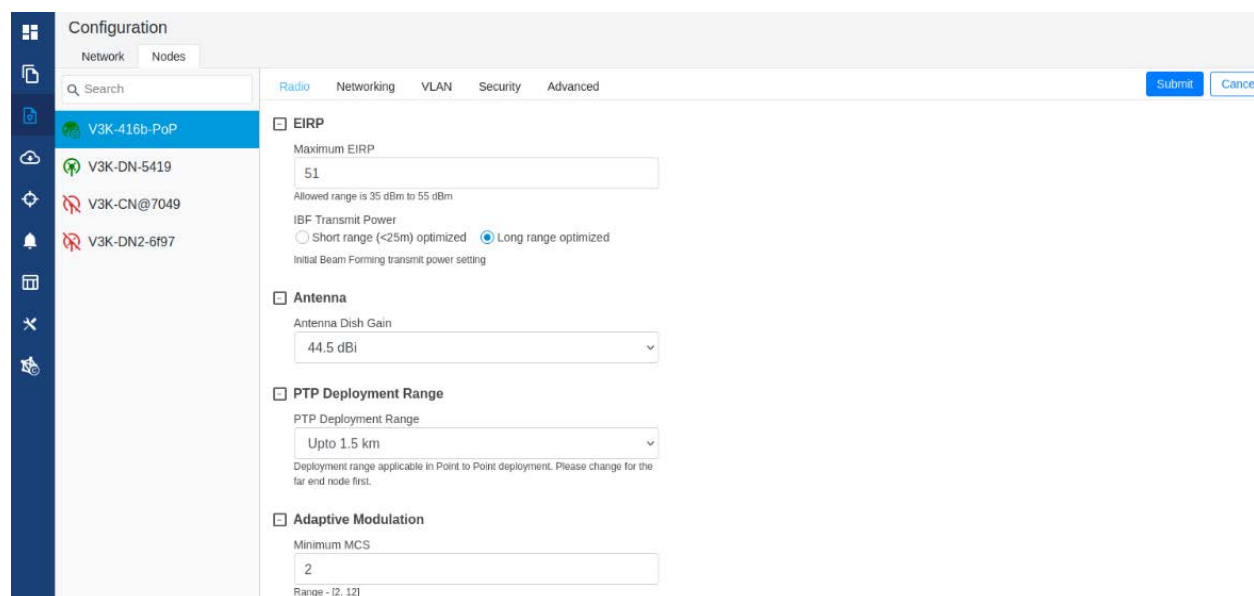
Caution

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 178: The Antenna section



Caution

Small dish is supported only for 60 GHz cnWave V3000.

Networking

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 179: The IPv4 Management section in the Networking page

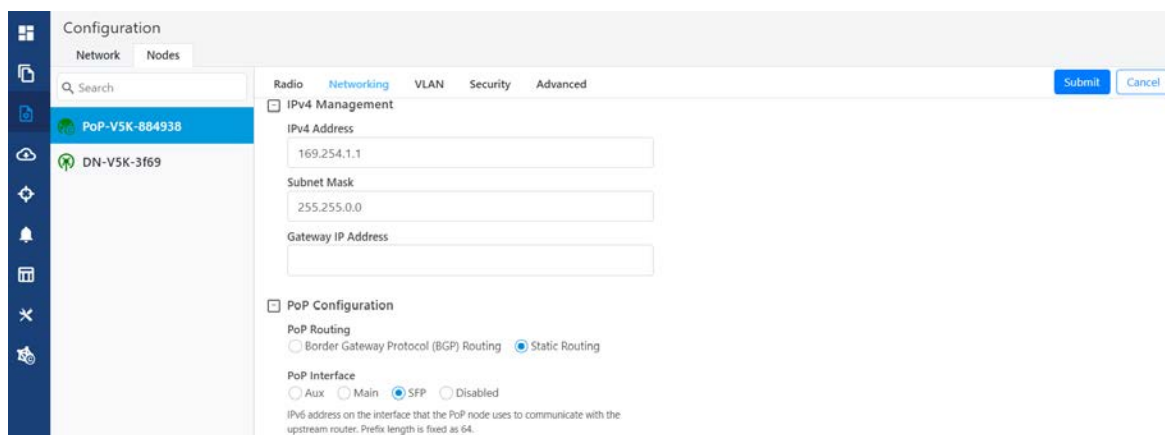


Table 48: Elements in the IPv4 Management section

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.

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

Figure 180: The PoP Configuration section in the Networking page

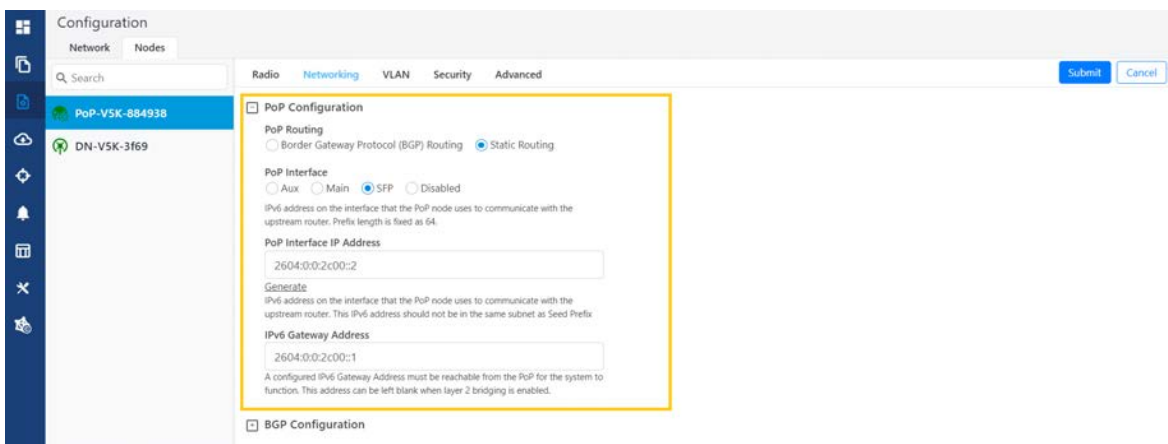


Table 49: Elements in the PoP Configuration section

Elements	Description
PoP Routing	<p>PoP nodes connect to the upstream IPv6 router in one of two ways:</p> <ul style="list-style-type: none"> • 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. <p>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.</p>
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.

- 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 50: 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.

- Select the required BGP configuration.

Figure 181: The BGP Configuration section

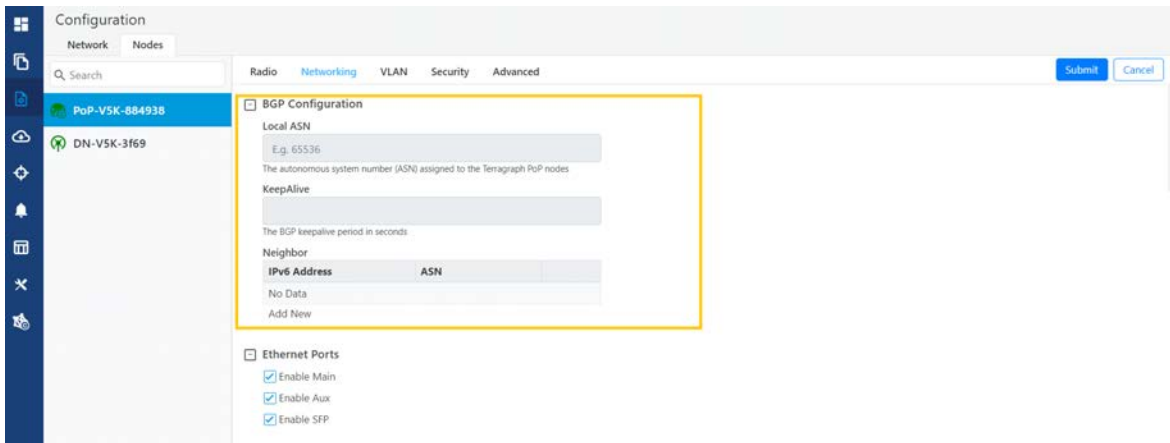
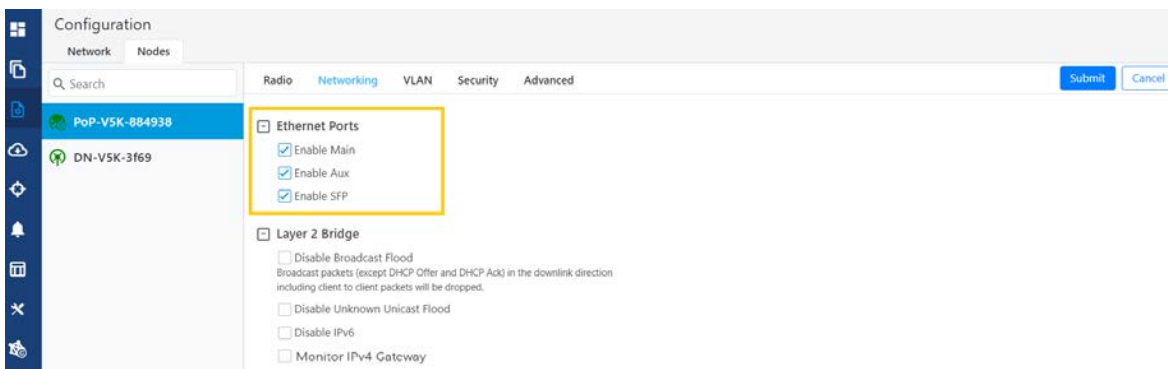


Table 51: Elements in the BGP Configuration section

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 182: 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 L2 GRE tunnels. When the option is enabled, PoP drops such packets.

Figure 183: The Layer 2 Bridge section in the Networking page

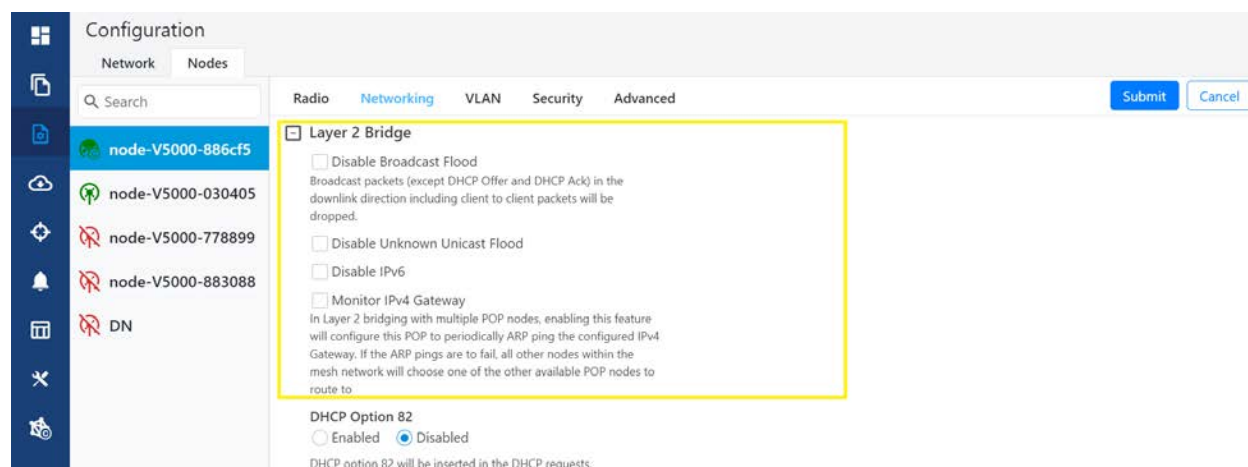


Table 52: Elements in the Layer 2 Bridge section

Elements	Description
Layer 2 Bridge	<p>It has three options:</p> <ul style="list-style-type: none"> • Disable Broadcast Flood • Disable Unknown Unicast Flood • Disable IPv6 • Monitor IPv4 Gateway <p>For information on Monitor IPv4 Gateway, refer to Configuring Monitor IPv4 Gateway,</p>
Aux PoE	<p>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.</p>
Multi-PoP / Relay Port	<p>Indicates the wired interfaces (or Ethernet) on which OpenR is running. This element must be used:</p> <ul style="list-style-type: none"> • 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 <p>Following options are supported:</p> <ul style="list-style-type: none"> • Aux • Main • SFP • Disabled

Enabling the DHCP Option 82 feature

When the **DHCP Option 82** feature is enabled, 60 GHz cnWave intercepts DHCPv4 REQUEST and DISCOVER packets and inserts option 82 fields.



Note
This feature is supported in the L2 bridge mode.

In addition, you can also configure **Circuit ID** and **Remote ID** fields. Use the following wildcards to configure **Circuit ID** and **Remote ID** fields:

- \$nodeMac\$ - MAC address of the node in ASCII format without colons. This is a default option.
- \$nodeName\$ - Topology name of the node.
- \$siteName\$ - Name of the site.
- \$networkName\$ - Network name as shown in cnMaestro.

Multiple wildcards can be combined with a : delimiter. The total length of the option (after replacing wildcards with corresponding values) is truncated to 120 characters. You can also configure a custom string, which must not start with a \$ character. For example, a customer's phone number.



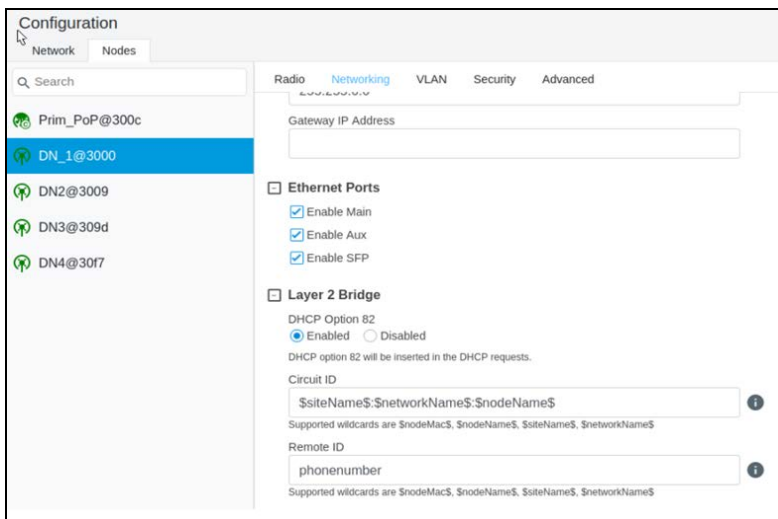
Note
You cannot use the customized string and predefined wildcards together as a single sub option (Circuit ID / Remote ID).

To enable the **DHCP Option 82** feature, perform the following steps:

1. Navigate to **Nodes > Networking** from the home page.

The **Networking** page appears. The **DHCP Option 82** feature is available in the Layer 2 Bridge section, as shown in [Figure 184](#).

Figure 184: The DHCP Option 82 feature



The enabled status of **DHCP Option 82** implies that the feature is activated.

2. Type appropriate values in **Circuit ID** and **Remote ID** text boxes.
3. To save the configuration, click **Submit**.

Configuring Monitor IPV4 Gateway

The **Monitor IPV4 Gateway** parameter is applicable when static routing and Layer 2 bridge are enabled in the device UI.

When you enable this parameter using the device UI, the IPv4 gateway is monitored. In Layer 2 bridging with multiple PoP nodes, this parameter (when enabled) configures the PoP to periodically ARP ping the configured IPv4 gateway. If the ARP ping fails for consecutive 12 seconds, all the other nodes (within the mesh network) choose one of the other available PoP nodes to route.

The **Monitor IPV4 Gateway** configuration results in failover of Layer 2 tunnels to next best PoP when the PoP cannot reach the IPv4 gateway. This configuration is applicable when static routing is used and IPv4 gateway is configured.

Before configuring the **Monitor IPv4 Gateway** parameter, perform the following configurations using the device UI:

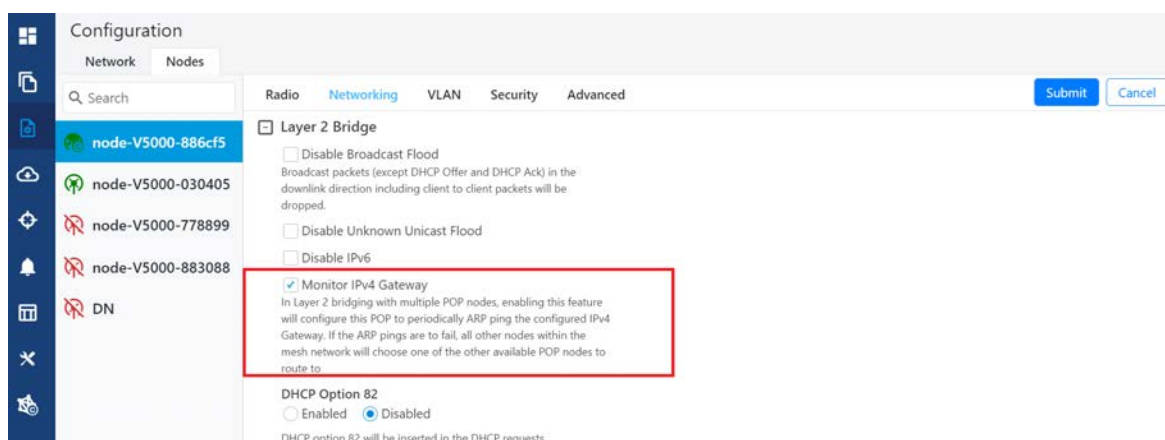
- Enable the **Layer 2 Bridge** parameter using the **Configuration > Network > Basic** page. This action enables Layer 2 network bridging (through automatically created tunnels) across all nodes connected to a PoP. This action also facilitates the bridging of IPv4 traffic across the wireless networks.
- Set the value of **PoP Configuration** parameter to Static Routing for the required PoP using the **Configuration > Nodes > Networking** page. This action results in failover of Layer 2 tunnels to next best PoP when the PoP cannot reach the IPv4 gateway. This configuration is applicable when static routing is used and IPv4 gateway is configured.

To enable and configure the **Monitor IPV4 Gateway** parameter, perform the following steps:

1. From the home page, navigate to **Configuration > Nodes > Networking**.

The **Networking** page appears. The **Monitor IPV4 Gateway** check box is available in the **Layer 2 Bridge** section, as shown in [Figure 185](#).

Figure 185: The Monitor IPV4 Gateway parameter

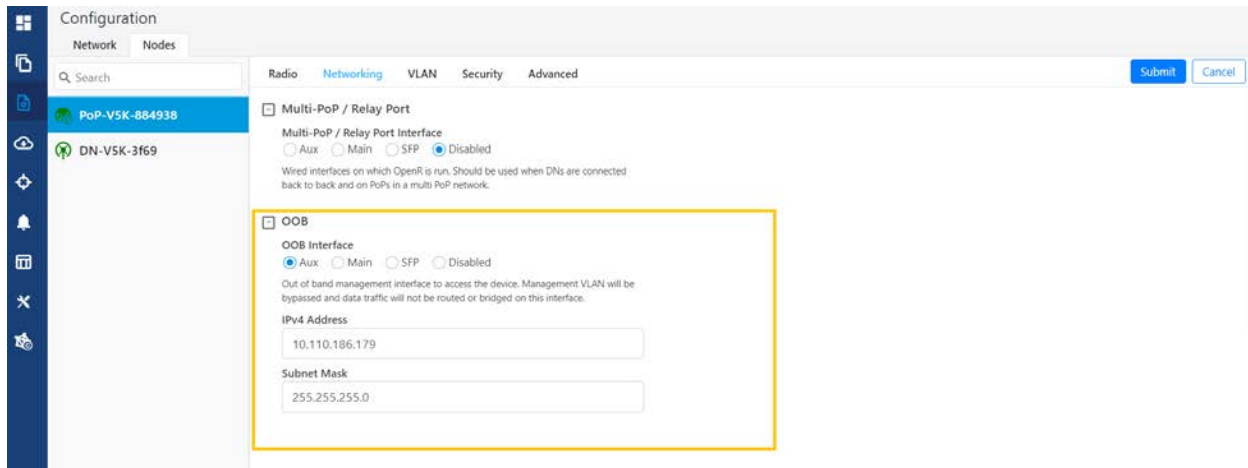


2. Select the **Monitor IPV4 Gateway** check box to enable the parameter.
3. Click **Submit** to save the changes.

Out of Band (OOB) interface

Out of band (OOB) management interface to access the device. Management VLAN is bypassed, and data traffic will not be routed or bridged on this interface. The OOB management interface is supported at PoP. A separate IPv4 address should be configured by bypassing the Management VLAN. Navigate to **Configuration > Nodes > Networking > OOB** and select the required option. Enter the IPv4 address and Subnet Mask to access the device.

Figure 186: The OCB section in the Networking page



PTP External failover

The **PTP External Failover** feature supports the failover of a 60 GHz cnWave RF link using external devices such as PTP450 and ePMP.



Note

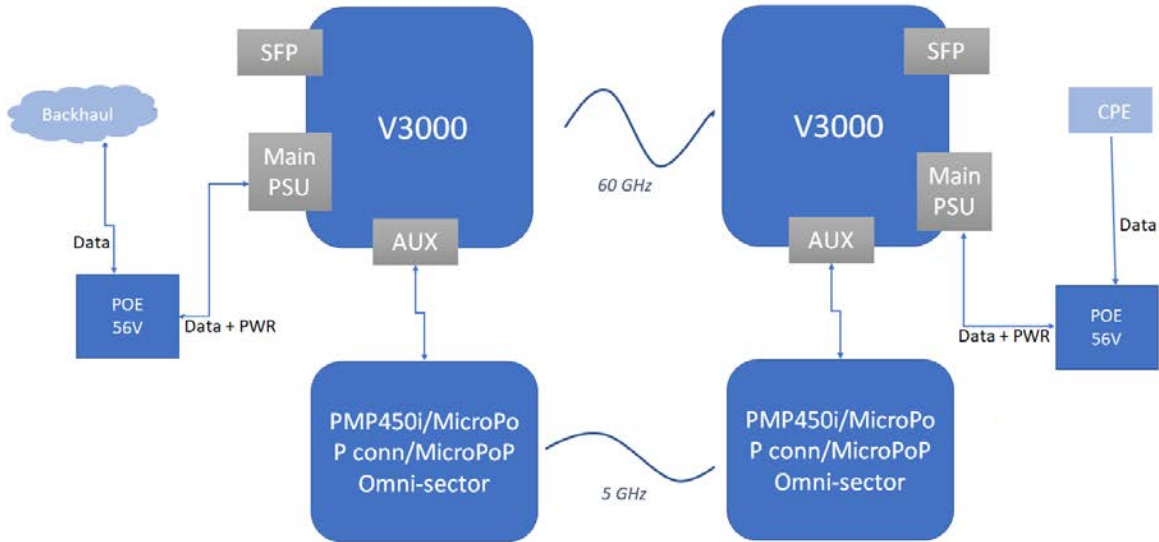
System Release 1.2.2 and later subsequent release versions support the external failover link feature for Point-to-Point (PTP) links. The external failover interface must not be same as PoP, Relay, or Out of Band (OOB) interface.

This feature does not support V1000 (which contains only one port).

Figure 187 shows how a 60 GHz cnWave PTP link is backed up with a PTP450 link. You can consider the 60 GHz link (as shown in Figure 187) as the primary link and 5 GHz link as the secondary link.

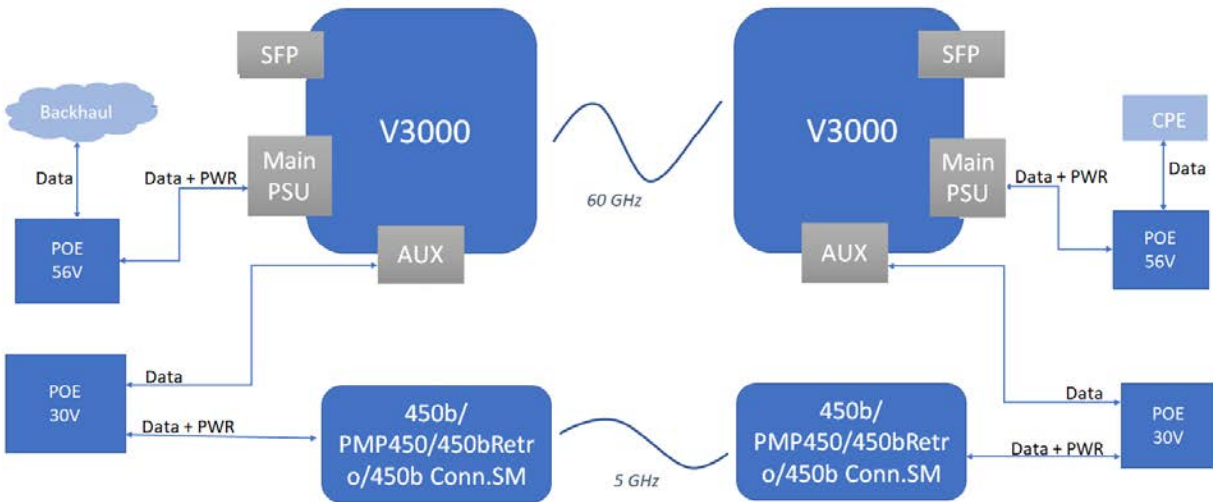
Figure 187: Backing up the 60 GHz cnWave PTP link

Scenario 1:



Note: Enable AUX PoE Power on V3000.

Scenario 2:



Note: Disable AUX PoE Power on V3000.

Whenever a 60 GHz link is up or active, traffic flows through the 60 GHz cnWave link. When the 60 GHz link is down, traffic fails over (shifts) to the 5 GHz link (PTP450). When the 60 GHz link is back (up), the traffic shifts instantly over to the 60 GHz cnWave link.

You can configure the external failover link feature using the [device UI](#) or the [cnMaestro UI](#).

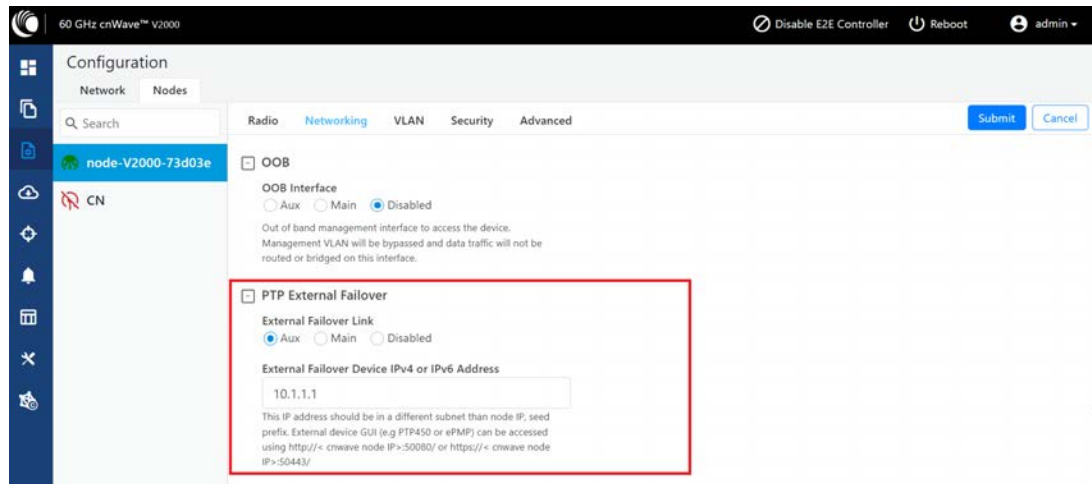
Using the device UI:

To enable and configure the external failover link feature using the device UI, perform the following steps:

1. From the home page of the device UI, navigate to the **Configuration > Nodes > Networking** page. The **Networking** page appears.
2. In the **PTP External Failover** section (as shown in [Figure 188](#)), set the following configurations:
 - a. To set the Ethernet interface for a node connected to external failover link, select either **Aux** or **Main** (Ethernet ports) from the **External Failover Link** parameter.

By default, the **Disabled** option is selected.

Figure 188: The PTP External Failover section in the device UI



- b. Enter either IPv4 or IPv6 address of the external failover device in the **External Failover Device IPv4 or IPv6 Address** text box.



Note

Ensure that IPv6 is enabled in the external failover device.

3. Click **Submit** to save the changes.

Using the cnMaestro UI

To configure the external failover link feature, add and manage the following configurations in the **Advanced** page of cnMaestro UI:

- **Ethernet interface for each node:** Configure the Ethernet interface in PoP and CN, which are connected to the failover link. You must select the Ethernet port to which the external device is connected. Open/R protocol runs on this interface.
- **External failover interface address (IP address):** An optional configuration that is required only if you want to access the AP or SM UI from upstream. You must configure the IP address of external devices (for example, PTP450 or ePMP). This IP address must be in a different subnet other than node IP address or seed prefix.

The IP address can be either IPv4 or IPv6. However, ensure that external failover devices have IPv6 enabled.

- **Remote external failover node address:** Configure the remote external failover node address. You can access the external failover device UI using `http://<cnwave node IP>:50080/` or `https://<cnwave node IP>:50443/`.

To configure the external failover link feature using the cnMaestro UI, perform the following steps:

1. From the dashboard page of the cnMaestro UI, navigate to the **Monitor and Manage > Networks > Configuration > Node > Advanced** page.

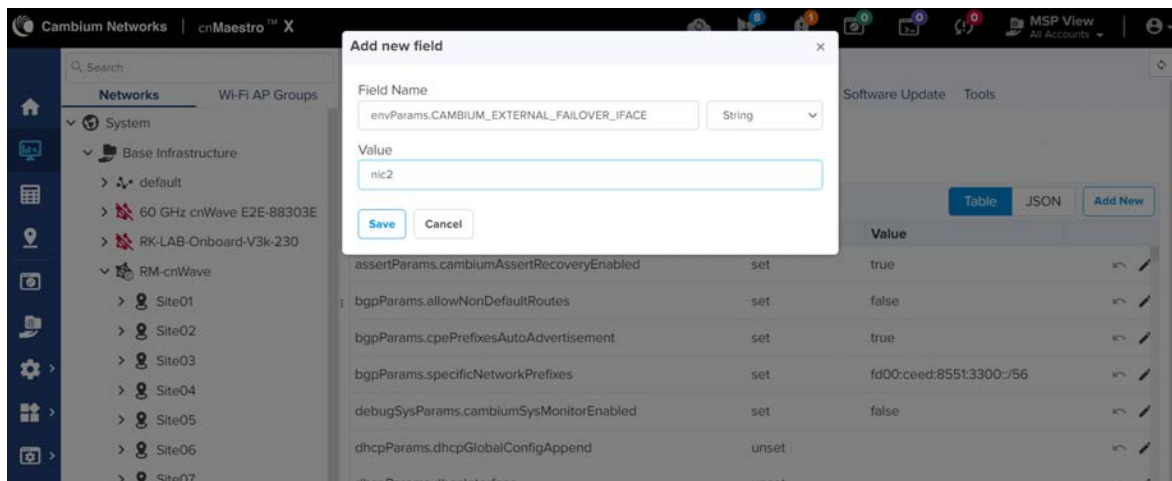
The **Advanced** page appears.

2. To add and manage the Ethernet interface for each node (PoP and CN), Click **Add New** located at the right side of the page.

The **Add new field** page appears.

3. In the **Field Name** text box, provide `envParams.CAMBIUM_EXTERNAL_FAILOVER_IFACE` (in String format) for each node, as shown in [Figure 189](#).

[Figure 189:](#) The Add new field page in the cnMaestro UI

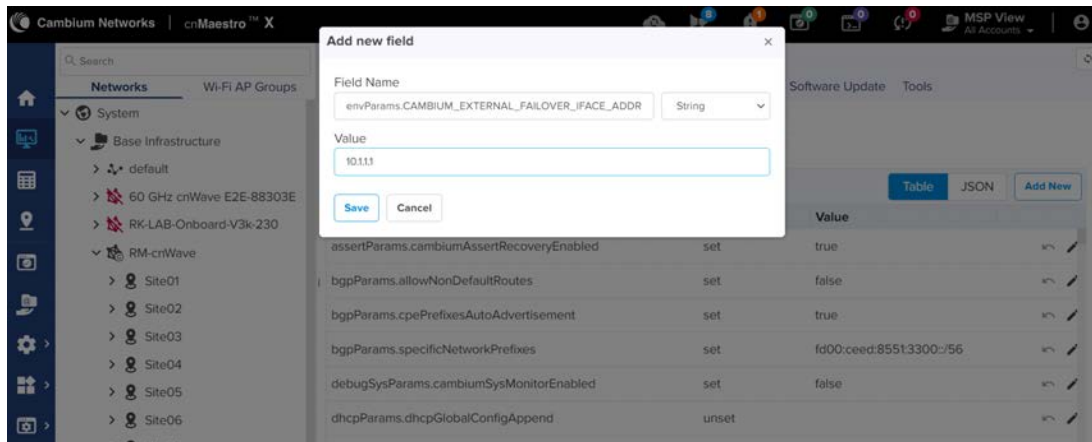


4. In the **Value** field, enter an appropriate value.
 5. Click **Save**.
- The **Advanced** page is updated the new entry that you added.
6. Click **Submit** located at the right side of the **Advanced** page.

Similarly, you must add and manage the following configurations, separately, using the **Add New** button on the **Advanced** page:

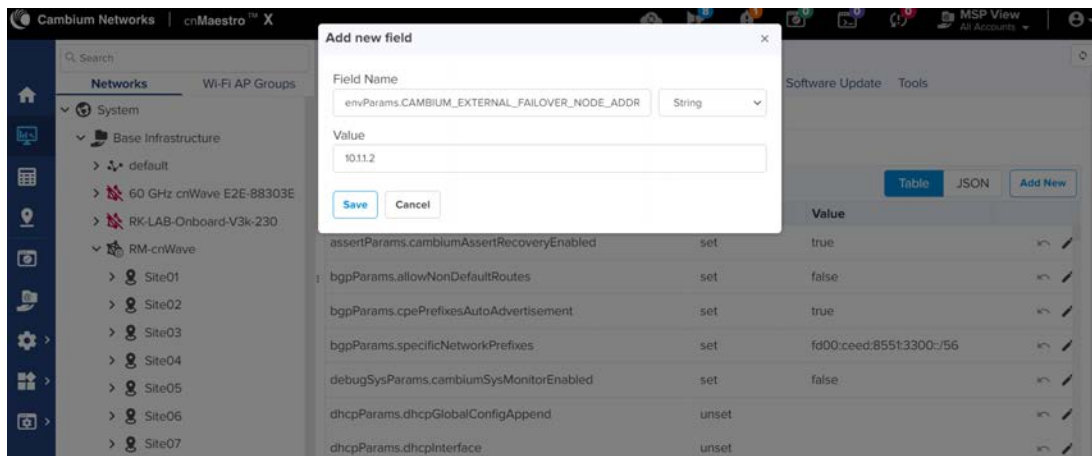
- For external failover interface address (IP address), provide `envParams.CAMBIUM_EXTERNAL_FAILOVER_IFACE_ADDR` (in String format) in the **Field Name** text box, as shown in [Figure 190](#).

Figure 190: Configuring the external failover interface address



- For remote external failover node address, provide `envParams.CAMBIUM_EXTERNAL_FAILOVER_NODE_ADDR` (in String format) in the **Field Name** text box, as shown in Figure 191.

Figure 191: Configuring the remote external failover node address



Then, you must ensure to provide an appropriate value in the **Value** text box for each configuration. Finally, you must save and submit each configuration.



Note

Following limitations are observed in this release specific to the external failover feature:

- There is no representation of an external failover link on the **Map** page.
- There are no statistics available on the external failover link.
- No other UI or cnMaestro used for configuring the external failover interface and address. This feature can be configured only through the **Configuration > Nodes > Advanced** page.

VLAN

Data VLAN

The following 802.1Q features are supported per port:

- Adding single VLAN tag to untagged packets
- Adding QinQ/double-tag to untagged packets
- Adding QinQ outer tag to single tagged packets
- Transparently bridge single/double-tagged packets (default behavior)
- Remarking VLAN ID
- Remarking 802.1p priority
- Option to allow only the selected range of VLAN IDs
- Option to drop untagged packets
- Option to drop single tagged packets
- Option to select the ethertype of the outer tag

These options are per Ethernet port.



Note

VLAN configuration is applicable only when Layer 2 bridge is enabled.

Port Type

Figure 192: The port types

Type
<input type="radio"/> Q
<input type="radio"/> QinQ
<input checked="" type="radio"/> Transparent

Transparent

By default, the Ethernet port is in transparent mode. Packets will be transparently bridged without any 802.1Q processing.

Q

Q mode allows adding a single C-VLAN tag to untagged packets.

Figure 193: Native VLAN ID and priority

The screenshot shows two input fields. The first is labeled "Native VLAN ID" and contains the value "23". Below it, the text "Allowed range is 1 - 4094" is displayed. The second field is labeled "Native VLAN Priority" and contains the value "2". Below it, the text "Allowed range is 0 - 7" is displayed.

Native VLAN ID and priority fields define the C-VLAN tag properties.

Figure 194: Allowed VLANs

The screenshot shows a single input field labeled "Allowed VLANs" containing the value "2". Below the field, the text "List of allowed VLANs. Comma separated, and/or range. e.g 100, 210-220. Filter based on outer tag." is displayed.

Allow only the listed range of VLAN IDs.

Figure 195: Untagged types

The screenshot shows a section titled "Untagged Packets" with two radio button options: "Allow" (which is unselected) and "Drop" (which is selected).

This option allows dropping untagged packets. Native VLAN properties are not necessary to fill when untagged packets are dropped.

QinQ

QinQ mode allows adding a double tag to untagged packets and outer S-VLAN to single-tagged packets.

Figure 196: Native C-VLAN ID and priority

The screenshot shows two input fields. The first is labeled "Native C-VLAN ID" and contains the value "23". Below it, the text "Allowed range is 1 - 4094" is displayed. The second field is labeled "Native C-VLAN Priority" and is currently empty. Below it, the text "Allowed range is 0 - 7" is displayed.

These are the C-VLAN tag properties of added tag.

Figure 197: Native S-VLAN ID and priority

Native S-VLAN ID

Allowed range is 1 - 4094

Native S-VLAN Priority

Allowed range is 0 - 7

These are the S-VLAN tag properties of the added outer tag.

Figure 198: Untagged and Single tagged packets

Untagged Packets

Allow Drop

Single Tagged Packets

Allow Drop

In QinQ mode, the above options allow dropping untagged/single-tagged ingress packets. Native C-VLAN fields are not necessary only when dropping single-tagged packets. Native S-VLAN fields are not necessary when dropping untagged and single tagged packets.

Figure 199: Allowed VLANs

Allowed VLANs

List of allowed VLANs. Comma separated, and/or range. e.g 100, 210-220. Filter based on outer tag.

Allow only the listed range of VLAN IDs. VLAN ID of the outer tag is used for this check.


Figure 200: QinQ EtherType

QinQ EtherType

EtherType indicates which protocol is encapsulated in the payload of an Ethernet Frame.

QinQ EtherType is used while adding an outer tag. There are no other checks for EtherType.

Figure 201: VLAN ID Remarking

VLAN Remarking		
Ingress VLAN	Remark VLAN	
10	100	 
Add New		



VLAN ID of the ingress packet is remarked. In the above example, if a packet with VLAN ID 10 enters an Ethernet port, it is remarked to 100. In the egress path, the reverse remarking occurs. VLAN ID 100 is remarked to 10 and egresses the ethernet port.

The VLAN ID of the outer tag is used for remarking. For a double-tagged packet, S-VLAN ID gets remarked and for a single-tagged packet, C-VLAN ID.

802.1p overriding

The Priority field in the (outer) VLAN tag of ingress packet can be overwritten using this option.

Figure 202: VLAN Priority Override

VLAN Priority Override		
Ingress VLAN	Override Priority	
20	7	 
Add New		

Management VLAN

A Single tag or double tag can be added to Management traffic.

Figure 203: The Management section

Management

Enabled Disabled

VLAN ID

Allowed range is 1 - 4094

VLAN Priority

Allowed range is 0 - 7

Add Outer Tag

S-VLAN ID

Allowed range is 1 - 4094

S-VLAN Priority

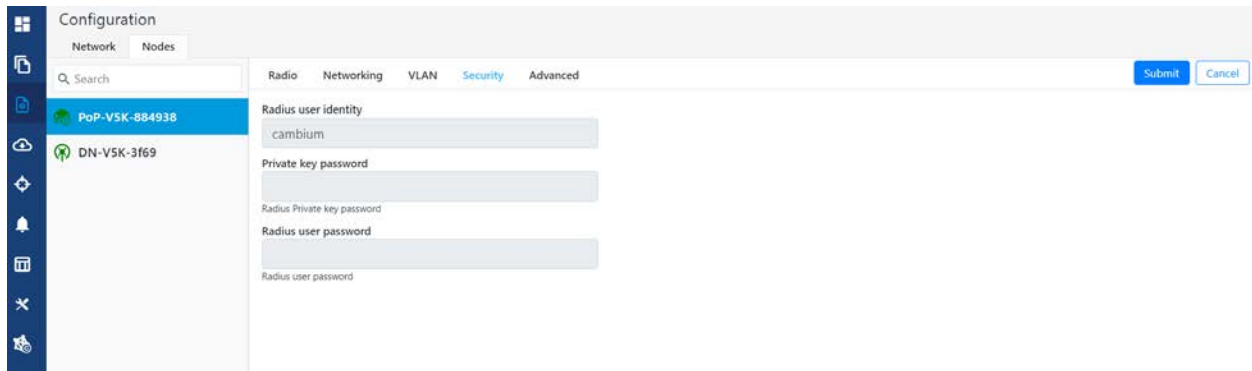
Allowed range is 0 - 7

Security

In the **Security** tab, enter **Private key password** and **Radius user password**.

- Private key password
- Radius user password

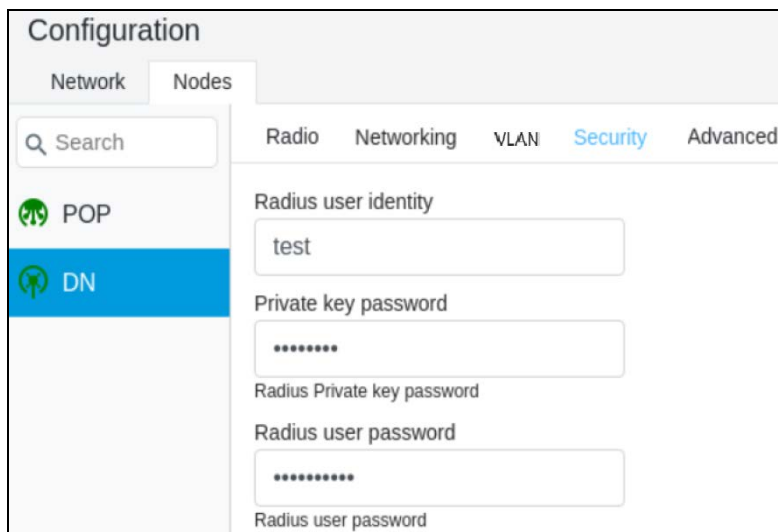
Figure 204: The Security page



Controller UI configuration

This Controller GUI configuration to be made on each DN.

Figure 205: Elements specific to Controller configuration



Node UI configuration

You can configure the **Security** page for a single node. The **Security** page is available on the single node UI.

Figure 206: Elements specific to node configuration

Private key password
••••••••

Radius Private key password

Radius server shared secret
••••••••

Radius user password

Radius user password

CA Certificate
ca.pem

Certificates sent by radius server are verified against this CA certificate

Client Certificate
client.pem

Private key with which client will encrypt

Client Private Key
client.key

Private key with which client will decrypt



Note
Both the configurations are important for a successful authentication.

RADIUS Server configuration

Any RADIUS server can be used for authentication. Perform the following steps to configure the RADIUS Server:

1. Ensure that RADIUS packets from IPv6 subnet (IP subnet) is accepted in RADIUS configuration.
2. Configure EAP-TLS for RADIUS Server and setup server certificate, key.



Note
Server certificate is signed by CA uploaded in node configuration.

3. Set the CA certificate which signed the client certificate installed on each node.

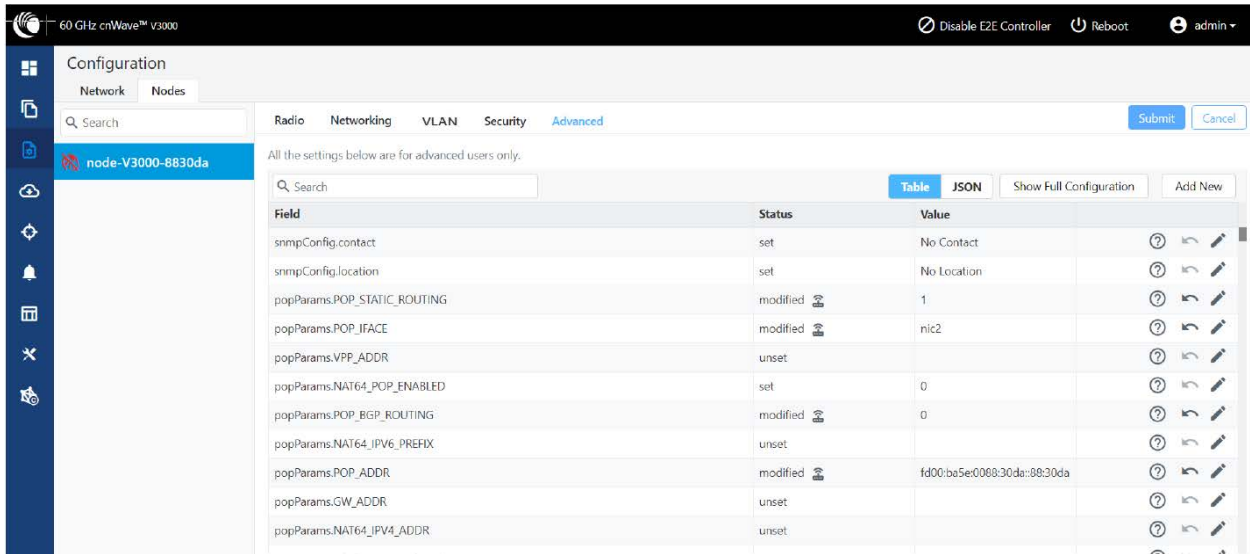
Advanced

These settings are for advanced users only.



Caution
Users are not recommended to do these settings.

Figure 207: The Advanced page - Node configuration



Configuration options under **Network > Advanced** and **Node > Advanced** are for advanced users who understand the cnWave configuration model well. It is not recommended to use these options. Shows the merged configuration from the Base layer to the Network override layer.

cnWave is based on Facebook's Terragraph architecture. It follows a layered configuration model, with a node's "full" configuration computed as the union of all layers in the following order:

- **Base configuration** - The default configuration, which is tied to a specific software version and is included as part of the image. The controller finds the closest match for a node's software version string and falls back to the latest if no match was found.
- **Firmware-specific base configuration** - The default configuration is tied to a specific firmware version, which is also included as part of the image. Values are applied on top of the initial base configuration layer.
- **Hardware-specific base configuration** - The default configuration is tied to a specific hardware type, which is also included as part of the image. Each hardware type supplies configuration that changes with software versions. Values are applied on top of the firmware-based configuration layer.
- **Automated node overrides** - Contains any configuration parameters for specific nodes that were automatically set by the E2E controller.
- **Network overrides** - Contains any configuration parameters that should be uniformly overridden across the entire network. This takes precedence over the base configuration and automatic overrides.
- **Node overrides** - Contains any configuration parameters that should be overridden only on specific nodes (e.g. PoP nodes). This takes precedence over the network overrides.

The E2E controller manages and stores the separate configuration layers. The cnWave nodes have no knowledge of these layers, except the base configuration on the image. The nodes copy the latest base version (via natural sort order) if the configuration file on disk is missing or corrupt.

Click **Submit** to apply the changes.

Operation

Software upgrade

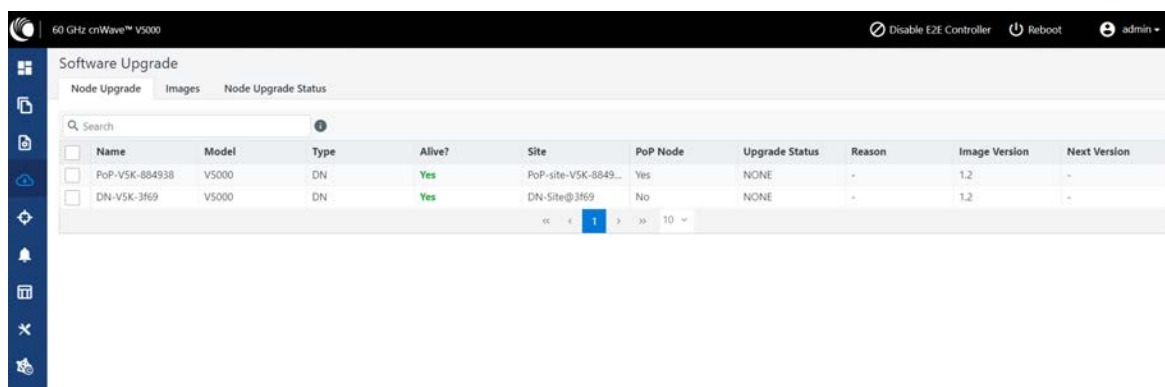
The **Software Upgrade** page is used to upgrade the installed software. This page contains the following three tabs:

- **Node Upgrade** - to upgrade the node
- **Images** - to upgrade the software images
- **Node Upgrade Status** - displays the upgrade status

To upgrade a node, perform the following steps:

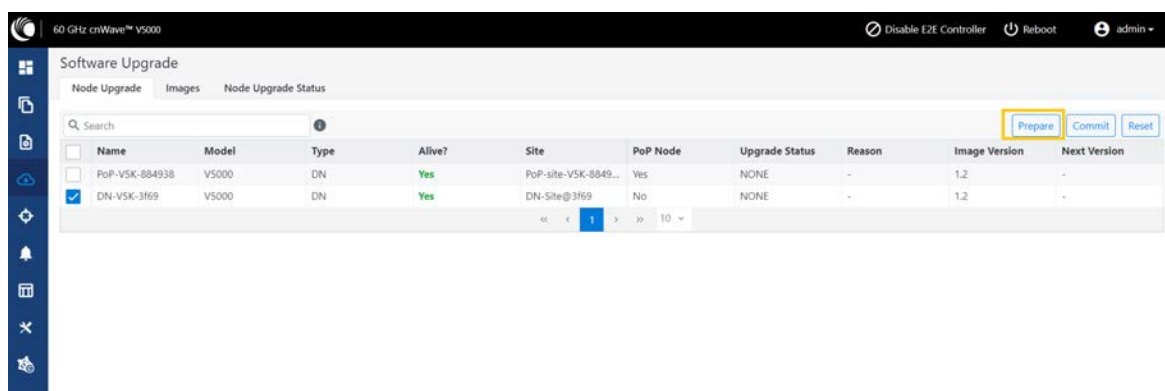
1. From the main dashboard page, click **Software upgrade** on the left navigation pane.

The **Software Upgrade** page appears, as shown below:



By default, the **Node Upgrade** tab is selected.

2. In the **Node Upgrade** page, select the required device for which you want to upgrade the node and click **Prepare** (as shown below).



The **Prepare Nodes** dialog box appears.

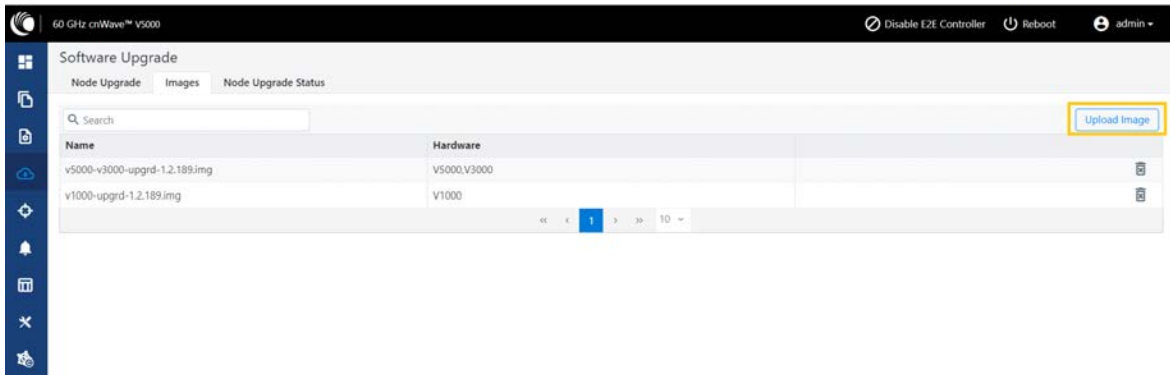
3. In the **Prepare Nodes** dialog box, select the required image file for the node and click **Save**.

You can also set additional options, if required, such as Upgrade Timeout, Download options, and Download Timeout.

4. Click **Commit** to upgrade the node.
5. To upgrade the software image, click on the **Images** tab in the **Software Upgrade** page.

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

Figure 208: The Images page



6. In the Images page, click **Upload Image**.

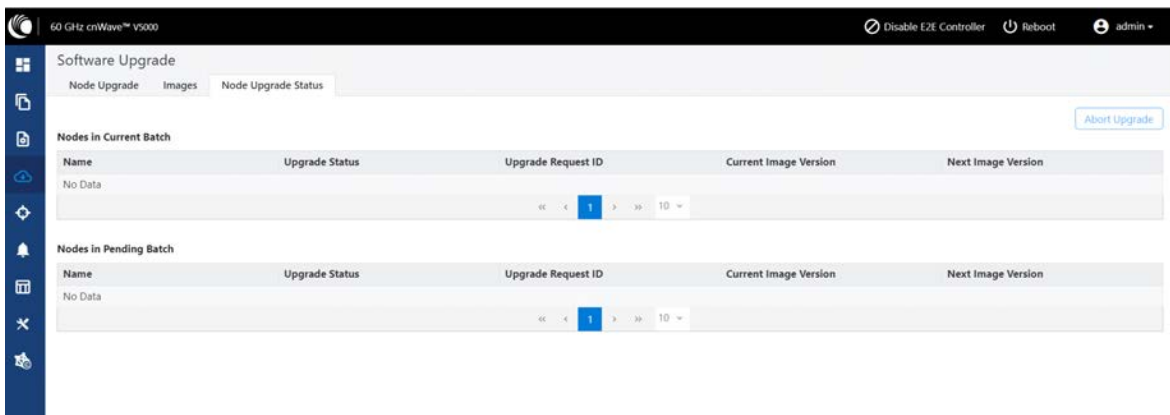
You must browse and select the required image file from your machine. Example: Software image or package (cnWave60-<release>.tar.gz). The selected image file gets uploaded.

You can also delete an existing image file in the **Images** page.

7. To view the node upgrade status, click on the **Node Upgrade Status** tab in the **Software Upgrade** page.

The **Node Upgrade Status** page appears, as shown below:

Figure 209: The Node Upgrade Status page



You can view the upgrade status for the required device nodes.

Diagnostics

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

- [Events](#)
- [DA Logs](#)
- [Engineering logs](#)

Events

The **Events** page displays the running and completed task list. These events can be exported. To export the event list, click **Export**.

Time	Level	Node Name	Event ID	Source	Reason
Sep 14, 2022, 6:28:26 AM	Info	v2k_cn	Scan resp	minion-app-DRIVER_APP	Received scan response View Details
Sep 14, 2022, 6:28:26 AM	Info	node-V3...	Scan resp	minion-app-DRIVER_APP	Received scan response View Details
Sep 14, 2022, 6:28:25 AM	Info	v2k_cn	Scan resp	minion-app-DRIVER_APP	Received scan response View Details
Sep 14, 2022, 6:28:25 AM	Info	node-V3...	Scan resp	minion-app-DRIVER_APP	Received scan response View Details
Sep 14, 2022, 6:28:24 AM	Info	v2k_cn	Driver link status	minion-app-IGNITION_APP	Received LINK_UP for neighbor 12:04:56:88:42:23 on interface terra0 (42:cb... View Details
Sep 14, 2022, 6:28:24 AM	Info	v2k_cn	Node info	minion-app-STATUS_APP	Minion is online View Details
Sep 14, 2022, 6:28:22 AM	Info	node-V3...	Link status	ctrl-app-TOPOLOGY_APP	link-node-V3000-884223-v2k_cn is UP View Details

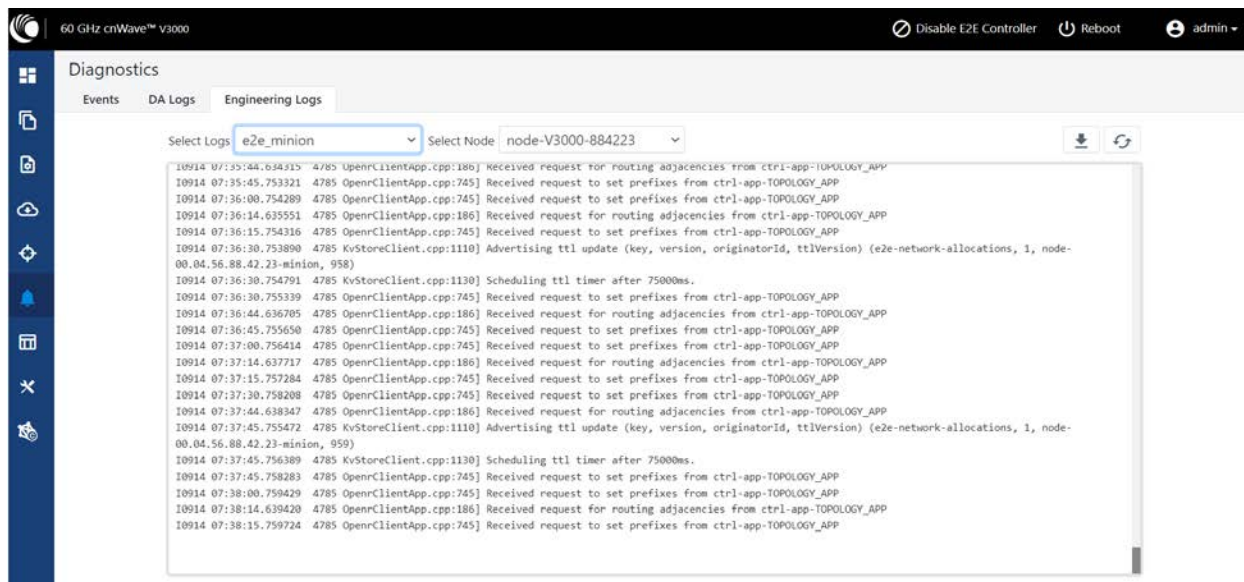
DA Logs

```

{"file": "e2e.go:210", "func": "e2e.(*E2E).Invoke", "level": "error", "msg": "Post `http://[::1]:8080/internal/local/getDeviceInfo`: dial tcp [::1]:8080: connect: connection refused", "name": "e2e", "time": "2022-09-13T11:36:09Z"}
{"file": "init.go:52", "func": "e2e.(*E2E).Init", "level": "error", "msg": "Post `http://[::1]:8080/internal/local/getDeviceInfo`: dial tcp [::1]:8080: connect: connection refused", "name": "e2e", "time": "2022-09-13T11:36:09Z"}
{"file": "init.go:206", "func": "agent.(*Agent).Init", "level": "error", "msg": "Unable to initialize the controller Error: Post `http://[::1]:8080/internal/local/getDeviceInfo`: dial tcp [::1]:8080: connect: connection refused", "name": "agent", "time": "2022-09-13T11:36:09Z"}
{"file": "main.go:118", "func": "main.main", "level": "info", "msg": "Will retry in sometime", "name": "main", "time": "2022-09-13T11:36:09Z"}
{"file": "main.go:102", "func": "main.main", "level": "info", "msg": "Configuration Loaded Successfully", "name": "main", "time": "2022-09-13T11:36:14Z"}
{"file": "e2e.go:824", "func": "e2e.(*E2E).GetSerialNo", "level": "info", "msg": "onboard e2e getDeviceInfo API (Type:POP Name:node-V3000-884223 Mac:00:04:56:88:42:23 Hsn:V5XC036Q2FDB Model:V3000)", "name": "e2e", "time": "2022-09-13T11:36:16Z"}
{"file": "conn.go:84", "func": "agent.(*Agent).routerConnect", "level": "info", "msg": "Connecting to router: https://10.110.186.92/cns-onboarding/device?&type=cnAgent&serialNo=V5XC036Q2FDB&mac=00:04:56:88:42:23&mode=e2e&deployment=onboard", "name": "agent", "time": "2022-09-13T11:36:16Z"}
{"file": "conn.go:85", "func": "agent.(*Agent).routerConnect", "level": "info", "msg": "User-agent header: cnDA/1.0 (e2e/1.2.2-dev185-1-gc604bc9e(W); DA/1.2.1-r8)", "name": "agent", "time": "2022-09-13T11:36:16Z"}
{"file": "conn.go:281", "func": "agent.(*Agent).connect", "level": "info", "msg": "Redirecting to Server: https://10.110.186.92/device", "name": "agent", "time": "2022-09-13T11:36:17Z"}
{"file": "e2e.go:930", "func": "e2e.(*E2E).GetMgtAddress", "level": "info", "msg": "onboard e2e minionConfigGet API (PopParams:(PopAddr:fd00:ba5e:0088:4223:188:4223 GwAddr:)) EnvParams:(MgtIPv4Addr:169.254.1.1)", "name": "e2e", "time": "2022-09-13T11:36:17Z"}
{"file": "conn.go:188", "func": "agent.(*Agent).serverConnect", "level": "info", "msg": "Connecting to Server: wss://10.110.186.92/device?deviceId=hv1XiborFXAcYbFFyKjHfYkVfsv7dEIVWgiuKAZisFist_H4V5d50uTxTPeuf403fzmkch8XrmR28DTu&type=cnAgent&serialNo=V5XC036Q2FDB&mac=00:04:56:88:42:23&mode=e2e&deployment=onboard", "name": "agent", "time": "2022-09-13T11:36:17Z"}
{"file": "msg_handler.go:211", "func": "agent.(*Agent).msgHandlerManaged", "level": "warning", "msg": "cnMaestro (1663068978) and agent(1663069097) time are not in sync", "name": "agent", "time": "2022-09-13T11:36:18Z"}

```

Engineering logs



Statistics

The **Statistics** menu contains the following options:

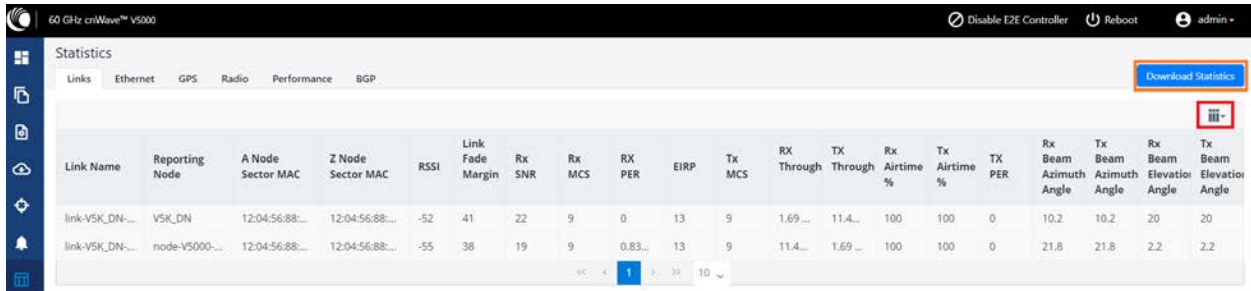
- [Links](#)
- [Ethernet](#)
- [GPS](#)
- [Radio](#)
- [Performance](#)
- [Prefix Zone Statistics](#)
- [Border Gateway Protocol \(BGP\)](#)

Links

The **Links** page contains Uplink and Downlink statistical data. It displays TX and RX data of the reporting nodes from A to Z and Z to A. The page also displays statistics (for example, Rx/Tx Throughput and Rx/Tx Airtime %) that provide the necessary insights to manage and optimize cnWave networks effectively.

Based on the filters that you select using the  icon (as shown in [Figure 210](#)), the **Links** page displays the relevant elements and statistics.

Figure 210: The Links page



The **Links** page displays the following elements:

Table 53: Elements in the Links page

Element	Description
Link Name	Link name
Reporting Node	Name of the reporting node for which the statistics are available.
A Node Sector MAC	MAC address of the initiator node.
Z Node Sector MAC	MAC address of the responder node.
RSSI	The Receiver Signal Strength Indicator (RSSI) value
Link Fade Margin	<p>The statistic value (in dB) available for each RF link</p> <p>The Link Fade Margin statistic values help operators to quickly assess any additional system gain or low marginal RF links (if any), which must be addressed.</p> <p>The Link Fade Margin statistic value calculation is based on:</p> <ul style="list-style-type: none"> • Checking the RSSI received from a remote transmitter, • Assessing the availability of TX power (from the remote transmitter), and • Considering the RSSI value that is calculated based on how far away it is from an established receiver sensitively floor of -72 dBm.
Rx SNR	Signal to Noise Ratio
Rx MCS	Modulation Code Scheme of Receiver
RX PER	Receiver packer error rate
TX Power Index	Transmitter power index
EIRP	The Effective Isotropic Radiated Power (EIRP) value.
Tx MCS	Modulation Code Scheme of Transmitter
Tx PER	Transmitter packer error rate

Element	Description
RX Errors	Receiver errors
RX Frames	Receiver frames
TX Errors	Transmitter errors
TX Frames	Transmitter frames
Rx Throughput	The receive throughput as received by the reporting node.
Tx Throughput	The throughput transmitted by the reporting node. Monitoring of this metric can clarify the data transmission rate, providing a clearer view of the network's outbound data performance.
Rx Airtime %	The percentage of airtime allocated by the scheduler to each link in the Rx direction from the perspective of reporting node. This metric is relevant for a DN as it indicates how airtime is shared across multiple links.
Tx Airtime %	The percentage of airtime allocated by the scheduler to each link in the Tx direction from the perspective of reporting node. Similar to Rx Airtime % , this metric provides insights into how airtime is distributed among links when transmitting data. This metric is only relevant for a DN.
Following replace Rx Scan Beams and Tx Scan Beam elements:	
Rx Beam Azimuth Angle	The angle of the selected fixed beam (in degrees) in the azimuth direction for each link. The selected beam is independent of transmit and receive directions. For more information on Tx/Rx azimuth beam angle statistics, refer to the Link diagnostics - Beam angle statistics section.
Tx Beam Azimuth Angle	
Tx Beam Elevation Angle	The angle of the selected fixed beam (in degrees) in the elevation direction for each link. The selected beam is independent of transmit and receive directions. For more information on Tx/Rx azimuth beam angle statistics, refer to the Link diagnostics - Beam angle statistics section.
Rx Beam Elevation Angle	

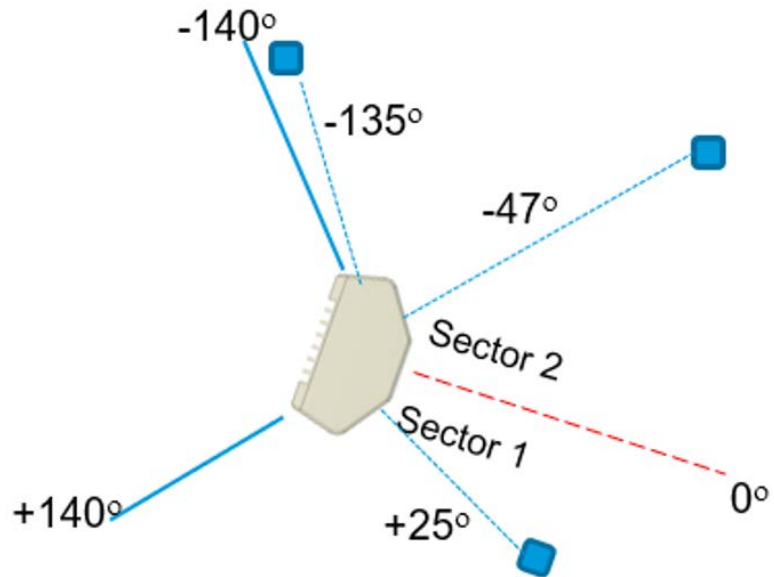
To download the statistics in .xls format, click **Download Statistics**.

Link diagnostics - Beam angle statistics

To understand about Tx/Rx azimuth and elevation beam angle statistics, let's consider the following examples:

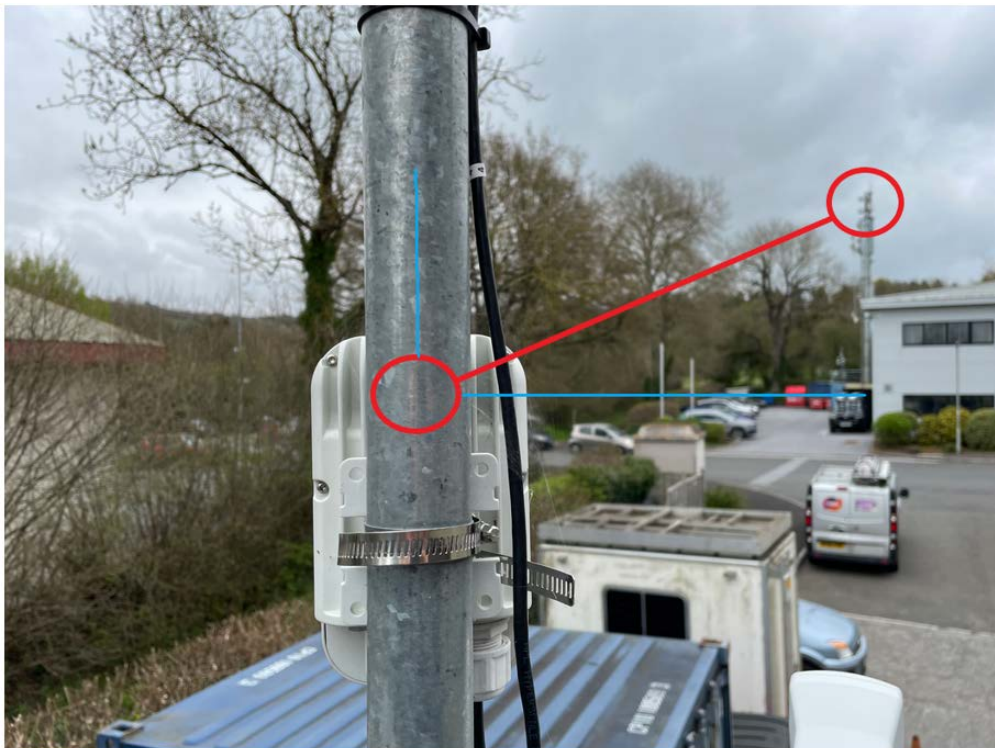
- In [Figure 211](#), the reported beam angle is relative to the reporting nodes boresight and not a bearing from North. Therefore, an **elevation angle** of +5 degrees is from the unit's perspective, choosing a fixed beam pointing of 5 degrees above the horizontal axis (towards the sky). An **azimuth angle** of +5 degrees is from the centre line or boresight of the unit with 5 degrees counting clockwise. An azimuth angle of -5 degrees is from the centre line or boresight of the unit with 5 degrees counting anti-clockwise.

Figure 211: An example of V5000 azimuth angles relative to boresight



- In Figure 212, a V1000 has been pole mounted with 0 degrees elevation tilt and is pointing approximately 20-30 degrees to the left of the target node (which is located on the tower, as shown in Figure 212). The location of the remote node is at the top of the cell tower so therefore has a higher elevation.

Figure 212: An example of V1000 installation



From V1000 CN's perspective, the reported beam angles are as follows:

- Tx Beam Azimuth Angle: +25.2 degrees
- Rx Beam Azimuth Angle: +25.2 degrees
- Tx Beam Elevation Angle: +14.3 degrees
- Rx Beam Elevation Angle: +14.3 degrees

Table 54 lists the fixed beam scan ranges for 60 GHz cnWave products.

Table 54: Fixed beam scan ranges

Product	Azimuth scan range	Elevation scan range
V1000	-45 degrees to +45 degrees	- 20 degrees to +20 degrees
V2000	-12 degrees to +12 degrees	-6 degrees to +4 degrees
V3000	-2.3 degrees to +2.3 degrees	-2 degrees to +1 degrees
V5000 (both sectors combined)	-140 degrees to +140 degrees	- 20 degrees to +20 degrees

The Tx/Rx x/Rx beam azimuth and elevation angle statistic help in:

- identifying links, which are operating near the boundary of the scan range, for example, within 5 degrees of +/- 140 degrees on a V5000. This implies that the link can be aligned off the edge of the sector and possibly requires the realignment.
- analysing whether interference affects the beam selection -
 - when the physical node alignment matches LINKPlanner but the beam angles are significantly out from what is predicted, and/or
 - when there is considerable variability in the beam angles used from linkup to linkup.
- determining whether signal obstruction, signal multipath, or interference causes an issue when there is a significant difference between the Tx and Rx beam angle for the same link at the same node.
- On a CN with only one wireless link to align, aiming at an azimuth beam angle close to 0 degrees is optimal.

Ethernet

The **Ethernet** page displays Transmitting and receiving data of the nodes.

Figure 213: The Ethernet page

Device Name	Device Model	Status	RX Packets	TX Packets	RX Bytes	TX Bytes	RX Errors	TX Errors	RX Dropped	TX Dropped	RX PPS	TX PPS	RX Throughput	TX Throughput
DN2@Po...	V5000	Down	0	0	0	0	0	0	0	0	0	0	0 kbps	0 kbps
Prim-PoP...	V5000	Down	0	0	0	0	0	0	0	0	0	0	0 kbps	0 kbps
DN1@Po...	V5000	10000 M...	1847	224256	86636	34573546	0	0	0	0	0	0	0 kbps	0 kbps
DN3@Po...	V5000	Down	0	0	0	0	0	0	0	0	0	0	0 kbps	0 kbps
DN4@Po...	V3000	Down	0	0	0	0	0	0	0	0	0	0	0 kbps	0 kbps

The following elements are displayed in the **Ethernet** page:

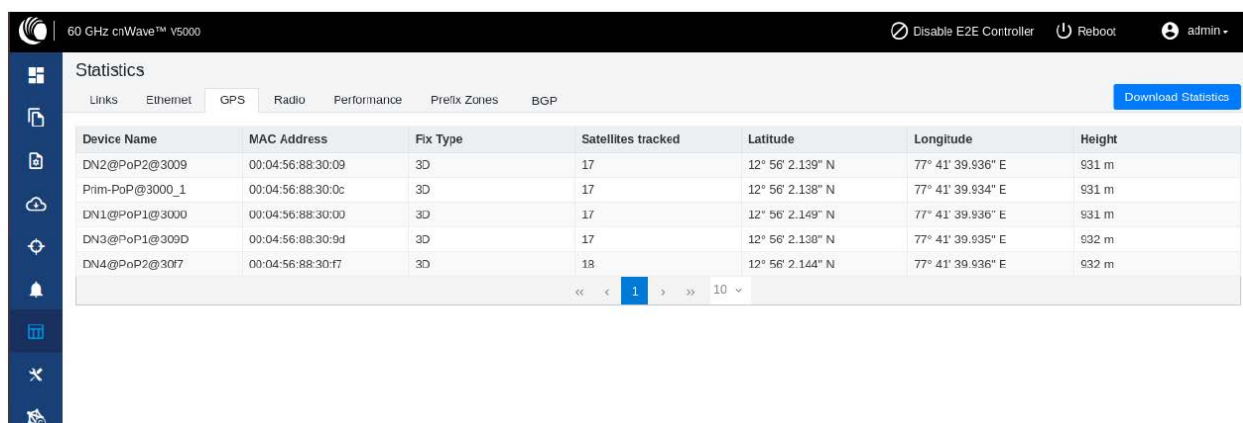
Table 55: Elements in the Ethernet page

Elements	Description
Device Name	Name of the device
Status	Ethernet link status
RX Packets	Receiver packets
TX Packets	Transmitter packets
RX Bytes	Receiver bytes
TX Bytes	Transmitter bytes
RX Errors	Receiver errors
TX Errors	Transmitter errors
RX Dropped	Receiver dropped
TX Dropped	Transmitter dropped
RX PPS	Receiver Packets Per Second
TX PPS	Transmitter Packets Per Second
RX Throughput	Receiver throughput
TX Throughput	Transmitter throughput

GPS

The **GPS** page displays geographical data of the nodes.

Figure 214: The GPS page



The following elements are displayed in the **GPS** page:

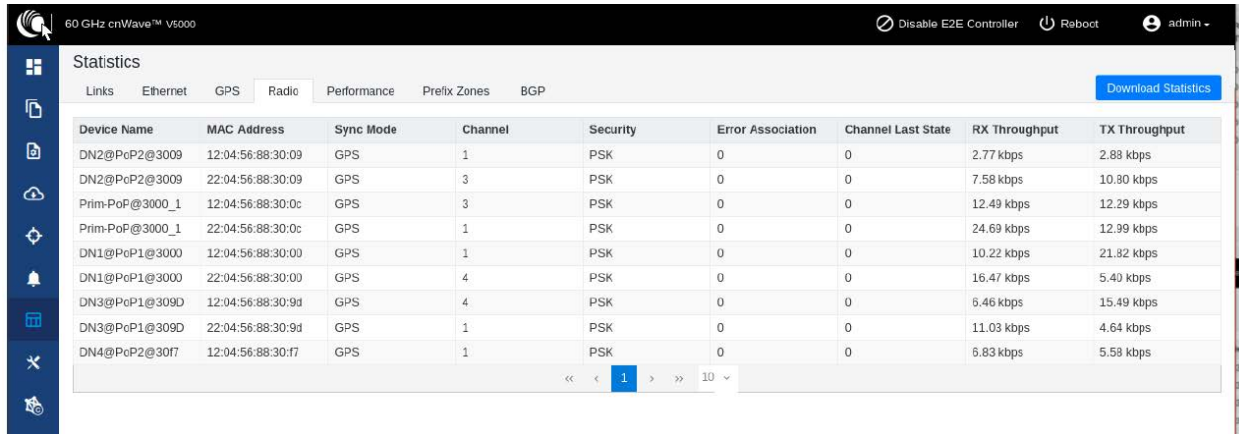
Table 56: Elements in the GPS page

Elements	Description
Device Name	Name of the device
MAC Address	MAC address of the device
Fix Type	GPS fix type. The fix status indicates the type of signal or technique being used by the GPS receiver to determine its location. The fix status is important for the GPS consumer, as it indicates the quality of the signal, or the accuracy and reliability of the location being reported.
Satellites tracked	The number of satellites tracked
Latitude	Latitude of the device
Longitude	Longitude of the device
Height	Height of the device

Radio

The **Radio** page displays the radio data of the nodes.

Figure 215: The Radio page



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

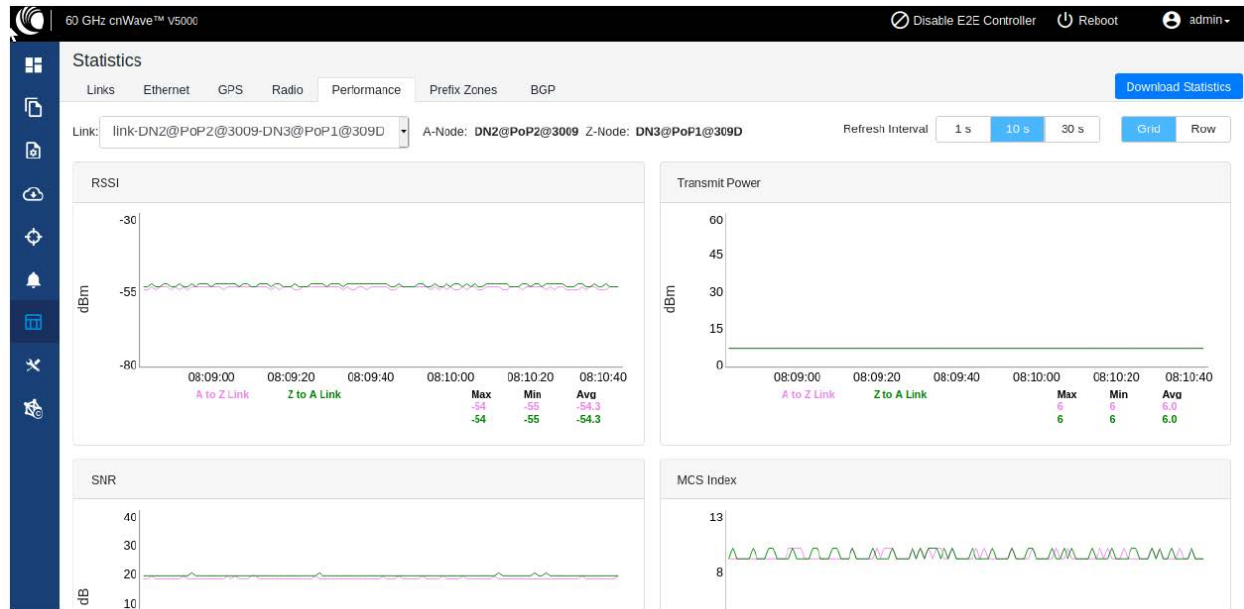
Table 57: Elements in the Radio page

Elements	Description
Device Name	Name of the device
MAC Address	MAC address of the device
Sync Mode	<ul style="list-style-type: none"> GPS sync: <ul style="list-style-type: none"> <i>Entry condition:</i> Valid samples from GPS have been received for a few consecutive seconds (typically 2 seconds). <i>Exit condition:</i> Valid samples from GPS have not been received for a few consecutive seconds (typically 10 seconds). RF sync: Not in “GPS sync”, but is reachable to a DN with “GPS sync” over wireless links (1-2 hops away). <ul style="list-style-type: none"> <i>Entry condition:</i> Conditions for “GPS sync” have not been met, but a link exists to at least one other DN from which to derive timing. <i>Exit condition:</i> Conditions for “GPS sync” have not been met and no links to other DNs exist from which to derive timing. No sync: Neither in GPS sync nor RF sync. This is the default state. <ul style="list-style-type: none"> <i>Entry condition:</i> Conditions for “GPS sync” or “RF sync” are not met. <i>Exit condition:</i> Condition for “GPS sync” or “RF sync” are met.
Channel	Operating channel
Security	Security type
Error Association	Error Association
Channel Last State	Channel Last State
RX Throughput	Receiver throughput
TX Throughput	Transmitter throughput

Performance

The **Performance** page displays the performance graph.

Figure 216: The Performance page



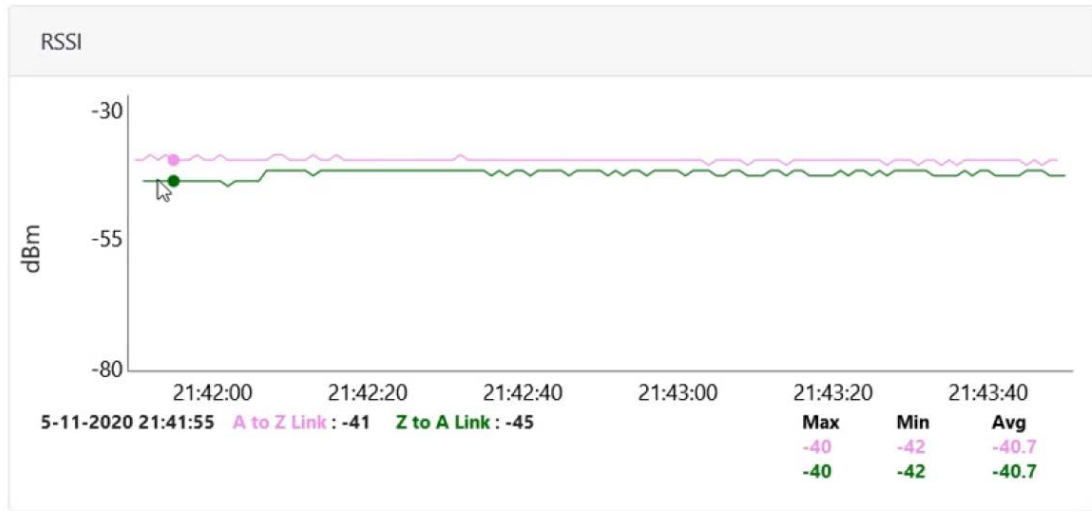
The **Performance** page contains the following graphs:

Table 58: Elements in the Performance page

Elements	Description
RSSI	Receiver Signal Strength Indicator. It is a measurement of the power present in a received radio signal
Transmit Power	Transmitting power
SNR	Signal to Noise Ratio
MCS Index	Modulation and Coding Scheme (MCS) Index Values can be used to determine the likely data rate of your wireless connection. The MCS value essentially summarizes the number of spatial streams, the modulation type and the coding rate that is possible when connecting your wireless access point.
Packet Error Ratio	Packet error ratio. It is the ratio, in percent, of the number of Test Packets not successfully received by the node to the number of Test Packets sent to the node by the test set.
Received Frames	The number of frames received at the node.
Transferred Frames	The number of frames transferred from the node.

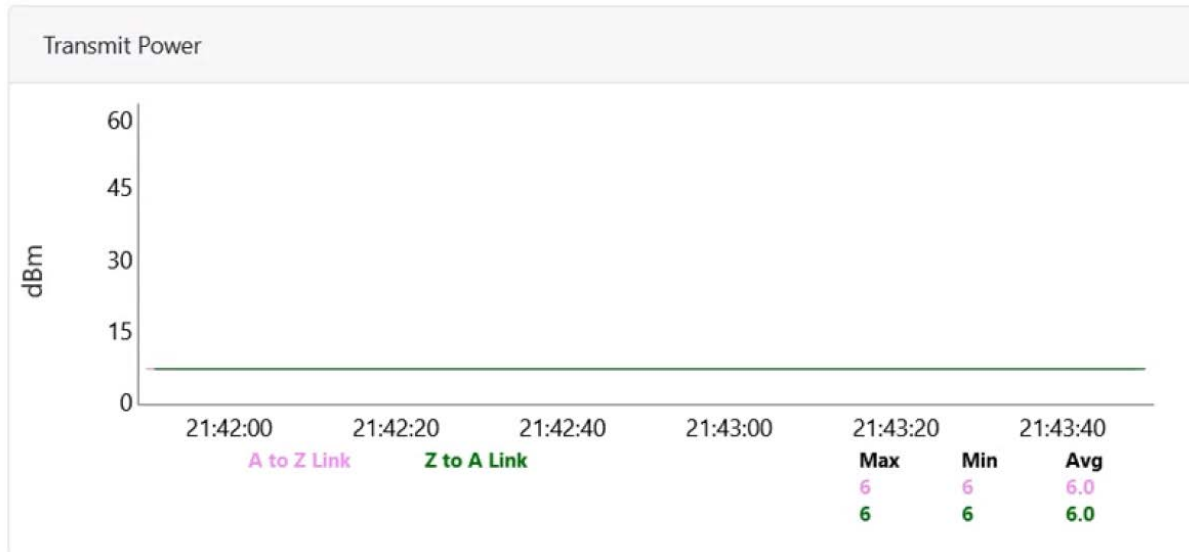
RSSI graph

Figure 217: RSSI graph



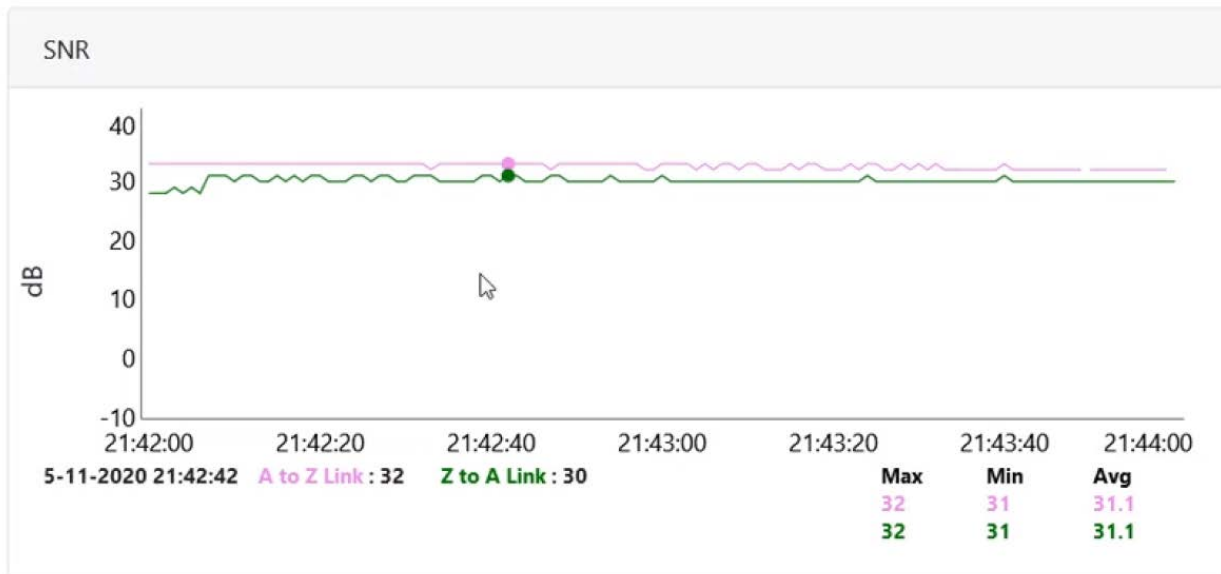
Transmit Power graph

Figure 218: Transmit Power graph



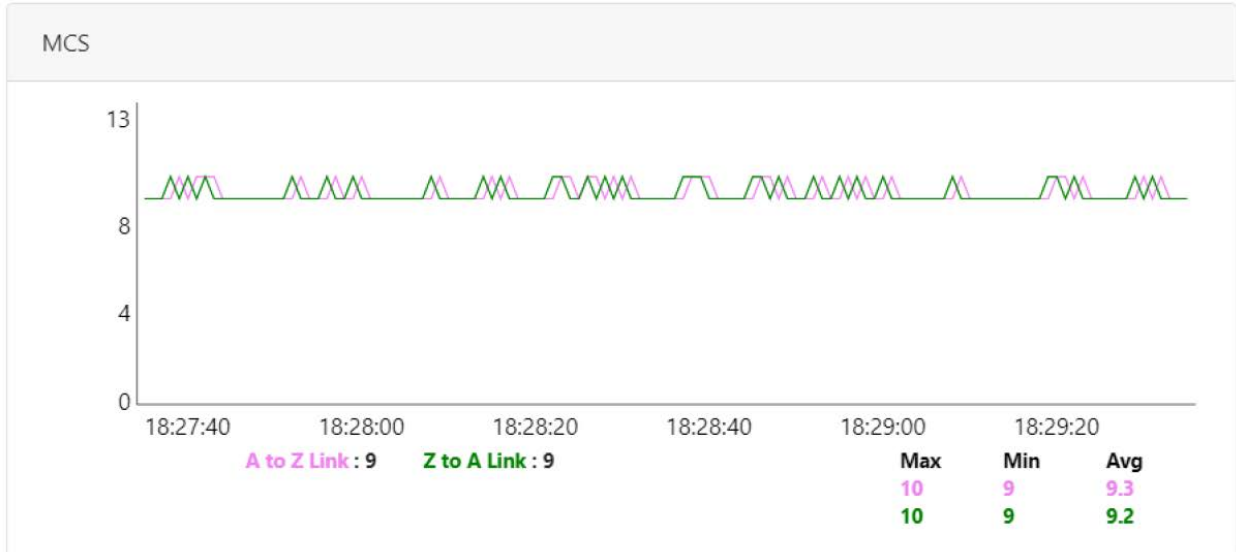
SNR graph

Figure 219: SNR graph



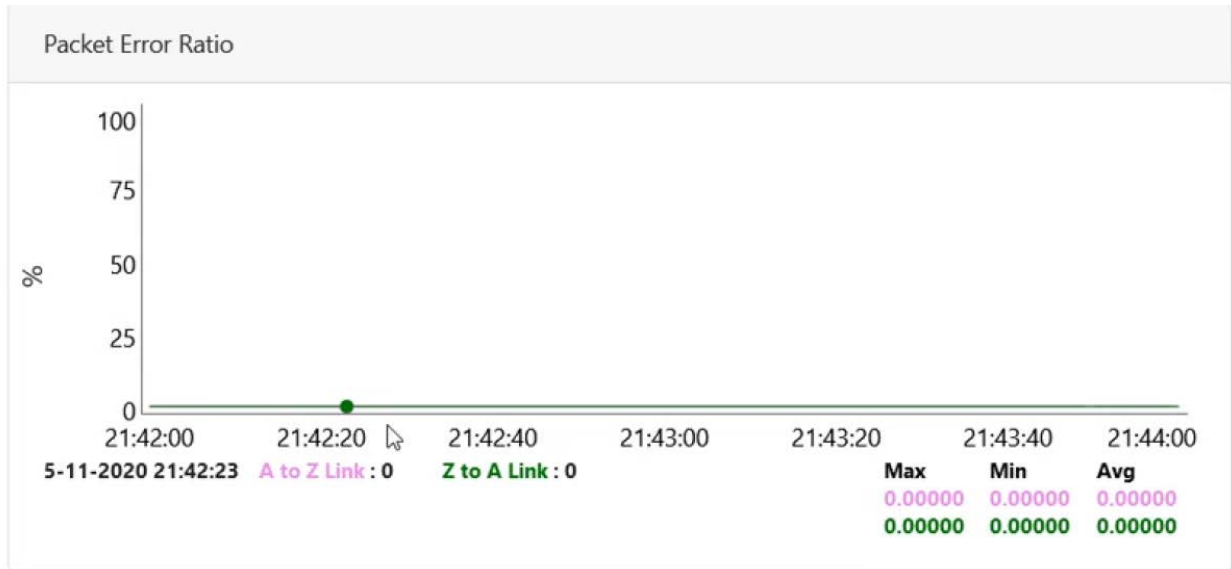
MCS Index graph

Figure 220: MCS Index graph



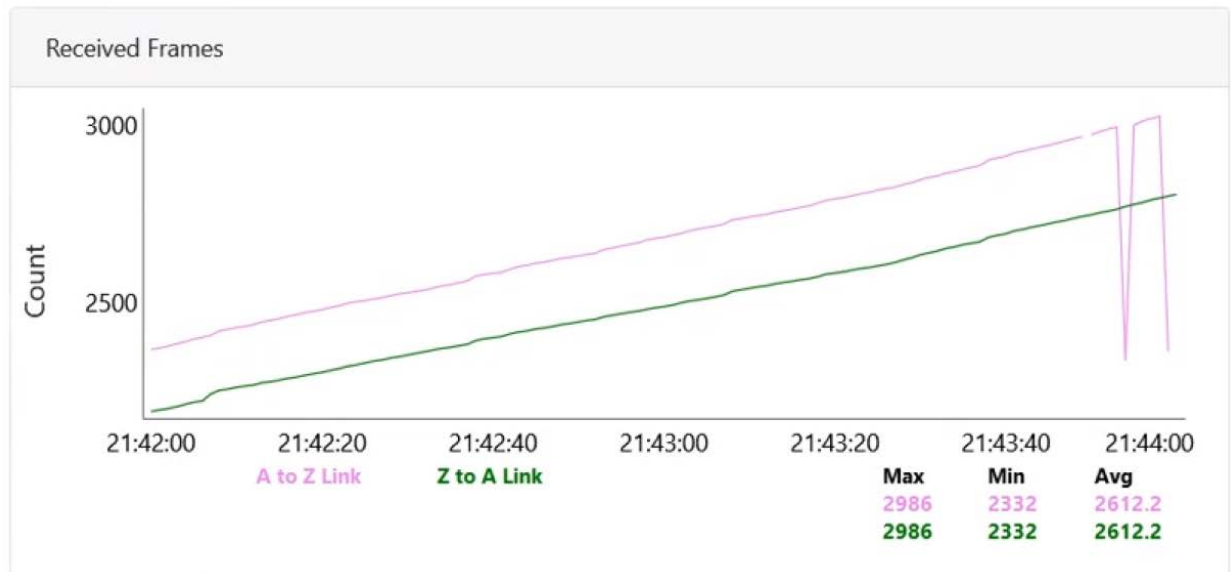
Packet Error Ratio graph

Figure 221: Packet Error Ratio graph



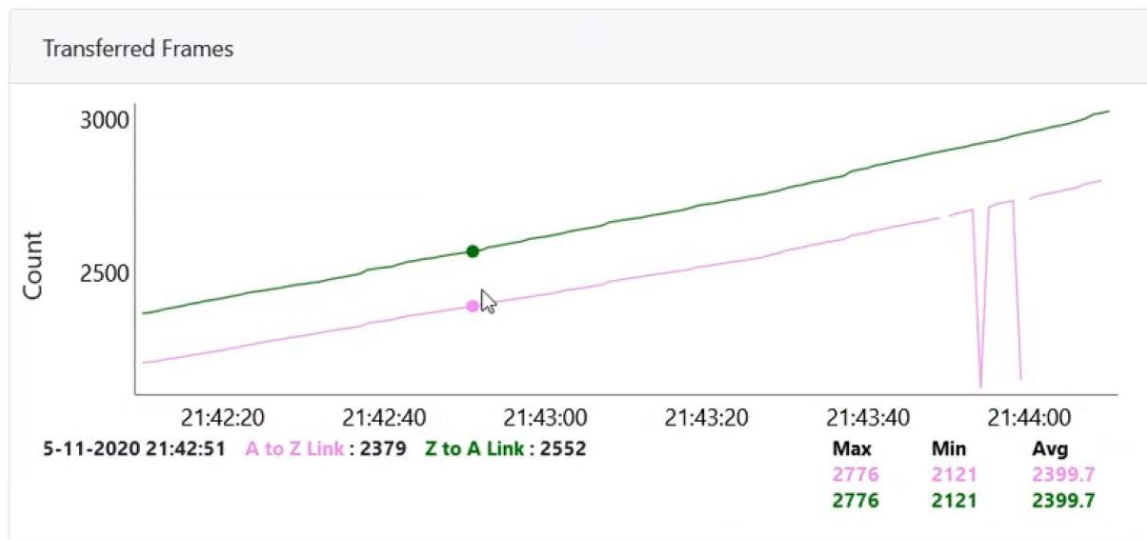
Received Frames graph

Figure 222: Received Frames graph



Transferred Frames graph

Figure 223: Transferred Frames graph



Prefix zone Statistics

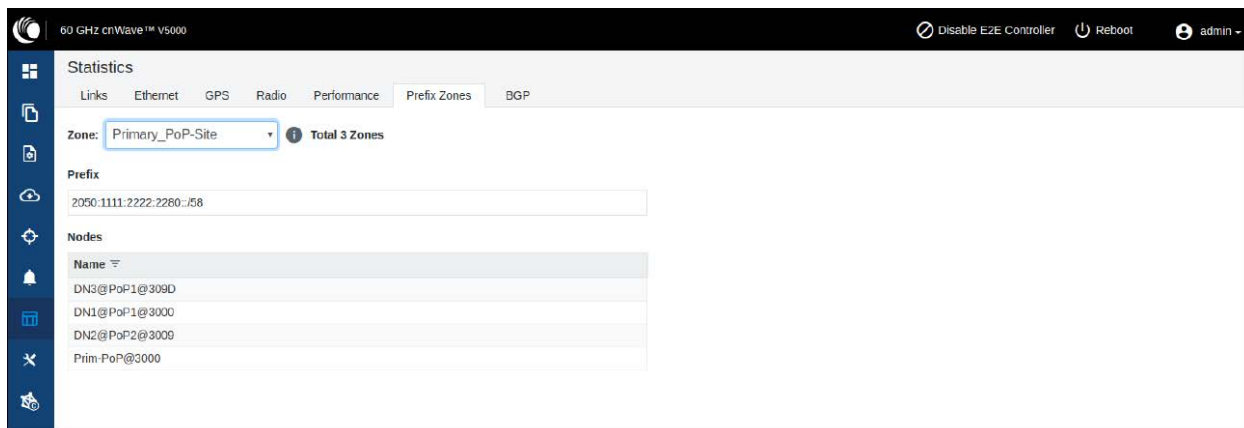
In the multi-PoP deployments, the mesh is divided into prefix zones. Prefix zone statistics are available on the **Statistics > Prefix Zone** page.



Note

You can view the prefix zone statistics only when Deterministic prefix (DPA) is enabled. With CPA enabled, the **Prefix Zone** tab is not visible on the **Statistics** page.

Figure 224: The Prefix Zones page



Border Gateway Protocol (BGP)

The BGP is the protocol used throughout the Internet to exchange routing information between networks. It is the language spoken by routers on the Internet to determine how packets can be sent from one router to another to reach their final destination. BGP has worked extremely well and continues to be protocol that makes the Internet work.

The **BGP** page displays the routing information. This page also contains the details of routes advertised by PoPs to their peers and the routes received by the peers.

Figure 225: The BGP page

The screenshot shows the BGP page in the cnWave interface. The page is titled "Statistics" and has tabs for "Links", "Ethernet", "GPS", "Radio", "Performance", "Prefix Zones", and "BGP". The "BGP" tab is selected.

There are two main sections for PoPs:

- A-Sec-PoP** (Status: Online, Uptime: 0d 0h 4m)
 - Details:**

IPv6 Address	2021::1
Status	Online
ASN	65534
Uptime	0d 0h 4m
 - Advertised Routes:**

Network	Next Hop
1 2020:1111:2222:2200::56	2021::100
 - Received Routes:**

Network	Next Hop
1 ::0	fe80::c6ad:34ff:fe45:aa00
2 2020:1111.2222.2200::56	fe80::c6ad:34ff:fe45:aa00
- Prim-PoP@3000** (Status: Offline, Uptime: NA)
 - Details:**

IPv6 Address	2021::1
Status	Offline
ASN	65534
Uptime	NA
 - Advertised Routes:**

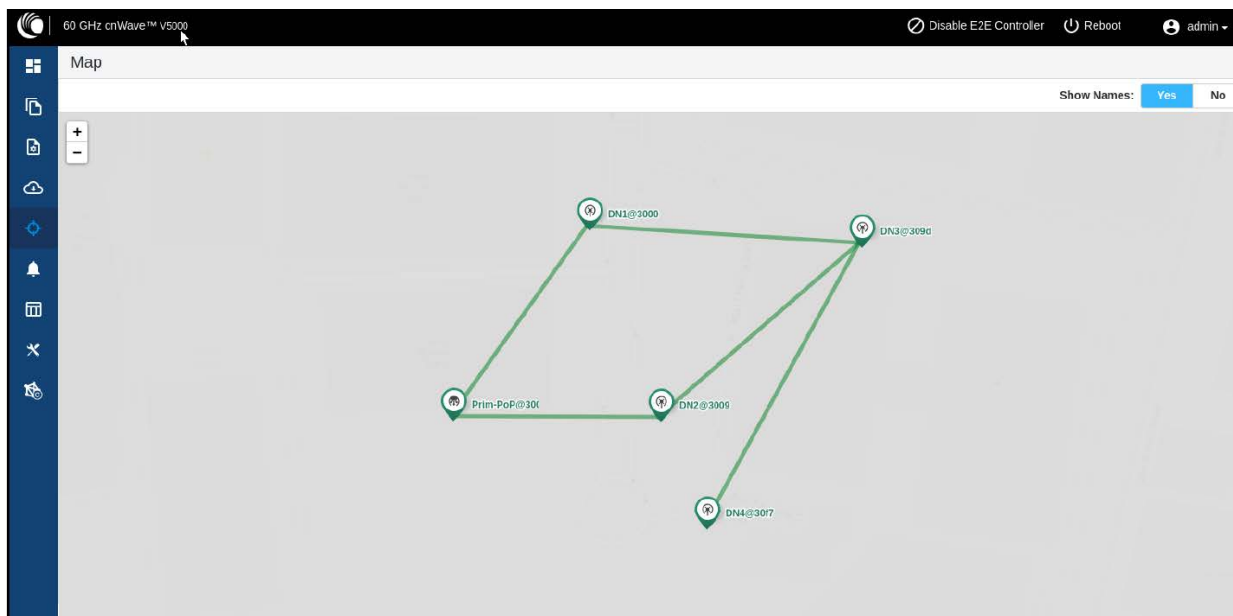
Network	Next Hop
 - Received Routes:**

Network	Next Hop
1 ::0	fe80::c6ad:34ff:fe45:aa00
2 2020:1111.2222.2200::56	fe80::c6ad:34ff:fe45:aa00

Maps

The **Maps** page displays the topology and location/sites of the deployed nodes in the cnWave network. Click the **Maps** icon on the left panel to display the nodes.

Figure 226: The Map page



Tools

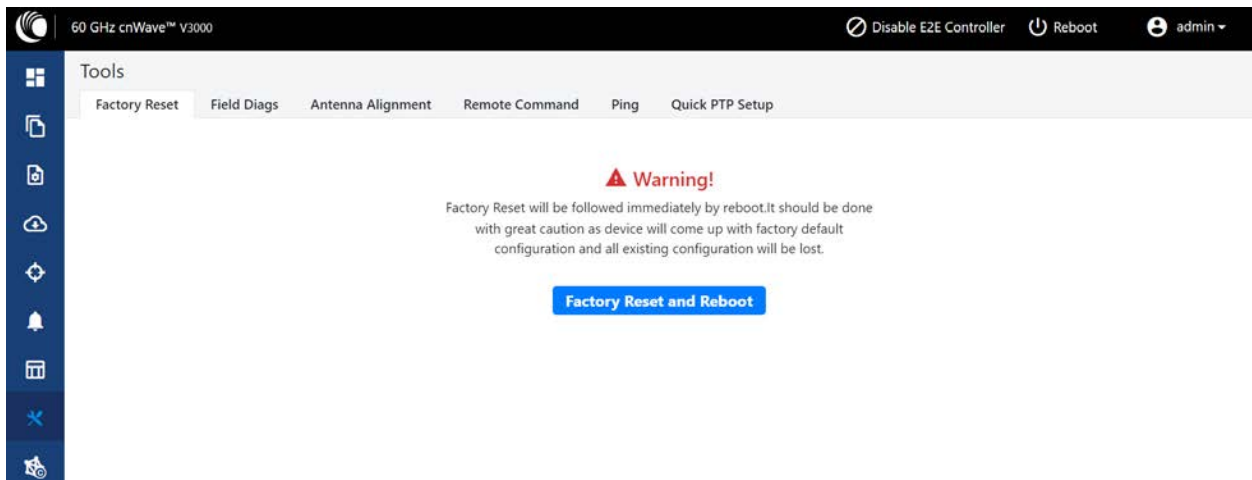
The **Tools** page contains the following tabs:

- [Factory Reset](#)
- [Field Diags](#)
- [Antenna Alignment](#)
- [Remote Command](#)
- [Ping](#)
- [Quick PTP Setup](#)
- [iPerf](#)

Factory reset

The **Factory Reset** page is used to set the default settings.

Figure 227: The Factory Reset page



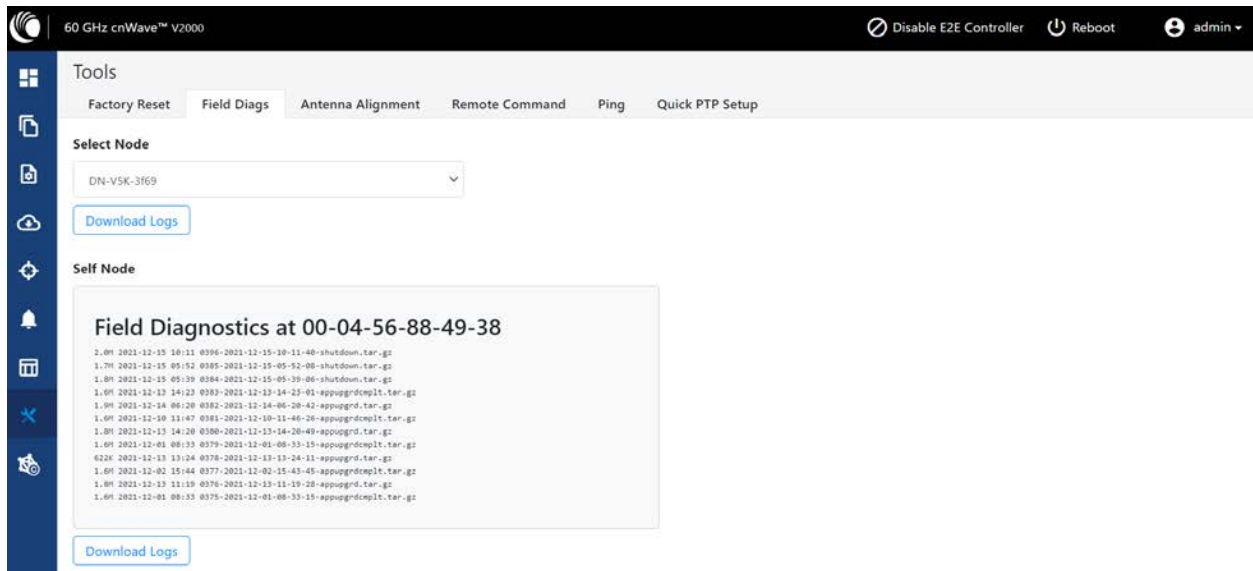
Warning

Factory reset is followed immediately by a system reboot. You must carefully configure the factory reset settings as the device comes up with the default settings. All the existing configurations are lost when the system comes up.

Field diags

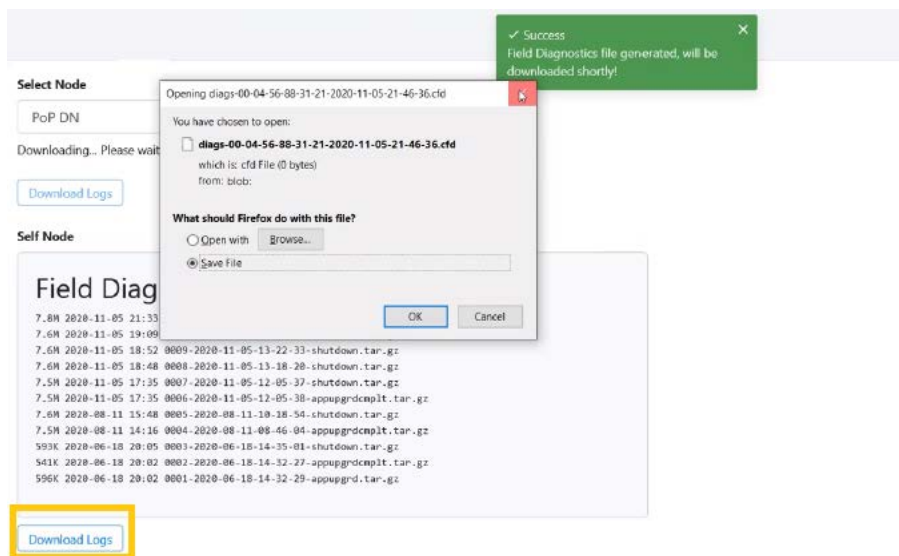
The **Field Diags** tab is used to view and download the error logs. To download the DN logs, select the DN node from the **Select Node** drop-down and click **Download Logs** (as shown in [Figure 228](#)).

Figure 228: The Field Diags page



To download the logs for a self-node, click **Download Logs** at the bottom of the page. Save the log file.

Figure 229: Saving log files



Antenna alignment

The Antenna Alignment tool assists in optimizing the alignment of V3000 to V3000, V5000, V2000, or V1000. This feature helps you to install and align the devices to achieve optimal performance.



Warning

The antenna alignment tool is not a substitute for optical alignment. The optical alignment is the key for getting the signal within the +/-2 degree azimuth and +/-1 degree Elevation window. At this window level, the tool can be used to get away from the edge, corner or spurious beams to ensure optimal alignment.

Prerequisite tasks:

- Complete a Link Plan with Link Planner from Cambium Networks. This prerequisite task provides the information on the RSSI expected for the PTP link. This must be used as a target while using the antenna alignment feature.
- Enter the PTP topology in cnMaestro or the UI of a device (with the Onboard Controller on it). Then, perform the following steps:
 - Create two Sites and nodes.
 - Set up the wireless link between the two nodes.
- Ensure that the nodes are already mounted at the sites.
- An installer must have access to the UI of the device.



Note

When the antenna alignment test is executed between the following devices, ensure that GPS is disabled at the CN side:

- V3000 PoP and V1000 CN
- V3000 PoP and V2000 CN
- V3000 PoP and V3000 CN

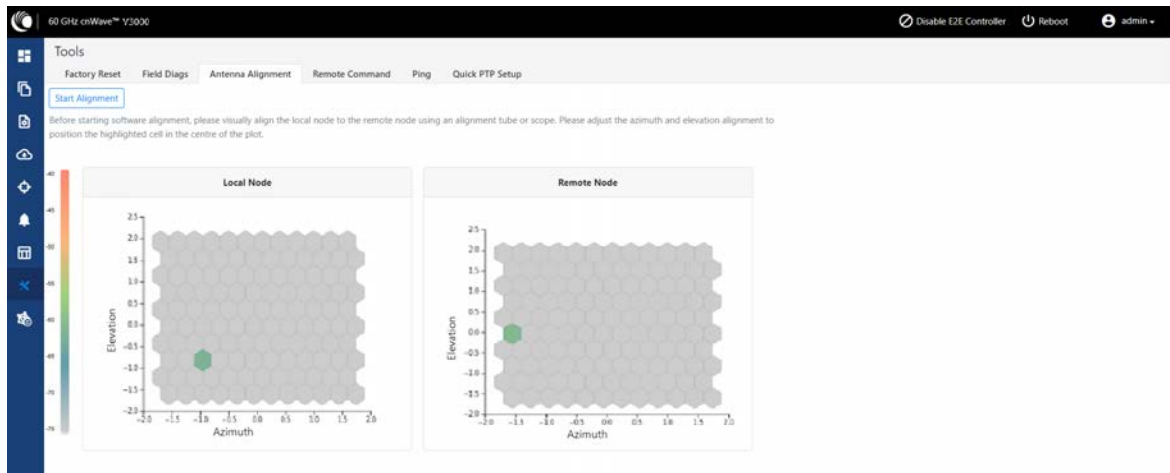
Using the Antenna Alignment tool

To use the Antenna Alignment tool, perform the following steps:

1. From the home page of the device UI, navigate to **Tools > Antenna Alignment**.

The Antenna Alignment page appears, as shown in [Figure 230](#).

Figure 230: The Antenna Alignment page



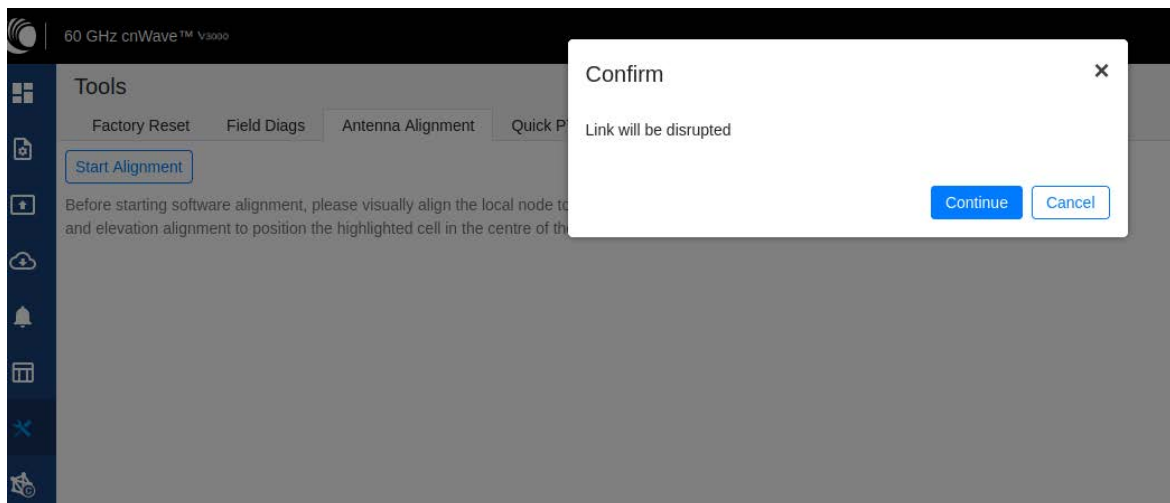
Note

If the alignment is initiated from a CN, ensure that the operating channel is set on the radio (before alignment). If the channel is not set, you must set the required channel in the **Configuration** page of the V3000 single node UI.

2. Click the **Start Alignment** button located at the top left side of the Antenna Alignment page.

The **Confirm** message box appears (as shown in Figure 231), indicating that the link will be disrupted. For running the antenna alignment tool, the auto ignition needs to be disabled. If a link has been established already, it is disassociated at this level.

Figure 231: The Confirm message box in the Antenna Alignment page



3. In the **Confirm** message box, click **Continue** to start the antenna alignment process.
The antenna alignment process begins.



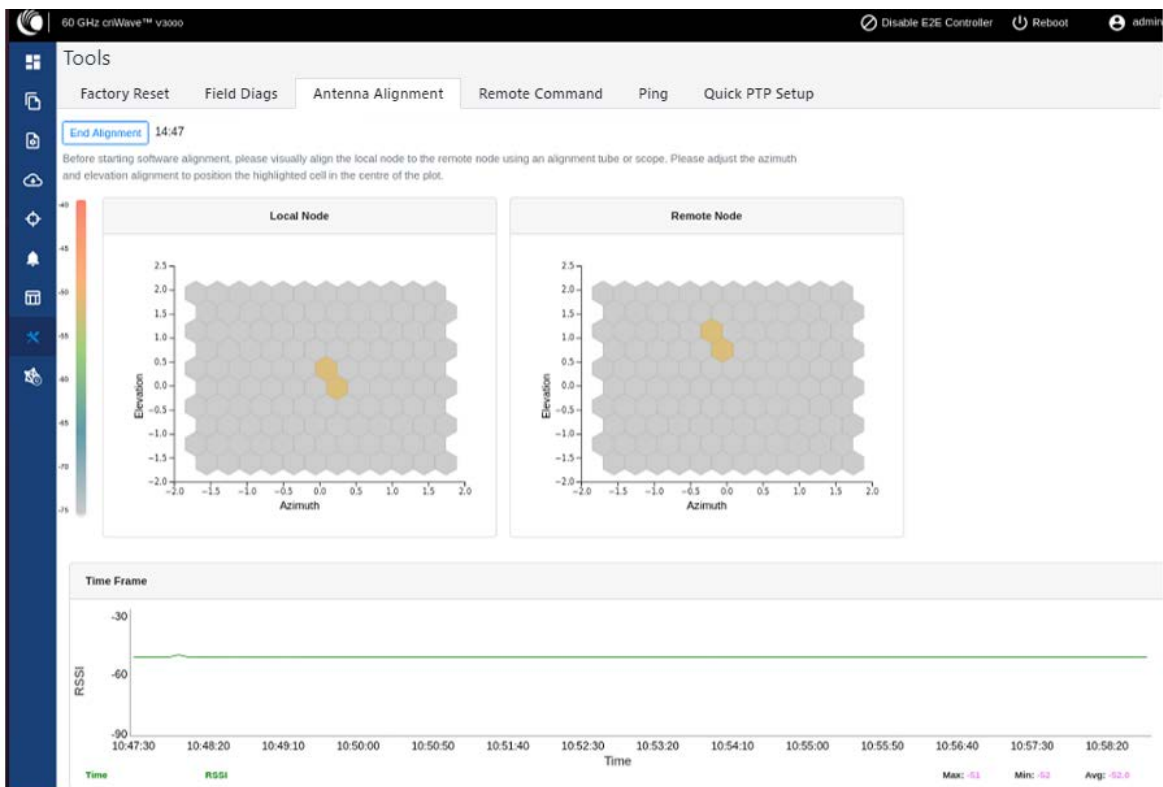
Note

If the alignment is initiated from a device (which is not running with Onboard Controller), perform the following actions:

- Disable the ignition of the link at the Controller.
- Send Dis-assoc for the link from the Controller.
- When the alignment starts, select the required node from the **Remote Node Model** drop-down list.

The **Time Frame** section populates the RSSI time series as shown in [Figure 232](#).

Figure 232: The RSSI time series



Following details explain about the RSSI time series that populates in the Antenna Alignment page:

- The **Local Node** section (located at the left side of the Antenna Alignment page) displays the direction of arrival angle with respect to the local (PoP) device.
- The **Remote Node** section (located at the right side of the Antenna Alignment page) displays the direction of arrival angle with respect to the remote device.
- In **Local Node** and **Remote Node** sections, a cell marks the direction of arrival. The color of the cell represents the RSSI based on the heatmap scale given on the left side.

- The **Time Frame** section (located at the bottom of the Antenna Alignment page) displays the RSSI time series, along with the peak RSSI time and the latest data point (on the right end of the plot).

The RSSI time series and the heatmap plots get updated every six seconds. This is due to the processing time taken for a complete sweep of all the combinations of beams and channels.

During the alignment phase, the transmit power used is the maximum configured power and the transmit power control is disabled.

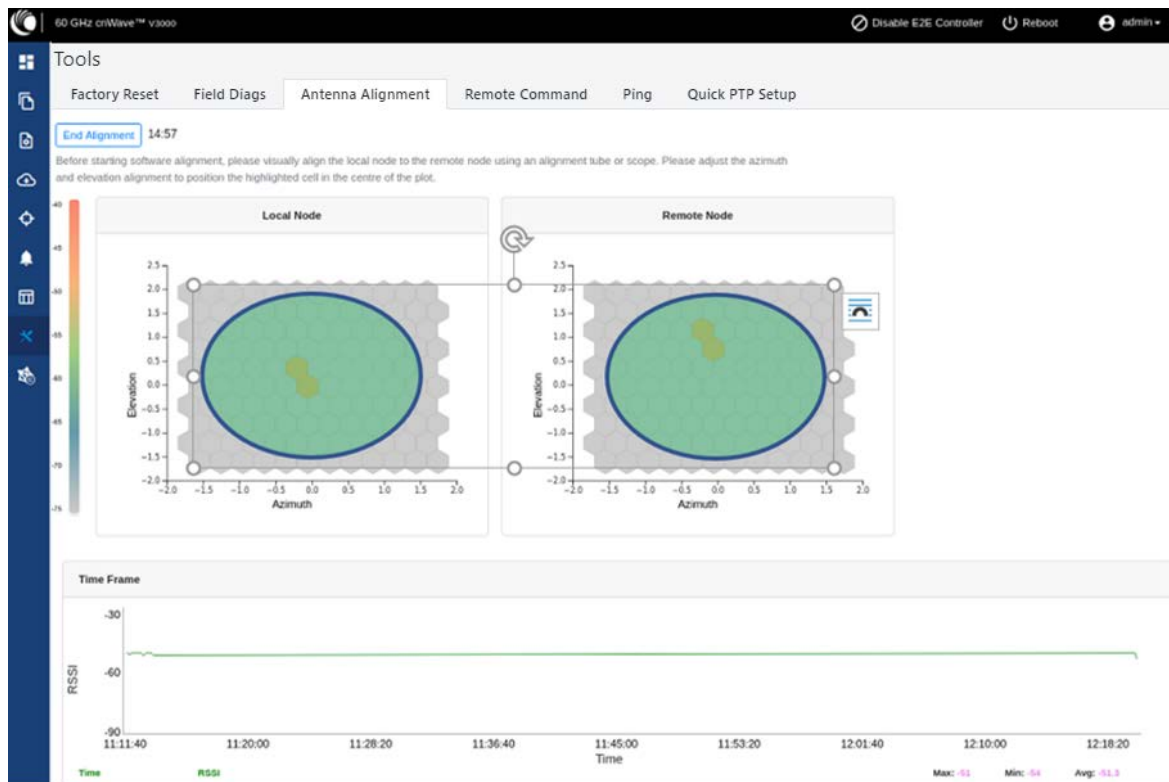


Note

If the installer has enabled the short-range installation in the radio configuration, the transmit power control is set to the minimum configured power.

4. Adjust the optimal RSSI that must be reached when the beams are close to the central region, as shown in [Figure 233](#).

Figure 233: The optional RSSI alignment



The RSSI time series must be close to the Link planner's predicted RSSI (the receive level when aligning, as shown in [Figure 234](#)), with an error of +/-5dB. Consider the following points when adjusting the optional RSSI:

- If the time series reporting RSSI is more than 10dB from that of the Link Planner's expected RSSI, then the device has been aligned incorrectly and is being picked up by the sidelobes or spurious beams.

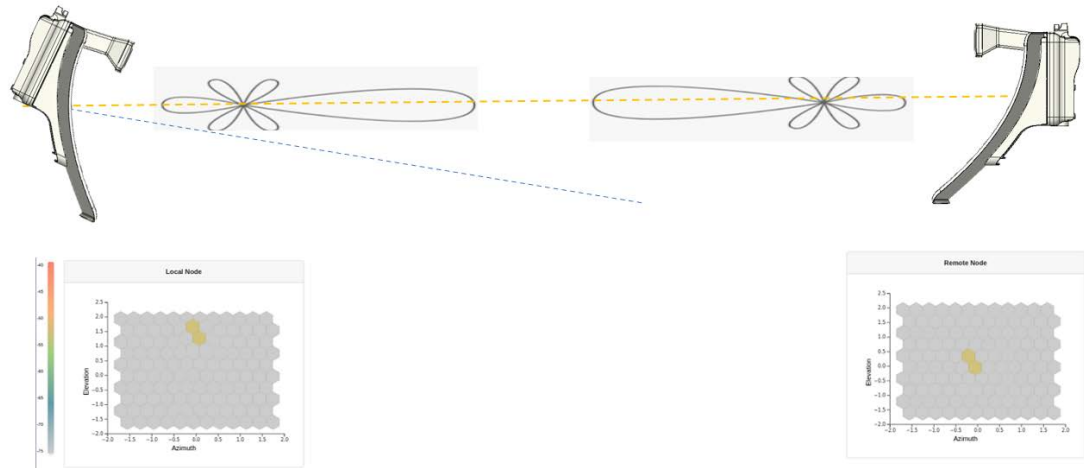
- If a cell is highlighted and the time series reporting RSSI is more than 10dB off the expected RSSI, then it is necessary to sweep beyond the current position of both azimuth and elevation, in turn to ride past the sidelobes.

Figure 234: An example of the receive level when aligning - Link planner

Radio Commissioning Notes for CN	
Model	V3000
Maximum EIRP	60 dBm
Minimum MCS	MCS 2
Maximum MCS	MCS12 (16QAM 0.75 Sngl)
Channel	64.80 GHz (Channel 4)
Polarity	Auto
Predicted Receive Power	-46 dBm \pm 5 dB while aligning
Operational EIRP	46 dBm
Operational Receive Power	-60 dBm \pm 5 dB
Predicted Link Loss	116.25 dB \pm 5.00 dB

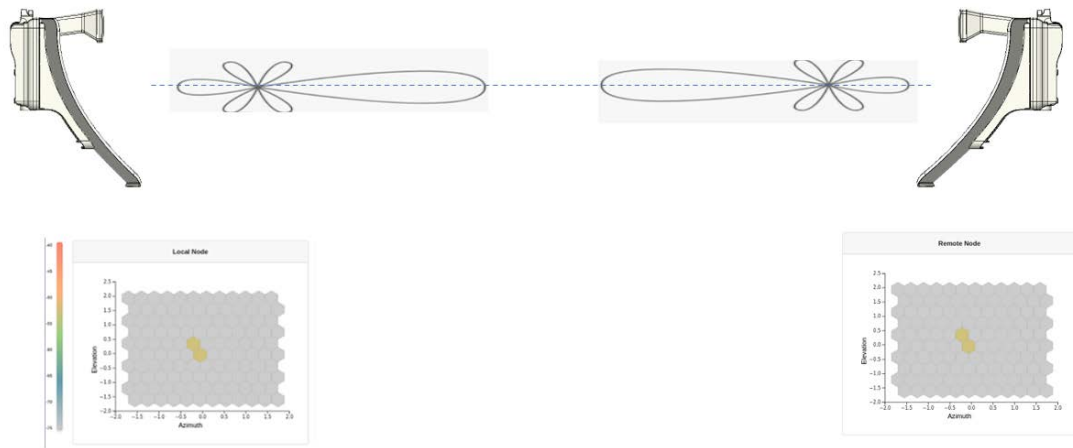
5. Make use of the direction of arrival information (if there is any elevation or azimuth mismatch) to physically align the radio antennas.
 - When there is an elevation mismatch (as shown in Figure 235):

Figure 235: Example of the elevation mismatch



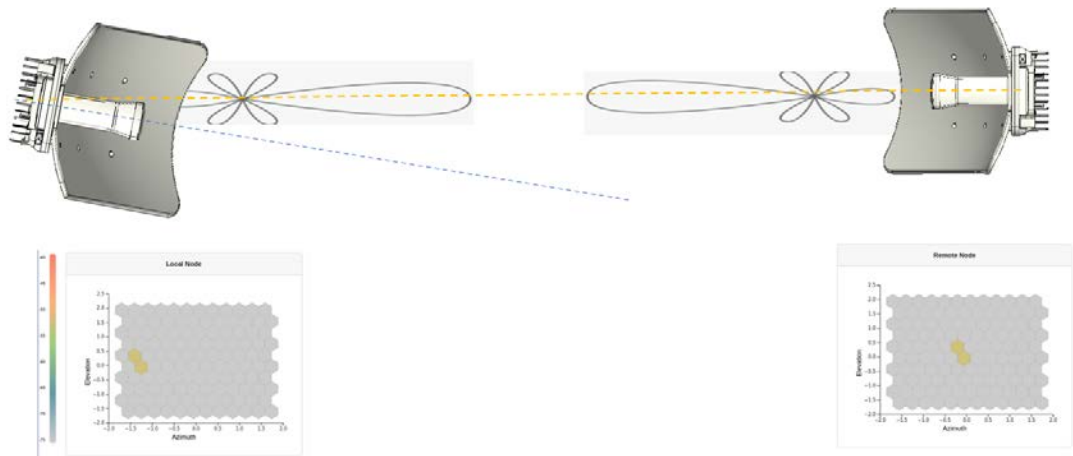
In Figure 235, the angles are exaggerated to show the point. In this example, consider that the radio has been misaligned by a down-tilt of 2 degrees behind the unit (from an installer's view side). This means that the angle of the beam selected might be in the +2 degrees direction in the elevation due to beamforming. The aim is to get the optimal boresight beam. Therefore, the radio must be up tilted in the elevation direction by 2 degrees. The selected beam is now closer to the boresight beam, as shown in Figure 236.

Figure 236: On correcting the elevation mismatch



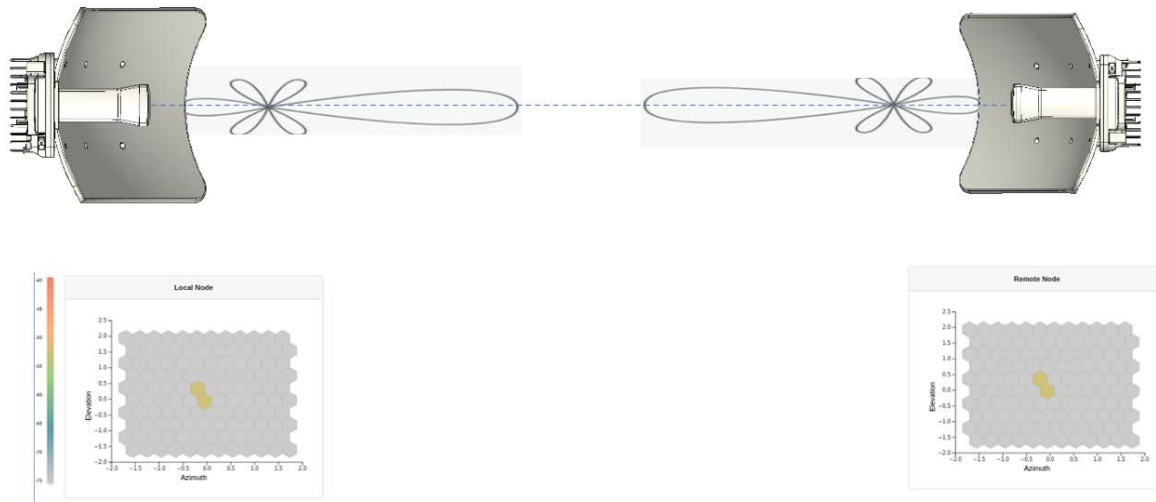
- When there is an azimuth mismatch (as shown in Figure 237):

Figure 237: Example of the azimuth mismatch



In Figure 237, the angles are exaggerated to show the point. In this example, consider that the radio has been misaligned in azimuth by 2 degrees to the right behind the unit (from an installer's view side). This means that the angle of the beam selected might be in the -2 degrees direction due to beamforming. The aim is to get the optimal boresight beam. Therefore, the radio must be tilted in the azimuthal direction to the left by 2 degrees. The selected beam is now closer to the boresight beam, as shown in Figure 238.

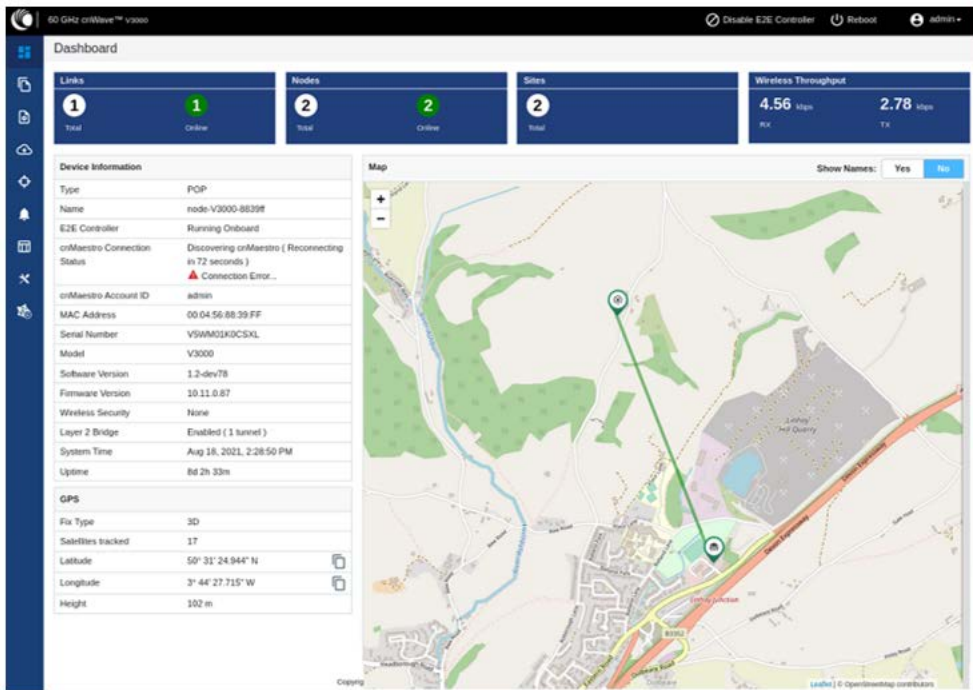
Figure 238: On correcting the azimuth mismatch



- When you achieve the desired alignment and RSSI, click the **End Alignment** button located at the top left side of the Antenna Alignment page.

If you do not click the **End Alignment** button, the alignment cycle ends automatically after 15 minutes. When the alignment cycle ends, the ignition state (disabled earlier) is enabled to auto ignition and the link is established. Figure 239 shows how the Antenna Alignment dashboard page looks on completing the antenna alignment task.

Figure 239: The updated Antenna Alignment dashboard page



Remote Command

The **Remote Command** tool page supports the following commands:

- [Show SFP power details](#)
- [Show ipv4 neighbors](#)
- [Show ipv6 neighbors](#)
- [Show Wired Interface State Changes](#)

Show SFP power details

The **Show SFP Power Details** command is available on the **Tools** page. When you execute this remote command from the Onboard Controller UI or the node CLI, the command provides the SFP power details (as an output) for the required SFP ports and interfaces.



Note

Currently, the **Show SFP Power Details** remote command is not available in cnMaestro.

To execute the **Show SFP Power Details** remote command, perform the following steps:

1. From the home page of the device UI, navigate to **Tools > Remote Command**.
The **Remote Command** page appears.
2. Select the required node from the **Select Node** drop-down list.
3. Select **Show SFP Power Details** from the **Select Command** drop-down list.
4. Click **Execute**.

The **Output** section displays the SFP power details for the selected node, as shown in [Figure 240](#).

Figure 240: The UI supported output - SFP Power details

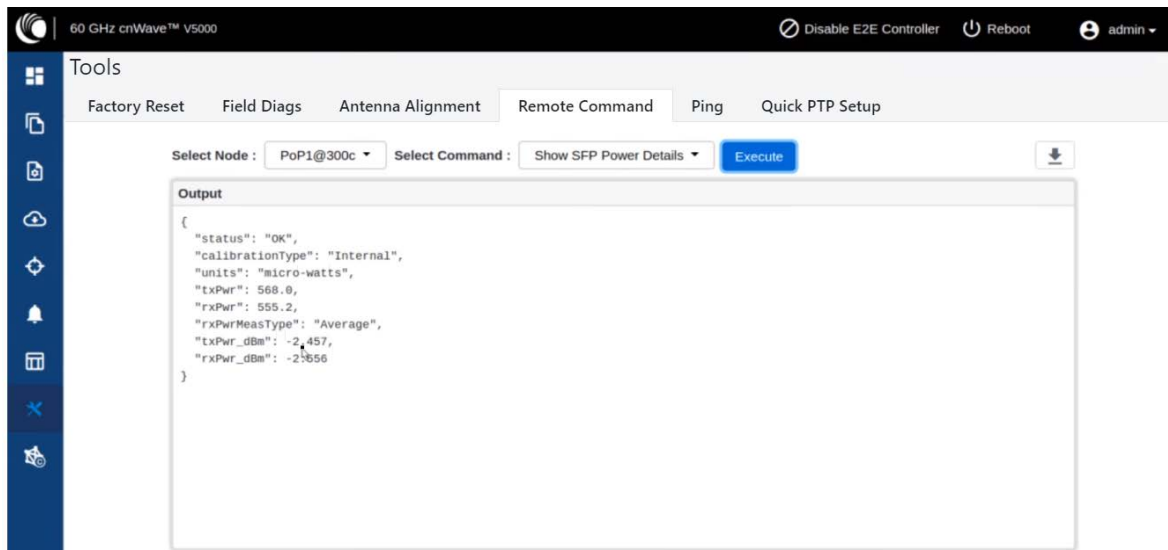


Table 59 lists and describes each parameter in the output.

Table 59: Output details

Output Parameter	Description
Status	<p>Determines whether the output is valid.</p> <p>If the Status field contains OK, it implies that the rest of the output is valid.</p> <p>If the Status field does not contain OK, it implies that only the Status field is valid. In such cases, the Status field provides the reason for not being able to read the laser powers.</p>
CalibrationType	<p>Indicates the measurement type that is calibrated over the criteria, such as the following (for example):</p> <ul style="list-style-type: none"> • Specified transceiver temperature, • Transceiver supply voltage, • TX output power, and • RX received optical power. <p>The value of this parameter is Internal.</p>
Units	<p>Indicates the unit of measurement.</p> <p>The value of this parameter is micro-watts (mW).</p>
txPwr	Indicates the TX output power in mW.
rxPwr	Indicates the RX received optical power in mW.
rxPwrMeasType	<p>Indicates whether the received power measurement represents an average input optical power.</p> <p>The value of this parameter is Average.</p>
txPwr_dBm	Indicates the TX output power in dBm.
rxPwr_dBm	Indicates the RX received optical power in dBm.

- To download the output, click the download icon located at the top left side of the **Remote Command** page.

You can also execute the **Show SFP Power Details** command by using the device CLI. Log on to the device and open the CLI. At the command prompt, provide the `Show SFP` value and hit **Enter** on your keyboard. The command displays the output, as shown in [Figure 241](#).

Figure 241: The CLI supported output - SFP Power details

```
CLISH>show sfp
{
  "status": "OK",
  "calibrationType": "Internal",
  "units": "micro-watts",
  "txPwr": 564.3,
  "rxPwr": 557.1,
  "rxPwrMeasType": "Average",
  "txPwr_dBm": -2.485,
  "rxPwr_dBm": -2.541
}
CLISH>
```

Show ipv4 neighbors

The **Show ipv4 neighbors** remote command reveals the Address Resolution Protocol (ARP) table for IPv4 addresses in the network. The ARP table, also known as the neighbour table for IPv4, links IP addresses to MAC addresses for devices within the same local network.

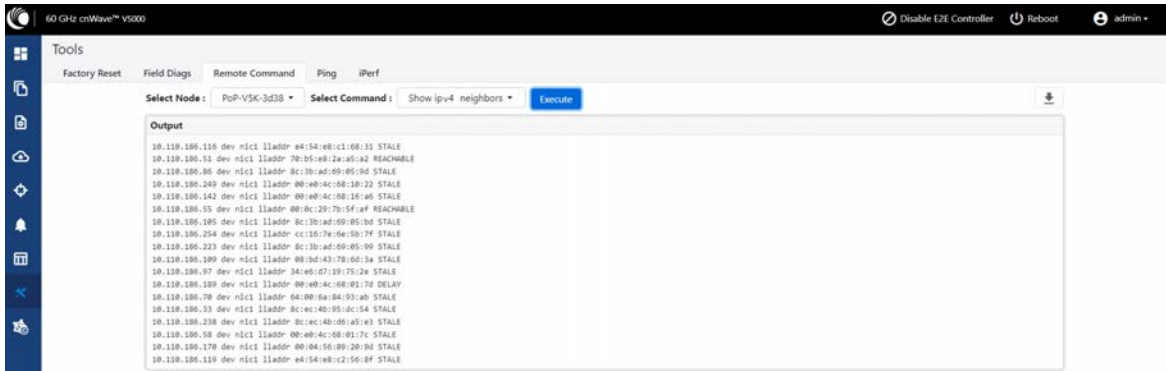
When you execute the **Show ipv4 neighbors** command using the **Tools > Remote Command** page, you can view information of the active IPv4 neighbours in the output. In addition, the output information can also aid in identifying potential network anomalies or connectivity issues.

To execute the **Show ipv4 neighbors** command, perform the following steps:

1. On the **Tools > Remote Command** Page, select the required node from the **Select Node** drop-down list.
2. Select **Show ipv4 neighbors** from the **Select Command** drop-down list.
3. Click **Execute**.

The **Output** section displays the IPv4 neighbor details for the selected PoP or CN, as shown in [Figure 242](#).

Figure 242: The Show ipv4 neighbors command output



You can use the  icon to download the output (in .txt format).

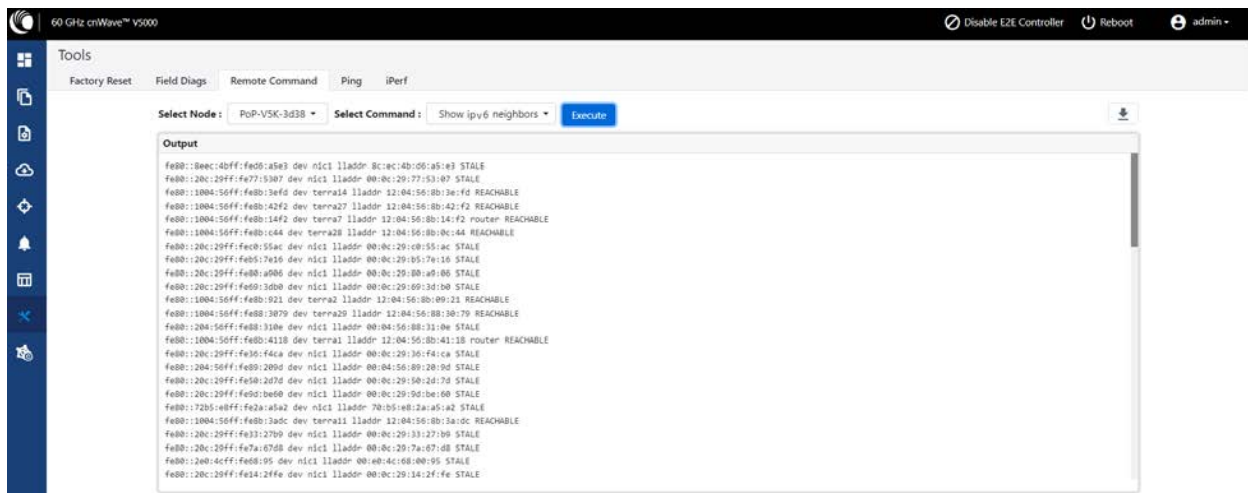
Show ipv6 neighbors


The **Show ipv6 neighbors** remote command displays the neighbour table for IPv6 addresses, analogous to the IPv4 ARP table but for IPv6 addresses. As the adoption of IPv6 continues to rise, the visibility into these connections becomes more critical.

When you run the **Show ipv6 neighbors** command from the **Tools > Remote Command** page, the command unveils the relationship between IPv6 addresses and MAC addresses within a local network. In addition, the command enables effective monitoring and troubleshooting of IPv6 network issues.

On selecting the required node from the **Select Node** drop-down list and **Show ipv6 neighbors** from the **Select Command** drop-down list, click **Execute**. The **Output** section displays the IPv6 neighbor details for the selected node, as shown in Figure 243.

Figure 243: The Show ipv6 neighbors command output



To download the output (in .txt format), use the  icon.

Show Wired Interface State Changes

The **Show Wired Interface State Changes** remote command displays up or down events on wired interfaces. This command is useful for debugging and troubleshooting network events.

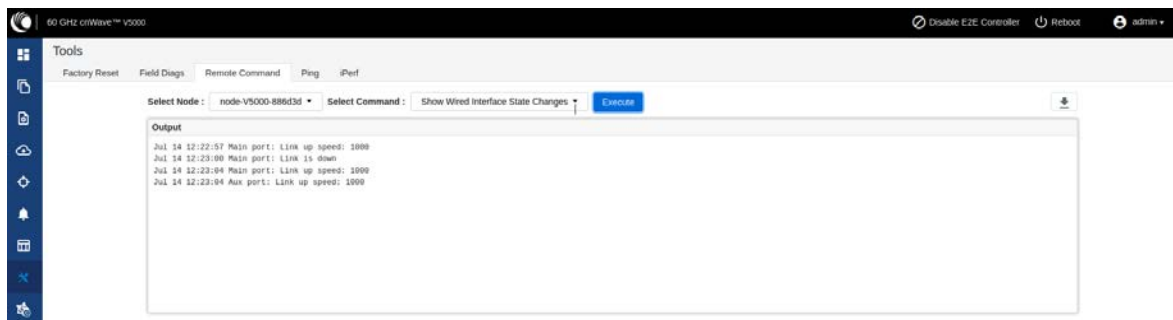
This remote command enables network administrators to identify and analyze Ethernet port state changes, and provides insights into network events such as connection issues or device status changes.

To execute the **Show Wired Interface State Changes** command, perform the following steps:

1. On the **Tools > Remote Command** Page, select the required node from the **Select Node** drop-down list.
2. Select **Show Wired Interface State Changes** from the **Select Command** drop-down list.
3. Click **Execute**.

The **Output** section displays the up or down events for the selected criteria, as shown in [Figure 244](#).

Figure 244: The Show Wired Interface State Changes output



To download the output, use the  icon.

Ping

The **Ping** tool provides information that is used to identify the reachability between the required node and another nodes or destination (for IPv4 and IPv6). The ping tool is useful in troubleshooting radio links.

To use the ping tool, perform the following steps:

1. From the home page of the device UI, navigate to **Tools > Ping**.
The **Ping** page appears.

2. Set the parameters with the required values, as described in [Table 60](#).

Table 60: List of parameters in the Ping page

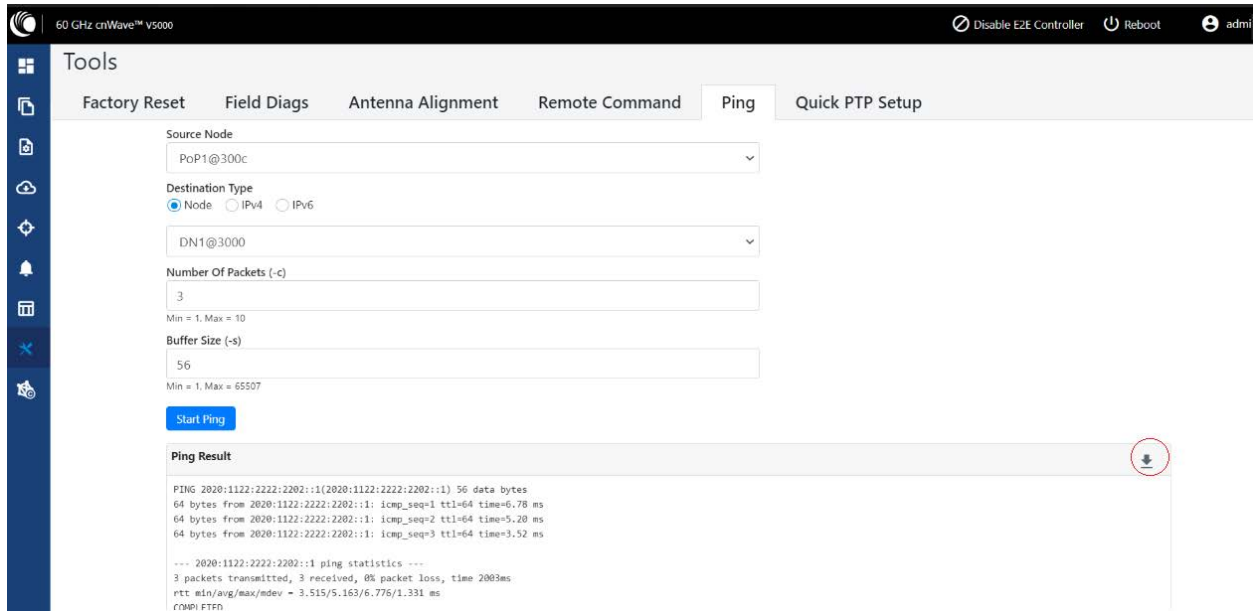
Parameter	Description
Source Node	The source node for which you want to find the reachability with another node or destination.


Parameter	Description
	Select the required source node from the drop-down list.
Destination Type	<p>The required node or destination address (IPv4 or IPv6) that for which the reachability has to be identified.</p> <p>Following options are supported:</p> <ul style="list-style-type: none"> • Node • IPv4 • IPv6 <p>Select the required option (mandatory).</p>
Number of Packets (-c)	<p>Number of times that a packet is transmitted to find the reachability.</p> <p>Default value: 3</p> <p>This parameter supports values between 1 (minimum) and 10 (maximum).</p> <p>Type an appropriate value in the text box.</p>
Buffer Size (-s)	<p>Size (in bytes) of the packet.</p> <p>Default value: 56</p> <p>This parameter supports values between 1 (minimum) and 65507 (maximum).</p> <p>Type an appropriate value in the text box.</p>

3. Click **Start Ping**.

The **Ping Result** section displays the information for the selected criteria, as shown in [Figure 245](#).

Figure 245: The Ping page



You can use the  icon to download the ping result.

Quick PTP setup

Quick PTP Setup is a simple user-friendly tool used for quickly creating a PTP link between the PoP and the CN. This option eliminates the long process of creating a PTP link with Onboard Controller in the **Topology** UI page.



Note

The Quick PTP Setup option is supported only on V1000, V2000, and V3000 products.

With the **Quick PTP Setup** option, you can skip the long process of creating a PTP link that involves the following actions:

1. Enabling Onboard Controller on the required node that can also act as a PoP node.
2. Adding a site for the CN node.
3. Adding a node for the CN node.
4. Creating a link between the PoP and the CN nodes.

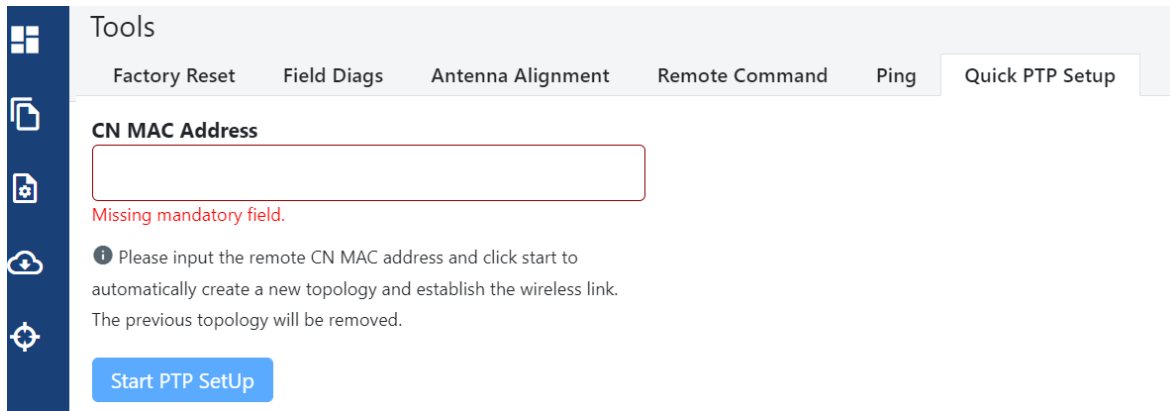
The **Quick PTP Setup** option enables you to create the PTP link using the simple process on the **Tools** page of the device UI.

To create the PTP link quickly for the required nodes, perform the following steps:

1. Navigate to **Tools > Quick PTP Setup** from the home page of device UI.

The **Quick PTP Setup** page appears, as shown in [Figure 246](#).

Figure 246: The Quick PTP Setup tab on the Tools page



2. In the **CN MAC Address** text box, enter the MAC address of the required CN node (which is connected).



Note

You can also access the MAC address of the connected CN in the **Device Information** section of the main **Dashboard** page (of the device UI).

3. Click **Start PTP Setup**.

This action creates the PTP link between the PoP and the CN nodes, quickly.

When you configure **Quick PTP Setup**, the unit turns to a DN running E2E Controller with Layer 2, and default IPv4 address of 169.256.1.1. When the client onboards, E2E Controller pushes the configuration to a CN with the IPv4 address of 169.254.1.2.

You can view the connected PoP and CN details on the **Topology** page of the device UI.

iPerf

The **iPerf** tool is a user-friendly tool for conducting network performance tests using the device UI. The tool makes network performance testing more accessible and manageable. It helps you with tools required for effective measuring and understanding the network's performance.

The iPerf tool is built around the widely recognized iPerf testing tool (open-source) and provides a graphical UI for conducting the network performance tests with ease.

Following are the features of the iPerf tool:

- **Server Node and Client Node selection:** The iPerf tool allows you to easily select the server and client nodes for your network performance tests. The node selection sets up the endpoints required for the test. In addition, the test traffic is unidirectional, flowing from the client to the server.
- **Time and Parallel Streams selection:** You can specify the time in seconds to customize the duration of the tests. You can also select the number of parallel streams to run during the test, providing more granular control over the testing parameters.
- **TCP, IPv6 Layer 3 Traffic Profile:** Network performance tests are conducted using a TCP, IPv6 Layer 3 traffic profile. The iPerf tool internally handles the selection and implementation of the

traffic profile, and simplifies the test process.

- **Network performance profiling:** The iPerf tool allows you to profile the performance of your network on a link-by-link basis. This tool is instrumental in identifying performance blockers and optimizing network performance.
- **Coexisting with customer data:** The iPerf tool tests traffic that competes with customer data, rather than blocks or stops. There is no prioritization given to either data, ensuring that the test results reflect real-world network conditions.
- **Complete iPerf output display:** On conducting the network performance test, you can view the entire iPerf output in a dedicated panel on the **Tools > iPerf** page. This tool offers an easy and a convenient way to interpret the results (within the interface).



Note

The throughput, measured by the iPerf tool, must only be used as a guideline. Using traffic testing software onboard the radio carries additional processing overheads, which are not present in the normal operation.

To use the **iPerf** tool, perform the following steps:

1. From the homepage of the device UI, navigate to **Tools > iPerf**.
The **iPerf** page appears.
2. Set the values for the parameters, as described in [Table 61](#).

Table 61: Parameters required for running the iPerf tool

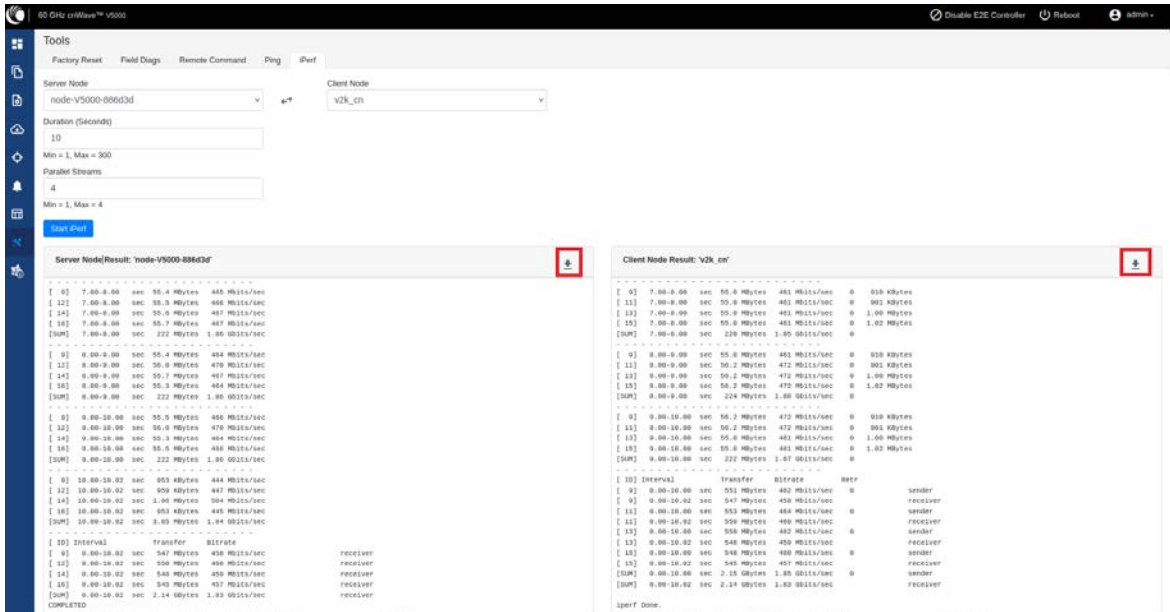
Parameter	Description
Server Node	The server node for which you want to conduct the network performance test. Select the required server node from the drop-down list. Note: You can use the ↔ icon to reverse the server and client node names.
Client Node	The client node for which you want to conduct the network performance test. Select the required client node from the drop-down list. Note: You can use the ↔ icon to reverse the server and client node names.
Duration (Seconds)	Period (in seconds) that you want to set for the test. Type an appropriate value (in seconds) in the text box. Default value: 10 seconds Note: This parameter supports values from 1 to 300 (in seconds).
Parallel Streams	Number of parallel streams that you want to run during the test.


Parameter	Description
	<p>Default value: 4</p> <p>Type the required value in the text box.</p> <p>Note: This parameter supports values from 1 to 4.</p>

3. Click **Start iPerf**.

The **Server Node Results** section and the **Client Node Results** section display the results for the selected criteria, as shown in [Figure 247](#).

Figure 247: The iPerf tool page



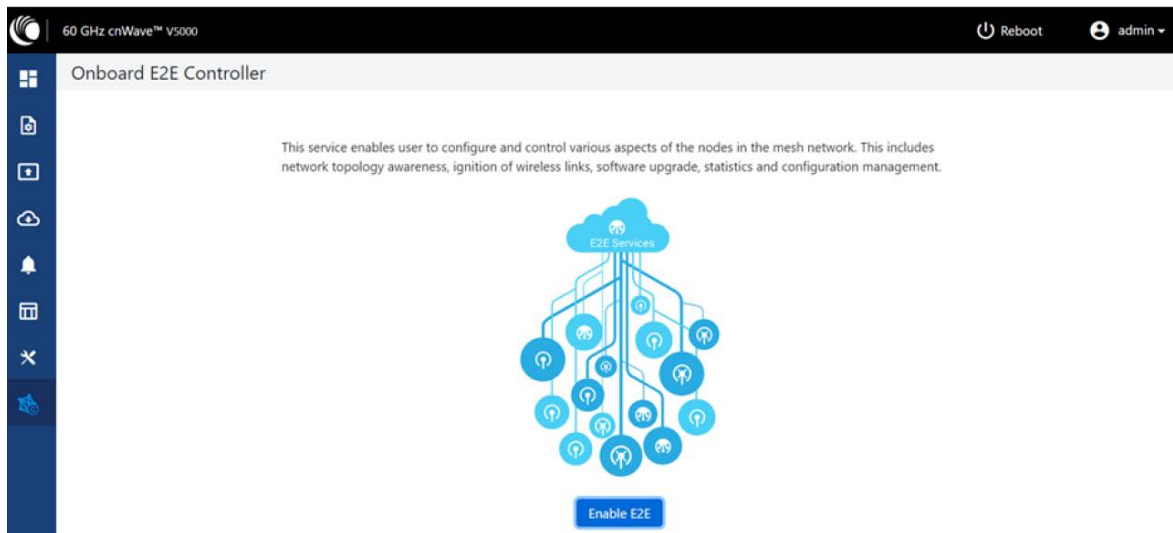
To download the server and client node results (in .txt format), use the  icon on the iPerf page.

cnMaestro support for Onboard Controller

From System Release 1.0.1 onwards, The Onboard E2E controller can be managed by cnMaestro 2.5.0 (on-premises) for network management.

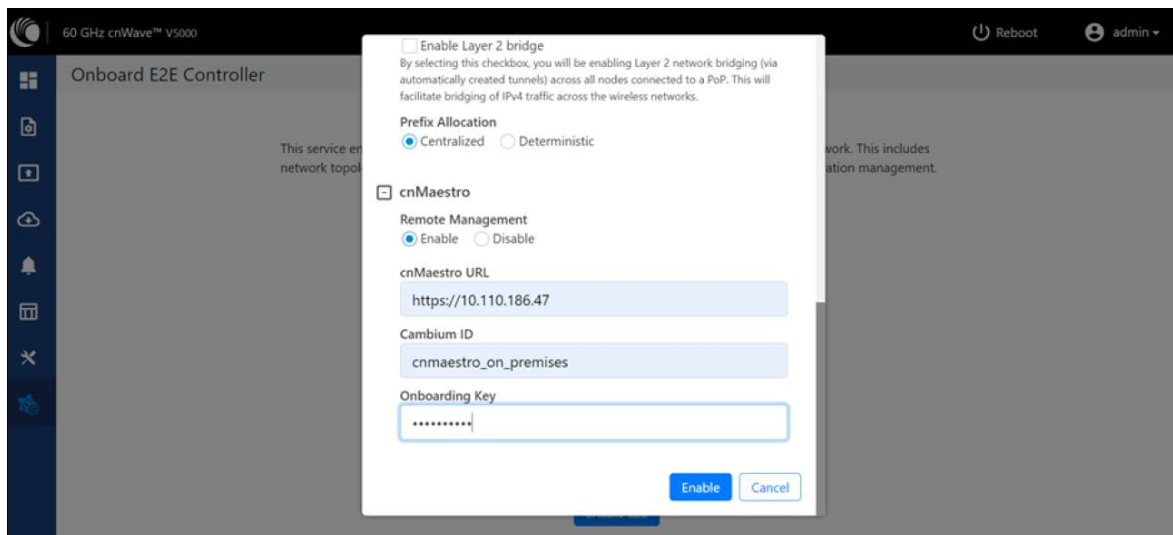
1. After the Onboard E2E controller is enabled from UI, enter the cnMaestro URL. If **Cambium ID based authentication** option is enabled in cnMaestro, then enter the Cambium ID and onboarding key.
2. Click **Enable E2E on Onboard E2E Controller** in UI.

Figure 248: The Onboard E2E Controller page



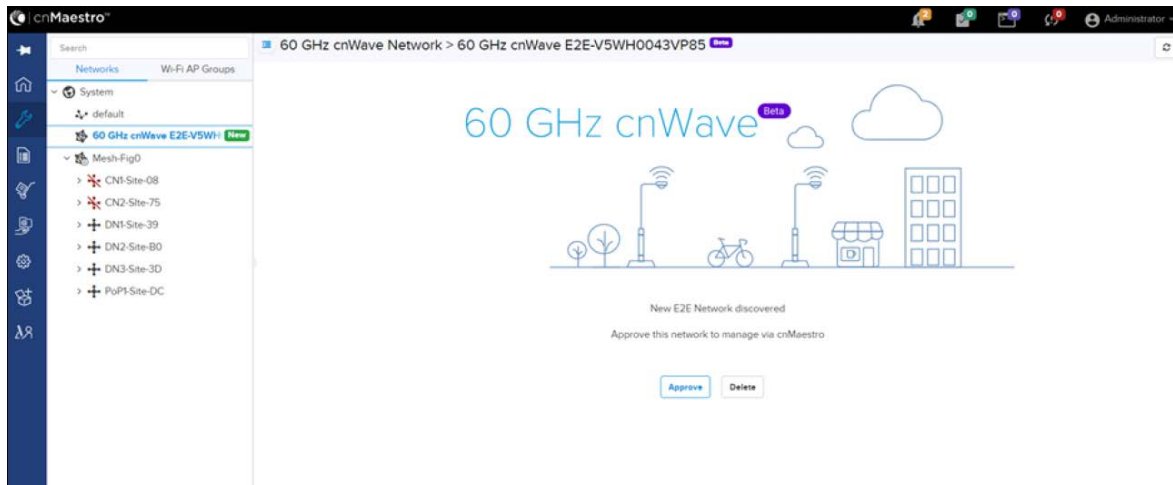
3. Enter the cnMaestro management configuration information.
 - Remote Management - Select the required remote management option
 - cnMaestro URL - cnMaestro address
 - Cambium ID - Cambium ID of the device
 - Onboarding key - Password to onboard the device

Figure 249: The cnMaestro section



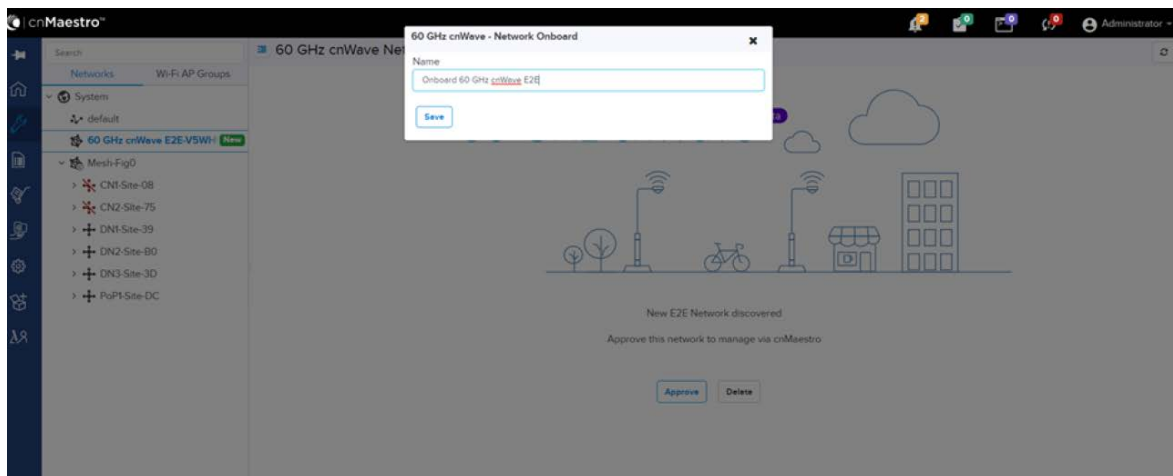
4. Click **Enable**.
5. A new E2E Network appears in cnMaestro. Click **Approve** to manage it.

Figure 250: Information on the new E2E network



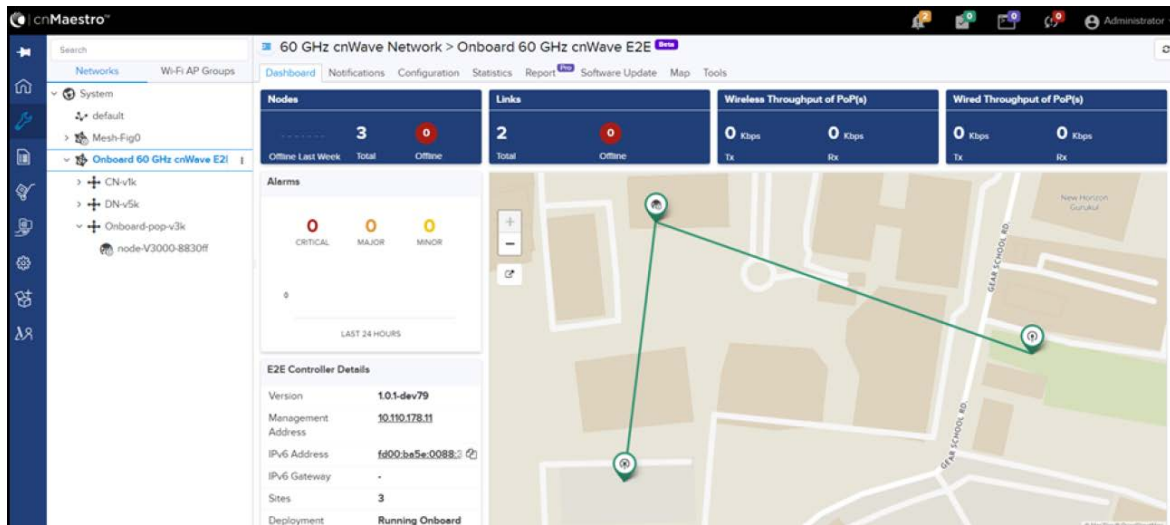
6. The **Network Onboard** window appears and provides an option to edit the network name.
7. Click **Save**.

Figure 251: The 60 GHZ cnWave - Network Onboard



After the successful onboarding of the E2E Network, it can be managed through cnMaestro.


Figure 252: The Onboard 60 GHz cnWave E2E dashboard page



Backup CN link

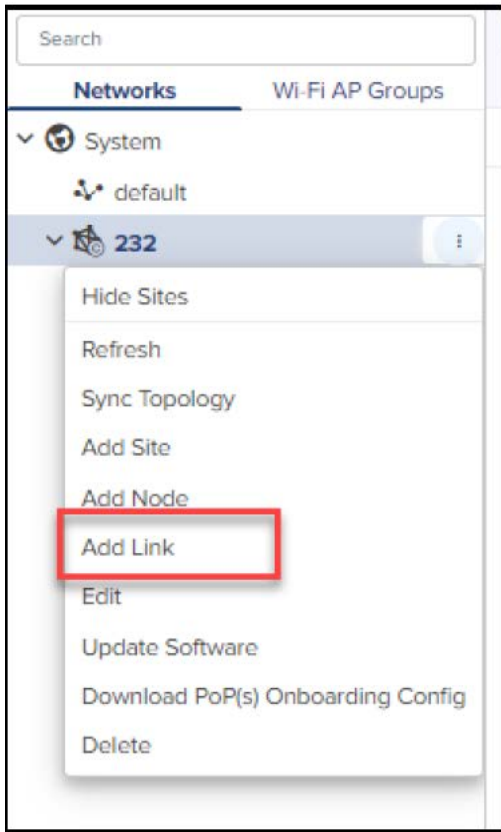
If a link between Pop or DN and CN gets disconnected, then a backup CN link (if enabled using the cnMaestro UI) provides connectivity from PoP or DN to a particular CN. CNs can form only one link but additional backup links can be provided for use when the primary link is unavailable (for at least 300 seconds).

To add and enable the backup CN link, perform the following actions:

1. From the landing page of the device UI, navigate to Networks > required link name and select the  icon.

A drop-down list appears with multiple options, as shown in [Figure 253](#).

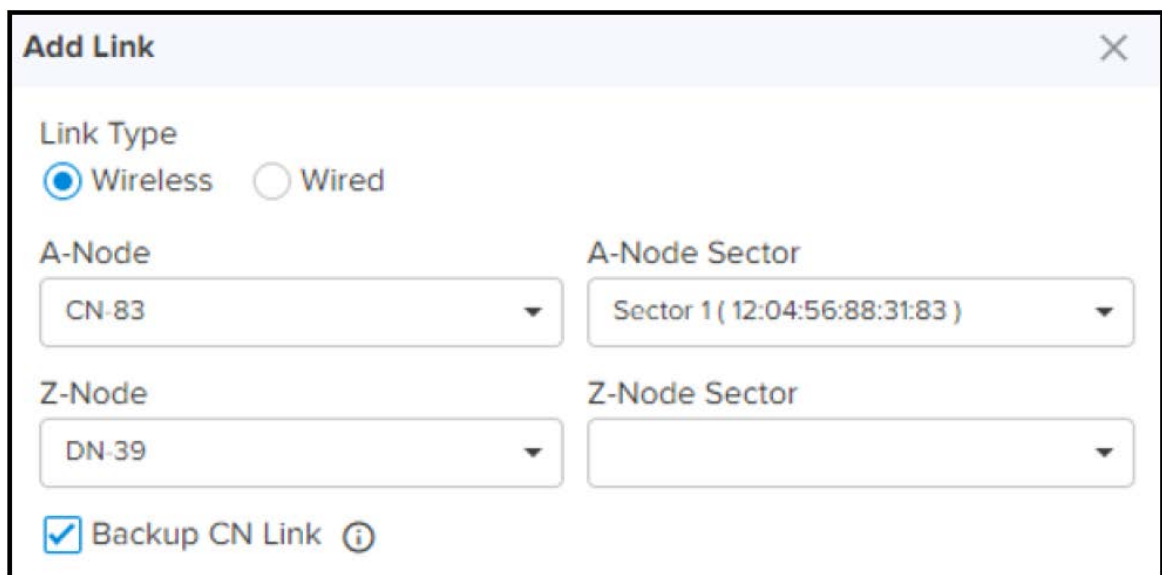
Figure 253: The drop-down list with the Add Link option



2. From the drop-down list, select **Add Link** as shown in Figure 253.

The **Add Link** page appears with the **Backup CN Link** checkbox, as shown in Figure 254.

Figure 254: The Backup CN Link checkbox

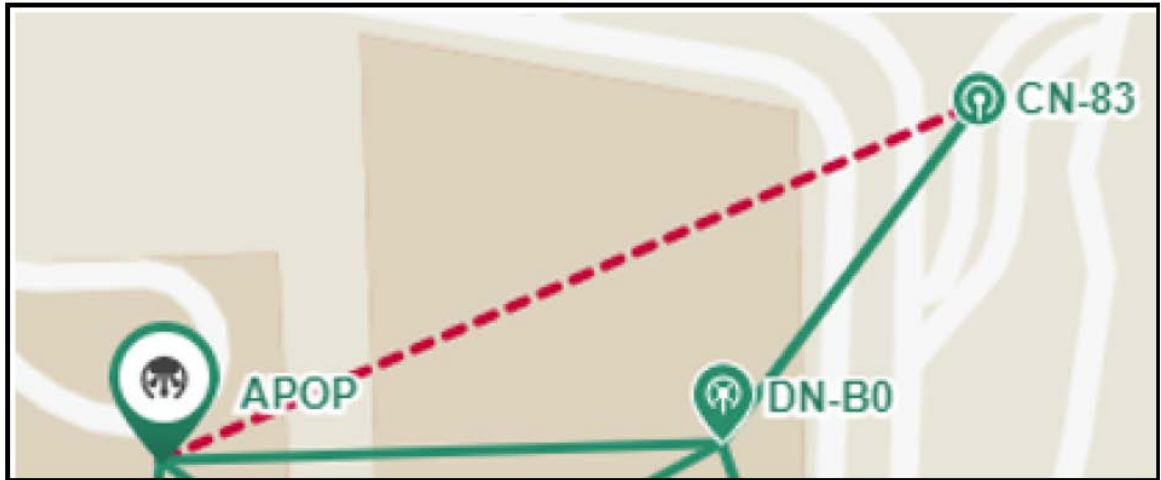


You must configure the required node-specific parameters, such as A-Node, A-Node Sector, and Z-Node, before enabling the backup CN link.

3. Select the **Backup CN Link** checkbox.

On the **Maps** page, backup CN links are shown in a dash line format (as shown in [Figure 255](#)).

Figure 255: Representation of the backup CN links on the Maps page



Auto Manage IPv6 Routes (External E2E Controller)

E2E Controller communicates with all nodes over IPv6. PoP nodes use IPv6 address of the statically configured interface to communicate with E2E Controller. CNs and DNs use the IPv6 address derived from Seed Prefix.



Note

The **Auto Manage Routes** feature requires cnMaestro 3.0.4.

The **Auto Manage Routes** feature adds and manages the IPv6 routes at E2E Controller. These IPv6 routes are required for routing the IPv6 packets to CNs and DNs.

The feature is applicable only when PoP and E2E Controller are in the same subnet.

Single PoP network

When the feature is disabled, you must add the IPv6 route by performing the following steps:

1. From the landing page of the device UI, navigate to **Tools > Settings > IPv6 Routes > Add new**.

The Add Route page appears, as shown in the [Figure 256](#).

Figure 256: The Add Route page in the cnMaestro UI



2. Type the seed prefix value in the **Destination** text box.
3. Type the required PoP's interface IP address in the **Gateway** text box.
4. Click **Add**.

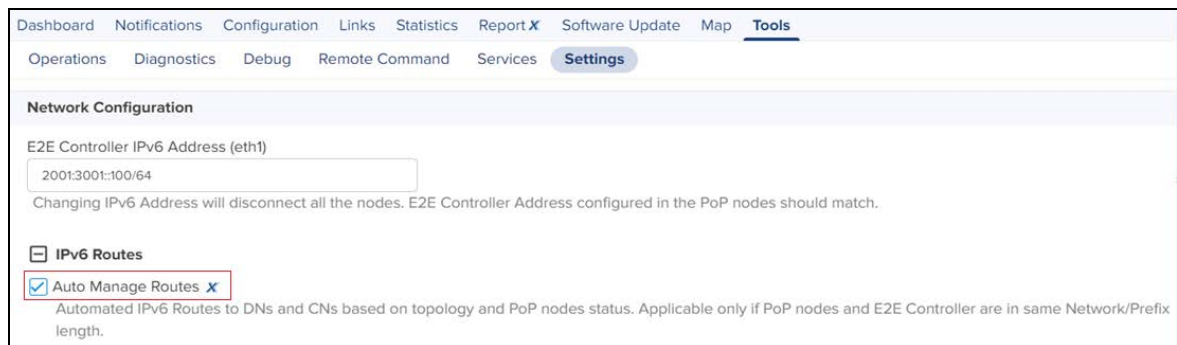
The IPv6 route is added.

When the feature is enabled, all the above steps (described from step 1 to step 5 in this section) are not required and IPV6 routes are added automatically.

5. Select the **Auto Manage Routes** check box in the IPv6 Routes page.

Figure 257 shows the location of the **Auto Manage Routes** check box in the IPv6 Routes page.

Figure 257: The Auto Manage Routes check box



Multi-PoP network

In a multi-PoP network, the **Auto Manage Routes** feature allows to avoid a BGP v6 router under the following conditions:

- When the Layer 2 bridge is enabled (which implies that the BGP v6 router is not required for managing data traffic).

- When PoPs and E2E Controller are in the same subnet or L2 broadcast domain.

In a multi-PoP network, Deterministic Prefix Allocation (DPA) is used. The mesh gets divided into zones. Each PoP is the best gateway to reach nodes in its zone. When a PoP is down, a different alive PoP must be used as a gateway to reach zones. When the **Auto Manage Routes** feature is enabled, it performs the following functions in a multi-PoP network:

- Understands the network topology of 60 GHz cnWave,
- Keeps a track of aliveness of PoPs, and
- Dynamically builds and manages the routing table.

Figure 258 is an example of an IPv6 route table that is built automatically by the feature for a four PoP network.

Figure 258: Example of IPv6 route entries in the IPv6 Routes page

Network Configuration

E2E Controller IPv6 Address (eth0)
 Changing IPv6 Address will disconnect all the nodes. E2E Controller Address configured in the PoP nodes should match.

IPv6 Routes

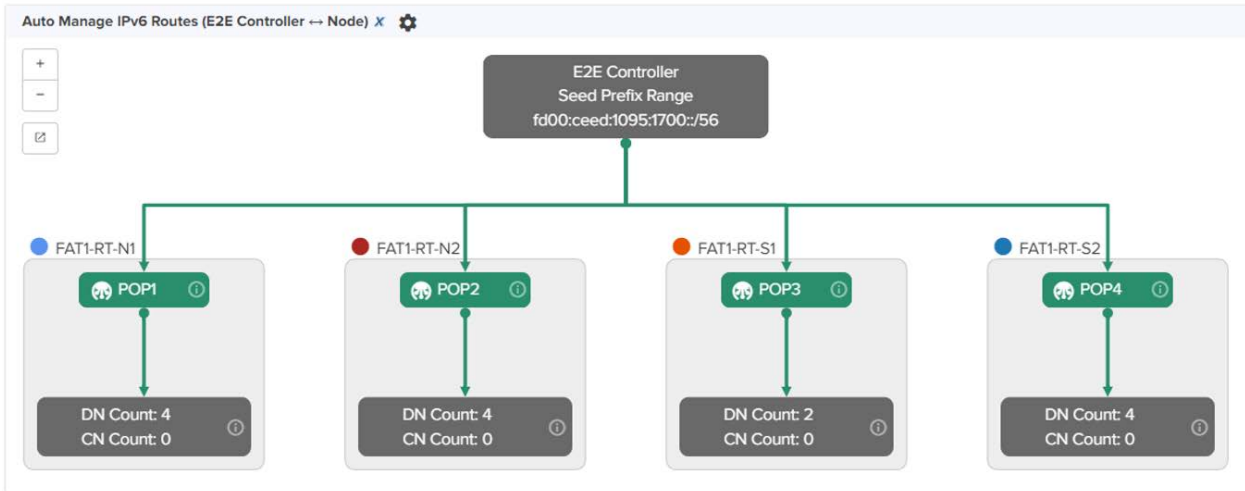
Auto Manage Routes ✕ Automated IPv6 Routes to DNS and CNs based on topology and PoP nodes status. Applicable only if PoP nodes and E2E Controller are in same Network/Prefix length.

Destination	Gateway	Type
fd00:ceed:1095:1700::/58	fd00:ba5e:6e57:3026:0:4:5688:4862	auto
fd00:ceed:1095:1740::/58	fd00:ba5e:6e57:3026:0:4:5688:4a3c	auto
fd00:ceed:1095:1780::/58	fd00:ba5e:6e57:3026:0:4:5688:4bca	auto
fd00:ceed:1095:17c0::/58	fd00:ba5e:6e57:3026:0:4:5688:48b0	auto
fd00:ceed:1095:1700::/56	fd00:ba5e:6e57:3026:0:4:5688:48b0	auto

Save

Figure 259 shows how the cnMaestro dashboard diagrammatically displays the routes taken by E2E Controller and the traffic controlled by cnWave nodes.

Figure 259: Diagrammatic representation of IPv6 routes and traffic control



Unconnected PoPs

In a multi-PoP network, PoPs must be able to exchange openR packets either on wired or wireless path. Otherwise, DNs might not receive the IPv6 address allocation and might not onboard to E2E Controller. This is observed when Controller sends the Prefix Allocation message to one of the PoPs and expects the message to reach other PoPs through openR.

In some cases, PoPs might be isolated temporarily, especially while building the network. Figure 260 is an example that shows two unconnected zones.

Figure 260: Unconnected zones due to isolated PoPs



To facilitate such a scenario, a new configuration parameter **flags.enable_pop_prefix_broadcast** has been introduced in this release. This parameter supports the following Boolean values:

- true - When the value of this parameter is set to true, E2E Controller sends the prefix allocation message to all PoPs individually.
- false -When the value of this parameter is set to false, E2E Controller sends the prefix allocation message to one of the PoPs.

The default value of this parameter is false (default setting).



Note

You must set this parameter’s flag to false when there is a wired or wireless path between PoPs.

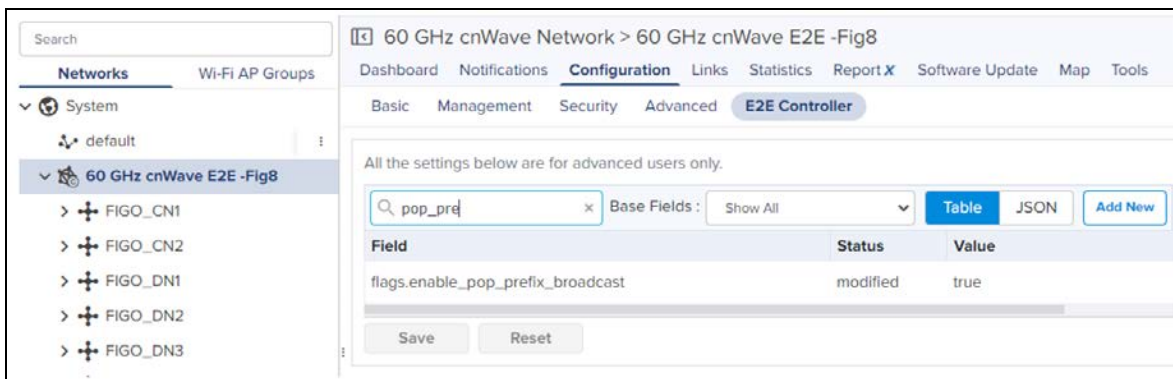
You can modify the **flags.enable_pop_prefix_broadcast** parameter in the UI of 60 GHz cnWave.

To configure the parameter, perform the following steps:

1. From the landing page of the device UI, navigate to **Configuration > E2E Controller**.

The E2E Controller page appears. The **flags.enable_pop_prefix_broadcast** parameter is available in the E2E Controller page, as shown in [Figure 261](#).

Figure 261: The flags.enable_pop_prefix_broadcast parameter



2. Modify the value of the parameter.
3. Click **Save** to save the configuration changes.

Regulatory Information

This chapter provides regulatory notifications.



Caution

Intentional or unintentional changes or modifications to the equipment must not be made unless under the express consent of the party responsible for compliance. Any such modifications could void the user's authority to operate the equipment and will void the manufacturer's warranty.



Attention

Les changements ou modifications intentionnels ou non intentionnels à l'équipement ne doivent pas être effectués sauf avec le consentement exprès de la partie responsable de la conformité. De telles modifications pourraient annuler l'autorisation de l'utilisateur à faire fonctionner l'équipement et annulera la garantie du fabricant.

The following topics are described in this chapter:

- Compliance with safety standards lists the safety specifications against which the 60 GHz cnWave family of ODUs has been tested and certified. It also describes how to keep RF exposure within safe limits.
- Compliance with radio regulations describes how the 60 GHz cnWave family of ODUs complies with the radio regulations that are in force in various countries.

Compliance with safety standards

This section lists the safety specifications against which the 60 GHz cnWave™ platform family is tested and certified. It also describes how to keep RF exposure within safe limits.

Electrical safety compliance

The 60 GHz cnWave platform family hardware is tested for compliance to the electrical safety specifications listed in following [Safety compliance specifications](#) table.

Table 62: Safety compliance specifications

Region	Specification
USA	UL 62368-1, UL 60950-22
Canada	CSA C22.2 No.62368-1, CSA C22.2 No. 60950-22
Europe	EN 62368-1, EN 60950-22
International	CB certified IEC 62368-1 Edition 2 IEC 60950 -22

Electromagnetic Compatibility (EMC) compliance

The EMC specification type approvals that are granted for 60 GHz cnWave platform family are listed in following table.

Table 63: EMC compliance

Region	Specification
USA	FCC Part 15 Class B
Canada	RSS Gen
Europe/International	EN 301 489-1 V2.2.3, EN 301 489-17 V3.2.4

Human exposure to radio frequency energy

Relevant standards (USA and EC) applicable when working with RF equipment are:

- ANSI IEEE C95.1-2005, IEEE Standard for Safety Levels with Respect to Human Exposure to Radio Frequency Electromagnetic Fields, 3 kHz to 300 GHz
- Council recommendation of 12 July 1999 on the limitation of exposure of the general public to electromagnetic fields (0 Hz to 300 GHz) (1999/519/EC) and respective national regulations
- *Directive 2013/35/EU - electromagnetic fields* of 26 June 2013 on the minimum health and safety requirements regarding the exposure of workers to the risks arising from physical agents (electromagnetic fields) (20th individual Directive within the meaning of Article 16(1) of Directive 89/391/EEC) and repealing Directive 2004/40/EC.
- US FCC limits for the general population. See the FCC web site at <http://www.fcc.gov>, and the policies, guidelines, and requirements in Part 1 of Title 47 of the Code of Federal Regulations, as well as the guidelines and suggestions for evaluating compliance in FCC OET Bulletin 65
- Health Canada limits for the general population. See the Health Canada web site at <https://www.canada.ca/en.html>.
- EN 62232: 2017 Determination of RF field strength, power density and SAR in the vicinity of radiocommunication base stations for the purpose of evaluating human exposure (IEC 62232:2017)
- EN 50385:2017 Product standard to demonstrate the compliance of base station equipment with radiofrequency electromagnetic field exposure limits (110 MHz - 100 GHz), when placed on the market
- ICNIRP (International Commission on Non-Ionizing Radiation Protection) guidelines for the general public. See the ICNIRP web site at <https://www.icnirp.org/cms/upload/publications/ICNIRPemfgdl.pdf> and Guidelines for Limiting Exposure to Time-Varying Electric, Magnetic, and Electromagnetic Fields.

Power density exposure limit

Install the radios for the 60 GHz cnWave platform family of wireless solutions to provide and maintain the minimum separation distances from all persons.

The applicable FCC power density exposure limit for RF energy in the 57 – 66 GHz frequency bands is 10 W/m². For more information, see [Human exposure to radio frequency energy](#).

Calculation of power density

The following calculation is based on the ANSI IEEE C95.1-1991 method, as that provides a worst-case analysis.

Peak power density in the far field of a radio frequency point source is calculated as follows:

$$S = \frac{P \cdot G}{4\pi d^2}$$

Where:

S: power density in W/m²

p: maximum average transmit power capability of the radio, in W

G: total Tx gain as a factor, converted from dB

d: distance from point source, in m

Rearranging terms to solve for distance yields:

$$d = \sqrt[3]{P \cdot G / 4\pi S}$$

Calculated distances and power compliance margins

The following table displays recommended calculated separation distances, for the 60 GHz cnWave™ for Europe the USA and Canada. These are conservative distances that include compliance margins.



Note

Les tableaux suivants indiquent les distances de séparation recommandées calculées pour le cnWave™ 60 GHz pour l'Europe, les États-Unis et le Canada. Ce sont des distances prudentes qui incluent des marges de conformité.

At these and greater separation distances, the power density from the RF field is below generally accepted limits for the general population.



Note

À ces distances de séparation et à des distances supérieures, la densité de puissance du champ RF est inférieure aux limites généralement acceptées pour la population générale.

60 GHz cnWave™ Platform Family ODU adheres to all applicable EIRP limits for transmit power when operating in MIMO mode. Separation distances and compliance margins include compensation for the antenna configuration of each product.



Note

L'ODU de la famille de plates-formes cnWave™ 60 GHz respecte toutes les limites EIRP applicables pour la puissance de transmission lors d'un fonctionnement en mode MIMO. Les distances de séparation et les marges de conformité incluent la compensation de la configuration d'antenne de chaque produit.

Table 64: Calculated distances and power compliance margins

Product	Countries	EIRP (dBm)	EIRP (W)	Maximum power density (W/m ²)	Compliance distance (m)
V1000	USA, Canada, EU	38	6.3	10	0.22
V2000	USA, Canada, EU	49	79.4	10	0.9
V3000	USA, Canada	60.5	1122	10	3.0
V3000	EU	55	316.2	10	1.6
V5000	USA, Canada, EU	38	6.3	10	0.22



Note

The regulations require that the power used for the calculations is the maximum power in the transmit burst subject to allowance for source-based time-averaging.

The calculations above are based upon platform maximum EIRP and worst case 100% duty cycle.



Remarque

Les réglementations exigent que la puissance utilisée pour les calculs soit la puissance maximale de la rafale d'émission sous réserve de la moyenne temporelle basée sur la source.

Les calculs ci-dessus sont basés sur la PIRE maximale de la plate-forme et le pire des cas, un cycle de service de 100%.

Compliance with radio regulations

This section describes how the 60 GHz cnWave platform family complies with the radio regulations that are in force in various countries.



Caution

Where necessary, the end user is responsible for obtaining any national licenses required to operate this product and these must be obtained before using the product in any particular country. Contact the appropriate national administrations for details of the conditions of use for the bands in question and any exceptions that might apply.



Attention

Le cas échéant, l'utilisateur final est responsable de l'obtention des licences nationales nécessaires pour faire fonctionner ce produit. Celles-ci doivent être obtenus avant d'utiliser le produit dans un pays particulier. Contactez les administrations nationales concernées pour les détails des conditions d'utilisation des bandes en question, et toutes les exceptions qui pourraient s'appliquer.



Caution

Changes or modifications not expressly approved by Cambium Networks could void the user's authority to operate the system.



Attention

Les changements ou modifications non expressément approuvés par les réseaux de Cambium pourraient annuler l'autorité de l'utilisateur à faire fonctionner le système.

Type approvals

The system is tested against various local technical regulations and found to comply. The [Radio specifications](#) section lists the radio specification type approvals that is granted for the 60GHz cnWave products.

Some of the frequency bands in which the system operates are "license exempt" and the system is allowed to be used provided it does not cause interference. In these bands, the licensing authority does not guarantee protection against interference from other products and installations.

Region	Regulatory approvals	FCC ID	IC ID
USA	Part 15C	QWP-60V1000 QWP-60V2000 QWP-60V3000 QWP-60V5000	-
Canada	ISED RSS-210	-	109AO-60V1000 109AO-60V2000 109AO-60V3000 109AO-60V5000

Federal Communications Commission (FCC) compliance

The 60 GHz cnWave V1000, V2000, V3000 and V5000 comply with the regulations that are in force in the USA.



Caution

If this equipment does cause interference to radio or television reception.

FCC Notification

This device complies with part 15C of the US FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) This device must accept any interference received, including interference that may cause undesired operation.

Innovation, Science and Economic Development Canada (ISED) compliance

The 60 GHz cnWave V1000, V2000, V3000 and V5000 comply with the regulations that are in force in Canada.



Caution

If this equipment does cause interference to radio or television reception.



Attention

Si cet équipement cause des interférences à la réception radio ou télévision.

60 GHz cnWave example product labels

Figure 262: 60 GHz cnWave™ V5000 Distribution Node











Model No/HVIN:V5000  Part No:C600500A004A  SERIAL NO (MSN):#####  MAC (ESN):##### 	 Cambium Networks™ Ashburton, TQ13 7UP, UK 60GHz cnWave V5000 Distribution Node VIN: 42.5-57V  IMAX: 1.41A E112443 COMPLIES WITH UL62368-1 / CSA C22.2 No. 62368-1-14 UL60950-22 / CSA C22.2 No. 60950-22-17	IP66/67
<p>This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation</p> <p>IMPORTANT: See the System User Guide before connecting to AC Power. The Guide is available online at www.cambiumnetworks.com/guides</p> MADE IN CHINA X-SZHO-H	FCC ID: QWP-60V5000 IC: 109AO-60V5000   	

Figure 263: 60 GHz cnWave™ V3000 Client Node Radio only











<p>Model No/HVIN:V3000  Part No:C600500C024A  SERIAL NO (MSN):#####  MAC (ESN):##### </p>	<p> Cambium Networks™ Ashburton, TQ13 7UP, UK 60GHz cnWave V3000 Client Node Radio Only VIN: 42.5-57V  IMAX:1.29A E112443 COMPLIES WITH UL62368-1 / CSA C22.2 No. 62368-1-14 UL60950-22 / CSA C22.2 No. 60950-22-17</p>	<p>IP66/67</p>
<p>This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation</p> <p>IMPORTANT: See the System User Guide before connecting to AC Power. The Guide is available online at www.cambiumnetworks.com/guides</p> <p>MADE IN CHINA X-SZHO-H</p>	<p>FCC ID: QWP-60V3000 IC: 109AO-60V3000</p> <p>  </p>	<p></p>

Figure 264: 60 GHz cnWave™ V2000 Client Node with no power cord




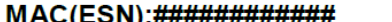







<p>Model No/HVIN:V2000  Part No:C600500C030A  Serial No(MSN):#####  MAC(ESN):##### </p>	<p> Cambium Networks™ Ashburton, TQ13 7UP, UK 60GHz cnWave V2000 Client Node no power supply no power cord VIN: 42.5-57V  IMAX: 1.38A E112443 COMPLIES WITH UL 62368-1 / CSA C22.2 No. 62368-1</p>	
<p>This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation</p> <p>CAUTION: Read the User Guide before Installation ATTENTION : Lisez le Guide de l'utilisateur avant l'Installation. The Guide is available online at www.cambiumnetworks.com/guides</p> <p>MADE IN CHINA X-SZHO-H IP66/67</p>	<p>FCC ID: QWP-60V2000 IC: 109AO-60V2000</p> <p>   </p>	<p></p>

Figure 265: 60 GHz cnWave™ V1000 Client Node with no cord

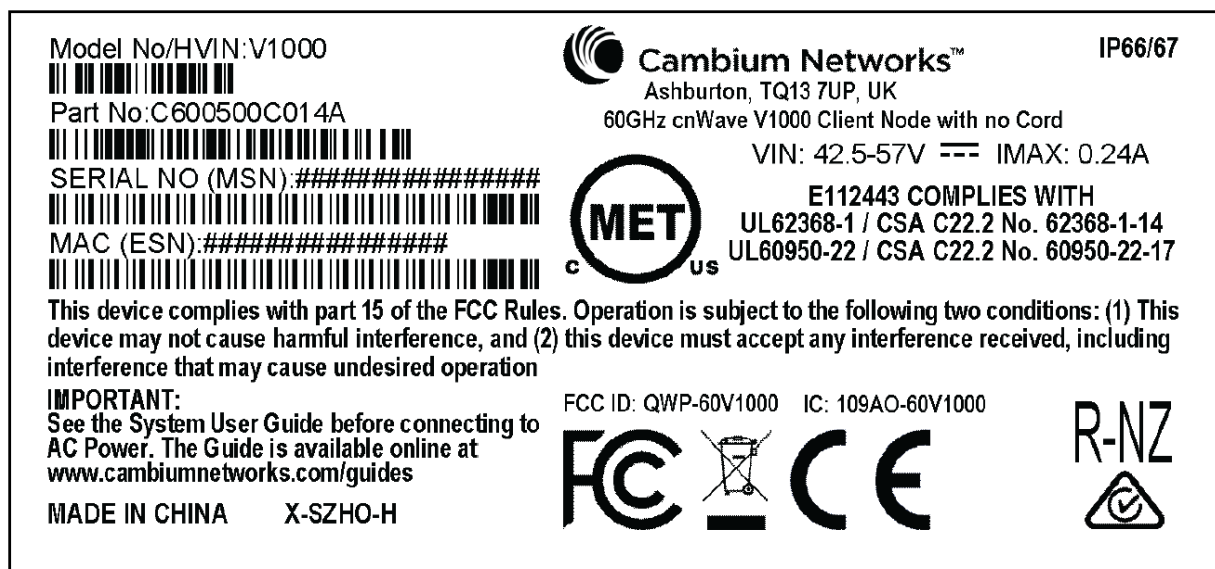


Figure 266: 60 GHz cnWave™ V1000 with US cord

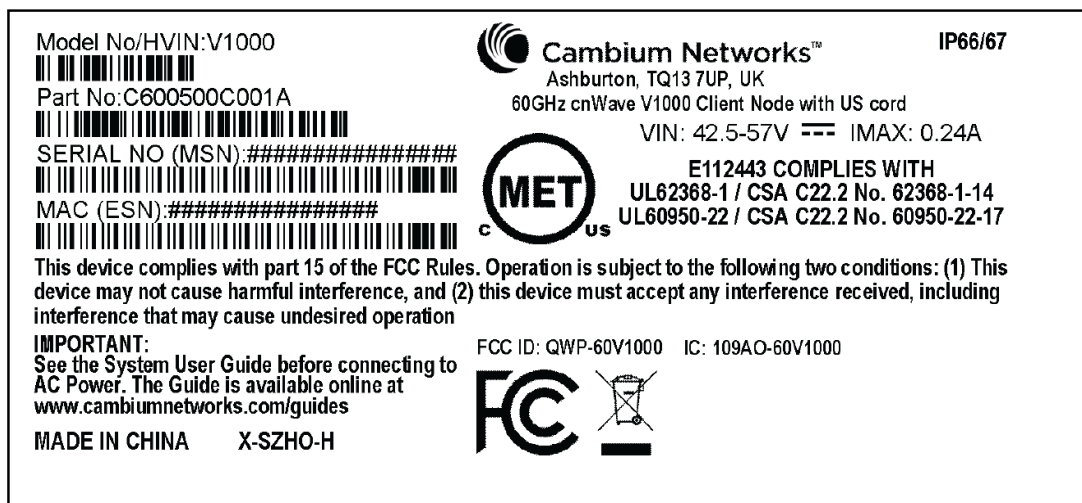


Table 65: Details of accessories, radio nodes, and part numbers

Accessories	Radio nodes	Cambium Part Number
60 GHz cnWave™ V5000 Distribution Node	V5000	C6000500A004A
60 GHz cnWave™ V3000 Client Node radio only	V3000	C600500C024A
60GHz cnWave V2000 Client Node no power supply, no power cord	V2000	C600500C030A
60 GHz cnWave™ V1000 Client Node with no cord	V1000	C600500C14A
60 GHz cnWave™ V1000 with US cord	V1000	C600500C001A

Troubleshooting

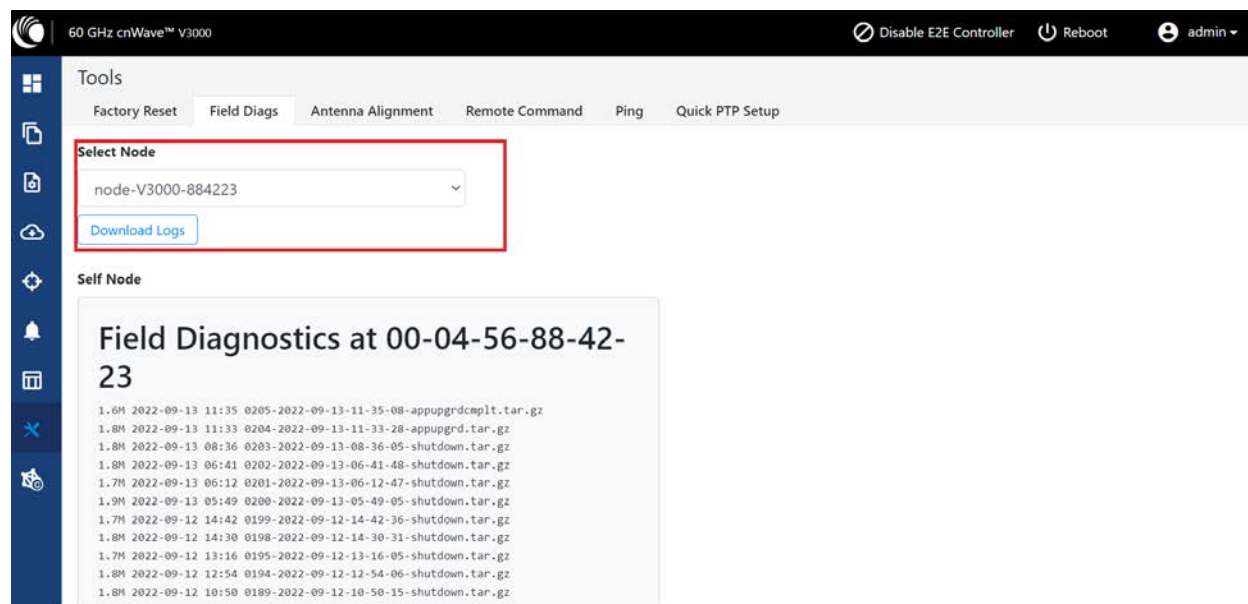
This section describes the troubleshooting steps and addresses frequently asked questions related to 60 GHz cnWave product deployment.

- [Field diagnostics logs](#)
- [Setup issues in IPv4 tunneling](#)
- [Link is not established](#)
- [PoP not online](#)
- [Link is not coming up](#)
- [Link is not having expected throughput performance](#)
- [Factory reset](#)

Field diagnostics logs

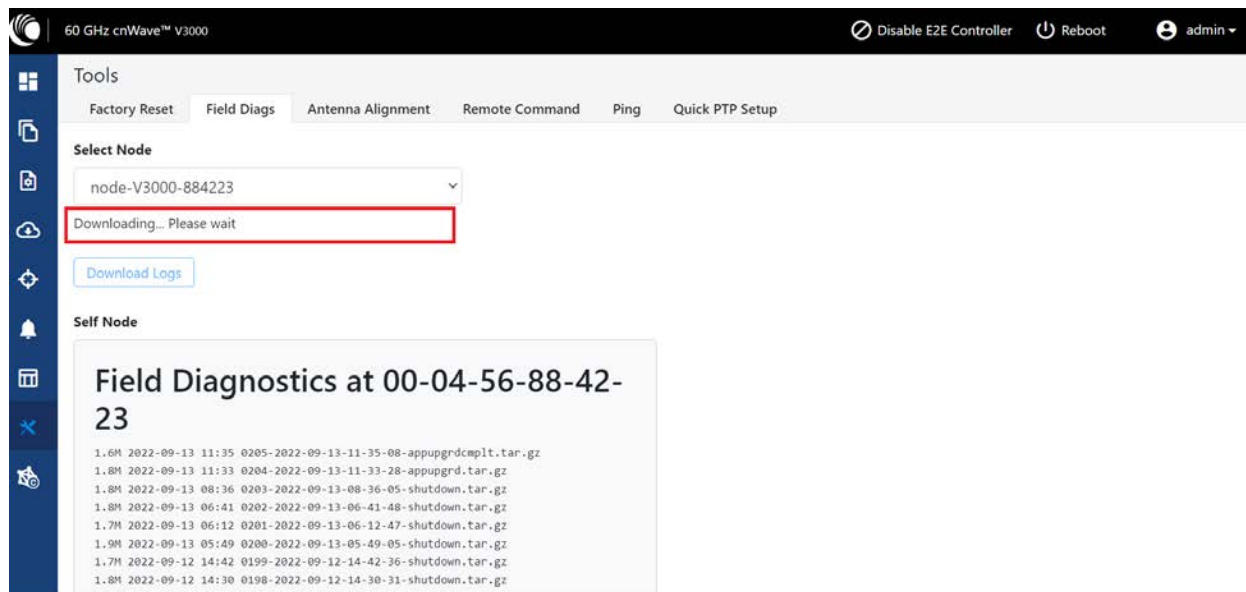
Download the logs to view more information about the error. To download the error logs select the node from the drop-down and click **Download Logs**.

Figure 267: The Logs tab in the Tools page



On clicking **Download Logs**, the status for download is displayed.

Figure 268: Downloading the logs

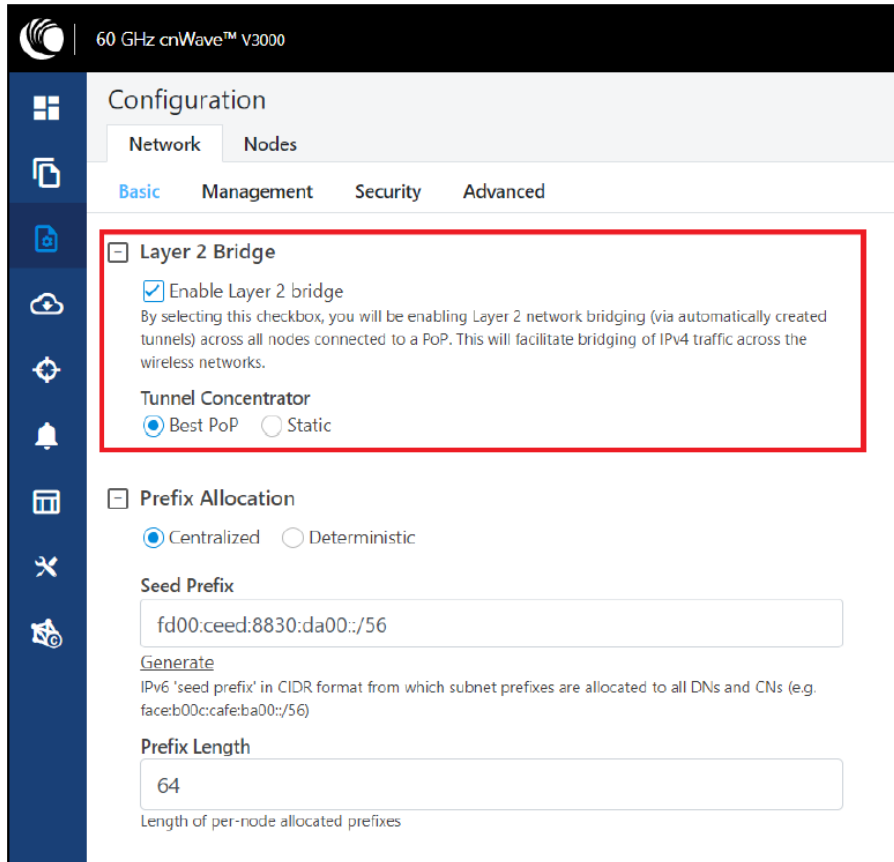


To download the logs for a self node, click **Download Logs** at the bottom and save the log file.

Setup issues in IPv4 tunneling

In IPv4 tunneling, if setup issues occur then perform the below steps:

1. Click **Configuration** on the left pane, navigate to **Network > Basic > Layer 2 Bridge** and verify **Enable Layer 2 bridge** is selected.



2. On the same page under **Configuration Management**, verify **E2E Managed Config** is selected.

60 GHz cnWave™ v3000

Configuration

Network Nodes

Basic Management Security Advanced

This configuration is used by the controller for auto config override. Channels set manually ignore this configuration.

DNS

DNS Servers

DNS server list, comma separated. IPv4 is only supported when Layer 2 bridge is enabled.

Time

Time Zone

NTP Servers

NTP Server hostnames or IP addresses, comma separated. IPv4 is only supported when Layer 2 bridge is enabled.

Configuration Management

E2E Managed Config
Determines whether the controller should manage the node's configuration.

3. Click **Configuration > Nodes > PoP DN > Networking > Layer 2 Bridge** and verify **Disable Broadcast Flood** and **Disable IPv6** are disabled.

60 GHz cnWave™ v5000

Disable E2E Controller Reboot admin

Configuration

Network Nodes

Search

node-V3000-884223 v2k_cn

Radio Networking VLAN Security Advanced

Submit Cancel

Ethernet Ports

Enable Main

Enable Aux

Enable SFP

Layer 2 Bridge

Disable Broadcast Flood
Broadcast packets (except DHCP Offer and DHCP Ack) in the downlink direction including client to client packets will be dropped.

Disable Unknown Unicast Flood

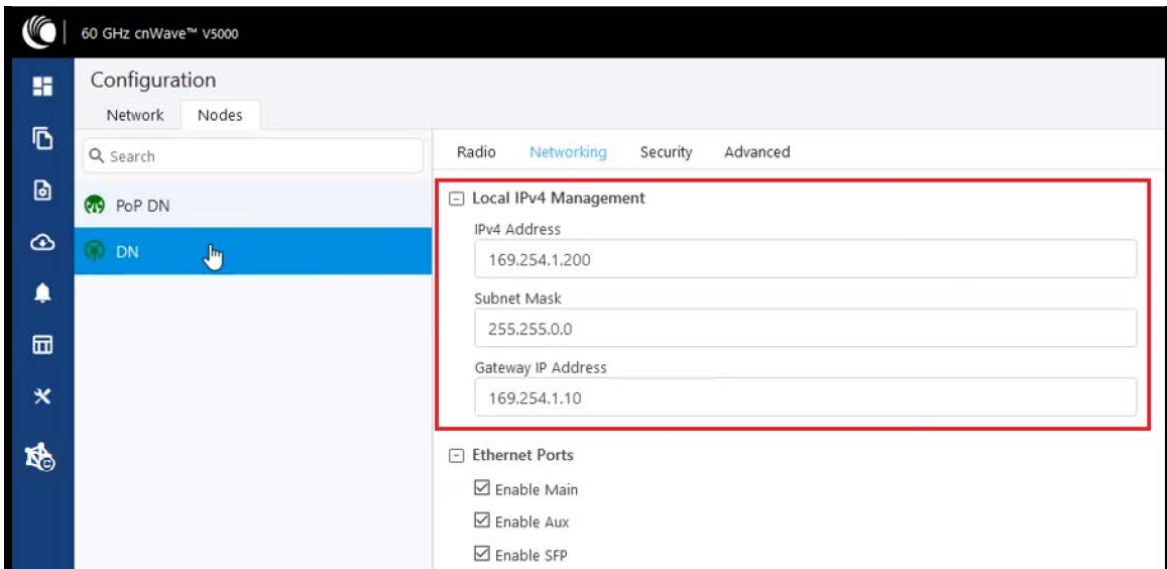
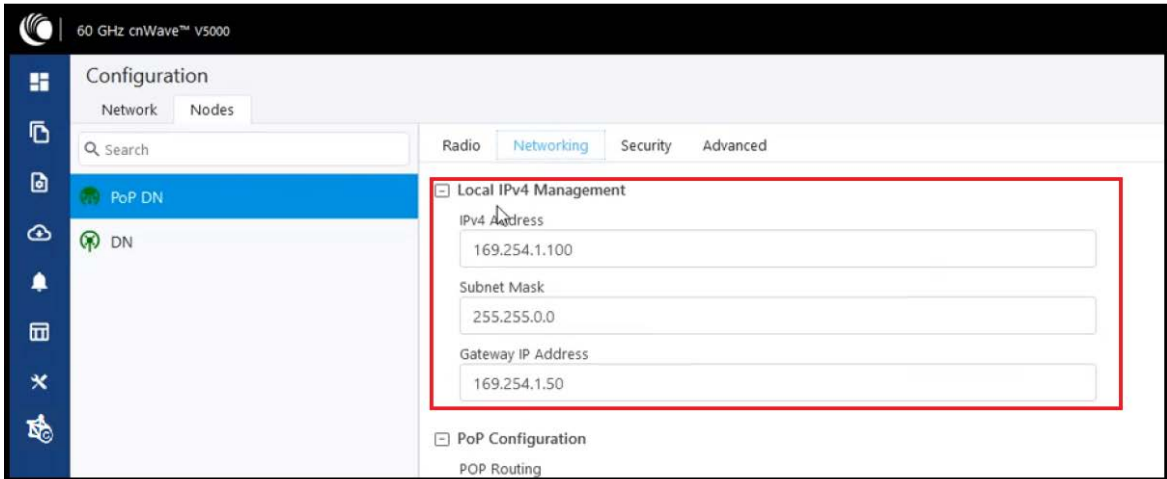
Disable IPv6

Monitor PoP Interface
Layer 2 tunnels will failover to next best PoP when the backhaul interface of this PoP is down. The configuration is applicable when static routing is used and IPv4 gateway is configured.

DHCP Option 82

Enabled Disabled

4. Ensure that PoP DN and DN's are in the same subnet and verify gateway is correct.

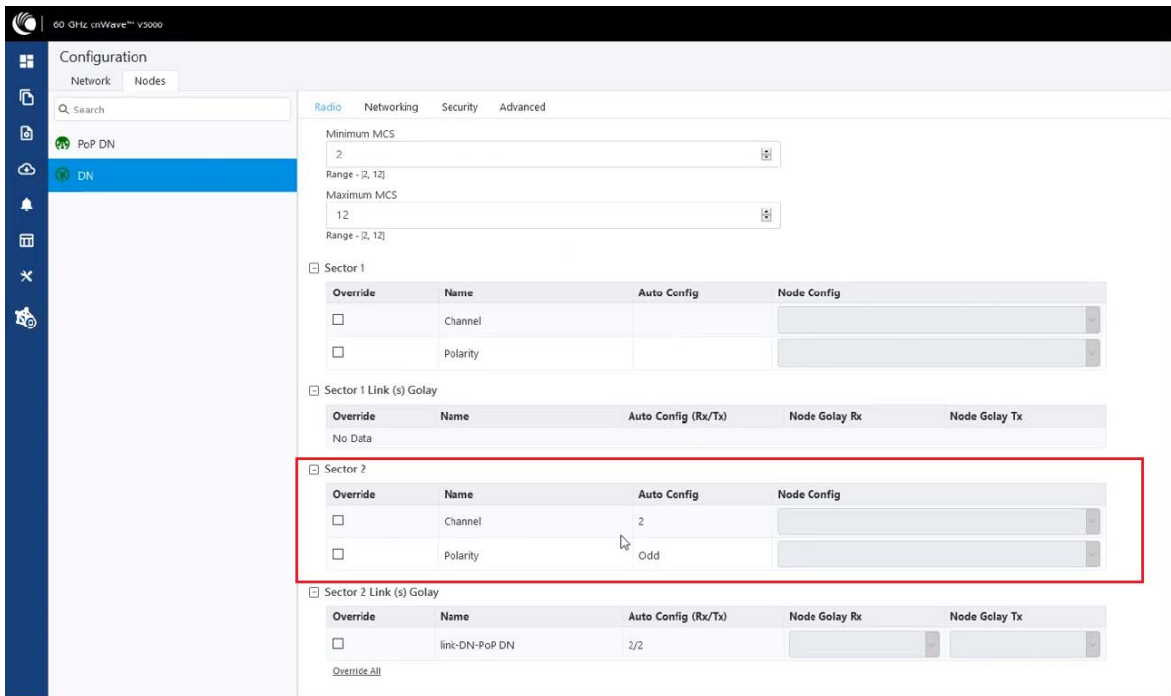


Link is not established

If link is not established between the nodes, then verify the below options:

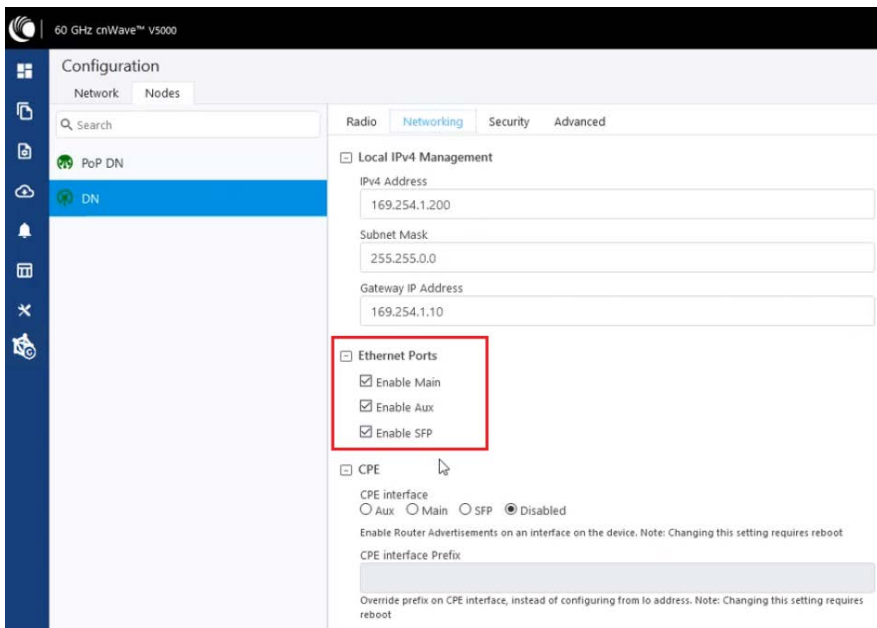
1. Click **Configuration** on the left navigation pane of the home UI page.
2. Navigate to **Nodes > Radio**. Verify Sector 2 PoP DN and DN's polarities, frequency, and Golay codes.

Figure 269: The Sector 2 section in the Radio page



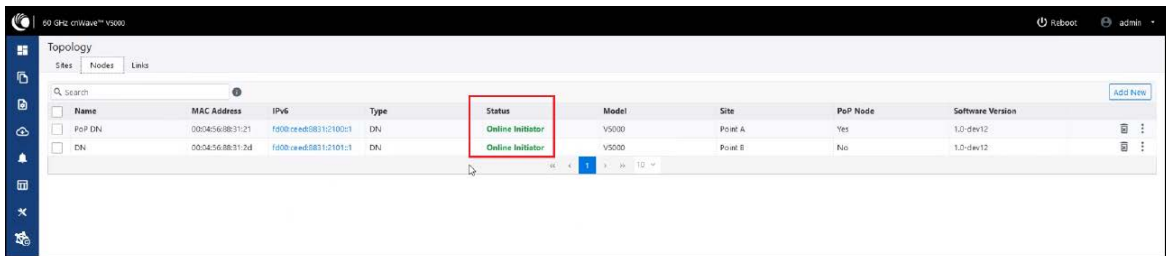
3. Select DN > **Networking** > **Ethernet Ports** and ensure that specific Ethernet ports are enabled.

Figure 270: The Ethernet Ports section in the Networking page



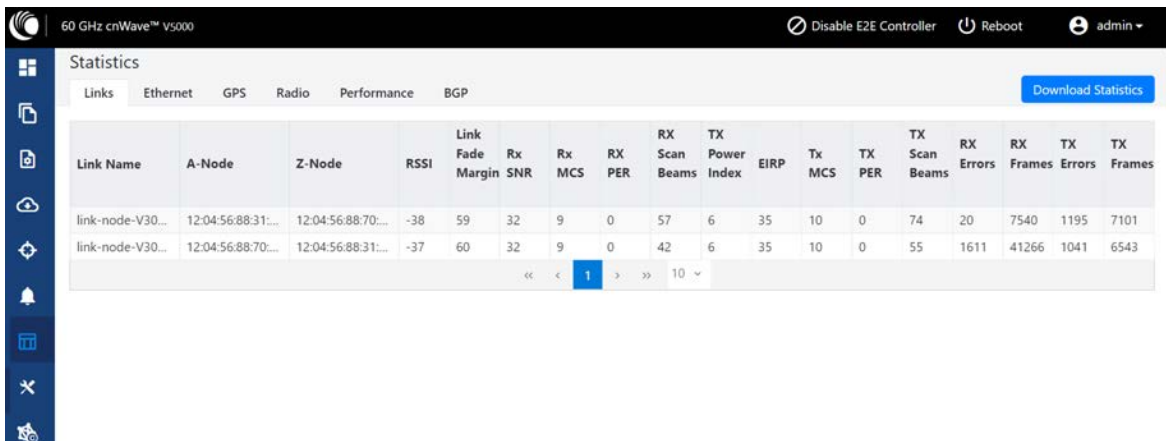
4. From the left navigation pane, navigate to **Topology** > **Nodes** and verify the Status is **Online Initiator**.

Figure 271: Status of nodes in the Topology page



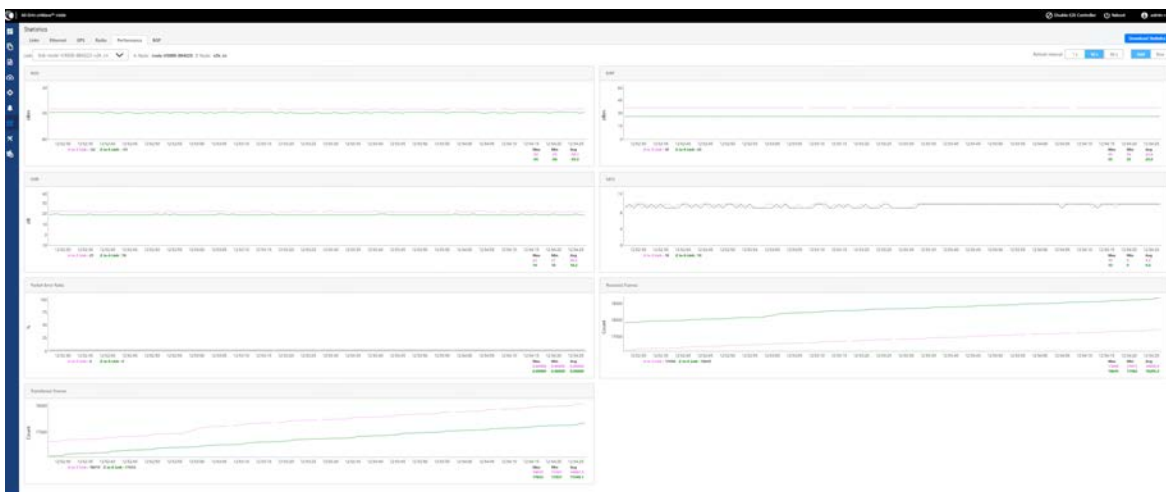
- From the left navigation pane, go to **Statistics** > **Links** and verify **RSSI**, **MCS**, and **TX Power Index**.

Figure 272: Link details in the Statistics page



- Go to **Performance** and verify the graphs.

Figure 273: Graphs in the Performance page



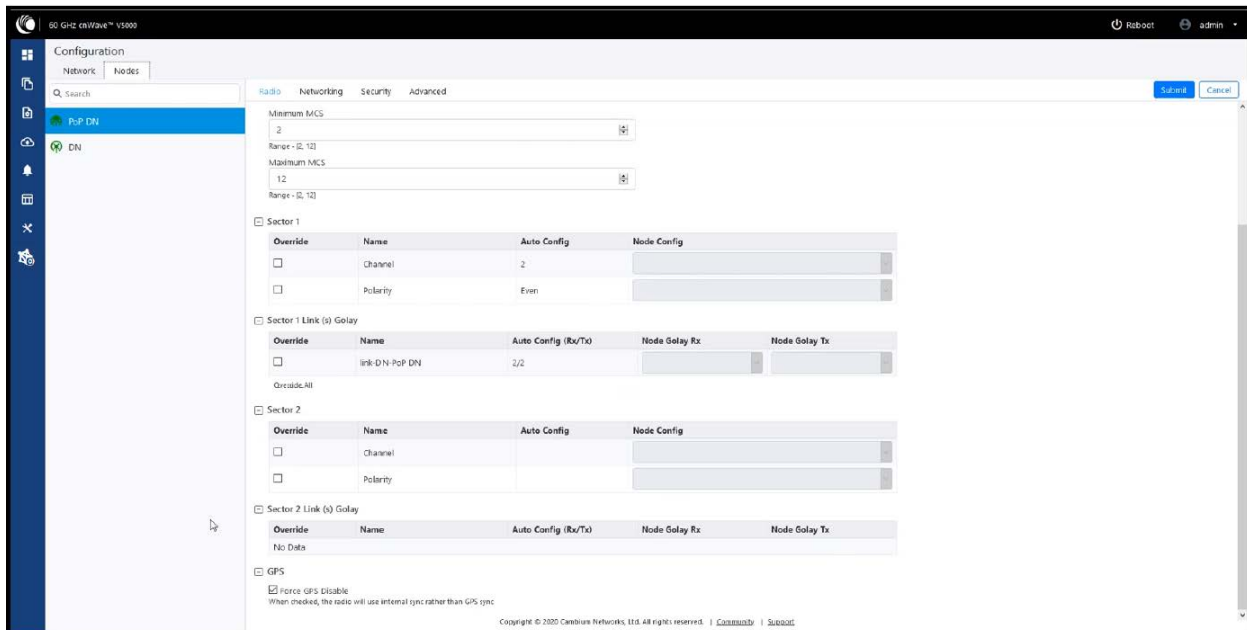
7. Go to **Radio** and monitor the throughput capacity.

Figure 274: Monitoring the throughput in the Radio page

Device Name	MAC Address	Sync Mode	Channel	Security	Error Association	Channel Last State	RX Throughput	TX Throughput
POP DN	1204568B3121	RF	2	None	0	0	7.86 kbps	1.63 kbps
POP DN	2204568B3121	RF	1	None	0	0	0 kbps	0 kbps
DN	1204568B312d	RF	1	None	0	0	0 kbps	0 kbps
DN	2204568B312d	RF	2	None	0	0	0.69 kbps	4.68 kbps

8. If internal GPS is used, then verify **Configuration > Nodes > Radio > GPS > Force GPS Disable** is enabled.

Figure 275: Verifying the Force GPS Disable check box



PoP not online from E2E or cnMaestro UI

This usually means that the PoP node is not able to talk to the E2E controller. Ensure that the PoP node has the E2E IPv6 configured properly. Also ensure that there is a route between the E2E controller and the PoP node, if they are not in the same VLAN. Try to ping the E2E from the PoP node (by logging in to SSH).

Link is not coming up

1. Ensure that the two ends of the radios can see each other (clear line of sight in between). If the link is using V3000, ensure that they are properly aligned.
2. Ensure that the MAC address of the radios is configured correctly in the E2E Controller.
3. Ensure that GPS sync is not enabled if indoor and ensure that GPS sync is enabled if outdoor.

4. Ensure that both ends of the link have the same software version.
5. Ensure to configure country code on the E2E GUI.
6. Ensure that the two ends of the link use opposite polarity and Golay codes that matches each other.
7. Ensure that the remote ends can reach the E2E Controller - IPv6 configuration (if beamforming is successful but the remote end cannot reach back to the E2E Controller, the E2E Controller/cnMaestro GUI displays link status as up, but the remote radio is offline).
8. If you already have experience in setting up a link and you are trying to set up a daisy chain, ensure that there is no any interference caused by the existing link. Example: Make sure that the two neighboring links use different Golay code.

Link does not come up after some configuration change

There is a possibility that the remote unit could be in a state that it uses different channel/Golay code/polarity from the near-end unit. Try to factory default the remote radio if possible.

On the E2E Controller/cnMaestro, it shows that the link is up, but the remote radio is NOT online - This means that link is established but the remote end radio cannot reply to the E2E Controller. Check the E2E configuration to make sure that the IPv6 default gateway is configured correctly to allow a route between the E2E controller and the remote radio.

Link is not having expected throughput performance

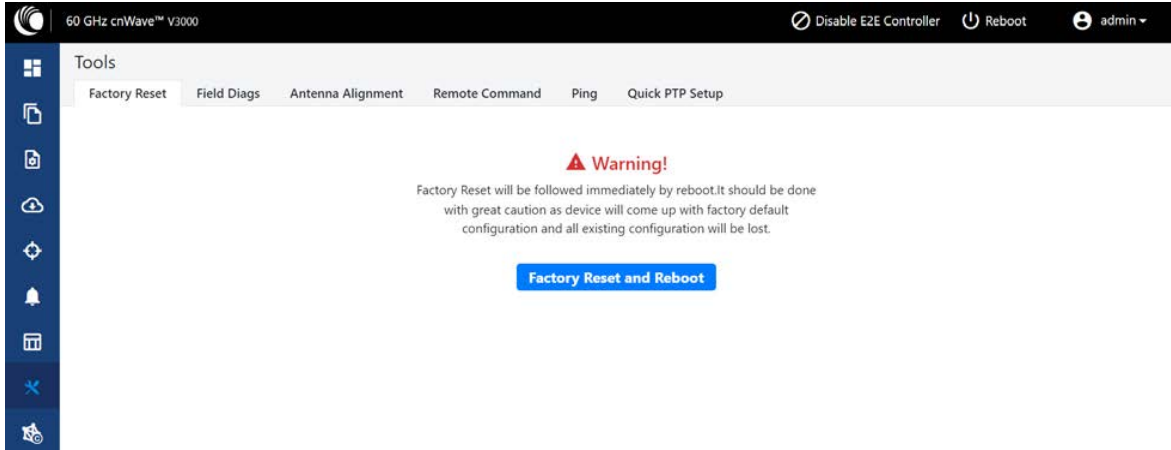
- Check the radio GUI to ensure that the link is running as the expected MCS mode when user data is passing through.
- Check to ensure that the Ethernet ports of the radios and the testing devices are negotiated to expected data rate (10Gbps).
- Ensure that your testing devices are capable of handling the throughput - run data throughput test by bypassing the radio link.
- Do not use radio internal iperf tool to test throughput.

Factory reset

Recovery mode is used to reset the configuration to the factory settings. To reset the configuration, perform the following steps:

1. From the main home page, navigate to **Tools > Factory Reset**.

The **Factory Reset** page appears, as shown in the following figure:

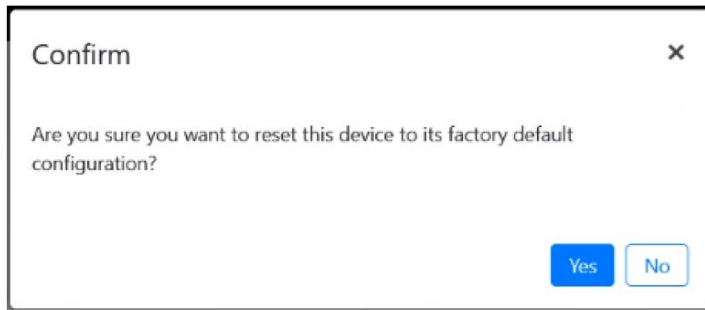


Warning

Factory reset is followed immediately by a system reboot. You must carefully configure the factory reset settings as the device comes up with the default settings. All the existing configurations are lost when the system comes up.

2. Click **Factory Reset and Reboot**.

The **Confirm** message box appears, as shown in the following figure:



3. Click **Yes** to confirm on the factory reset of the system.

The system reboots immediately following the factory reset.

4. When the reboot is complete, access the device using **169.254.1.1** (IP address).



Note

After factory reset, all configurations are set to default mode.

Cambium Networks

Cambium Networks delivers wireless communications that work for businesses, communities, and cities worldwide. Millions of our radios are deployed to connect people, places and things with a unified wireless fabric that spans multiple standards and frequencies of fixed wireless and Wi-Fi, all managed centrally via the cloud. Our multi-gigabit wireless fabric offers a compelling value proposition over traditional fiber and alternative wireless solutions. We work with our Cambium certified ConnectedPartners to deliver purpose built networks for service provider, enterprise, industrial, and government connectivity solutions in urban, suburban, and rural environments, with wireless that just works.

Installation and User Guides	http://www.cambiumnetworks.com/guides
Technical training	https://learning.cambiumnetworks.com/learn
Support website (enquiries)	https://support.cambiumnetworks.com
Main website	http://www.cambiumnetworks.com
Sales enquiries	solutions@cambiumnetworks.com
Warranty	https://www.cambiumnetworks.com/support/standard-warranty/
Telephone number list to contact	http://www.cambiumnetworks.com/contact-us/
Address	Cambium Networks Limited, Unit B2, Linhay Business Park, Eastern Road, Ashburton, Devon, TQ13 7UP United Kingdom



Cambium Networks and the stylized circular logo are trademarks of Cambium Networks, Ltd. All other trademarks are the property of their respective owners.

© Copyright 2023 Cambium Networks, Ltd. All rights reserved.