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 176: *The OCB section in the Networking page*
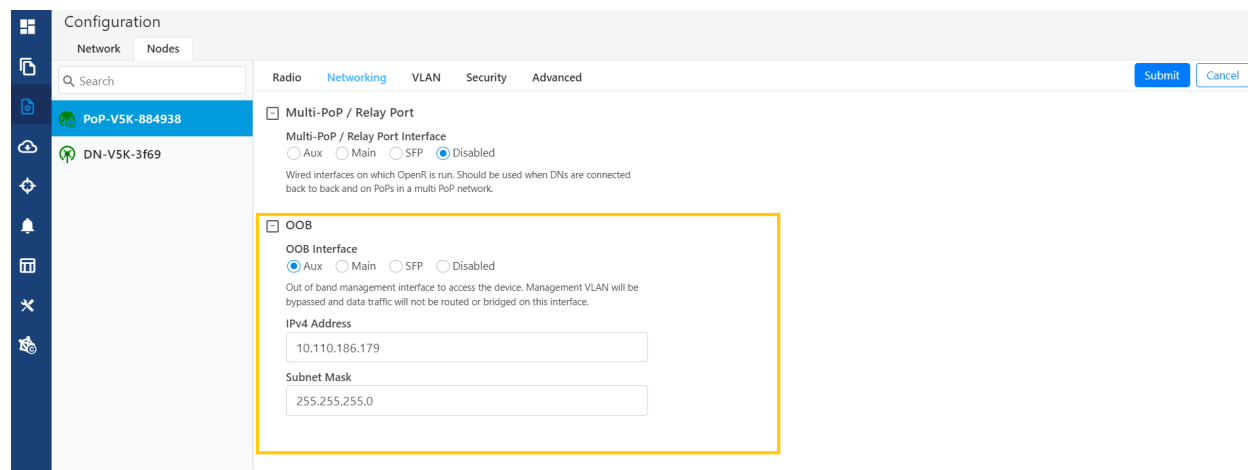
Enabling the DHCP Option 82 feature

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. 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 177.

    Figure 177: *The DHCP Option 82 feature*
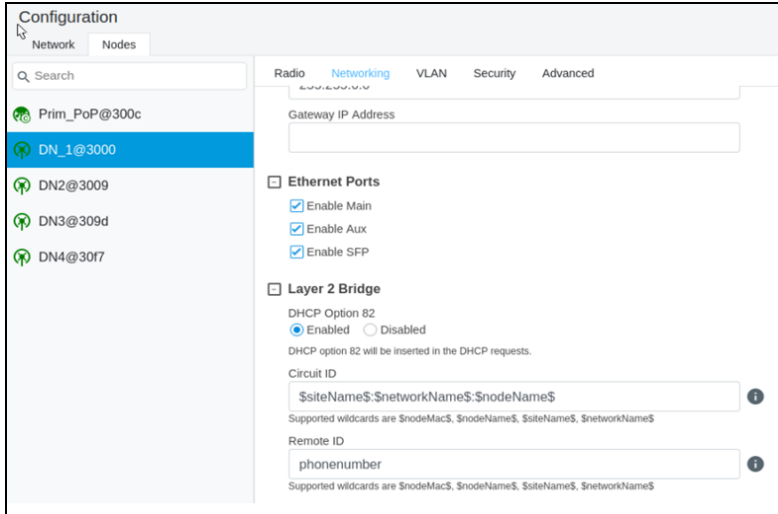
    The enabled status of **DHCP Option 82** implies that the feature is activated.

2. Type appropriate values in **Circuit ID** and **Remote ID** text boxes.

3. To save the configuration, click **Submit**.

Configuring Monitor PoP Interface

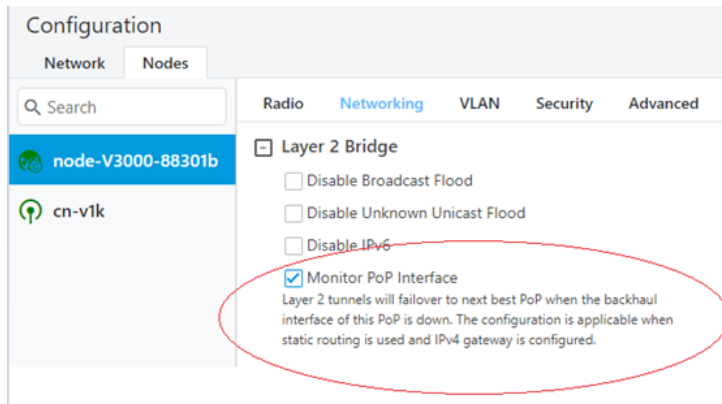The **Monitor PoP Interface** feature is applicable to static routing and Layer 2 bridge.

When the feature is enabled, the PoP interface is monitored. If the PoP interface is down, tunnels move to the next best PoP (which is best available). When there is no activity on the PoP interface, an attempt to reach the IPv4 gateway is made. Therefore, the IPv4 gateway configuration is necessary to activate this feature.

To configure the **Monitor PoP Interface** feature, perform the following steps:

1. Select **Nodes** > **Networking** in the home page.

    The **Networking** page appears. The **Monitor PoP Interface** check box is available in the Layer 2 Bridge section, as shown in Figure 178.

2. Select the **Monitor PoP Interface** check box to enable the feature.

VLAN tab

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 Layer2 bridge is enabled.
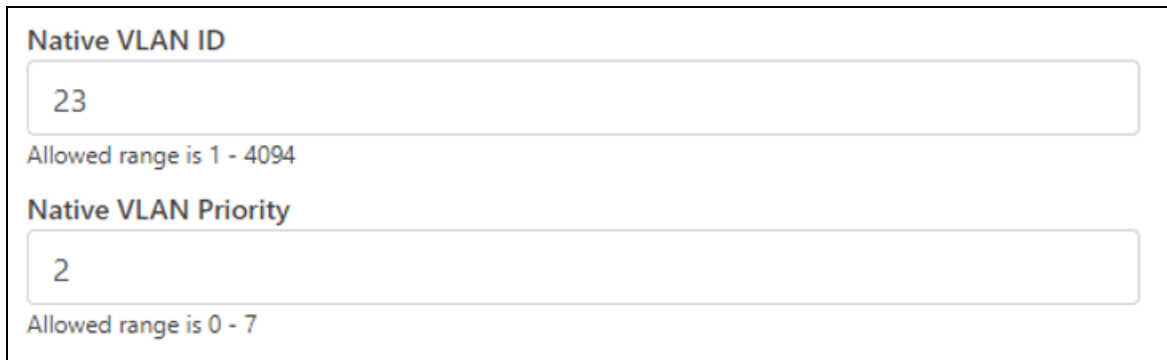
Port Type

Figure 179: *The port types*
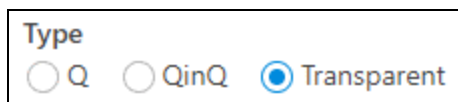
Transparent

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 180: *Native VLAN ID and priority*

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

Figure 181: *Allowed VLANs*

Allow only the listed range of VLAN IDs.

Figure 182: *Untagged types*

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 183: *Native C-VLAN ID and priority*

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

Figure 184: *Native S-VLAN ID and priority*

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

Figure 185: *Untagged and Single tagged packets*

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 186: *Allowed VLANs*

Allowed VLANs

2

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 187: *QinQ EtherType*

QinQ EtherType

0x8100 (802.1Q)

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 188: *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 remaking. For a double-tagged packet, S-VLAN ID gets remarked and for a single-tagged packet, C-VLAN 1D.

802.1p overriding

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

Figure 189: *VLAN Priority Override*

VLAN Priority Override

Ingress VLAN	Override Priority	
20	7	✏️ 🗑️
Add New		

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

Management VLAN

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

Figure 190: *The Management section*

Security tab

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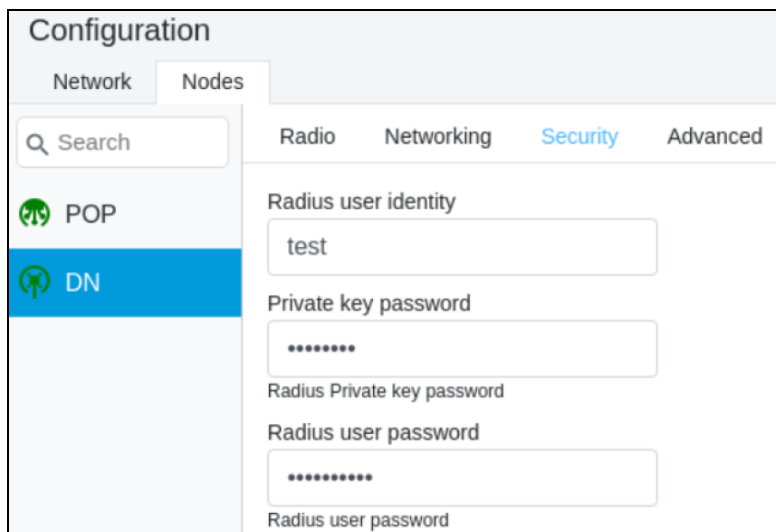
- Private key password
- Radius user password

Figure 191: *The Security tab*
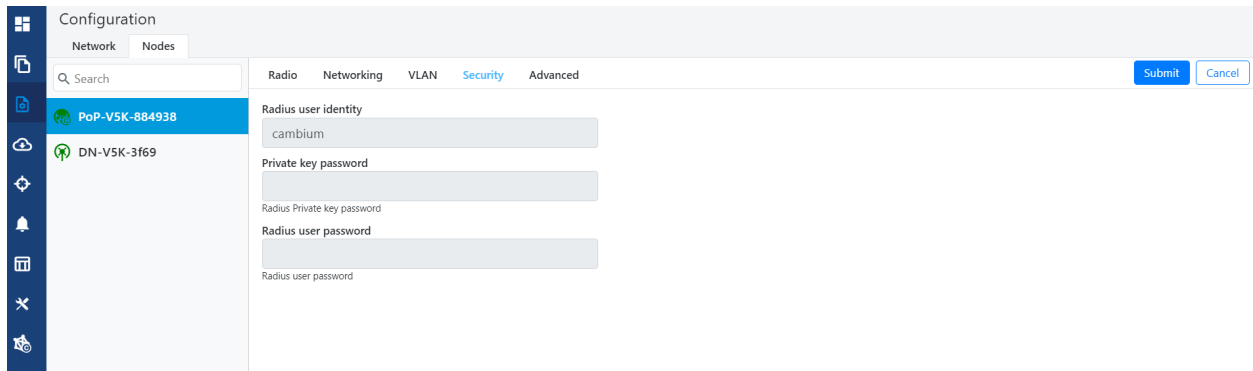
Controller GUI configuration

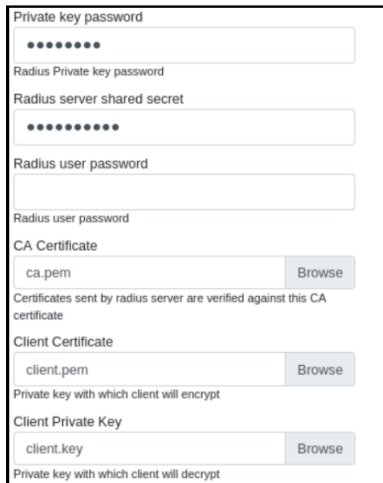This Controller GUI configuration to be made on each DN.

Figure 192: *Elements specific to Controller configuration*

Node GUI configuration

Figure 193: *Elements specific to node configuration*

> **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 RADIUS packets from IPv6 subnet (i.e., lo 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.
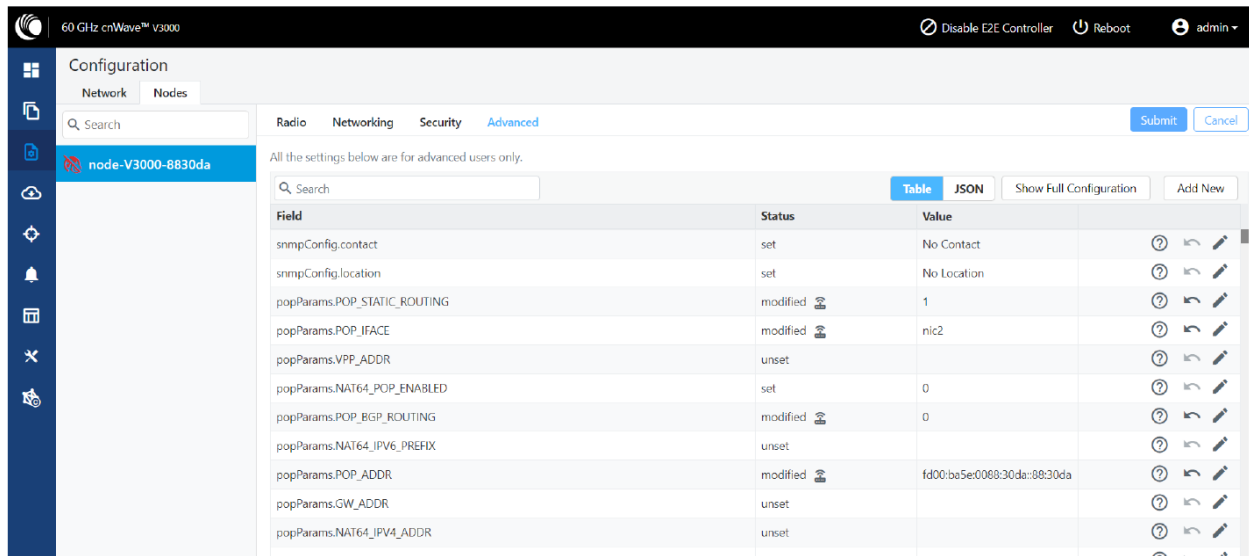
Advanced tab

These settings are for advanced users only.

> **Caution**
>
> Users are not recommended to do these settings.

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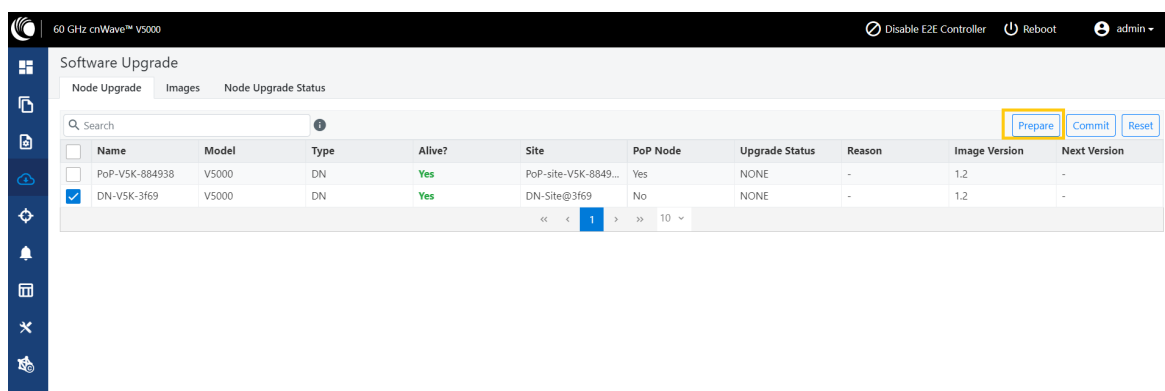
1. From the main dashboard page, click **Software upgrade** on the left navigation pane.

    The **Software Upgrade** page appears, as shown below:
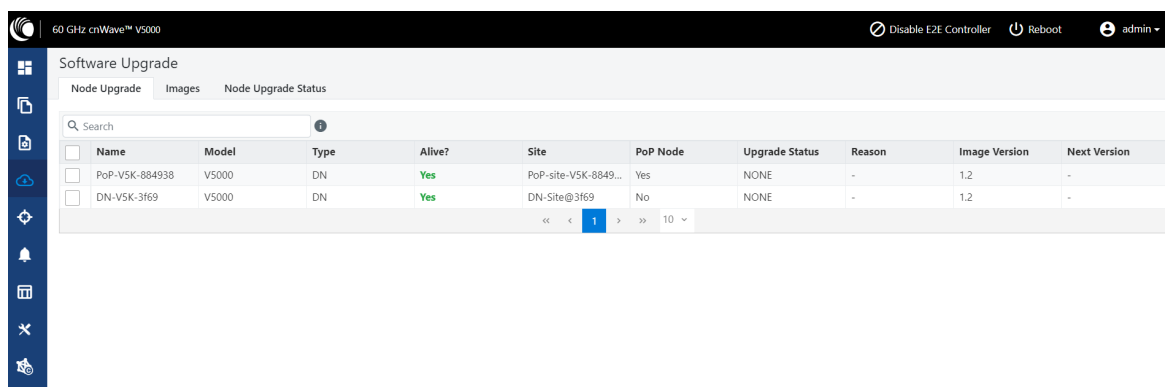
    By default, the **Node Upgrade** tab is selected.

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 195: *The Images page*
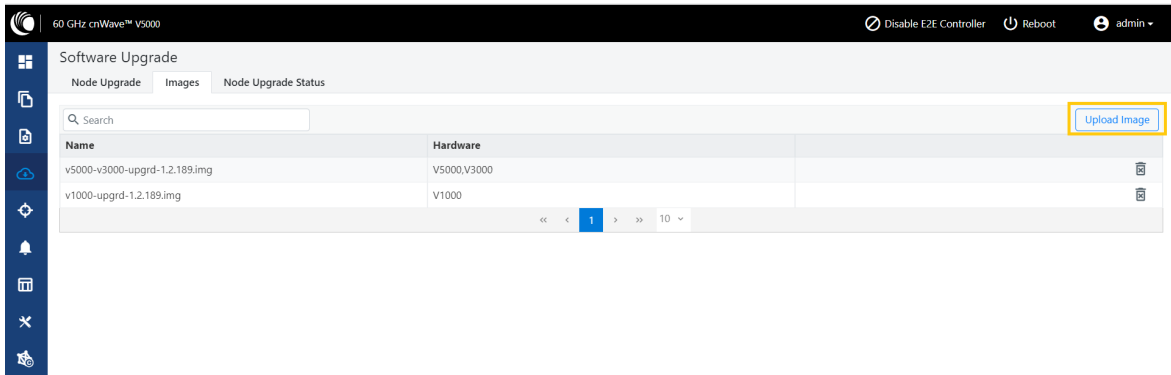
6. In the Images page, click **Upload Image**.

   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 196: *The Node Upgrade Status page*
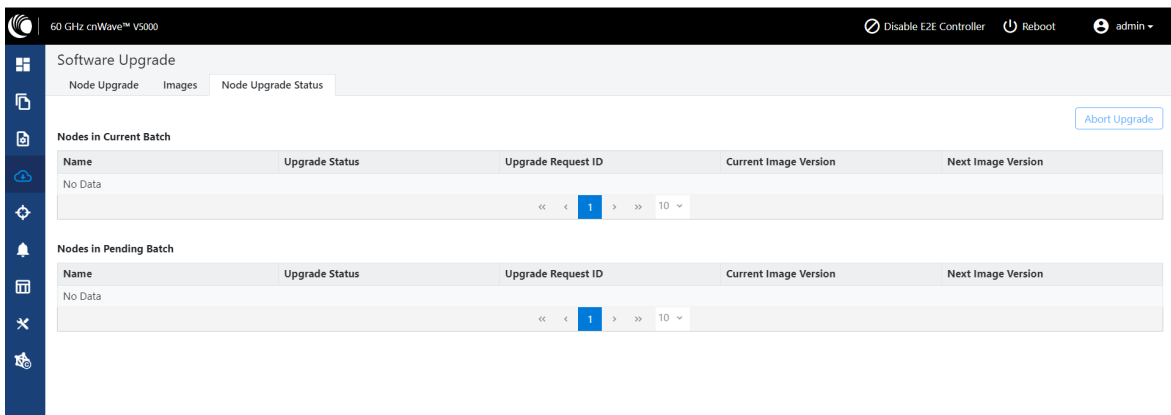
You can view the upgrade status for the required device nodes.

Events

The **Events** page displays the running and competed tasks list and these events can be exported. To export the event list click **Export**.

Statistics

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

- Links
- Ethernet
- GPS
- Radio
- Performance
- Prefix Zone Statistics
- Engineering
- Border Gateway Protocol (BGP)

Links

The **Links** page has Uplink and Downlink statistical data. It displays TX and RX data of the nodes from A to Z and Z to A.

Figure 197: *The Links page*

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

Table 45: Elements in the Links page

Elements	Description
Link Name	Link name
A-Node	Initiator Node
Z-Node	Responder Node
RSSI	Receiver Signal Strength Indicator
Link Fade Margin	The statistic value (in dB) available for each RF link 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.

Elements	Description
	The **Link Fade Margin** statistic value calculation is based on: • 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
RX Scan Beams	Receiver scan beam index
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
TX Scan Beams	Transmitter scan beam index
RX Errors	Receiver errors
RX Frames	Receiver frames
TX Errors	Transmitter errors
TX Frames	Transmitter frames

Ethernet

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

Figure 198: *The Ethernet page*

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

Table 46: 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 199: *The GPS page*
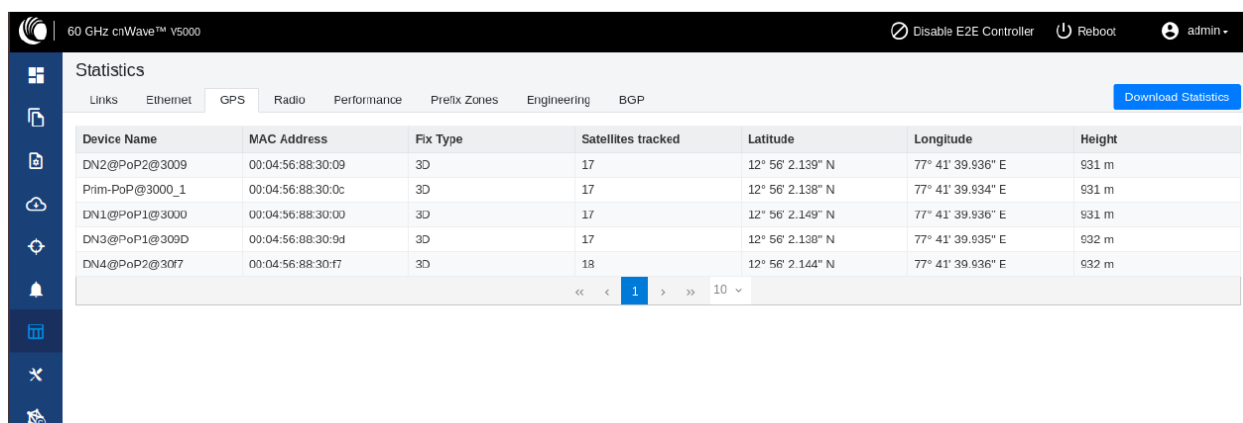
The following elements are displayed in the **GPS** page:

Table 47: 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 200: *The Radio page*
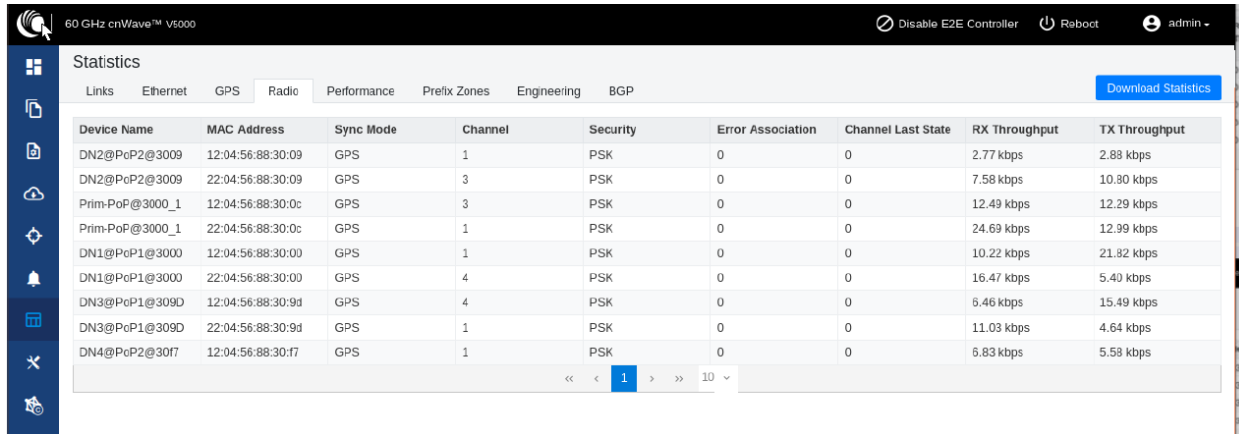
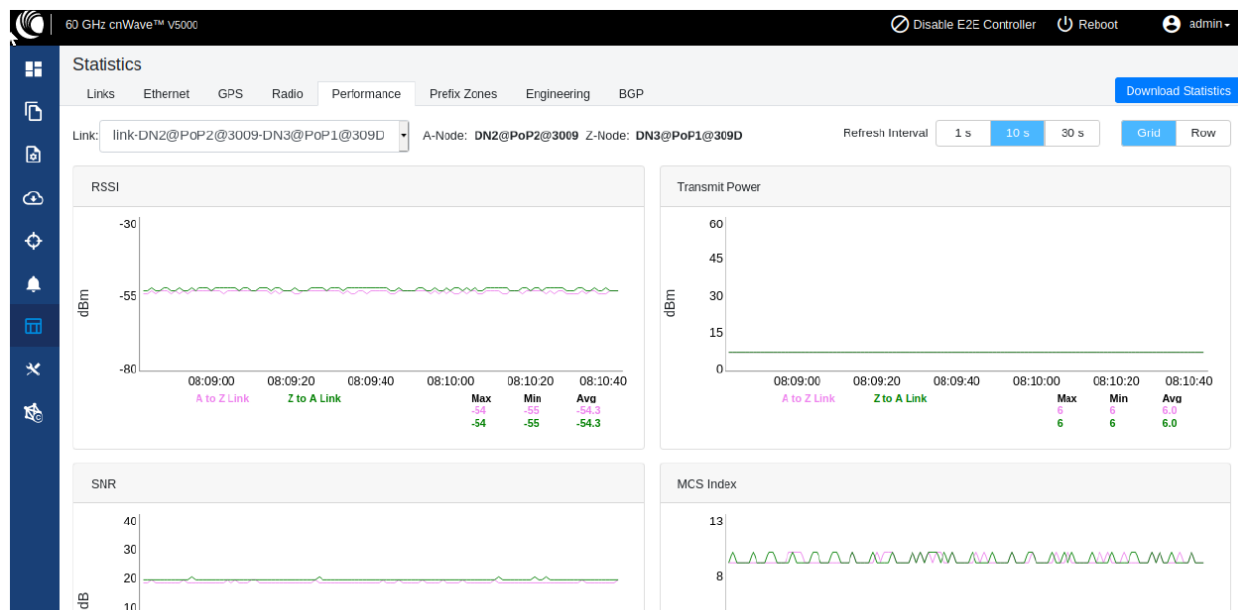The **Radio** page has the following elements:

Table 48: Elements in the Radio page

Elements	Description
Device Name	Name of the device
MAC Address	MAC address of the device
Sync Mode	**GPS sync**: *Entry condition*: Valid samples from GPS have been received for a few consecutive seconds (typically 2 seconds). *Exit condition*: 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). *Entry condition*: Conditions for "GPS sync" have not been met, but a link exists to at least one other DN from which to derive timing. *Exit condition*: 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. *Entry condition*: Conditions for "GPS sync" or "RF sync" are not met. *Exit condition*: 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 201: *The Performance page*

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

Table 49: 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

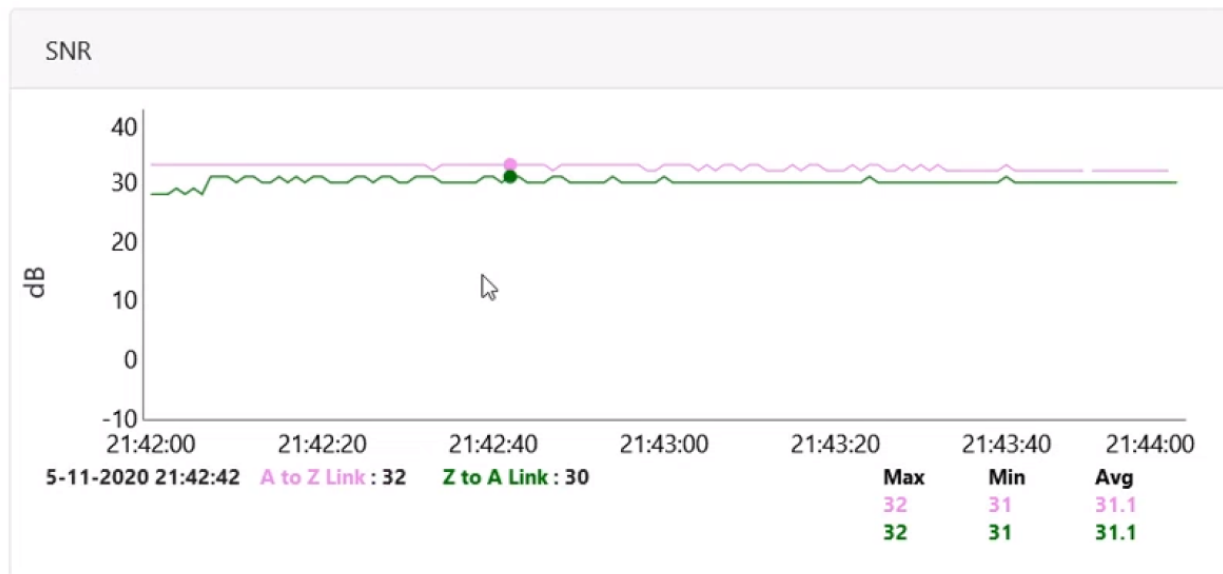Figure 202: *RSSI graph*
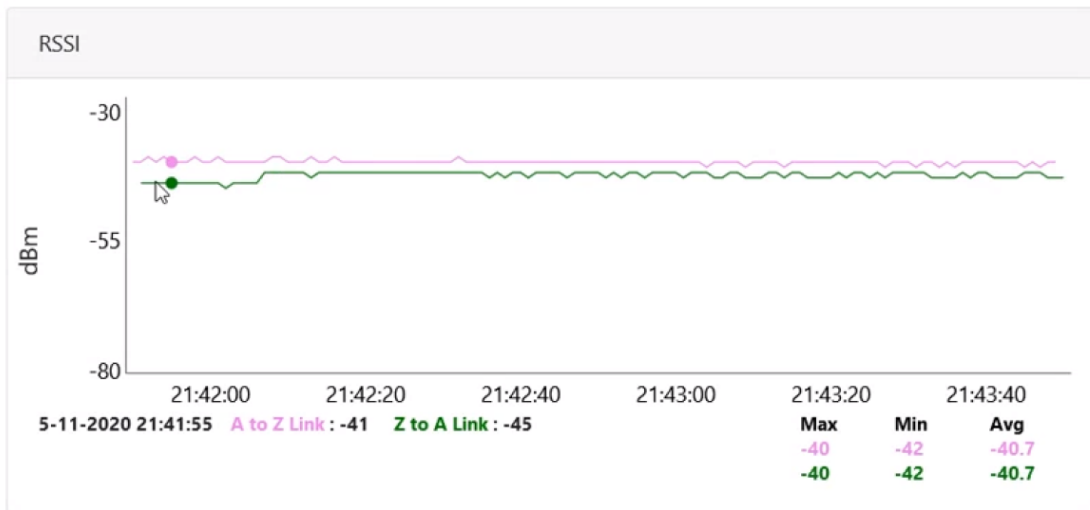
Transmit Power graph

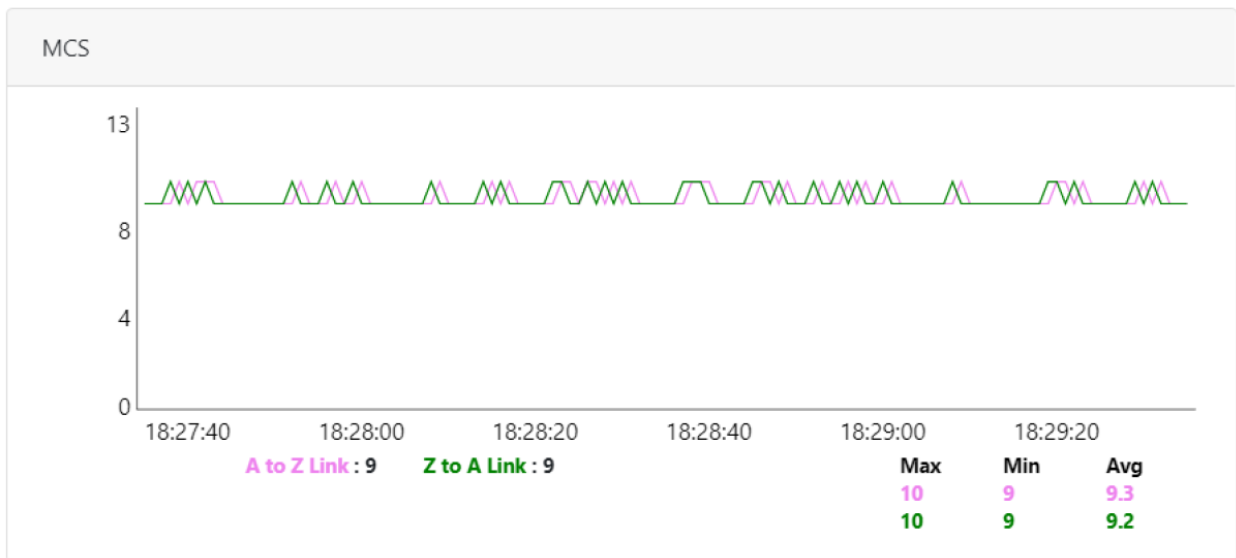Figure 203: *Transmit Power graph*
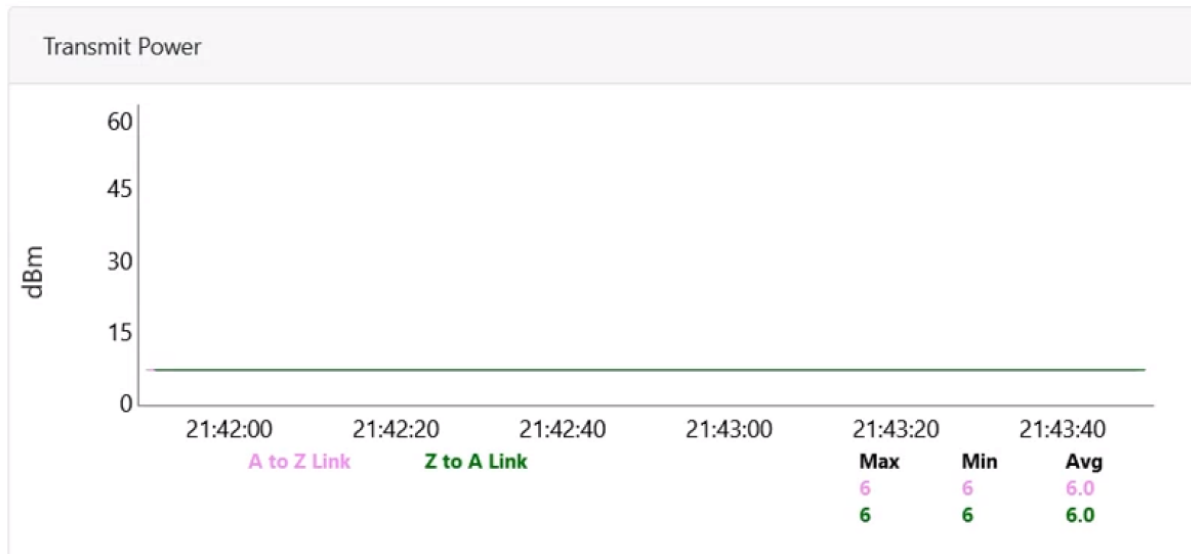
SNR graph

Figure 204: *SNR graph*

MCS Index graph

Figure 205: *MCS Index graph*

Packet Error Ratio graph

Figure 206: *Packet Error Ratio graph*
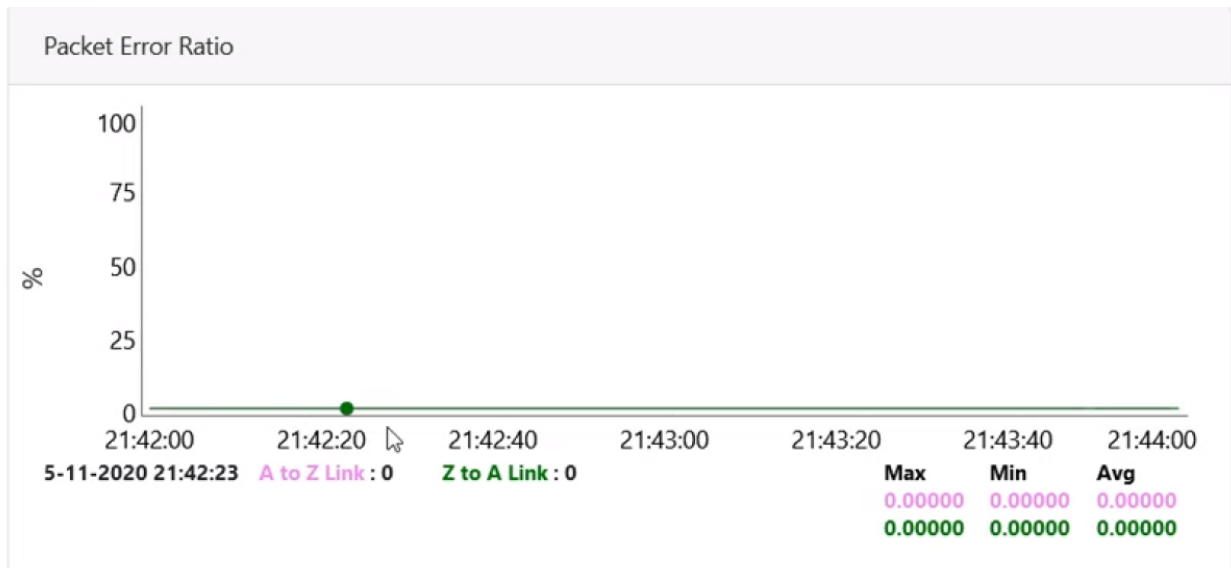
Received Frames graph

Received Frames graph

Transferred Frames graph

Transferred Frames graph

Prefix Zone Statistics

When a **Deterministic prefix** is enabled and in the multi-PoP deployments, the mesh is divided into prefix zones. Prefix Zone statistics are available on the **Statistics > Prefix Zone** page.

Figure 209: *The Prefix Zones page*

Engineering

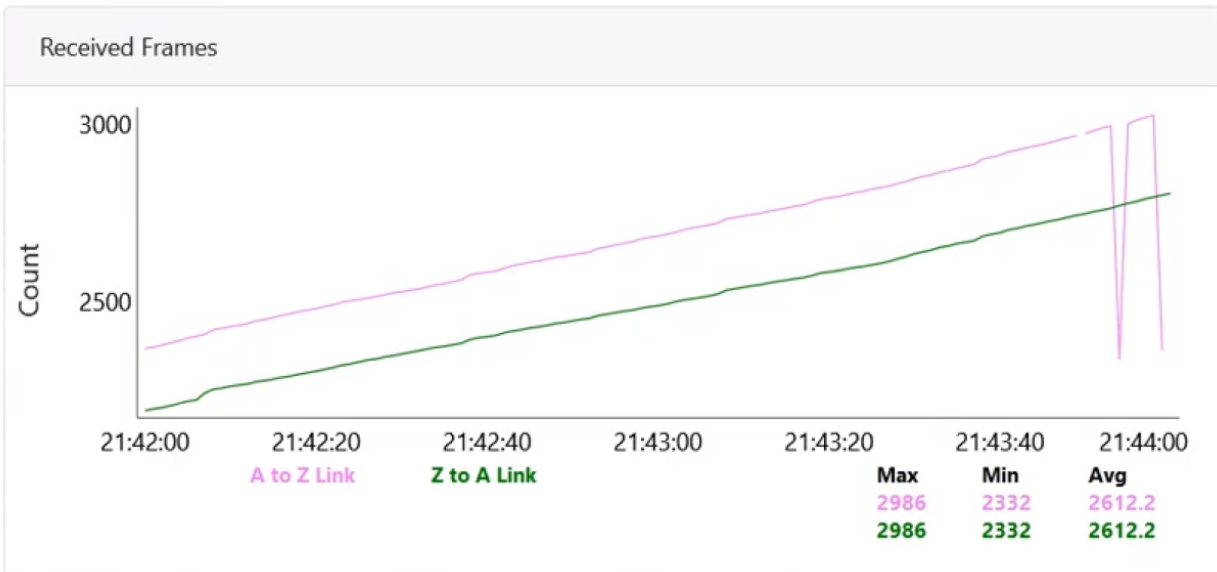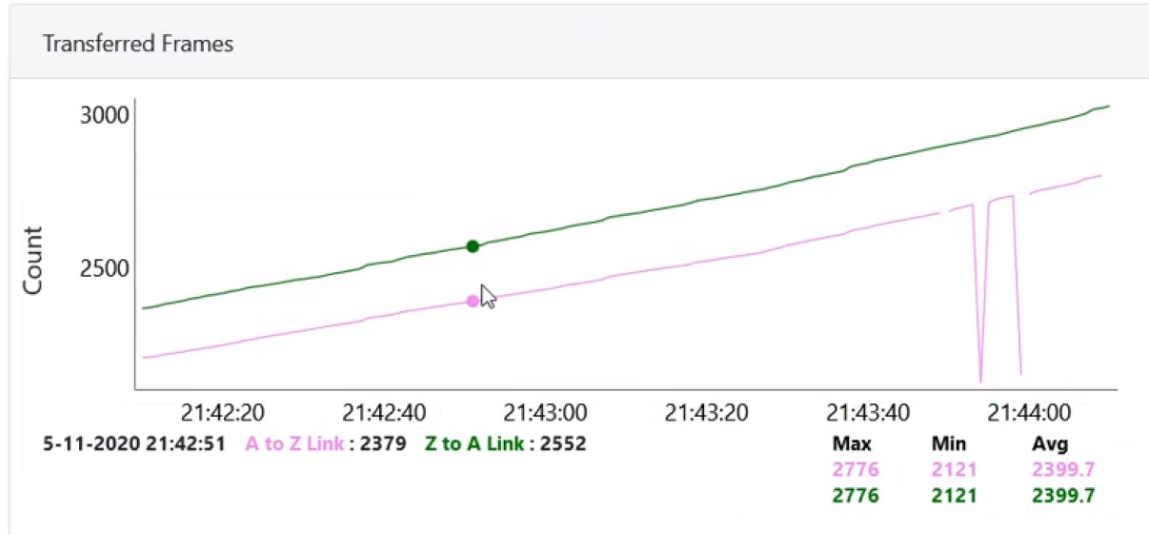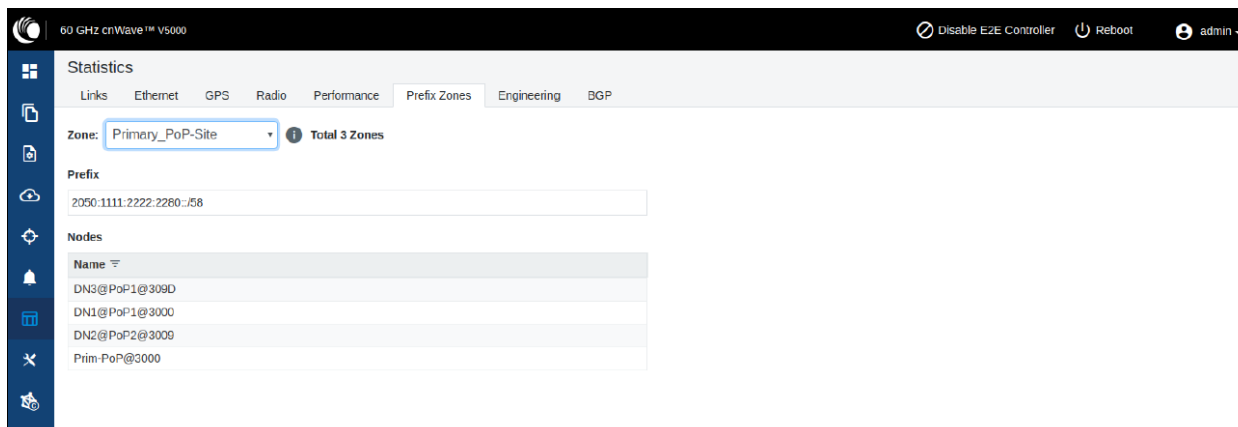The **Engineering** page displays the engineering information of the system and sector.

Figure 210: *The Engineering page*
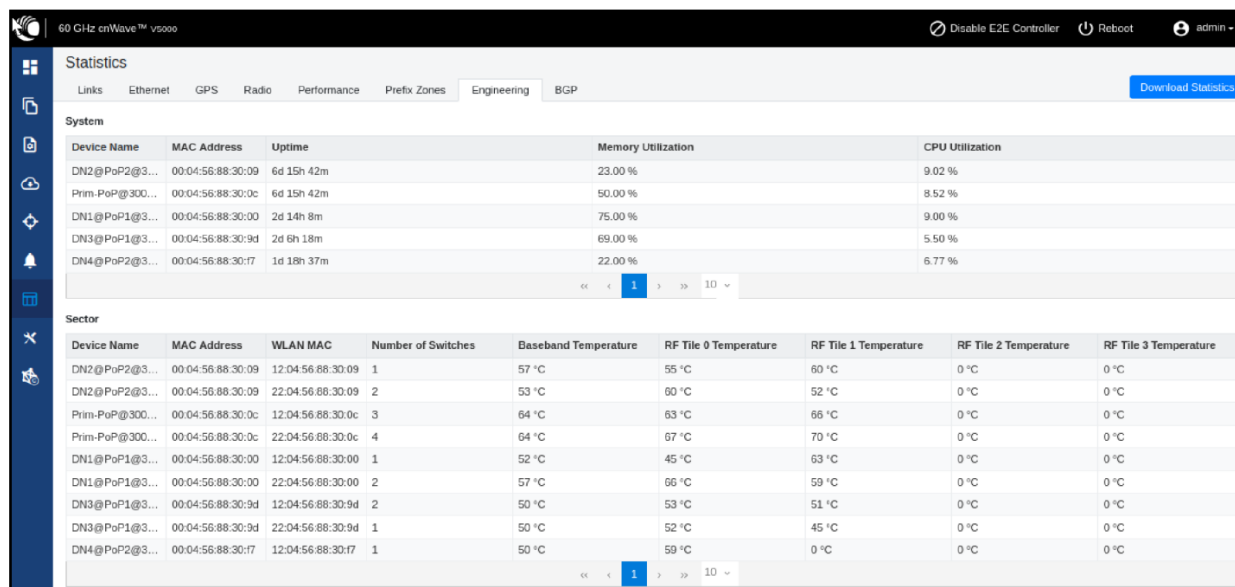
Border Gateway Protocol (BGP)

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 the 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 211: *The BGP page*

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 212: *The Map page*

Tools

The **Tools** menu contains **Factory Reset** and **Logs** options. Factory Reset is used to set the default settings.
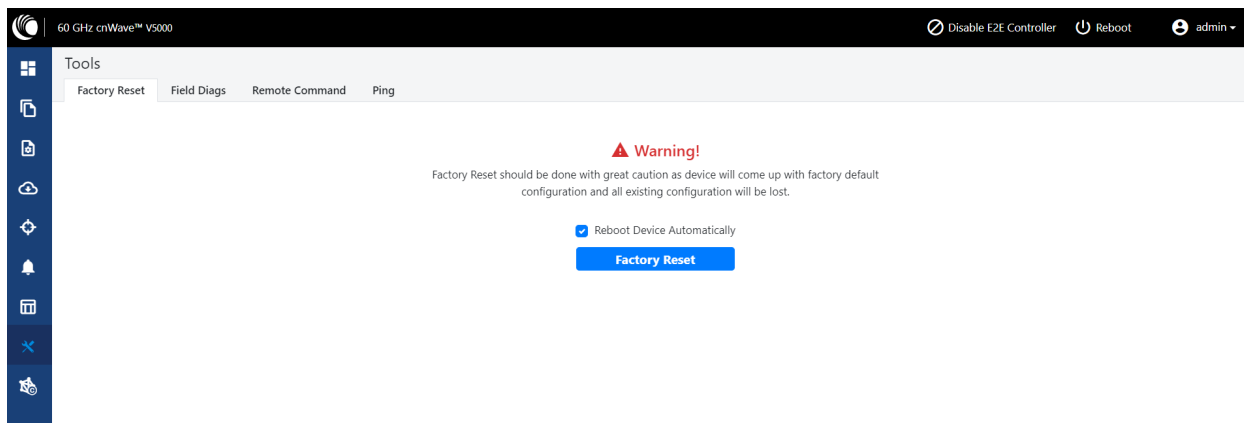
The **Field Diags** tab is used to view and download the error logs. To download the DN logs, select the DN node from the **Select Node** drop-down and click **Download Logs** (as shown below).

Figure 214: *The Field Diags page*
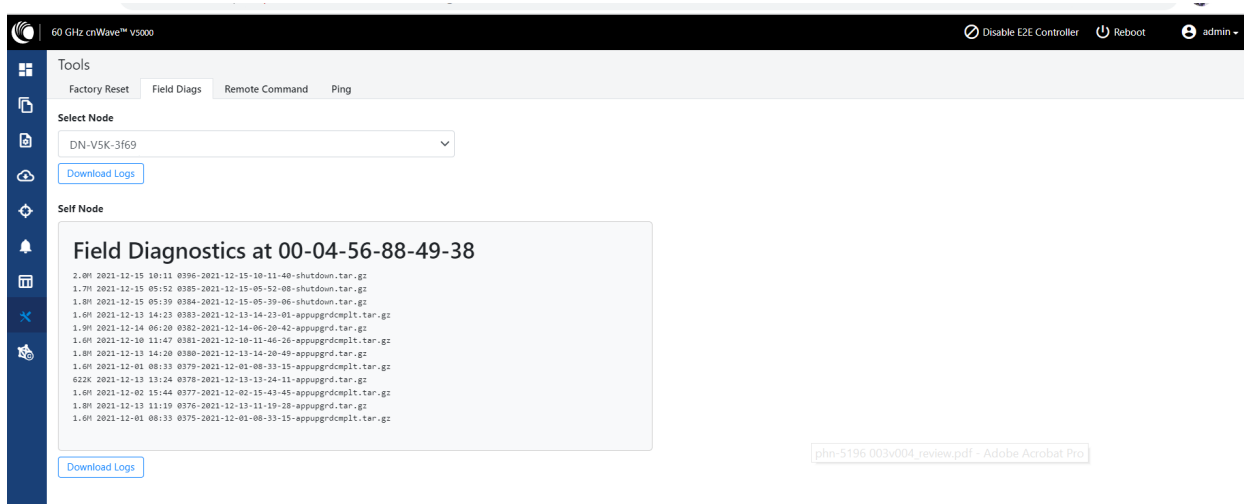
To download the logs for self node, click **Download Logs** at the bottom and save the log file.

Figure 215: *Saving log files*

Antenna Alignment

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

> ⚠️ **Warning**
>
> The antenna alignment tool is not a substitute for optical alignment. The optical alignment is the key to get 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 the help of a Link Planner from Cambium Networks. This prerequisite task provides the information on the RSSI expected for the PTP link. This must be used as target while using the antenna alignment tool.

- Enter the PTP topology in cnMaestro or in the UI of a device (with the Onboard Controller on it). Then, ensure that the following tasks are performed:

  - Creating two Sites and nodes.

  - Setting 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.

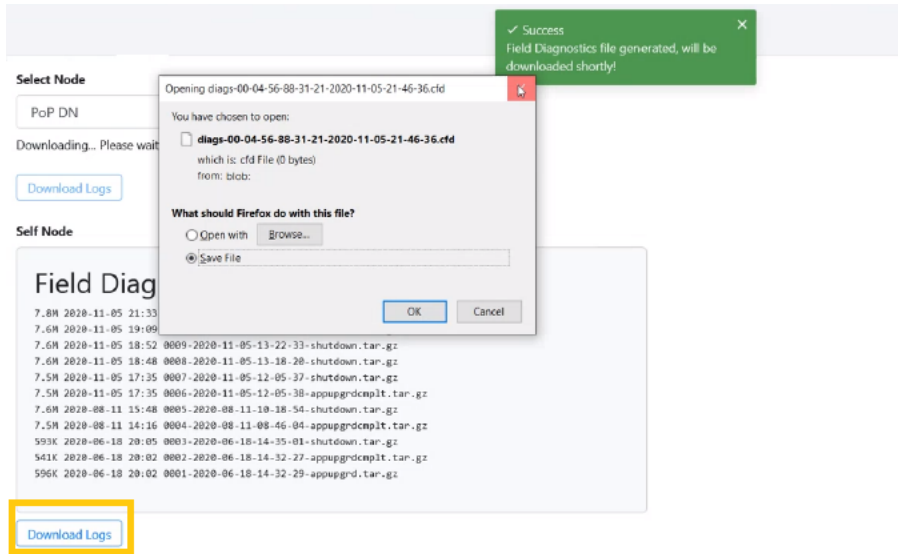## Using the Antenna Alignment tool

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

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

   The Antenna Alignment page appears, as shown in Figure 216.

Operation   197

Figure 216: *The Antenna Alignment page*
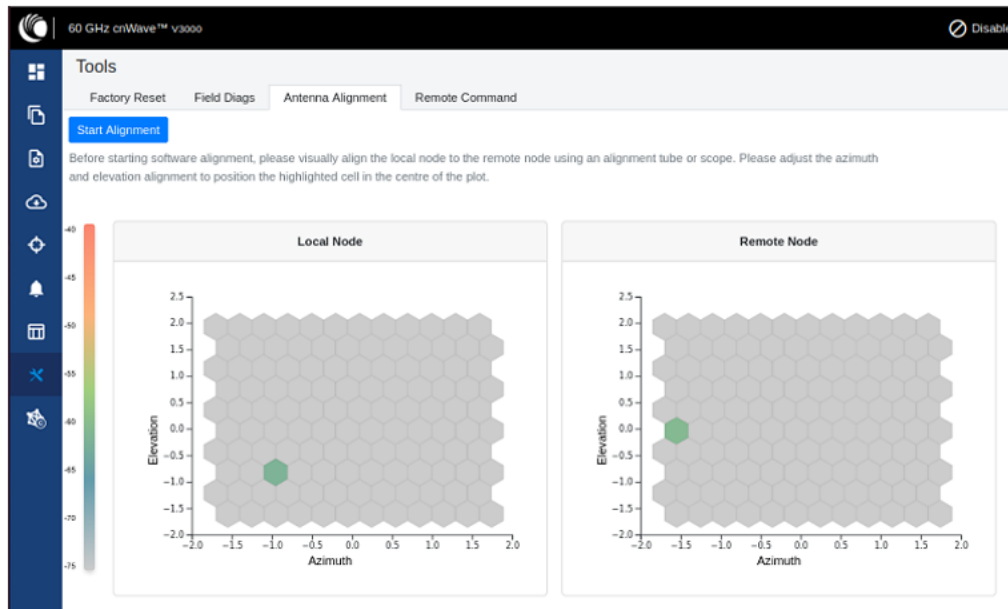
> **Note**
>
> If the alignment is initiated from a CN, ensure that the operating channel is set on the radio (before alignment). If the channel is not set, you must set the required channel in the **Configuration** page of the V3000 single node UI.

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 217), indicating that the link ignition will be disabled. 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.
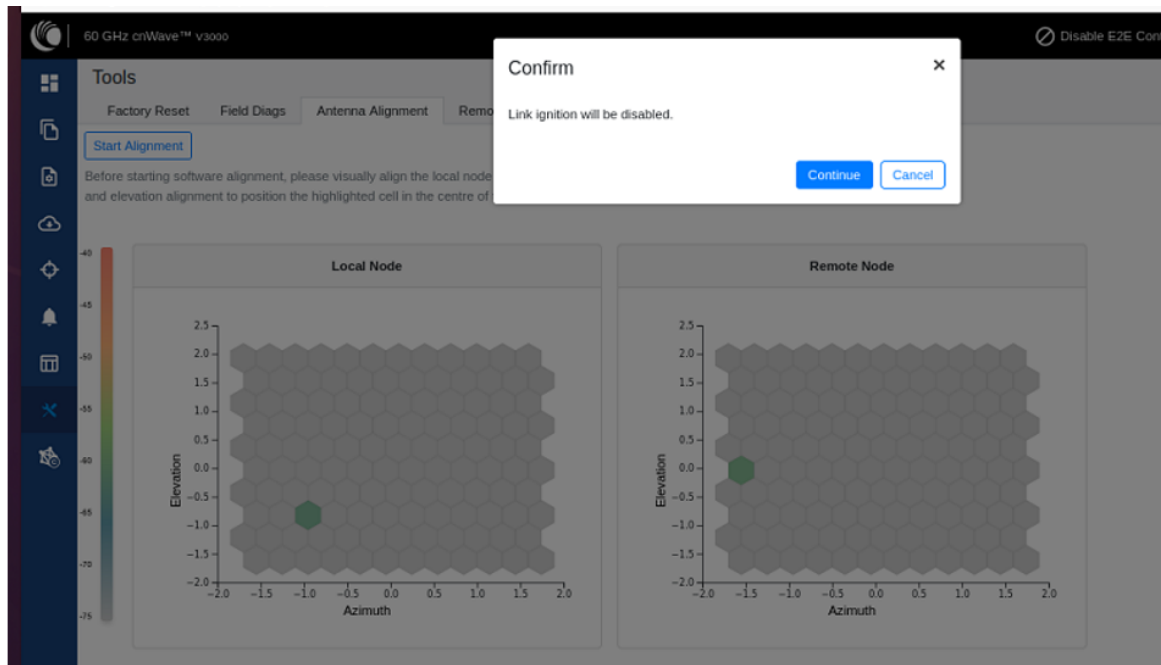
3. In the **Confirm** message box, click **Continue** to start the antenna alignment process.

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:
>
> a. Disable the ignition of the link at the Controller.
>
> b. Send Dis-assoc for the link from the Controller.
>
> c. 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 218.

Figure 218: *The RSSI time series*
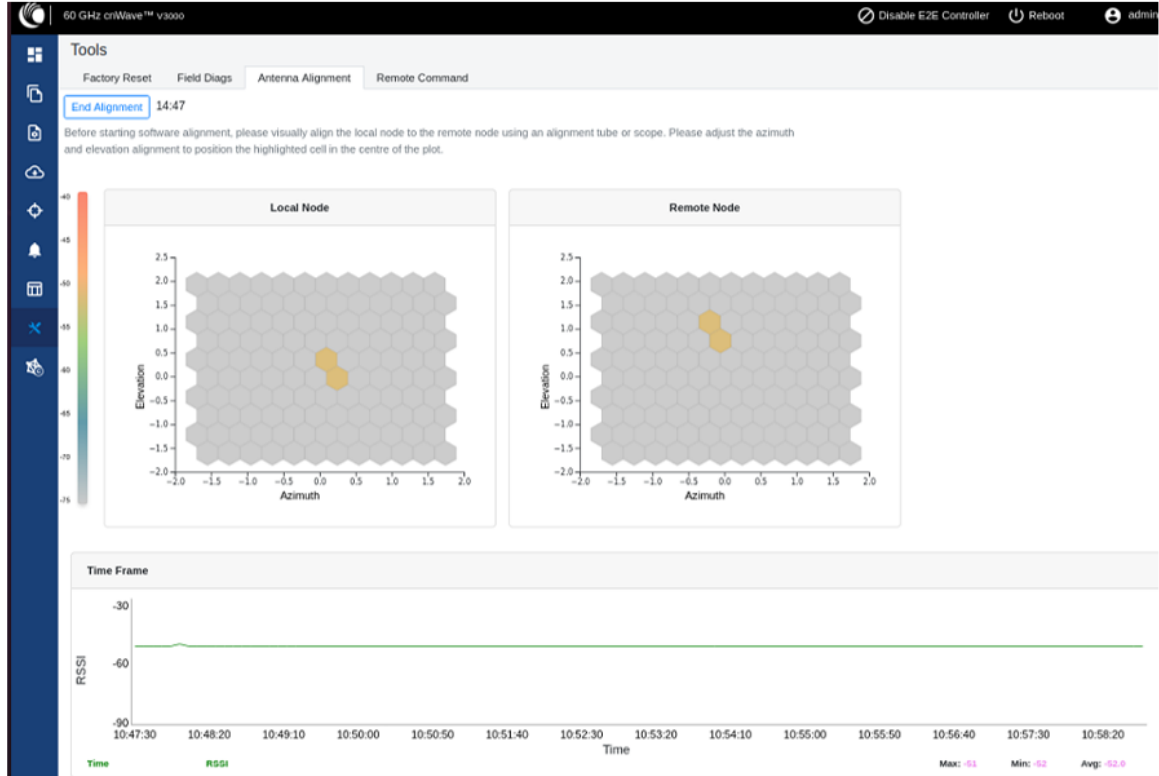
Following details explain about the RSSI time series that populates in the Antenna Alignment page:

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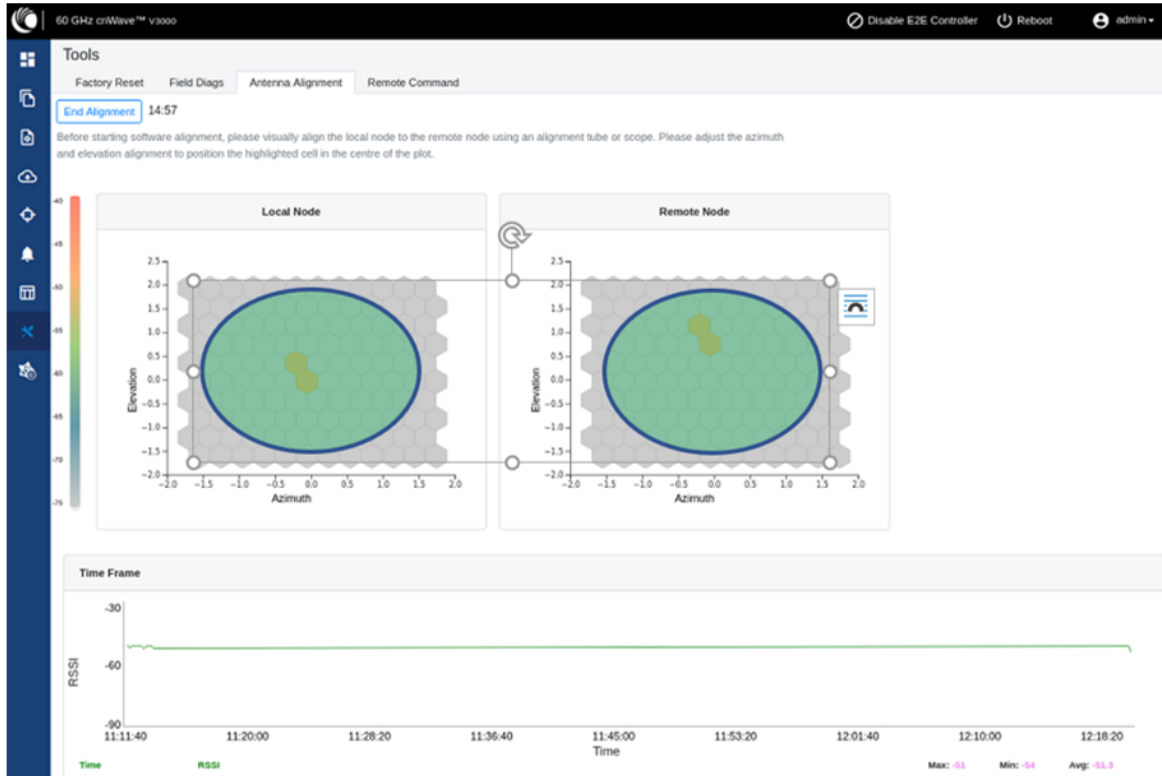
> **Note**
>
> If the installer has enabled the short-range installation in the radio configuration, the transmit power control is set to the minimum configured power.

4. Adjust the optimal RSSI that must be reached when the beams are close to the central region, as shown in Figure 219.

Figure 219: *The optional RSSI alignment*

The RSSI time series must be close to the Link planner's predicted RSSI, 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.

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 220):

Figure 220: *Example of the elevation mismatch*
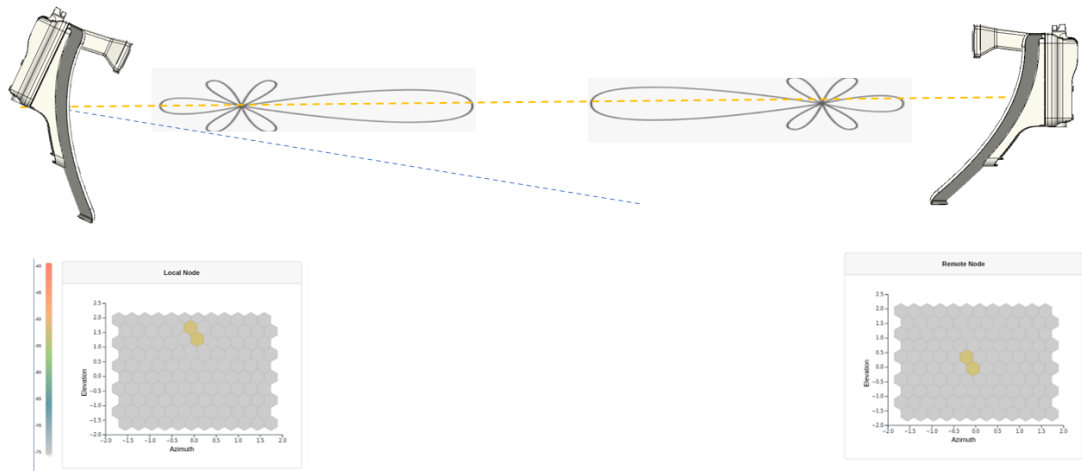
In Figure 220, the angles are exaggerated to show the point. In this example, consider that the radio has been misaligned by a down-tilt of 2 degrees behind the unit (from an installer's view side). This means that the angle of the beam selected might be in the +2 degrees direction in the elevation due 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 221.
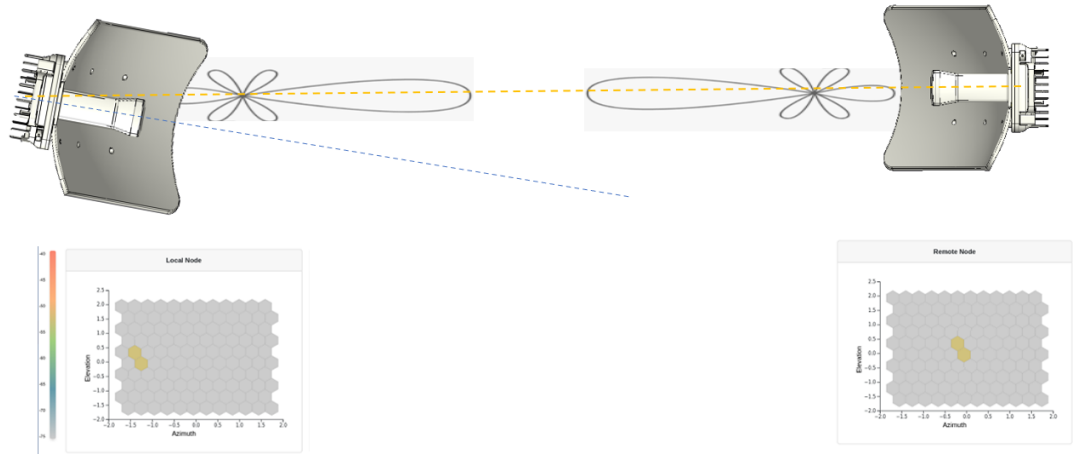
Figure 221: *On correcting the elevation mismatch*
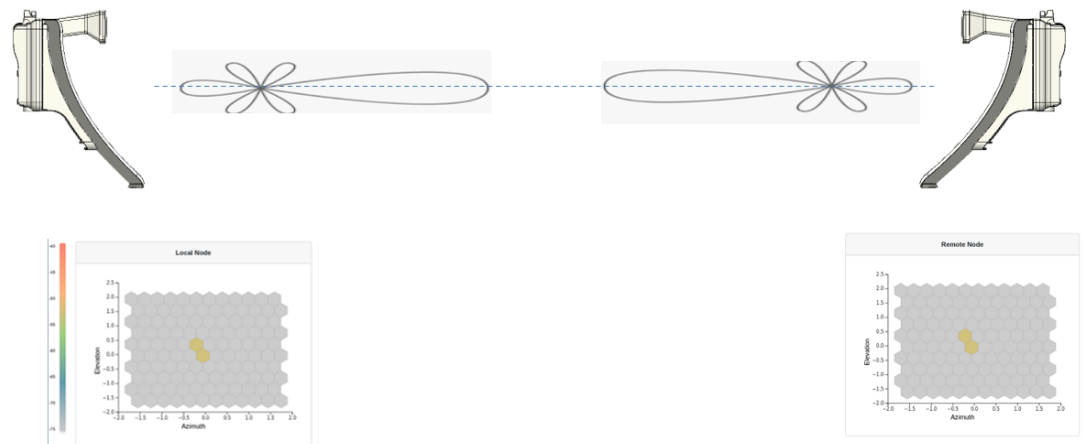
- When there is an azimuth mismatch (as shown in Figure 222):

Figure 222: *Example of the azimuth mismatch*

In Figure 222, 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 223.

Figure 223: *On correcting the azimuth mismatch*
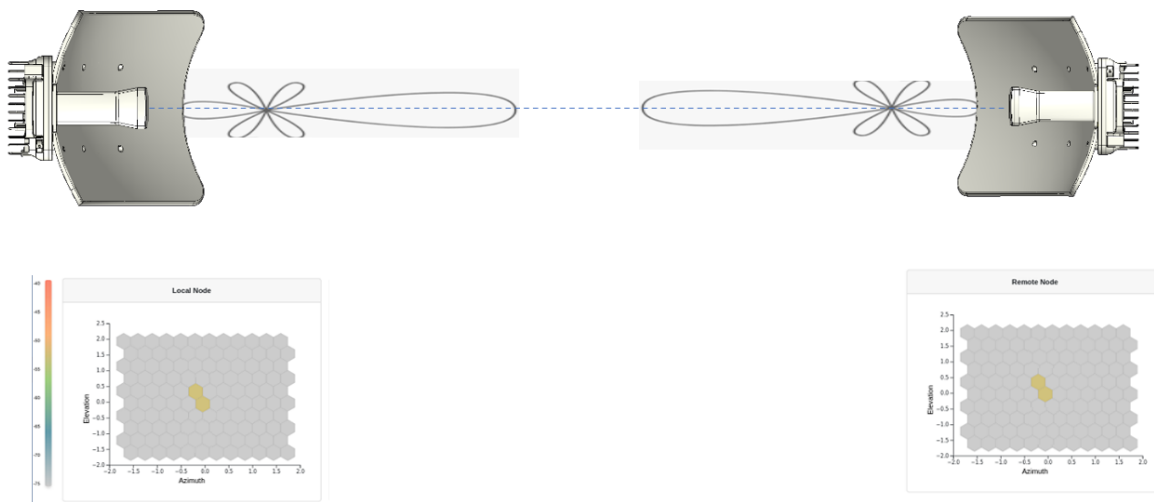
6. When you achieve the desired alignment and RSSI, click the **End Alignment** button located at the top left side of the Antenna Alignment page.

   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 224 shows how the Antenna Alignment dashboard page looks on completing the antenna alignment task.

Figure 224: *The updated Antenna Alignment dashboard page*
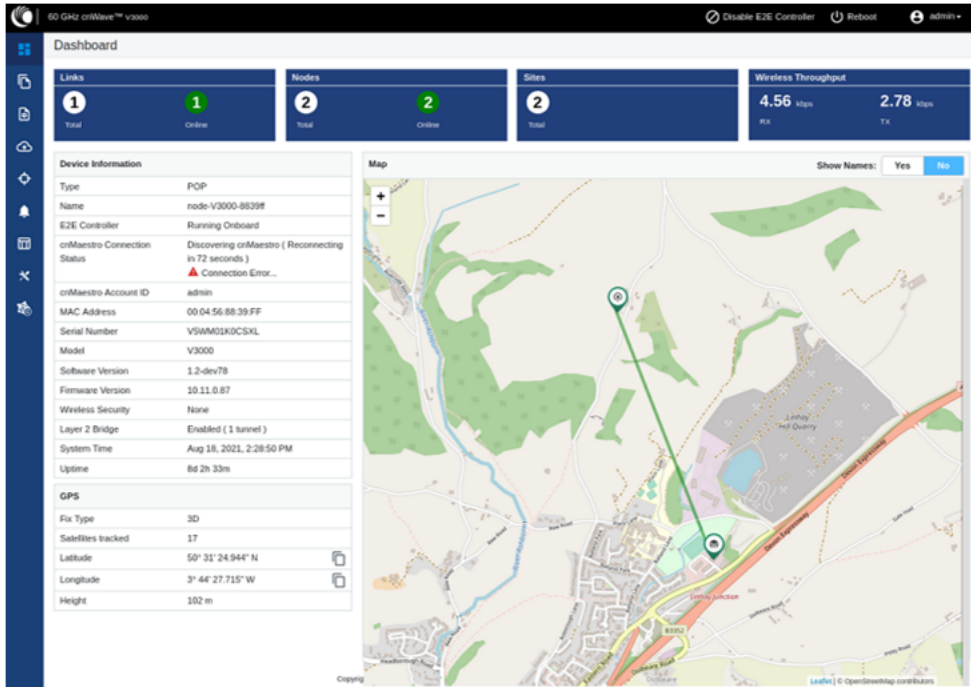
Ping tool

The **Ping** feature (a 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 the radio links.

To use the ping tool, perform the following steps:

1. Navigate to **Tools** > **Remote Command** from the home page of Onboard Controller UI.

   The **Ping** page appears.

2. Set the parameters with the required values, as described in Table 50.

Table 50: 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. Select the required source node from the drop-down list.
Destination Type	The required node or destination address (IPv4 or IPv6) that for which the reachability has to be identified. Following options are supported:

Parameter	Description
	• Node • IPv4 • IPv6 Select the required option (mandatory).
Number of Packets (-c)	Number of times that a packet is transmitted to find the reachability. Default value: 3 This parameter supports values between 1 (minimum) and 10 (maximum). Type an appropriate value in the text box.
Buffer Size (-s)	Size (in bytes) of the packet. Default value: 56 This parameter supports values between 1 (minimum) and 65507 (maximum). Type an appropriate value in the text box.

3. Click **Start Ping**.

   The **Ping Result** section displays the information for the selected criteria, as shown in Figure 225.

Figure 225: *The Ping page*
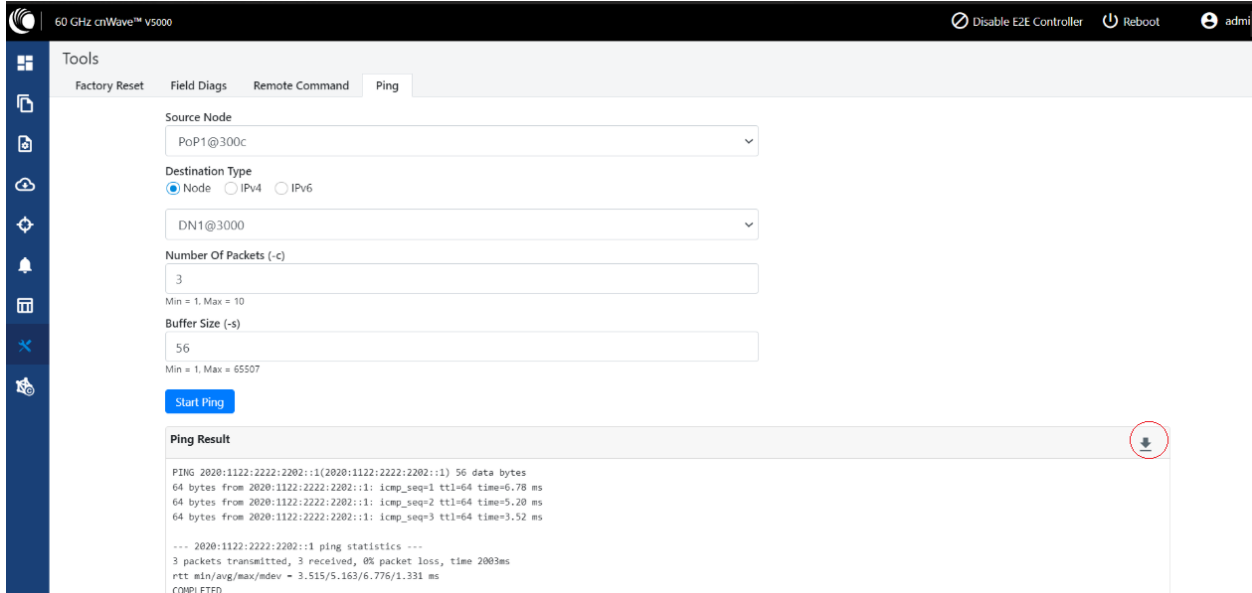
You can use the icon to download the ping result.

Show SFP Power details

The **Show SFP Power Details** feature (a remote command) has been introduced in this release. 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. Navigate to **Tools** > **Remote Command** from the home page of Onboard Controller UI.

   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 226.

Figure 226: *The UI supported output - SFP Power details*
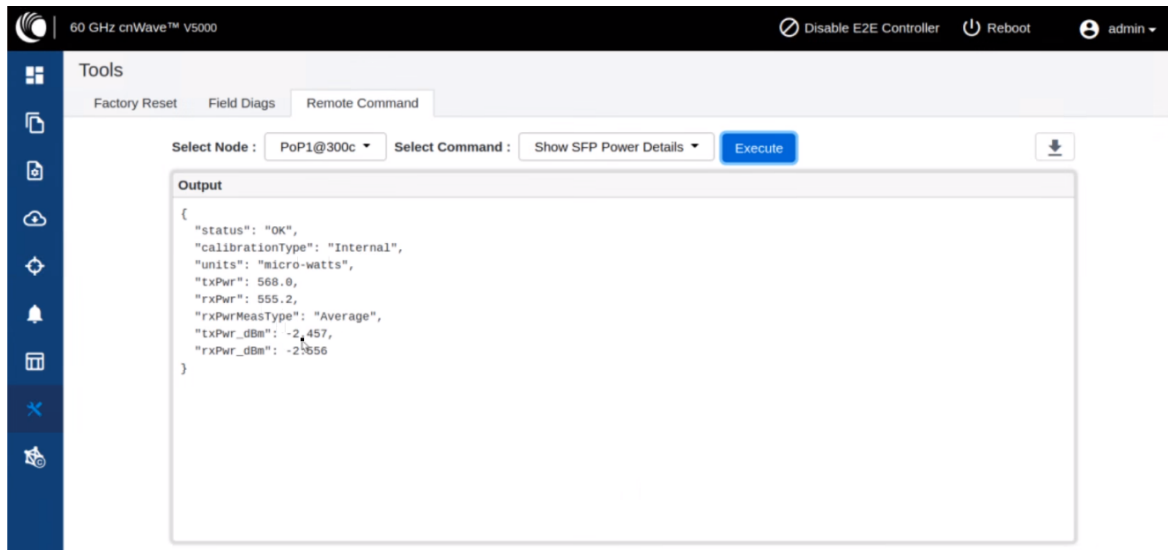
Table 51 lists and describes each parameter in the output.

Table 51: Output details

Output Parameter	Description
Status	Determines whether the output is valid. If the **Status** field contains OK, it implies that the rest of the output is valid.

Output Parameter	Description
	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.
CalibrationType	Indicates the measurement type that is calibrated over the criteria, such as the following (for example): • Specified transceiver temperature, • Transceiver supply voltage, • TX output power, and • RX received optical power. The value of this parameter is Internal.
Units	Indicates the unit of measurement. The value of this parameter is micro-watts (mW).
txPwr	Indicates the TX output power in mW.
rxPwr	Indicates the RX received optical power in mW.
rxPwrMeasType	Indicates whether the received power measurement represents an average input optical power. The value of this parameter is Average.
txPwr_dBm	Indicates the TX output power in dBm.
rxPwr_dBm	Indicates the RX received optical power in dBm.

5. 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 227.

Figure 227: *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>
```

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 228: *The Onboard E2E Controller page*
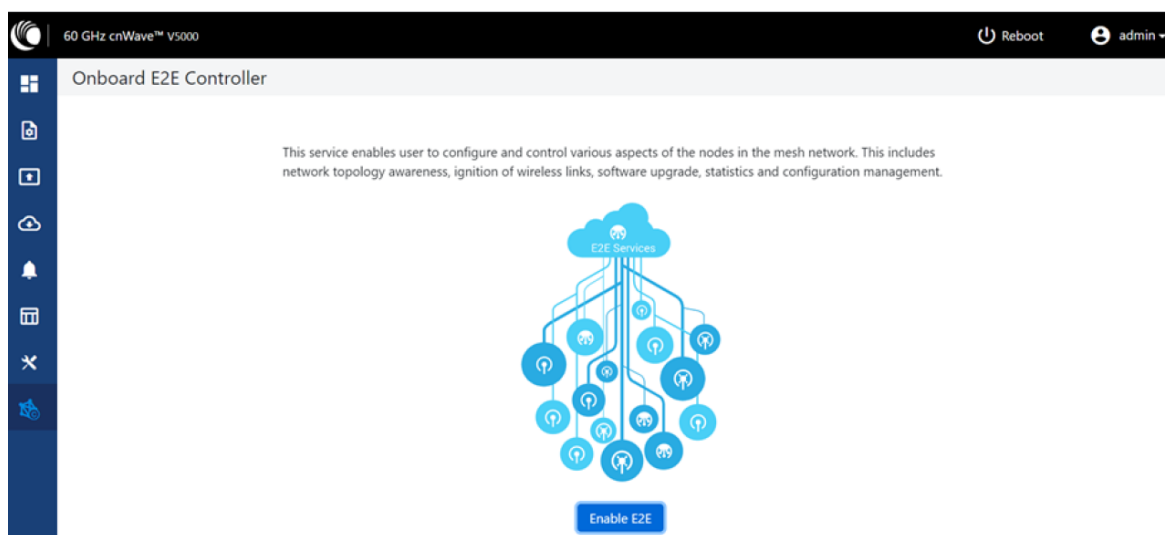
3. Enter the cnMaestro management configuration information.

- 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
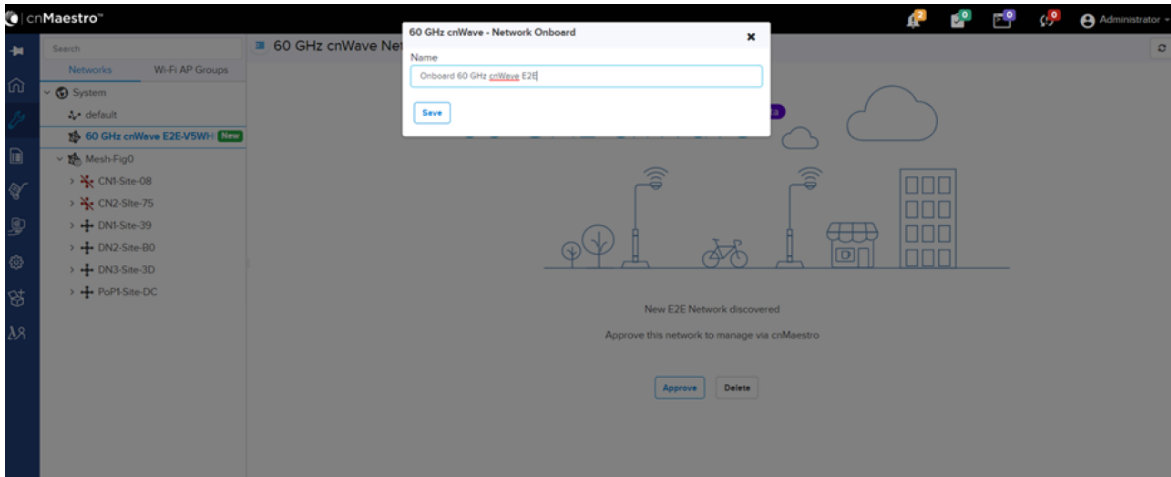
Figure 229: *The cnMaestro section*
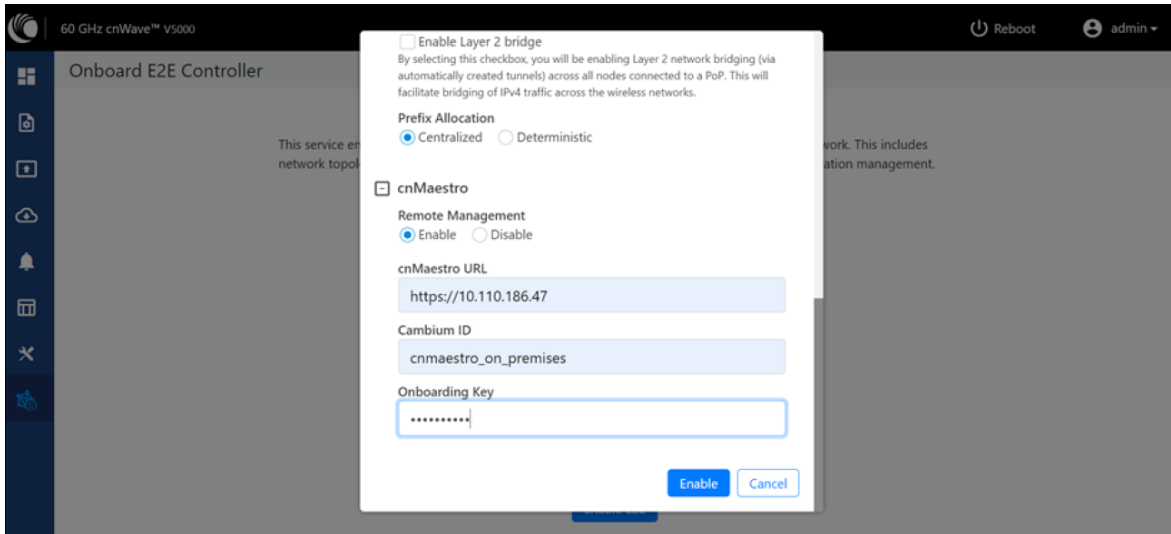
4. Click **Enable**.

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

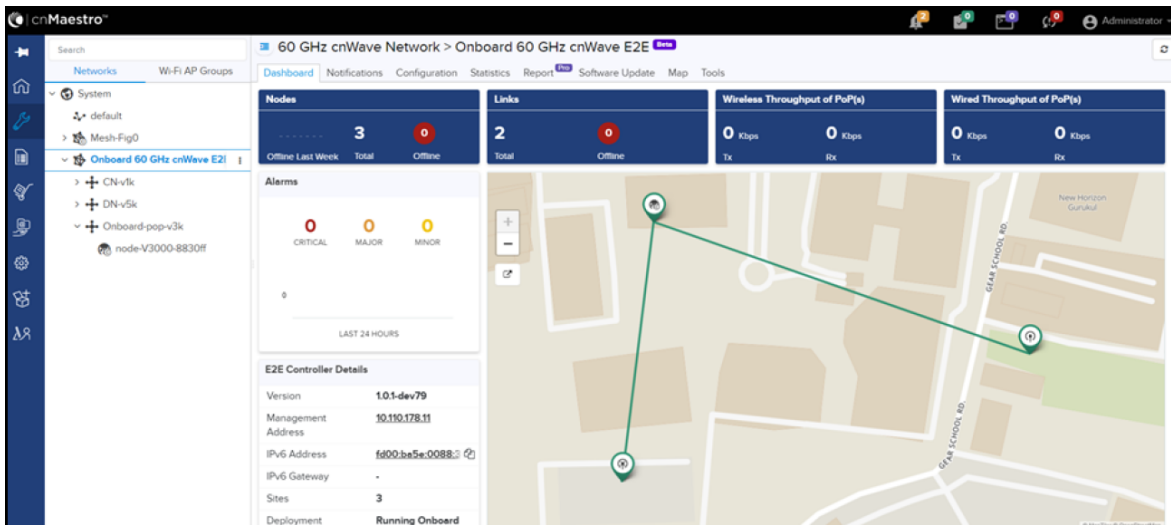Figure 230: *Information on the new E2E network*
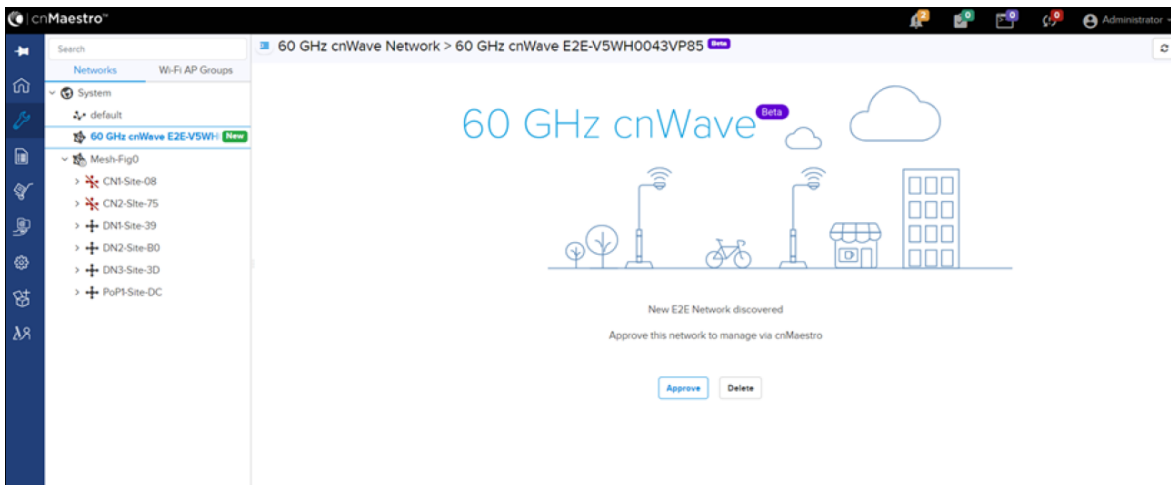
6. The **Network Onboard** window appears and provides an option to edit the network name.

7. Click **Save**.

Figure 231: *The 60 GHZ cnWave - Network Onboard*

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

Figure 232: *The Onboard 60 GHZ cnWave E2E dashboard 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 233.

    Figure 233: *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.
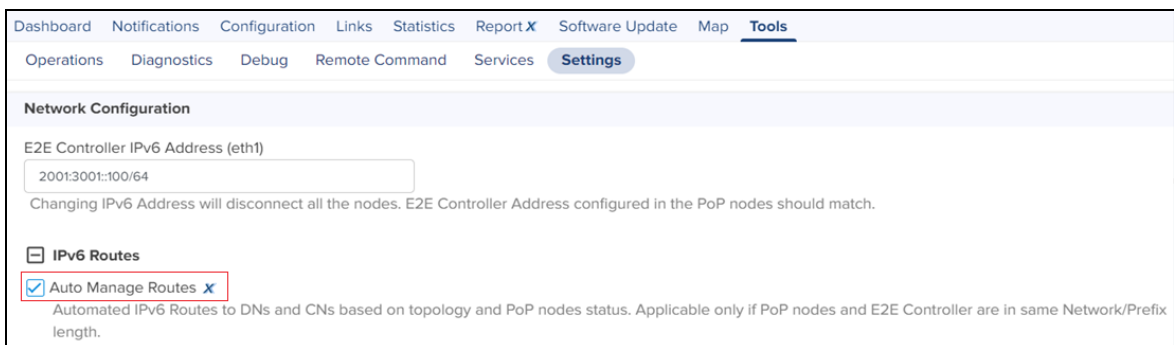
4. Click **Add**.

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

    Figure 234: *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:
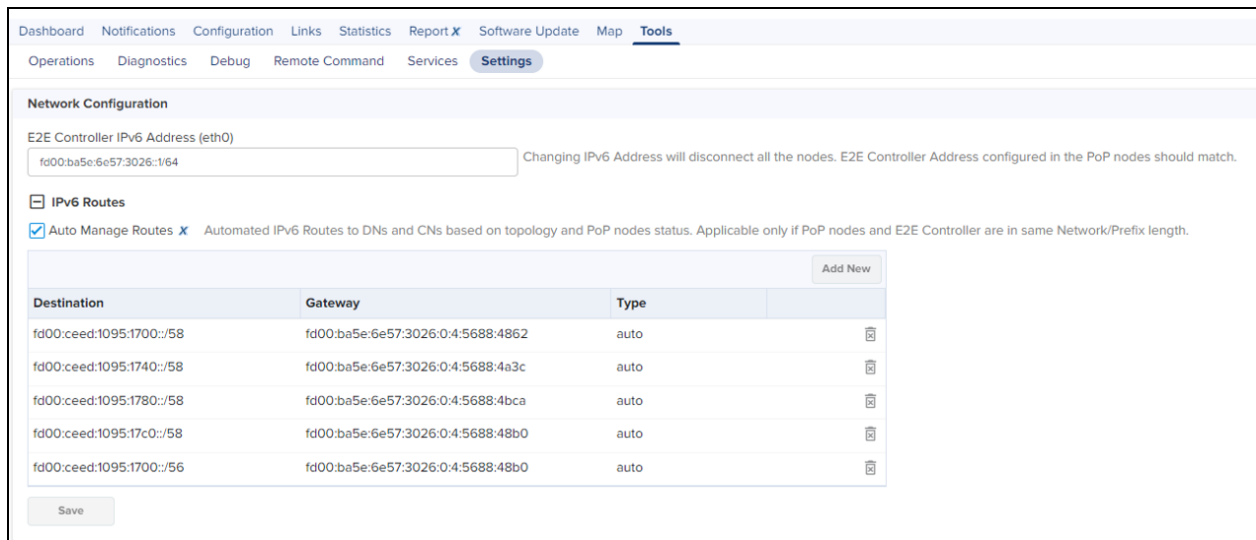
- When the Layer 2 bridge is enabled (which implies that the BGP v6 router is not required for managing data traffic).

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

Figure 235: *Example of IPv6 route entries in the IPv6 Routes page*

Figure 236 shows how the cnMaestro dashboard diagrammatically displays the routes taken by E2E Controller and the traffic controlled by cnWave nodes.