### Figure 167: The Network page with multiple tabs

	60 GHz cnWave <sup>114</sup> v5000	O Disable E2E Controller	() Reboot	😫 admin -
	Configuration			
	Network Nodes			
10	Basic Management Radio Security Advanced		S	ubmit Cancel
۵	Layer 2 Bridge			
•	Enable By selecting this checkbox, you will be enabling Layer 2 network bridging (via automatically created tunnels) across all nodes connected to a PoP. This will facilitate bridging of IPv4 traffic across the wireless networks.			
Φ	Prefix Allocation			
۵	Centralized     Deterministic			
	Seed Prefix			
and a second	fd00:ceed:8849:3800::/56			
*	Generate IPv6 'seed prefix' in CIDR format from which subnet prefixes are allocated to all DNs and CNs (e.g. fdce.b00c.cate/ba00c.56) Prefix L enoth			
	64			
	Length of per-node allocated prefixes			
	Country			
	Country			
	Other •			
	Channels			
	Enabled Channels			
	2			
	This configuration is used by the controller for auto config override. Channels set manually ignore this configuration.			
	DNS Sequere			
	Una activita			
	DNS server list, comma separated. IPv4 is only supported when Layer 2 bridge is enabled.			

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

	Configuration		
	Network Nodes		
ß	Basic Management Radio Security Advanced	Submit	Cancel
۵	Prefix Allocation		
<u>~</u>	Centralized      Deterministic		
	Seed Prefix		
¢	2016:4321:4321:4300::/56		
۰	Generate IP/6 Seed prefix in CIDR format from which subnet prefixes are allocated to all DNs and CNs (e.g., fore:b0cc:exteabl00:56)		
	Prefix Length		
	64		
×	Length of per-node allocated prefixes		
1	Country		
	Country		
	Other 👻		
	Channels		
	Enabled Channels		
	2		
	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 3001:0:00XY::/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

Config	juration				
Netwo	rk Nodes				
Basic	Management	Radio	Security	Advanced	
10	.110.186.32				
NTP : bridge	Server hostnames o e is enabled.	r IP addresses,	comma separa	ted. IPv4 is only supported when Layer 2	
- Con	figuration Mar	nagement			
E	2E Managed Co	nfig			
Deter	mines whether the c	ontroller should	d manage the n	de's configuration.	
- Wire	eless Scans				
Scho	duled Ream Adia	etmont			
OE	nabled 💿 Disa	abled			
Scar	Interval				
14	400				
Interv	al between wireless	scans in secor	nds		
- IPv6	Layer3 CPE	Address			
• s	LAAC ODHC	Pv6 Relay			
- CPE	Prefix Zoning	1			
Sum	marized CPE Pre	fix			
30	01::/58				6
Prefix	summarizing netwo	ork wide custom	nized CPE Prefit	es/Prefixes allocated by DHCPv6 Relay	

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

Netwo Basic SNN Syst Syst	Management Radio Security Advanced MP Enable SNMP			
Basic SNM F Syst Syst No Syst	Management Radio Security Advanced MP Enable SNMP			Conservation of the second
- SNM Syst Syst Syst	MP Enable SNMP			Submit
Syst No Syst	Enable SNMP			
Syst N Syst				
N- Syst	em Contact			
Syst	lo Contact			
5.1	em Location			
14	lo Location			
-] SNN	MPv2C Settings			
SNN	MP Community string			
PL	ublic			
SNM	IP community with read-only access to all OIDs			
IPv4	\$ Source Address			
Allow	ved IPv4 source address subnet (Example: 10.10.10.0/24)			
IPv6	5 Source Address			
Allow	ved IPv6 source address prefix (Example: fdceb000ccafeb000;/64) MPv3C Settings 40:01 Linex			
JININ	sor1			
Seci O M	urity Level None Authentication Only Authentication & Privacy hentication type			
Auth	horization Key			
g GUI	Users			
Adm	nin User Password			
Insta	aller User Password			
Mon	nitor User Password			

- 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.

Parameter	Description
Scheduled Beam Adjustment	Allows you to enable or disable the scheduled beam adjustment feature.
	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 <b>Scan Schedule Type</b> parameter.
Scan Schedule Type	Allows you to select the scan scheduling option for beam adjustment.
	This parameter supports the following scan scheduling options:
	<ul> <li>Day/Time: This schedule option allows you to select any day (or all days) of the week and time of the day.</li> </ul>
	When you select the <b>Day/Time</b> option, following parameters are applicable:
	<ul> <li>Schedule Day(s): Select the check boxes to choose the day(s).</li> </ul>
	<ul> <li>Schedule Time: Use the Schedule Time: Use the time of the day.</li> </ul>
	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.
	• Interval: This scan schedule option allows you to set an interval (in seconds) for wireless scans. The default value is 3600 seconds.

Table 45: Parameters in the Wireless Scans section

- 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

60 GHz cnWave** v5000	🖉 Disable E2E Controller 🔱 Reboot 🕒 admin -
Configuration Network Nodes	
Basic Management Radio Security Advanced	Submit Cancel
Wireless Scans         Scheduled Beam Adjustment         Emabled       Disabled         Scan Schedule Type       Day/Time I Interval         Day/Time I Interval       3600         Interval between wireless scans in seconds.       Interval	
CN Channel Re-scan     Otsable     CN Channel Re-scan Timeout     120     A CN without a wireless link established beyond this timeout will automatically initiate channel scanning.	

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 <b>Enable</b> 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	<ul> <li>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).</li> <li>By default, the value of this timeout option is set to 120 seconds. This option allows the value ranging from 120 to 3600 seconds.</li> </ul>

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

	Configuration
-	Network Nodes
U	Basic Management Radio Security Advanced Submit Cancel
۵	Wireless Security
٩	◯ Disabled ◯ PSK ● 802.1x Enable wireless security and set the method
¢	Radius server IP
•	IP address of auth (i.e., radius) server Radius server port
*	Auth server shared secret
1	

#### 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.



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

#### Figure 176: The Advanced page

Caution

	60 GHz cnWave <sup>3w</sup> V3000		O Disable E2E Controller	Reboot	8 ad	min 🕶
	Configuration Network Nodes Basic Management Radio Security Advanced			Subm	a) C	lancel )
0	All the settings below are for advanced users only.					
æ	Q, Search Base: default	<ul> <li>Hardware: V10</li> </ul>	000_188_11	Table JSON	Add N	5M.
¢.	Field	Status	Value			
¥	snmpConfig.contact	set	No Contact	0	5	/
	snmpConfig.location	set	No Location	0	5	1
-	popParams,POP_STATIC_ROUTING	set	0	0	5	1
	popParams.POP_IFACE	unset		0	5	1
*	popParams.VPP_ADDR	unset		0	5	1
略	popParams.NAT64_POP_ENABLED	set	0	0	5	1
~	popParame.POP_BGP_ROUTING	set	0	0	5	1
	popParams.NAT64_IPV6_PREFIX	unset		0	0	1
	popParams.POP_ADDR	unset		0	10	1
	popParams.GW_ADDR	unset		0	10	1
	popParams.NAT64_IPV4_ADDR	unset		0	10	1
	1960 81 G.			6		

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 CAMBIUM_POP_UNREACHABLE_REBOOT_ TIMEOUT_INTERVAL parameter), after which it reboots.
	Note: The CAMBIUM_POP_UNREACHABLE_REBOOT_TIMEOUT_ INTERVAL parameter is available on the <b>Configuration</b> > <b>Advanced</b> 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: 1. The DN will lose all its links and recovery will be slower, necessitating careful usage of this feature.

FAQ	Answer
	<ol> <li>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> <li>Scanning of CB1 and CB2 channels at a time is not supported.</li> </ol>

# 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
- <u>VLAN</u>
- 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

Configuration									
Q Search	Rad	lo Netwo	orking VLAN Securit	v Advanced				Submit C	an
PoP-V5K-884938	- E	IRP							
🖗 DN-V5K-3f69	Ň	Aaximum EIR 38	P						
	II (	BF Transmit P	ower e (<25m) optimized () Long	g range optimized					
	" ۹ ⊡	atial Beam Form	ning transmit power setting						
	N	Ainimum MC	S						
	N	Ange - (z. 12) Aaximum MC 12	5						
		lange - [2, 12] Sector 1							
	h	hannel/Polari igher up on [ Override	ity change should originate fro DNs. Name	Auto Config	e make sure to change	on the CNs first and	then		
			Channel	1	1		~		
		0	Polarity	Even			~		
	<u> </u>	iector 1 Link	(s) Golay						
		Override	Name	Auto Config (Rx/Tx)	Node Golay Rx	Node Golay Tx			
			link-DN-V5K-3f69-PoP	2/2		*	~		
	<u> </u>	Override All ector 2							
	C h	'hannel/Polari igher up on D	ity change should originate fro INs.	om the leaf nodes.Pleas	e make sure to change	on the CNs first and	then		
		Override	Name	Auto Config	Node Config				
		0	Channel				~		
		0	Polarity				~		
	- S	ector 2 Link	c (s) Golay						
		Override No Data	Name	Auto Config (Rx/Tx)	Node Golay Rx	Node Golay Tx			
		Force GPS	Disable he radio will use internal sync rathe	er than GPS sync					

# The Radio page contains the following elements:

Table 47: Elements in the Radio page

Elements	Description
EIRP	Transmit power of the radio
	<ul> <li>Maximum EIRP - The maximum EIRP transmitted by the radio. Range differs based on the platform and country selected (in the Network page).</li> <li>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.</li> </ul>

Elements	Description				
Adaptive Modulation	Select minimum and maximum coding scheme ranging from 2 to 12.				
Sector 1	<ul> <li>Select the frequency channel and polarity.</li> <li>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.</li> </ul>				
Sector 1 Link (s) Golay	Golay codes help in avoiding inter-sector interference. In rare scenarios, individual links might require separate Golay codes. In most scenarios, all the links belonging to a sector are configured same Golay code. The controller automatically sets the Golay code. To manually override, select the check box and set the Golay from the drop-down. <b>Override All</b> button helps in setting the same Golay code for all the links.				
	Note           Golay codes and frequency on both ends of the link should match.				
Sector 2	Select the frequency channel and polarity.				
Sector 2 Link (s) Golay	Golay code.				
GPS	If enabled, 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

-	Configuration		
5	Network Nodes		
U)	Q Search	Radio Networking VLAN Security Advanced Submit	Cancel
	💏 V3K-416b-PoP		
④	🖗 V3K-DN-5419	51	
ф	💦 V3K-CN@7049	Allowed range is 35 dBm to 55 dBm	
۵	🕅 V3K-DN2-6f97	Short range (<25m) optimized  Cong range optimized	
		india Beam Forming transmit power setting	
*		Antenna Dish Gain	
1		44.5 dBi ~	
-0		PTP Deployment Range	
		PTP Deployment Range	
		Upto 1.5 km v	
		Deployment range applicable in Point to Point deployment. Please change for the far end node first.	
		Adaptive Modulation	
		Minimum MCS	
		2	
		Range - [2, 12]	
	Cautic	n	
1	Small	lish 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

onfiguration Network Nodes		
Search PoP-V5K-884938	Radio Networking VLAN Security Advanced IPv4 Management IPv4 Address	Submit Cancel
DN-V5K-3f69	169,254,1.1         Subnet Mask         255,255.0.0         Gateway IP Address         PoP Configuration         PoP Routing         Border Gateway Protocol (BGP) Routing         PoP Interface         Aux       Main         SFP       Disabled         Hy6 address on the interface that the POP node uses to communicate with the upstream outer. Prefix flexing is freed a c4.	

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

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

Q Search	Radio Networking VLAN Security Advanced	Submit	Cancel
PoP-V5K-884938	PoP Configuration		
C DN-V5K-3f69	PoP Routing Border Gateway Protocol (BGP) Routing  Static Routing		
>	PoP Interface		
s	IPv6 address on the interface that the PoP node uses to communicate with the upstream router. Prefix length is fixed as 64.		
-	PoP Interface IP Address		
<b>"</b>	2604:0:0:2c00::2		
×	Generate		
	upstream router. This IPv6 address should not be in the same subnet as Seed Prefix		
0	IPv6 Gateway Address		
	2604:0:0:2c00::1		
	A configured IPv6 Gateway Address must be reachable from the PoP for the system to		

Figure 180: The PoP Configuration section in the Networking page

Table 49	9: Elements	in the	PoP	Configuration	section
				configuration	30001

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

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

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

1	
ŕ	2
L	レ

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

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.

Table 50: Elements in the E2E Controller Configuration section

4. Select the required BGP configuration.

Note

Figure 181: 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

Table 51: Elements in the BGP Configuration section

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

-	Configuration Network Nodes		
D	Q. Search	Radio Networking VLAN Security Advanced Submit Cance	н
۵	🥐 PoP-V5K-884938	Ethernet Ports	
۲	🖗 DN-V5K-3f69	✓ Enable Main	
¢		✓ Inable Aux ✓ Enable SFP	
۰		Layer 2 Bridge	
		Disable Broadcast Flood Broadcast packets (except DHCP Offer and DHCP Ad) in the downlink direction including client to client packets will be dropped.	
*		Disable Unknown Unicast Flood	
16		Disable IPv6 Monitor IPv4 Gateway	

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.

-	Configuration		
Ē	Network Nodes		
	Q Search	Radio Networking VLAN Security Advanced	Submit Cancel
۵	node-V5000-886cf5	Layer 2 Bridge     Disable Broadcast Flood	
٢	🖗 node-V5000-030405	Broadcast packets (except DHCP Offer and DHCP Ack) in the downlink direction including client to client packets will be	
¢	🕅 node-V5000-778899	Disable Unknown Unicast Flood	
4	🕅 node-V5000-883088	Disable IPv6 Monitor IPv4 Gateway	
	R DN	In Layer 2 bridging with multiple POP nodes, enabling this feature will configure this POP to periodically ARP ping the configured IPv4 Gateway: If the ARP pings are to fail all other nodes within the	
*		mesh network will choose one of the other available POP nodes to route to	
1		DHCP Option 82 Enabled  DHCP option 82 will be inserted in the DHCP requests.	

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	It has three options: Disable Broadcast Flood Disable Unknown Unicast Flood Disable IPv6 Monitor IPv4 Gateway
	For information on <b>Monitor IPv4 Gateway</b> , refer to <u>Configuring Monitor IPv4 Gateway</u> ,
Aux PoE	Enable PoE out (25 W) on V5000/V3000 aux port. 802.3af and 802.3at compliant devices could be powered up, passive PoE devices cannot be powered up. Note that the aux port cannot power another V5000/V3000.
Multi-PoP / Relay	Indicates the wired interfaces (or Ethernet) on which OpenR is running. This element must be used:
Port	<ul> <li>When DNs are connected back-to-back.</li> <li>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</li> </ul>
	Following options are supported:
	<ul> <li>Aux</li> <li>Main</li> <li>SFP</li> <li>Disabled</li> </ul>

## 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 18	4: The DI	HCP Optior	n 82 feature
-----------	-----------	------------	--------------

Configuration		
Q, Search	Radio Networking VLAN Security Advanced	
Rim_PoP@300c	Gateway IP Address	
(R) DN_1@3000		
R DN2@3009	Ethernet Ports	
🖗 DN3@309d	Enable Main     Enable Aux	
DN4@3017	Enable SFP	
	Layer 2 Bridge	
	DHCP Option 82     Enabled     Disabled	
	DHCP option 82 will be inserted in the DHCP requests.	
	Circuit ID	
	<pre>\$siteName\$:\$networkName\$:\$nodeName\$</pre>	0
	Supported wildcards are \$nodeMac\$, \$nodeName\$, \$siteName\$, \$networkName\$	
	Remote ID	
	Supported wildcards are SourieMan's SourieMame's SociaName's Sociationaries	•

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

	Configuration			
۵	Network Nodes	Radio Networking VLAN Security Advanced	Submit	Cancel
۵	node-V5000-886cf5	Layer 2 Bridge     Disable Broadcast Flood		
ᢙ	🖗 node-V5000-030405	Broadcast packets (except DHCP Offer and DHCP Ack) in the downlink direction including client to client packets will be		
¢	🕅 node-V5000-778899	dropped.		
۵	🕅 node-V5000-883088	Disable IPv6		
	R DN	<ul> <li>Monitor in we cateway         In Layer 2 bridging with multiple POP nodes, enabling this feature         will configure this POP to periodically ARP ping the configured IPv4         Gateway. If the ARP pings are to fail, all other nodes within the     </li> </ul>		1
*		mesh network will choose one of the other available POP nodes to route to		
\$		DHCP Option 82 Enabled  DHCP option 82 will be inserted in the DHCP requests.		

- 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

	Configuration Network Nodes		
٥	Q Search	Radio Networking VLAN Security Advanced	Submit Cancel
۵	PoP-V5K-884938	Multi-PoP / Relay Port	
() ()	ℜ DN-V5K-3f69	Multi-PoP / Relay Port Interface Aux Main SFP  Disabled Wired interfaces on which OpenR is num. Should be used when DNs are connected back to back and on PDPs in a multi POP network.	
▲ □ × ₺		OOB     NoteFace     Nutrian SFP Disabled     Out of hand management interface to access the device. Management VLAN will be     bypassed and data traffic will not be routed or bridged on this interface.     IPV4 Address     10.110.186.179     Subnet Mask     255.255.255.0	

#### **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:



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 <u>device UI</u> or the <u>cnMaestro UI</u>.

# Using the device UI:

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

- 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

	60 GHz cnWave <sup>16</sup> V2000		O Disable E2E Controller	() Reboot 👌 admin	•
	Configuration Network Nodes				
D	Q, Search	Radio Networking VLAN Security Advanced		Submit Cano	el
۵	node-V2000-73d03e	- OOB			
٩	R CN	OOB Interface			
ф		Out of band management interface to access the device. Management VLAN will be bypassed and data traffic will not be			
۵		routed or bridged on this interface.			
		PTP External Failover External Failover Link     Aux Main Disabled			
*		External Failover Device IPv4 or IPv6 Address			
1		10.1.1.1			
		This IP address should be in a different subnet than node IP, seed prefix. External device GUI (e.g PTP450 or ePMP) can be accessed using http://c.rwave.node IP>50080/ or https://c.rwave.node IP>50442/			

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



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.

Cambium Networks | cnMaestro <sup>14</sup> X 0 Add new field Field Name Networks Wi-Fi AP Group A envParams.CAMBIUM\_EXTERNAL\_FAILOVER\_IFACE String Syster Value v 🖢 Base Infrastructure nic2 > . default > 1 60 6 > 🔯 RK-L NA RM 0 > 9 5 ٩ 0 0 \*

Figure 189: The Add new field page in the cnMaestro UI

- 4. In the Value fie
- 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.

CIIVAVE E2E-00303E	Save Cancel		Value	
Onboard-V3k-230	assertParams.cambiumAssertRecoveryEnabled	set	true	~ /
ive	+ bgpParams.allowNonDefaultRoutes	set	false	~ /
	bgpParams.cpePrefixesAutoAdvertisement	set	true	~ /
	bgpParams.specificNetworkPrefixes	set	fd00:ceed:8551:3300::/56	~ /
	debugSysParams.cambiumSysMonitorEnabled	set	false	~ 1
	dhcpParams.dhcpGlobalConfigAppend	unset		~ 1
ř.				

Ca our	normal rectronal Childrand A	Add new field		×		2.5	All Accou	ntis. 👻 丨	~
	Q. Search								
	Networks Wi-Fi AP Groups	Field Name			Software Update	Tools			
Π	V 🕄 System	envParams.CAMBIUM_EXTERNAL_FAILOVER_IFACE_ADDR	String	~					
	✓ ➡ Base Infrastructure	Value							
-	> 🎝 default	10.1.1.1				-	_		
•	> 💸 60 GHz cnWave E2E-88303E					Table	JSON	Add Nev	1
9	> 🕅 RK-LAB-Onboard-V3k-230	Save Cancel			Value				
-	✓ 🏂 RM-cnWave	assertParams.cambiumAssertRecoveryEnabled	set		true			15 J	1
۳	> g Site01	j bgpParams.allowNonDefaultRoutes	set		false			5	1
	> 8 Site02	bgpParams.cpePrefixesAutoAdvertisement	set		true			10517	1
-	> g Site03				600 an and 01		an e l'		,
-	> g Site04	bgpParants.specificivetworkerteitxes	561		idoo.ceed.s:	513300	250	-	1
<b>11</b> •	> g Site05	debugSysParams.cambiumSysMonitorEnabled	set		false			5	1
	Site06	dhcpParams.dhcpGlobalConfigAppend	unse	et					1

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

Ce Ca	mbium Networks cnMaestro <sup>™</sup> X		a 📴 🖓		(!) MSP V	iew O
-	Q Source	Add new field	×		All Acco	0
	Networks Wi-Fi AP Groups	Field Name		Software Update	Tools	
	<ul> <li>✓ System</li> </ul>	envParams.CAMBIUM_EXTERNAL_FAILOVER_NODE_ADDR	String ~			
<b>H</b>	✓ D Base Infrastructure	Value				
▦	> V default	10.11.2			Table JSON	Add New
9	> 🕅 RK-LAB-Onboard-V3k-230	Save Cancel		Value		
1757	∽ 📸 RM-cnWave	assertParams.cambiumAssertRecoveryEnabled	set	true		~/
9	> g Site01	F bgpParams.allowNonDefaultRoutes	set	false		~1
9	> g Site02	bgpParams.cpePrefixesAutoAdvertisement	set	true		~ /
<b>\$</b>	> g Site03	bgpParams.specificNetworkPrefixes	set	fd00:ceed:85	551:3300::/56	~ /
<b>#</b> *	> g Site05	debugSysParams.cambiumSysMonitorEnabled	set	false		~ /
<b>b</b>	> g Site06	dhcpParams.dhcpGlobalConfigAppend	unset			~ 1
1.00	> g Site07	dhcoParams.dhcointerface	unset			51

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

 Q
 QinQ

 Image: Constraint of the second secon

## **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

Native VLAN ID	
23	
Allowed range is 1 - 4094	
Native VLAN Priority	

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

Figure 194: Allowed VLANs

2		
2		

Allow only the listed range of VLAN IDs.

Figure 195: Untagged types

Untagged	Packets
Allow	Orop

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



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

Figure 197: Native S-VLAN ID and priority

Native S-VLAN ID	
34	
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

Allow Drop	
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

-	

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

#### 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	<b>Override Priority</b>	
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
	2
	Allowed range is 1 - 4094
	VLAN Priority
	1
	Allowed range is 0 - 7
	Add Outer Tag
	S-VLAN ID
	3
	Allowed range is 1 - 4094
	S-VLAN Priority
	2
	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

	Configuration		
5	Network Nodes		
U	Q Search	Radio Networking VLAN Security Advanced	Submit Cance
۵	PoP-V5K-884938	Radius user identity	
Ð	DN-V5K-3f69	cambium	
4	4	Private key password	
٠		Radius Private key password Radius user password	
		Radius user password	
*			
ъ			

#### Controller UI configuration

This Controller GUI configuration to be made on each DN.

Figure 205: Elements specific to Controller configuration

Configuration	
Network Nod	les
Q Search	Radio Networking VLAN Security Advanced
POP	Radius user identity
	test
WY DIN	Private key password
	•••••
	Radius Private key password
	Radius user password
	•••••
	Radius user password

# 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	Browse
Certificates sent by radius server are certificate	e verified against this CA
Client Certificate	
client.pem	Browse
Private key with which client will enc	rypt
Client Private Key	
client.key	Browse
Private key with which client will dec	rypt



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.



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.

Note



# Caution

Users are not recommended to do these settings.

Figure 207: The Advanced page - Node configuration

	<sup>−</sup> 60 GHz cnWave™ V3000			O Disable E2E Controller U Reb	oot	<b>8</b> a	dmin <del>•</del>			
	Configuration Network Nodes									
D	Q Search	Radio Networking VLAN Security Advanced	Submit							
	node-V3000-8830da	All the settings below are for advanced users only.								
⊛		Q. Search		Table JSON Show Full Configura	tion	Add	New			
		Field	Status	Value						
φ		snmpConfig.contact	set	No Contact	0	5	1			
۵		snmpConfig.location	set	No Location	0	5	1			
		popParams.POP_STATIC_ROUTING	modified 🚘	1	0	5	/			
ш		popParams.POP_IFACE	modified 🚘	nic2	0	5	1			
*		popParams.VPP_ADDR	unset		0	5	1			
**		popParams.NAT64_POP_ENABLED	set	0	0	5	1			
-0	9	popParams.POP_BGP_ROUTING	modified 🚉	0	0	5	1			
		popParams.NAT64_IPV6_PREFIX	unset		0	5	-			
		popParams.POP_ADDR	modified 🖀	fd00:ba5e:0088:30da::88:30da	0	5	1			
		popParams.GW_ADDR	unset		0	5	1			
		popParams.NAT64_IPV4_ADDR	unset		0	5	1			
					0					

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:

	60 GHz cnWave™ V5000							Ø Disable	e E2E Controller 🔱 Reb	oot 🔒 admin •
-	Software Upgrade									
۵	Node Upgrade Imag	ges Node Up	grade Status							
B	Q. Search		0							
	Name	Model	Туре	Alive?	Site	PoP Node	Upgrade Status	Reason	Image Version	Next Version
æ	PoP-V5K-884938	V5000	DN	Yes	PoP-site-V5K-8849	Yes	NONE	2	1.2	
	DN-V5K-3f69	V5000	DN	Yes	DN-Site@3f69	No	NONE	÷	1.2	
¢					st i 1 2	ю 10 м				
۰										
*										
40										

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).

	60 GHz cnWave <sup>™</sup> V50	20						Ø Disabl	e E2E Controller 🔱 Rebo	ot 🕴 admin -
	Software Upgr	ade								
۵	Node Upgrade	Images Node Up	grade Status							
ត	Q Search		0						Prepa	Commit Reset
-	Name	Model	Туре	Alive?	Site	PoP Node	Upgrade Status	Reason	Image Version	Next Version
	PoP-V5K-88	4938 V5000	DN	Yes	PoP-site-V5K-8849	Ves	NONE	-	1.2	22
	DN-V5K-3f6	9 V5000	DN	Yes	DN-Site@3f69	No	NONE	1	1.2	50
¢					« ( <u>1</u> )	ю 10 ч				
٠										
*										
1										

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

	60 GHz cnWave <sup>w</sup> VS000			O Disable E2E Controller	() Reboot	😑 admin 🕶
	Software Upgrade Node Upgrade Images Node Upgrade Status					
ני הו	Q. Search					Upload Image
	Name	Hardware				
۲	v5000-v3000-upgrd-1.2.189.img	V5000,V3000				8
*	v1000-upgrd-1.2.189.img	V1000				茵
Ŷ		•	c 1 > >> 10 ~			
٩						
•						
*						
16						

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

	60 GHz cnWave <sup>™</sup> V5000				O Disable E2E Controller	ot 😮 admin -
-	Software Upgrade					
۵	Node Upgrade images	Node Upgrade Status				Abort Upgrade
۵	Nodes in Current Batch					
	Name	Upgrade Status	Upgrade Request ID	Current Image Version	Next Image Version	
æ	No Data					
¢			«c « 1 » »» 10	*		
٠	Nodes in Pending Batch					
	Name	Upgrade Status	Upgrade Request ID	Current Image Version	Next Image Version	
ш	No Data					
*			« « <mark>1</mark> » » 10	*		
稔						

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**.

	60 GHz cnWave™ V3000					O Disable E2E Controller	U Reboot	e admin-
	Diagnostics Events DA Logs I	Engineering	Logs					
B			1577.7					Export
0	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 <u>View Details</u>		
¥.	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 <u>View Details</u>		
*	Sep 14, 2022, 6:28:25 AM	Info	node-V3	Scan resp	minion-app-DRIVER_APP	Received scan response <u>View Details</u>		
	Sep 14, 2022, 6:28:24 AM	Info	v2k_cn	Driver link status	minion-app-IGNITION_APP	Received LINK_UP for neighbor 12:04:56:88:4. View Details	2:23 on interface	terra0 (42:cb
NO.	Sep 14, 2022, 6:28:24 AM	Info	v2k_cn	Node info	minion-app-STATUS_APP	Minion is online <u>View Details</u>		
	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**

	60 GHz crWave <sup>w</sup> v3000 🖉 Disable EZE Controller 🔱	Reboot	e admin
	Diagnostics Events DA Logs Engineering Logs	€ G	
9 (-)	<pre>connection refused","name":"e2e","time":"2022-09-13T11:36:092") ["file":"init.go:S2","func":"e2e.("#E2E).Init","level":"error","msg":"Post \"http://[::1]:8080/internal/local/getDeviceInfo\": dial tcp [::1]:8080: conne connection refused","name":"e2e","time":"2022-09-13T11:36:092") ["file":"init.go:200","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":"2022-09-13T11:36:092") </pre>	ect:	
•	<pre>('file':main.go:118', 'func':main.main', 'level':mino', 'msg'''All retry in sometime', 'name':'main', 'time'':2022-09-13111;36:092') ('file':main.go:128', 'func':'main.main', 'level':mino', 'msg''', 'onfiguration Loadéd Successfully, 'name'':main', 'time'':2022-09-13111;36:142') ('file':"e2e.go:824', 'func':'e2e.(*E2E).GetSerialNo', 'level':'info', "msg'':'onboard e2e getDeviceInfo API (Type:POP Name:node-V3000-884223 Nac:00:04:56:88:42:23 Msn:VSKO306Q2FDB NodeLV3000]', "name''' "e2e', 'time'':'2022-09-13111;36:162') ('file':"con.go:84', 'func':'agent.('fagent).routerConnect', "level':'info', "msg'':'onboard e2e getDeviceInfo API (Type:POP Name:node-V3000-884223 Nac:00:04:56:88:42:23 Msn:VSKO306Q2FDB NodeLV3000]', "name'''' each', 'time'''''''''''''''''''''''''''''''''''</pre>		
*	<pre>("file":"con.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":"agent","agent","agent","level":"info","msg":"Redirecting to Server: https://10.110.186.92/device","name":"agent","time":" 09-13711:36:1727) ("file":"can.go:281","func":"agent.("Agent).connect","level":"info","msg":"nedirecting to Server: https://10.110.186.92/device","name":"agent","time":" 09-13711:36:1727)</pre>	"2022- 88:4223	
¥©.	Guddr: ] Env@rams:(MgmtTPvAddr:169.254.1.1)", "name"."22e", "time": 2020-013T1136:122") ("file":"con.go:188", "finc":"agent.("Agent).serverConnect", "level":"info", "msg":"Connecting to Server: wss://10.110.186.92/device? deviceId=hvlXtxborKfacVbfFylKCHYVKFfsvJdETVxydIXXJ2fi5ts_UtsY263OuTXPDuFA03FpzmCch8xrm8280Tw8type=cnAgent&serialNovVXX036Q2FD8&mac=00:04:56:88:42:22 e2e&deployment=conboard.", "name": "agent.", "time": "2022-09-13T11:36:127") ("file":"msg_handler.go:211","func": "agent.("Agent).ssgHandlerUnManaged", "level": "warning", "msg":"cnMaestro (1663068978) and agent(1663069097) time are sync", "name": "agent", "time": "2022-09-13T11:36:182")	3&mode= not in	

## **Engineering logs**

	60 GHz cnWa	ve™ V3000								O Disable E2E Contro	oller 🕛 Reboot	e admin -
	Diagnos	tics										
100	Events	DA Logs E	naineerina Loa									
<b>F</b>			5 5 5									
		Select Logs	e2e_minion	~	Select Node	node-V3000-	884223	*			± €3	
B		109714-071	5144 644415 A	(X5 Uneart Litenter	C00-1851 M	CALLAR PROMAT	TOP POUTINE	1112 ADC 185 *00	e ctrl.ann.libtiliby	100		
		10914 07:	35:45.753321 4	785 OpenrClientAp	.cpp:7451 Re	ceived request	to set prefi	kes from ctrl-a	pp-TOPOLOGY APP			
1.00		10914 07:	36:00.754289 4	785 OpenrClientAp	.cpp:745] Re	ceived request	to set prefi	kes from ctrl-a	pp-TOPOLOGY APP			
Ð		10914 07:	36:14.635551 4	785 OpenrClientAp	.cpp:186] Re	eceived request	for routing	adjacencies fro	m ctrl-app-TOPOLOGY	APP		
		10914 07:	36:15.754316 4	785 OpenrClientAp	.cpp:745] Re	sceived request	to set prefi	kes from ctrl-a	pp-TOPOLOGY_APP			
4		I0914 07:	36:30.753890 4	785 KvStoreClient	cpp:1110] Ad	overtising ttl u	pdate (key,	version, origin	atorId, ttlVersion)	(e2e-network-allocations,	, 1, node-	
¥		00.04.56.1	88.42.23-minion	, 958)								
		10914 07:	36:30.754791 4	785 KvStoreClient	cpp:1130] Sc	cheduling ttl ti	mer after 75	000ms.				
		10914 07:	36:30,755339 4	785 OpenrClientAp	o.cpp:745] Re	eceived request	to set prefi	kes from ctrl-a	pp-TOPOLOGY_APP			
		10914 07:	36:44.636705 4	785 OpenrClientAp	o.cpp:186] Re	eceived request	for routing	adjacencies fro	m ctrl-app-TOPOLOGY	_APP		
Final Action		10914 07:	36:45.755650 4	785 OpenrClientAp	o.cpp:745] Re	eceived request	to set prefi	kes from ctrl-a	pp-TOPOLOGY_APP			
		10914 07:	57:00.750414 4	785 OpenrClientAp	0.cpp:/45] Re	sceived request	to set prefi	kes from ctri-a	pp-TUPULUGY_APP	400		
		10914 07.	57.45 75750A A	785 OpenrClientAp	crep: 2451 Rd	scelved request	to set croff	as from stol a	en TOPOLOGY ADD	APP		
*		10914 07:	37:30.758208 4	785 OpenrClientAp	. con: 7451 Re	ceived request	to set prefi	es from ctrl-a	no-TOPOLOGY APP			
		10914 07:	37:44.638347 4	785 OpenrClientAp	.cpp:1861 Re	ceived request	for routing	idiacencies fro	m ctrl-app-TOPOLOGY	APP		
164		10914 07:	37:45.755472 4	785 KvStoreClient	cpp:1110] Ad	vertising ttl u	pdate (key,	version, origin	atorId, ttlVersion)	(e2e-network-allocations,	1, node-	
AC)		00.04.56.0	88.42.23-minion	, 959)								
		10914 07:	37:45.756389 4	785 KvStoreClient	cpp:1130] Sc	heduling ttl ti	mer after 75	ooms.				
		I0914 07:	37:45.758283 4	785 OpenrClientAp	.cpp:745] Re	rceived request	to set prefi	kes from ctrl-a	pp-TOPOLOGY_APP			
		I0914 07:	38:00.759429 4	785 OpenrClientAp	.cpp:745] Re	rceived request	to set prefi	kes from ctrl-a	pp-TOPOLOGY_APP			
		10914 07:	38:14.639420 4	785 OpenrClientAp	o.cpp:186] Re	eceived request	for routing	adjacencies fro	m ctrl-app-TOPOLOGY	_APP		
		10914 07:	38:15.759724 4	785 OpenrClientAp	o.cpp:745] Re	rceived request	to set prefi	kes from ctrl-a	PP-TOPOLOGY_APP			

# **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 **III** icon (as shown in Figure 210), the **Links** page displays the relevant elements and statistics.

## Figure 210: The Links page

	60 GHz cnWave™ VS	000													Ø Dis	able E2E (	Controller	U Reboot	9	admin +
	Statistics																			
Б	Links Etherr	vet GPS R	tadio Performa	nce BGP															Download	Statistics
ര																				iii-
<b>(</b> )	Link Name	Reporting Node	A Node Sector MAC	Z Node Sector MAC	RSSI	Link Fade Margin	Rx SNR	Rx MCS	RX PER	EIRP	Tx MCS	RX Through	TX Through	Rx Airtime %	Tx Airtime %	TX PER	Rx Beam Azimuth	Tx Beam Azimuth	Rx Beam Elevation	Tx Beam Elevation
\$																	Angle	Angle	Angle	Angle
	link-V5K_DN	V5K_DN	12:04:56:88:	12:04:56:88:	-52	41	22	9	0	13	9	1.69	11.4	100	100	0	10.2	10.2	20	20
	link-V5K_DN	node-V5000	12:04:56:88:	12:04:56:88:	-55	38	19	9	0.83	13	9	.11.4	1.69	100	100	0	21.8	21.8	2.2	2.2
								- 95	1 2	>> 10	~									

The Links page displays the following elements:

Tabl	e 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	The statistic value (in dB) available for each RF link
Margin	The <b>Link Fade Margin</b> statistic values help operators to quickly assess any additional system gain or low marginal RF links (if any), which must be addressed.
	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
	<ul> <li>Considering the RSSI value that is calculated based on how far away it is from an established receiver sensitively floor of -72 dBm.</li> </ul>
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 <b>Rx Airtime %</b> , this metric provides insights into how airtime is distributed among links when transmitting data. This metric is only relevant for a DN.
Following repl	ace <b>Rx Scan Beams</b> and <b>Tx Scan Beam</b> elements:
Rx Beam	The angle of the selected fixed beam (in degrees) in the azimuth direction for each link.
Azimuth Angle	The selected beam is independent of transmit and receive directions. For more information on $T_{x}/P_{x}$ azimuth beam angle statistics, refer to the Link diagnostics -
Tx Beam Azimuth Angle	Beam angle statistics section.
Tx Beam Elevation Angle	The angle of the selected fixed beam (in degrees) in the elevation direction for each link.
Rx Beam Elevation Angle	information on Tx/Rx azimuth beam angle statistics, refer to the <u>Link diagnostics</u> - <u>Beam angle statistics</u> section.

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

Lini	ks E	thernet	GPS Radio	Perform	ance Prefix	Zones E	3GP							Downlo	oad Statistics
٩ :	Search				0									Aux Main	SFP
Devi Nam	ice Ie	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 Throughpu
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:

Та	ble	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

Statistics							
Links Eth	emet GPS	Radio Perform	ance Prefix Zones	BGP			Download Statis
Device Name		MAC Address	Fix Type	Satellites tracked	Latitude	Longitude	Height
DN2@PoP2@3	009	00:04:56:88:30:09	3D	17	12° 56' 2.139" N	77° 41' 39.936" E	931 m
Prim-PoP@300	0_1	00:04:56:88:30:0c	3D	17	12° 56' 2.138" N	77° 41' 39.934" E	931 m
DN1@PoP1@	000	00:04:56:88:30:00	3D	17	12" 56 2.149" N	77° 41' 39.936" E	931 m
DN3@PoP1@	09D	00:04:56:88:30:9d	3D	17	12° 56' 2.138" N	77° 41' 39.935" E	932 m
DN4@PoP2@3	10f7	00:04:56:88:30:f7	3D	18	12° 56' 2.144" N	77° 41' 39.936" E	932 m
				« « <b>1</b> » »	10 ~		

## 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 Туре	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

1

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

## Figure 215: The Radio page

G	60 GHz cnWave™ V5000	í.					Ø Disable E28	E Controller 🔱 Rel	poot 😫 admin -
	Statistics Links Ethernet	GPS Radio	Performance F	Prefix Zones BGP					Download Statistics
	Device Name	MAC Address	Sync Mode	Channel	Security	Error Association	Channel Last State	RX Throughput	TX Throughput
6	DN2@PoP2@3009	12:04:56:88:30:09	GPS	1	PSK	0	0	2.77 kbps	2.88 kbps
	DN2@PoP2@3009	22:04:56:88:30:09	GPS	3	PSK	0	0	7.58 kbps	10.80 kbps
Ð	Prim-PoP@3000_1	12:04:56:88:30:0c	GPS	3	PSK	0	0	12.49 kbps	12.29 kbps
<b>6</b>	Prim-PoP@3000_1	22:04:56:88:30:0c	GPS	1	PSK	0	0	24.69 kbps	12.99 kbps
*	DN1@PoP1@3000	12:04:56:88:30:00	GPS	1	PSK	0	0	10.22 kbps	21.82 kbps
2	DN1@PoP1@3000	22:04:56:88:30:00	GPS	4	PSK	0	0	16.47 kbps	5.40 kbps
	DN3@PoP1@309D	12:04:56:88:30:9d	GPS	4	PSK	0	0	6.46 kbps	15.49 kbps
11	DN3@PoP1@309D	22:04:56:88:30:9d	GPS	1	PSK	0	0	11.03 kbps	4.64 kbps
20	DN4@PoP2@30f7	12:04:56:88:30:f7	GPS	1	PSK	0	0	6.83 kbps	5.58 kbps
^					« < 1 >	» 10 v			
8									

## 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> <li>GPS sync:         <ul> <li>Entry condition: Valid samples from GPS have been received for a few consecutive seconds (typically 2 seconds).</li> <li>Exit condition: Valid samples from GPS have not been received for a few consecutive seconds (typically 10 seconds).</li> </ul> </li> <li>RF sync: Not in "GPS sync", but is reachable to a DN with "GPS sync" over</li> </ul>
	<ul> <li><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.</li> <li><i>Exit condition</i>: Conditions for "GPS sync" have not been met and no links to other DNs exist from which to derive timing.</li> <li><b>No sync</b>: Neither in GPS sync nor RF sync. This is the default state.</li> </ul>
	<ul> <li><i>Entry condition</i>: Conditions for "GPS sync" or "RF sync" are not met.</li> <li><i>Exit condition</i>: Condition for "GPS sync" or "RF sync" are met.</li> </ul>
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.





#### 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





## Packet Error Ratio graph

Figure 221: Packet Error Ratio graph



## **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

Statistics         Links       Ethernet       GPS       Radio       Performance       Prefix Zones       BGP         Zone:       Primary_POP-Site <ul> <li>Total 3 Zones</li> </ul> Prefix <li>2050:1111:2222:2280:/58</li> <li>Nodes</li> <li>Name <ul> <li>DN3@PoP1@309D</li> <li>DN1@PoP1@3000</li> <li>DN1@PoP2@3009</li> <li>DN1@PoP2@3009</li> <li>DN2@PoP2@3009</li> </ul></li>	Statistics Links Ethernet GPS Radio Performance Prefix Zones BGP Zone: Primary_PoP-Site  Total 3 Zones Prefix 2050:1111:2222:2280:J58 Nodes
Links         Ethemet         GPS         Radio         Performance         Prefix Zones         BGP           Zone:         Primary_PoP-Site         •	Links Ethemet GPS Radio Performance Prefix Zones BGP Zone: Primary_PoP-Site  Total 3 Zones Prefix 2050:1111.2222.2280:358 Nodes
Zone:         Primary_PoP-Site         Total 3 Zones           Prefix         2050:111:222:2280:358           Nodes         Nodes           Name 중         DN3@PoP1@309D           DN1@PoP1@3000         DN1@PoP2@3000           DN2@PoP2@3009         Ontegeneration	Zone: Primary_PoP-Site  Total 3 Zones Prefix 2050:1111:2222:2280:38 Nodes
Prefix         2050.1111.2222.228058         Nodes         Name 〒         DN3@PoP1@309D         DN1@PoP1@3000         DN2@PoP2@3000         DN2@PoP2@3000	Prefix         2050.1111.2222.2280/58           Nodes         Nodes
2050:1111:222:2280:358         Nodes         Name 〒         DN3@PoP1@309D         DN1@PoP1@3000         DN2@PoP2@3000	2050:1111:2222:2280:58           Nodes
Nodes           Name ▼           D3@PoP1@309D           DN1@PoP1@3000           DN1@PoP2@3000           DN2@PoP2@3000	> Nodes
Name 〒           DN3@PoP1@309D           DN1@PoP1@3000           DN2@PoP2@3009	
DN3@P0P1@309D           DN1@P0P1@3000           DN2@P0P2@3009	Name =
DN1@PoP1@3000 DN2@PoP2@3009	DN3@P0P1@309D
DN2@PoP2@3009	DN1@PoP1@3000
	DN2@PoP2@3009

# **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

	60 GHz cnWave™ v5000					Ø	Disable E2E Controller	Reboot S admin -
	Statistics Links Ethernet	GPS Radio Performance	Prefix Zones	BGP				
D	A-Sec-PoP							
٦	- 2021::1							
⊕	Details		Advertised I	Routes		Receive	d Routes	
	IPv6 Address	2021::1		Network	Next Hop		Network	Next Hop
ф	Status	Online	1	2020:1111:2222:2200::/56	2021::100	1	::/0	fe80::c6ad:34ff:fe45:aa00
	ASN	65534				2	2020:1111:2222:2200::/56	fe80::c6ad:34ff:fe45:aa00
1	Uptime	0d 0h 4m						
∎ * *	Prim-PoP@300 ter-PoP ⊡ 2021::1	0						
	Details		Advertised I	Routes		Receive	d Routes	
	IPv6 Address	2021::1		Network	Next Hop		Network	Next Hop
	Status	Offline				1	::/0	fe80::c6ad:34ff:fe45:aa00
	ASN	65534				2	2020:1111:2222:2200::/56	fe80::c6ad:34ff:fe45:aa00
	Uptime	NA						

# 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

	60 GHz cnWave™ √5000 Øisable E2E Controller	U Reboot	<b>8</b> a	dmin <del>-</del>
E	Мар			
Б		Show Names:	Yes	No
6				
ຝ				
φ	(%) DN1@3000			
۵				
*				
18	Prim-PoP@300 (P) DH2@3009			
	@ DN4@30/7			

# 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



# **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

	60 GHz cnWave <sup>™</sup> V20	000					O Disable E2E Controller	U Reboot	😫 admin -
	Tools		17						
ħ	Factory Reset	Field Diags	Antenna Alignment	Remote Command	Ping	Quick PTP Setup			
	Select Node								
۵	DN-V5K-3f69			~					
٩	Download Logs	)							
ф	Self Node								
۵	Field Dia	gnostics a	at 00-04-56-88	-49-38					
	2.04 2021-12-15 10:1 1.74 2021-12-15 05:1 1.04 2021-12-15 05:1 1.04 2021-12-15 05:1	11 0396-2021-12-15-1 52 0305-2021-12-15-0 39 0384-2021-12-15-0 23 0383-2021-12-15-0	0-11-40-shutdown.tar.gz 5-52-00-shutdown.tar.gz 5-35-06-shutdown.tar.gz 4-25-01-soquegerdemelt.tar.gz						
*	1.94 2021-12-14 06:2 1.64 2021-12-10 11:4 1.84 2021-12-10 11:4 1.84 2021-12-13 14:2 1.64 2021-12-01 08:2	20 0382-2021-12-14-0 47 0381-2021-12-10-1 20 0380-2021-12-13-1 33 0379-2021-12-01-0	6-20-42-appupgrd.tar.gz 1-46-26-appupgrd.mplt.tar.gz 4-20-49-appupgrd.tar.gz 6-33-15-appupgrd.tmlt.tar.gz						
1	622K 2021-12-13 13:2 1.6M 2021-12-02 15:4 1.6M 2021-12-03 15:1 1.6M 2021-12-13 11:1 1.6M 2021-12-01 00:1	24 0378-2021-12-13-1 44 0377-2021-12-02-1 19 0376-2021-12-13-1 35 0375-2021-12-01-0	3-24-11-appungrd.tar.gz 5-43-45-appungrdcmplt.tar.gz 1-19-28-appungrd.tar.gz 8-33-15-appungrd.mplt.tar.gz						
	Download Logs	]							

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

Select Node       Opening diags-00-04-56-88-31-21-2020-11-05-21-46-36.ctd       Image: Comparing diags-00-04-56-88-31-21-2020-11-05-21-46-36.ctd         PoP DN       Downloading Please wat       Image: Comparing diags-00-04-56-88-31-21-2020-11-05-21-46-36.ctd       Image: Comparing diags-00-04-56-88-31-21-2020-11-05-21-46-36.ctd         Downloading Please wat       Image: Comparing diags-00-04-56-88-31-21-2020-11-05-21-46-36.ctd       Image: Comparing diags-00-04-56-88-31-21-2020-11-05-21-46-36.ctd         Download Logs       Image: Comparing diags-00-04-56-88-31-21-2020-11-05-21-46-36.ctd       Image: Comparing diags-00-04-56-88-31-21-2020-01-05-21-46-36.ctd         Download Logs       Image: Comparing diags-00-04-56-88-31-21-2020-01-05-21-46-36.ctd       Image: Comparing diags-00-04-56-88-31-21-2020-01-05-21-46-36.ctd         Self Node       Image: Comparing diags-00-04-56-88-31-21-2020-01-05-21-46-36.ctd       Image: Comparing diags-00-04-56-88-31-21-2020-01-05-21-46-36.ctd         Field Diags       Image: Comparing diags-00-04-56-88-31-21-2020-01-05-21-46-38.ctd       Image: Comparing diags-00-04-56-98-99-99-99-99-99-99-99-99-99-99-99-99-			✓ Success Field Diagnostics file generated, will be downloaded shortly!	×
POP DN         Downloading Please wat	Select Node	Opening diags-00-04-56-88-31-21-2020-11-05-21-46-36.cfd		
DownloadingPlease with       I diage-00-04-56-88-31-21-2020-11-05-21-46-36.cfd         Download Logs       which is cfd File (0 bytes)         Self Node       What should Filefox do with this file?         Open with       Erostea         0.80 2020-11-05 21:33       What should Filefox do with this file?         0.91 2020-11-05 13:52       0009-2020-11-05 13:52         0.60 2020-11-05 13:52       0009-2020-11-05 13-32-33-shoutdown.tar.gz         7.60 2020-11-05 17:55       0007-2020-11-05 13-52-33-shoutdown.tar.gz         7.60 2020-11-05 17:55       0007-2020-11-05-12-05-37-shutdown.tar.gz         7.60 2020-81-11 55:11:55       0007-2020-11-05-12-05-37-shutdown.tar.gz         7.60 2020-81-11 55:11:56       0007-2020-11-05-12-05-37-shutdown.tar.gz         7.60 2020-81-11 55:11:56       0007-2020-81-10-81-4-32-27-39puggrdcmp11.tar.gz         7.50 2020-86-11 15:86       0007-2020-86-11-10-51-2-45-30         7.50 2020-86-11 15:86       0007-2020-86-11-10-51-2-45-30         7.50 2020-86-11 15:86       0007-2020-86-11-10-51-2-45-30         7.50 2020-86-11 15:86       0007-2020-86-11-10-51-2-45-30         7.50 2020-86-11 15:86       0007-2020-86-11-10-51-2-45-30         7.50 2020-86-11 15:86       0007-2020-86-11-10-51-2-45-30         7.50 2020-86-11 15:86       0007-2020-86-11-10-51-2-45-30         7.50 2020-86-11 205-102	PoP DN	You have chosen to open:		
Download Logs         from: blob:           Self Node         What should Firefox do with this file?           Description         Open with growse.           @ Save File         OK cancel           7.68 2020-11-05 12:33         OK cancel           7.68 2020-11-05 18:52 0009-2020-11:05-13-22-33-shutdown.tar.gz         OK cancel           7.69 2020-11-05 18:40 0000-2020-11:05-13-22-33-shutdown.tar.gz         OK cancel           7.69 2020-81-165 17:35 0007-2020-11:05-13-82-00-inurdown.tar.gz         OK cancel           7.69 2020-81-165 17:35 0007-2020-01:10-13-18-20-inurdown.tar.gz         Tar.gz           7.69 2020-81-11:05-138-20-inurdown.tar.gz         Tar.gz           7.69 2020-81-11:05-138-20-inurdown.tar.gz         Tar.gz           7.69 2020-81-11:05-138-20-inurdown.tar.gz         Tar.gz           7.69 2020-81-11:05-138-20-00-11:05-12-05-39-appugredmplt.tar.gz         Tar.gz           7.69 2020-81-11:552 0007-2020-01:1-15-138-20-inurdown.tar.gz         Tar.gz           7.69 2020-81-11:552 0007-2020-01:1-15-138-4-inurdown.tar.gz         Tar.gz           7.69 2020-81-11:552 0007-2020-01:1-15-51-15-50-1-01-01-000-11-15-51         Tar.gz           7.69 2020-81-12 2050-000-12020-000-11-15-51         Tar.gz         Tar.gz           7.69 2020-81-12 2020-000-12020-000-18-14-12-22-appugredmplt.tar.gz         Tar.gz           7.60 2020-80-12 2020-000-12020-000-18-14-1	Downloading Please wait	diags-00-04-56-88-31-21-2020-11-05-21-46-36.cfd which is: cfd File (0 bytes)		
Self Node         Ogen with this field                • Gave Field	Download Logs	from: blob:		
Save File           Save File           OK         Cancel           7.68 2020-11-05 19:09         OK           Conception         Conception           7.68 2020-11-05 19:09         OK           7.68 2020-11-05 19:09         OK           7.68 2020-11-05 19:09         OK           7.68 2020-11-05 19:100         OK           7.68 2020-11-05 19:100         OK           7.69 2020-81-05 19:15 0001-2020-11-05-13-18-20-shutdown.tar.gz           7.58 2020-11-05 17:15 0001-2020-11-05-12-05-30-spupgrdcaplt.tar.gz           7.69 2020-81-11 15:58 0005-2020-01-10-18-12-05-30-spupgrdcaplt.tar.gz           7.69 2020-81-11 15:58 0005-2020-01-10-18-58-4-shutdown.tar.gz           7.59 2020-06-18 20:05 0000-2020-08-11-05-12-05-30-spupgrdcaplt.tar.gz           7.59 2020-06-18 20:05 0000-2020-08-11-05-12-05-30-spupgrdcaplt.tar.gz           750 2020-06-18 20:05 0000-2020-08-11-05-14-5-20-spupgrdcaplt.tar.gz           750 2020-06-18 20:05 0000-2020-06-18-14-52-27-spupgrdcaplt.tar.gz           596 2020-06-18 20:05 0001-2020-06-18-14-12-27-spupgrdcaplt.tar.gz           596 2020-06-18 20:05 0001-2020-06-18-14-12-27-spupgrdcaplt.tar.gz           596 2020-06-18 20:02 0001-2020-06-18-14-12-27-spupgrdcaplt.tar.gz	Self Node	Open with Browse.		
7.64 2029-11-05 19:09 7.64 2029-11-05 19:09 7.64 2029-11-05 19:52 0009-2020-11-05-13-22-33-shutdown.tar.gz 7.64 2029-11-05 19:54 0009-2020-11-05-13-18-20-shutdown.tar.gz 7.64 2029-11-05 17:55 0006-2020-11-05-12-05-39-appuggrdap1t.tar.gz 7.64 2029-08-11 15:43 0006-2020-11-05-12-05-39-appuggrdap1t.tar.gz 7.64 2029-08-11 15:43 0006-2020-10-05-45-09-10-2020-10-12-05-20 7.64 2029-08-11 15:43 0005-2020-08-11-08-46-04-appuggrdap1t.tar.gz 7.64 2029-08-11 20:55 0003-2020-08-11-08-46-04-appuggrdap1t.tar.gz 554 2029-08-11 20:05 0003-2020-08-11-08-14-35-01-shutdown.tar.gz 554 2029-08-11 20:02 0002-2020-08-18-14-35-27-appuggrdap1t.tar.gz 556 2029-06-18 20:02 0001-2020-06-18-14-32-29-appuggrdap1t.tar.gz	Field Diag	⊕ <u>Save File</u> OK	Cancel	
	7.60 2020-11-05 13:00 7.60 2020-11-05 13:02 7.60 2020-11-05 13:02 7.50 2020-11-05 17:35 7.50 2020-11-05 17:35 7.50 2020-11-05 17:35 7.50 2020-10-15 7:35 7.50 2020-06-11 2:00 593X 2020-06-12 20:02 596X 2020-06-18 20:02	0009-2820-11-05-13-22-33-shutdown.tar.gr 0008-2820-11.05-13.18.20-shutdown.tar.gr 0007-2820-11.05-12.05-37-shutdown.tar.gr 0007-2820-11.05-12-05-39-spupgrdcmplt.tar.gr 0006-2820-08-11-08-16-05-shutdown.tar.gr 0004-2820-08-11-08-66-03-appuggrdcmplt.tar.gr 0003-2820-08-11-08-46-03-appuggrdcmplt.tar.gr 0003-2820-08-18-14-32-29-appuggrdcmplt.tar.gr		

# 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.



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.

# $\widehat{}$

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

Note

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



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.

0 Confirm × Tools Factory Reset Field Diags Antenna Alignment Quick P Link will be disrupted Start Alignment • Before starting software alignment, please visually align the local node Cancel and elevation alignment to position the highlighted cell in the centre of th Ð 

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:

- 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 232.





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.

1	0	)
$ \  \  \  \  \  \  \  \  \  \  \  \  \ $	ř	1

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

Note

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 ± 5 dB while aligning			
Operational EIRP	46 dBm			
Operational Receive Power	-60 dBm ± 5 dB			
Predicted Link Loss	116.25 dB ± 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



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 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

Note

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.



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* 

	60 GHz cnWave™ ∨5000		O Disable E2E Controller	U Reboot	admin -
	Tools				
Ē	Factory Reset Field Diags Antenna Alignment Remote	Command Ping	Quick PTP Setup		
6	Select Node : PoP1@300c  Select Command : Show	SFP Power Details -	cute	<u>+</u>	
⊕	Output				
¢	"status": "OK", "calibrationType": "Internal", "units": "micro-watts",				
۰	"txPwr": 568.0, "rxPwr": 555.2, "rxPwrMeasType": "Average",				
	"txPwr_dBm": -2,457, "rxPwr_dBm": -2%556 }				
1					

Table 59 lists and describes each parameter in the output.

Table 59: Output details

Output Parameter	Description
Status	Determines whether the output is valid.
	If the <b>Status</b> field contains OK, it implies that the rest of the output is valid.
	If the <b>Status</b> field does not contain OK, it implies that only the <b>Status</b> field is valid. In such cases, the <b>Status</b> 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 241.

Figure 241: The CLI supported output - SFP Power details



## 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** dropdown 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

Q	60 GHz cnWave™ VS	000				Disable E2E Controller	Reboot	e admin
	Tools							
ī,	Factory Reset	Field Diags Remote Co	ommand Ping i	Perf				
-		Select Node : PoP-V5K	-3d38 • Select Com	mand : Show ipv4 neighbors •	Execute		*	
6		Output						
2		10.110.186.116 dev mici 10.110.186.51 dev mici	lladdr e4:54:e8:c1:68: lladdr 70:b5:e8:2a:a5:a	31 STALE 32 REACHABLE				
>		10.110.105.05 dev nic1 10.110.105.249 dev nic1 10.110.105.142 dev nic1	<pre>11addr 8c:3b:ad:69:05:5 11addr 00:e0:4c:68:10: 11addr 00:e0:4c:68:16:</pre>	Pd STALE 22 STALE 285 STALE				
1		10.110.185.55 dev nic1 10.110.185.105 dev nic1 10.110.185.254 dev nic1	11addr 00:0c:20:7b:5f:a 11addr 8c:3b:ad:69:05 11addr cc:16:7e:6e:5b	NF REACHABLE IDJ STALE ITF STALE				
<b>=</b>		10.110.105.223 dev mic1 10.110.105.109 dev mic1 10.110.105.97 dev mic1	lladdr 0c:3b:ad:69:05: 1laddr 08:bd:43:78:6d: 1laddr 34:e6:d7:19:75:2	09 STALE 3# STALE 20 STALE				
		10.110.185.189 dev mic1 10.110.185.70 dev mic1	lladdr 00:e0:4c:68:01 lladdr 64:00:6a:84:93:4	76 DELAY ab STALE				
6		10.110.100.33 dev nici 10.110.100.238 dev nici 10.110.100.58 dev nici 10.110.100.58 dev nici	lladdr 8c:e0:40:95:00:1 lladdr 8c:e0:40:66:85: lladdr 80:e0:40:68:01:1 lladdr 80:e0:40:68:90:20	e STALE TC STALE TC STALE ON STALE				
		10,110,186,119 dev mict	lladdr ed:54:e8:c2:56	of STALE				

You can use the  $\blacksquare$  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

0 GHz cnWave™ v5	000				O Disable E2E Controller	e admin
Tools						
Factory Reset	Field Diags	Remote Command	Ping iPerf			
	Select Node :	PoP-V5K-3d38 •	Select Command :	Show ipy6 neighbors - Execute	<u>*</u>	
	Output					
	fe80::8eec:40	bff:fed6:a5e3 dev ni	cl lladdr 8c:ec:4b:d0	:a5:e3 STALE	1	
	fe80::200:291 fe80::1004:56	ff:fe77:5307 dev nic 5ff:fe8b:3efd dev te	1 lladdr 00:0c:29:77: rrai4 lladdr 12:04:56	53:07 STALE :8b:3e:#d REACHABLE		
	fe88::1084:50	5ff:feSb:42f2 dev te	rra27 lladdr 12:04:50	:8b:42:f2 REACHABLE		
	fe00::1004:50	off:fe8b:c44 dev ter	ra28 lladdr 12:04:56:	80:14:12 FOULEF REACHABLE 80:00:44 REACHABLE		
	fe80::20c:29	ff:fec0:55ac dev nic	1 lladdr 00:0c:29:c0:	SS:ac STALE		
	fe00::20c:29	ff:fe88:a006 dev nic	1 lladdr 00:00:29:05: 1 lladdr 00:00:29:00:	20:05 STALE		
	fe80::20c:29	ff:fe69:3dbð dev nic	1 lladdr 00:0c:29:69:	3d:b0 STALE		
	fe80::1004:50	5ff:fe8b:921 dev ter	ra2 lladdr 12:04:56:8	5:09:21 REACHABLE		
	fe80::204:56	ff:fe88:310e dev nic	1 lladdr 00:04:56:88:	31:00 STALE		
	fe88::1004:50	off:fe8b:4118 dev te	rral lladdr 12:04:56:	8b:41:18 router REACHABLE		
	fe80::20c:29	ff:fe36:f4ca dev nic	1 lladdr 00:0c:29:16:	f4:ca STALE		
	Fe88::284:561	ff:fe89:209d dev nic	1 11addr 00:04:56:89:	28:9d STALE		
	fe00::200:20	ff:feGd:he60 dev nic	1 11addr 00:00:29:50:	ke sa stale		
	fe00::72b5:el	lff:fe2a:ala2 dev nl	c1 lladdr 70:b5:e8:2a	:a5:a2 STALE		
	fe80::1004:50	Sff:fe6b:3adc dev te	rral1 lladdr 12:04:50	:8b:3a:dc REACHABLE		
	fe80::20c:29	ff:fe33:27b9 dev mic	1 11addr 00:0c:29:33:	27:09 STALE		
	fe80::20c:20	ff:fe7a:67dB dev nic	1 lladdr 00:8c:29:7a:	67:d8 STALE		
	fe80::2e0:4c1	ff:fe68:95 dev nic1	11addr 00:e0:4c:68:00	:95 STALE		
	fe80::20c:291	ff:fe14:2ffe dev nic	1 11addr 00:0c:29:14:	2f:fe STALE		

To download the output (in .txt format), use the  $\stackrel{\bullet}{ع}$  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** dropdown 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.

# CONSC CONSCI CONSCI

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.

#### Figure 244: The Show Wired Interface State Changes output

Parameter	Description
	Select the required source node from the drop-down list.
	The required node or destination address (IPv4 or IPv6) that for which the reachability has to be identified.
	Following options are supported:
Destination Type	• Node
	• IPv4
	• IPv6
	Select the required option (mandatory).
	Number of times that a packet is transmitted to find the reachability.
Number of Deckets ( c)	Default value: 3
Number of Packets (-C)	This parameter supports values between 1 (minimum) and 10 (maximum).
	Type an appropriate value in the text box.
	Size (in bytes) of the packet.
	Default value: 56
Buffer Size (-s)	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 245.

#### Figure 245: The Ping page

	60 GHz cnWave <sup>W</sup> V5000	Oisable E2E Controller	U Reboot	e adm
-	Tools			
6	Factory Reset Field Diags Antenna Alignment Remote Command Ping Quick PTP Setup			
	Source Node			
۵	PoP1@300c ~			
œ	Destination Type			
	Node      IPv4     IPv6			
¢	DN1@3000			
	Number Of Packets (-c)			
	3			
□	Mm = 1. Max = 10			
1	Buffer Size (-s)			
	56			
1	Min = 1, Max = 65507			
1.000	Start Ping			
	Ping Result		( <u>•</u> )	
	PING 2020:1122:2222:2202::1(2020:1122:2222:22			

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

	Tools					
	Factory Reset	Field Diags	Antenna Alignment	Remote Command	Ping	Quick PTP Setup
D	CN MAC Address					
•	Missing mandatory fi	eld.				
④	Please input the reautomatically create a	emote CN MAC add a new topology and	dress and click start to d establish the wireless link.			
Φ	The previous topolog	y will be removed.				
	Start PTP SetUp					

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



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.

Note

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.

Parameter	Description
	The server node for which you want to conduct the network performance test.
Server Node	Select the required server node from the drop-down list.
	<b>Note</b> : 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.
	<b>Note</b> : 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
	<b>Note</b> : 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
	Default value: 4
	Type the required value in the text box.
	<b>Note</b> : This parameter supports values from 1 to 4.

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

60 GHz cr/Wave ** V5000		O Disable E2E Controller (U) Reboot	e admi
Tools			
Factory Reset Field Diags Remote Command Ping	iPerf		
Server Node	Client Node		
node-V5000-888d3d v +*	v2k cn v		
Duration (Calcorda)			
10			
Min = 1, Max = 300			
Parallel Steams			
4			
Min = 1, Max = 4			
Start Pwrt			
Press Middl Brough Stade (1976) Bit (20		Charlenge Barrier Late and	
Serve Hole (Head, Hole 7340 Gelese	±		<u>+</u>
1 01 7 80.8.00 sec 55.4 Mbytes 885 Mbits/sec		7 01 2.00.0.00 see 85.0 HButes 481 Hbits/see 8. 010 KButes	
[ 12] 7.60-8.00 sec 55.5 MBytes 466 Mbits/Sec		[ 11] 7.00-8.00 sec 55.0 MBytes 401 Mbits/sec 8 901 KBytes	
[ 14] 7.00-8.09 sec 55.6 Mbytes 457 Mbits/sec		[ 13] 7.00-0.00 sec 15.0 MBytes 401 Mbits/sec 0 1.00 MBytes	
[ 16] 7.80.8.00 sec 55.7 MBytes ALT Hbits/sec		[ 15] 7.08-0.00 sec 55.0 MBytes 461 Mbits/Lec 0 1.02 MBytes	
[50M] 7.80-8.00 sec 222 MBytes 1.86 051ts/sec		[SUM] 7.00-0.00 sec 220 MBytes 1.05 Sbits/sec 0	
		The second se	
[ 0] 0.00-0.00 SEC 35.4 MEYES 404 MOITS/SEC		[ V] B. B V. B. Sec. 50. B. HEPTER. 451 MELES/DEC. B. MID HEPTER.	
T 141 0.00-0.00 sec 55.7 MDytes 007 Mbits/sec		T 11 0 00 0 00 0 00 100 100 100 100 100	
[ 16] 8.00-0.00 Mpc 55.3 MDytes 464 Mbits/Amc		151 8.08-0.08 Sec 56.2 MBytes 472 MBits/sec 8 1.02 MBytes	
[3uH] 0.00-9.00 sec 222 MBytes 1.00 051ts/sec		[50H] 0.00-0.00 sec 224 MBytes 1.68 Obits/Sec 0	
[ 0] 0.00-10.00 sec 55.5 MBytes 460 Mbits/sec		[ 0] 0.00-10.00 sec 16.2 MBytes 472 Mbits/Gec 0 010 KBytes	
[ 12] 0.60-10.00 set 16.0 MBytes 470 Mbits/set		[ 15] 0.00-10.00 sec 50.2 MBytes 472 Mbits/sec 0 001 RBytes	
[ 14] 0.00-10.00 sec 55.3 MBytes 484 MS1ts/sec		[13] 9.00-10.00 Sec 55.0 HBytes 401 HBits/sec 0 1.00 HBytes	
[ 16] 0.80.50.08 sec 55.5 MBytes 488 M53ts/sec		[ 15] 9.08-18.00 Sec 15.6 MBytes 441 Mbits/Sec 0 1.02 MBytes	
[304] 0.00-20.00 Sec 222 Maytes 1.00 00213/Sec		Total a national sec 111 mailes 1 supplicable a	
I BI 10.00.10.07 say 053 stores all Moltacher		[ 10] Interval Transfer Birrare Berr	
1 121 10.00-10.02 sec 959 MBytes 447 Mbits/sec		[ 9] 0.00-10.00 sec 551 Miytes 462 Mbits/sec 0 sender	
[ 14] 10.00-10.0J sec 1.00 MBytes 504 Mbits/sec		[ 0] 0.00-10.02 sec 547 MBytes 450 Mbits/sec receiver	
[ 10] 10.40-10.02 sec 003 kBytes 445 Mblts/sec		[ 11] 0.00-10.00 sec 553 MBytes 464 Mbits/Sec 0 serder	
[5UM] 10.00-10.02 Sec 3.05 MBytes 1.04 02113/Sec		[ 11] 0.00-10.02 sec 550 MBytes 400 Mbits/Sec receiver	
		[ 13] 0.00-10.00 sec 558 MBytes 482 Mbits/sec 0 sender	
[ ID] Interval Transfer Bitrate		[ 13] 0.00-10.02 sec 548 MBytes 459 MBits/Lec /ecciver	
[ 9] 0.00+10.02 sec 547 Mbytes 450 Hblts/sec	receiver	[13] 0.00-10.00 sec 348 MBytes 450 MB115/bes 0 sender	
[ 12] H.HO-1H.HZ DEC 100 MBytes 400 MDits/Sec	receiver	[ 13] W. WHILE W. THEO SHE PHYTEL HIST PRITY/NOC PRECEASE FORM 0.01.00.00 SHE 2.14 COurtes 1.58 Contract 0. Samahar	
[ 14] 0.00-10.00 Sec 3-4 Moytes 450 Mosts/sec	receiver	[IMM] 0.00-18.82 Sec 2.14 OWYES 1.83 OB12/ARC Feedbar	
[5100] 0.00-10.02 sec 2.14 60vtes 1.03 6bits/sec	receiver	Tank and were and end when you are area and a	
the second		Loss f Door	

To download the server and client node results (in .txt format), use the  $\frac{1}{2}$  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.

- 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

	60 GHz cnWave™ V5000	Enable Layer 2 bridge	U Reboot	😝 admin 🗸
	Onboard E2E Controller	By selecting this checkbox, you will be enabling Layer 2 network bridging (via automatically created tunnels) across all noders connected to a POP. This will facilitate bridging of IPV4 traffic across the wireless networks.		
0	This s	Prefix Allocation ice er  Centralized Deterministic work. This includes		
Ð	netwo	topol ation management.		
•		Remote Management		
۰		cnMaestro URL		
		https://10.110.186.47 Cambium ID		
×		cnmaestro_on_premises		
1		Onboarding Key		
		Enable Cancel		

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

Figure 250: Information on the new E2E network

C   Cr	Maestro"	🦧 😰 📴 🖓 😝 Administrate	юг -
-	Search	60 GHz cnWave Network > 60 GHz cnWave E2E-V5WH0043VP85	¢
~	Networks Wi-Fi AP Groups		
ល	∽ 🕲 System		
14	🎝 default	$60 \text{ GHz cn} \text{Maxo}^{\text{Bess}}$	
	to GHz cnWave E2E-V5WH New		
	✓ 1 Mesh-Fig0		
ø	> 🔆 CNI-Site-08		
<b>B</b>	> 🤆 CN2-Site-75		
9	> + DN1-Site-39		
-	> 🕂 DN2-Site-B0		
83	> 🕂 DN3-Site-3D		
85	> + PoPI-Site-DC		
		New E2E Network discovered	
8.8		Approve this network to manage via cnMaestro	
		Approve Delete	

- 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

CI	Maestro		60 Cide collines Natural Onboard	<i>P</i> 2	2 🖓	\$! <b>,</b> °	Administrator -
ŧ	Search	60 GHz cnWave Net	Nome				0
	Networks Wi-Fi AP Groups		Onboard 60 GHz cnWave E2E				
ណ	~ 😨 System						
	🎶 default		Seve				
	to GHz cnWave E2E-V5WH						
	<ul> <li>✓           Mesh-FigD</li></ul>						
105	> 🤆 CNI-Site-08			a Innn			
. <del>S</del>	> 🔆 CNZ-Site-75						
9	> + DN1-Site-39						
-	> + DN2-Site-B0						
199	> 🕂 DN3-Site-3D						
儲	> + PoP1-Site-DC						
*			New E2E Network discovered				
¥Я			Approve this network to manage via ch	Maestro			
			Approve Delete				

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

()   cr	n <b>Maestro</b> <sup>®</sup>							🧬 😰 🖻	🚱 😝 Administrato
-	Search	60 GHz cnl	Wave Network > On	board 60 GI	Hz cnWave E2E 🚥				
~	Networks Wi-Fi AP Groups	Dashboard Notif	ications Configuration 5	tatistics Repor	Software Update Map	Tools			
ហ	~ 😨 System	Nodes		Links		Wireless Thro	ughput of PoP(s)	Wired Through	nput of PoP(s)
	å≁ default > 🏷 Mesh-Fig0		3 🧿	2		O Khps	0 Каря	O Khps	O Khps
	✓ ☆ Onboard 60 GHz cnWave E2( )	Offline Last Week	Total Offine	Total	Offline	Tx	Rx	Tx	Rx
Ŷ	> 🕂 CN-v1k > 🕂 DN-v5k	Alerms			0				New Horizon Gunukul
9	~ 🕂 Onboard-pop-v3k	0	0 0	+				2	
۲	node-V3000-8830ff	CRITICAL	MAJOR MINOR	-				AR SCHOOL	
명		0						er	
٨ß		LA	ST 24 HOURS						0
		E2E Controller De	tails						
		Version	1.0.1-dev79						
		Management Address	10.110.178.11					CHOOL R	
		IPv6 Address	fd00:be5e:0088:3 @		6			and a second sec	
		IPv6 Gateway	·		Ŷ				
		Sites	3						
		Deployment	Running Onboard				11 and		a line for a first first state

#### 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

s	earch		
_	Networks	Wi-Fi AP Group	S
~ (	System		
	♣ default		
,	232		1
	Hide Sites		
	Refresh		
	Sync Topology	/	
	Add Site		
	Add Node	_	
	Add Link		
	Edit		
	Update Softwa	are	
	Download PoP	(s) Onboarding Cor	nfig
	Delete		

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

Add Link			$\times$
Link Type Wireless Wired			
A-Node		A-Node Sector	
CN-83	•	Sector 1 ( 12:04:56:88:31:83 )	•
Z-Node		Z-Node Sector	
6			-

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

Add Route	×
Destination	
2001:470:c31b:200::/56	
Gateway	
2403:0:529:d:a00:27ff:fe01:2121	
Add Cancel	

- 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

Dashboard	Notifications	Configuration	n Links	Statistics	Report X	Software Update Map Tools
Operations	Diagnostics	Debug	Remote C	Command	Services	Settings
Network Co	onfiguration					
E2E Contro	ler IPv6 Addres	ss (eth1)				
2001:3001:	100/64					
Changing I	Pv6 Address w	ill disconnect a	all the nod	es. E2E Cor	ntroller Addr	ess configured in the PoP nodes should match.
- IPv6 Ro	outes					
🖌 Auto Ma	inage Routes 🗴	5				
Automa	ted IPv6 Route	s to DNs and C	CNs based	on topolog	y and PoP r	odes status. Applicable only if PoP nodes and E2E Controller are in same Network/Prefi
length.						

#### **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:	Fxampl	e of IPv6	route	entries il	n the	IPv6	Routes	page
iguic	200.	Example		route	critines ii	1 1110	11 10	1.outes	puge

Operations Diagnostics Debu	g Remote Command Services Settings			
Network Configuration				
E2E Controller IPv6 Address (eth0)				
fd00:ba5e:6e57:3026::1/64	Changir	g IPv6 Address will disconn	ect all the nodes. E2E Controller Ad	ddress configured in the PoP nodes should match
IPv6 Routes				
Auto Manage Routes X Autom	ated IPv6 Routes to DNs and CNs based on topology a	nd PoP nodes status. Applic	able only if PoP nodes and E2E Cor	ntroller are in same Network/Prefix length.
- nate manage neares a fratem		re i er, rie ees statust i oppre		
			Add New	
Destination	Gateway	Туре		
	fd00:ba5e:6e57:3026:0:4:5688:4862	auto		
fd00:ceed:1095:1700::/58				
fd00:ceed:1095:1700::/58 fd00:ceed:1095:1740::/58	fd00:ba5e:6e57:3026:0:4:5688:4a3c	auto	Í	
fd00:ceed:1095:1700::/58 fd00:ceed:1095:1740::/58 fd00:ceed:1095:1780::/58	fd00:ba5e:6e57:3026:0:4:5688:4a3c fd00:ba5e:6e57:3026:0:4:5688:4bca	auto	) I	
fd00:ceed:1095:1700::/58 fd00:ceed:1095:1740::/58 fd00:ceed:1095:1780::/58 fd00:ceed:1095:17c0::/58	fd00:ba5e:6e57:3026:0:4:5688:4a3c fd00:ba5e:6e57:3026:0:4:5688:4bca fd00:ba5e:6e57:3026:0:4:5688:48b0	auto auto auto	図 図 図	
fd00:ceed:1095:1700::/58 fd00:ceed:1095:1740::/58 fd00:ceed:1095:1780::/58 fd00:ceed:1095:17c0::/58 fd00:ceed:1095:17c0::/56	fd00:ba5e:6e57:3026:0:4:5688:4a3c fd00:ba5e:6e57:3026:0:4:5688:4bca fd00:ba5e:6e57:3026:0:4:5688:48b0 fd00:ba5e:6e57:3026:0:4:5688:48b0	auto auto auto	8	

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

Search		60 GHz cnWave N	etwork > 60 G	Hz cnW	lave E2E	-Fig8			
Networks	Wi-Fi AP Groups	Dashboard Notifications	Configuration	Links	Statistics	Report X	Software Upda	ite Ma	ap Tools
✓ ⓒ System		Basic Management	Security Adva	anced	E2E Contr	oller			
🎝 default	1								
✓ ★ 60 GHz cnV	Vave E2E -Fig8	All the settings below are t	for advanced user	s only.					
> + FIGO_CN	41	Q pop_pre	× Base Field	ds : Sho	W All	~	Table	ISON	Add New
> + FIGO_CN	12	Field				Status	Value		
> + FIGO_DM	N1	flags.enable_pop_prefix_		modified	true				
	12								
> + FIGO_DM	13	Save Reset							

- 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 <u>Safety compliance specifications</u> table.

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

Tabla 6	2. Safe	tycom	nlianco	specifi	cations
aple o	Z: Sale	ety com	pliance	specifi	cations

#### **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 <a href="http://www.fcc.gov">http://www.fcc.gov</a>, 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 <a href="https://www.canada.ca/en.html">https://www.canada.ca/en.html</a>.
- 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 <u>https://www.icnirp.org/cms/upload/publications/ICNIRPemfgdl.pdf</u> 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  $W/m^2$ . For more information, see <u>Human exposure to radio frequency energy</u>.

#### **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:

$$S = \frac{P.G}{4\pi d2}$$

Where:

- S: power density in  $W/m^2$
- 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:

$$d = \sqrt[n]{P.G/4\pi S}$$

#### 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<sup>™</sup> 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 <sup>™</sup> 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.

Product	Countries	EIRP (dBm)	EIRP (W)	Maximum power density (W/m <sup>2</sup> )	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

#### Table 64: Calculated distances and power compliance margins



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 <u>Radio</u> <u>specifications</u> 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 (ISEDC) 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



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



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



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

Model No/HVIN:V1000	Cambium Networks <sup>™</sup> Ashburton, TQ13 7UP, UK	IP66/67
III		AX: 0.24A
N	UL62368-1 / CSA C22.2 No UL60950-22 / CSA C22.2 No	60950-22-17
This device complies with part 15 of the FCC Rules device may not cause harmful interference, and (2 interference that may cause undesired operation	s. Operation is subject to the following two cond ) this device must accept any interference recei	ditions: (1) This ved, including
IMPORTANT: See the System User Guide before connecting to AC Power. The Guide is available online at www.cambiumnetworks.com/guides	FCC ID: QWP-60V1000 IC: 109AO-60V1000	R-NZ
MADE IN CHINA X-52HO-H		Ś

#### 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

	60 GHz cnWave™ V3000	O Disable E2E Controller	U Reboot	e admin -
	TOOIS Factory Reset Field Diags Antenna Alignment Remote Command Ping Quick PTP Setup			
	Select Node node-V3000-884223 ~ Download Logs			
♦	Self Node Field Diagnostics at 00-04-56-88-42- 23			e admin -
*	<pre>1.6M 2022-09-13 11:35 0205-2022-09-13-11-35-08-appupgrdcmplt.tar.gz 1.6M 2022-09-13 11:33 0204-2022-09-13-11-33-28-appupgrd.tar.gz 1.6M 2022-09-13 08:36 0203-2022-09-13-08-36-05-shutdown.tar.gz 1.6M 2022-09-13 06:14 0202-022-09-13-06-14-48-shutdown.tar.gz 1.7M 2022-09-13 06:12 0201-2022-09-13-06-12-47-shutdown.tar.gz 1.7M 2022-09-13 05:40 0200-2022-09-13-06-12-47-shutdown.tar.gz 1.7M 2022-09-12 14:42 0199-2022-09-12-042-36-5shutdown.tar.gz 1.7M 2022-09-12 14:130 0198-2022-09-12-142-36-5shutdown.tar.gz 1.6M 2022-09-12 13:16 0195-2022-09-12-142-05-shutdown.tar.gz 1.7M 2022-09-12 13:16 0195-2022-09-12-142-06-shutdown.tar.gz 1.6M 2022-09-12 12:56 0194-2022-09-12-142-06-shutdown.tar.gz 1.6M 2022-09-12 10:50 0189-2022-09-12-145-56-15-shutdown.tar.gz</pre>			

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

#### Figure 268: Downloading the logs

	60 GHz cnWave <sup>w</sup> V3000	O Disable E2E Controller	U Reboot	e admin -
-	Tools Factory Reset Field Diags Antenna Alignment Remote Command Ping Quick PTP Setup			
D	Select Node			
۵	node-V3000-884223 🗸			
٩	Downloading Please wait			
ф	Download Logs			
	Self Node			
	Field Diagnostics at 00-04-56-88-42-			
*	23			
\$	1.6M 2022-09-13 11:35 0205-2022-09-13-11-35-08-appupgrdcmplt.tar.gz 1.6M 2022-09-13 11:35 0204-2022-09-13-11-33-28-appupgrd.tar.gz 1.6M 2022-09-13 06:36 0203-2022-09-13-08-36-05-shutdown.tar.gz 1.6M 2022-09-13 06:14 0202-2022-09-13-06-41-48-shutdown.tar.gz 1.7M 2022-09-13 06:12 0201-2022-09-13-06-12-47-shutdown.tar.gz 1.7M 2022-09-13 05:149 0208-2022-09-13-06-12-47-shutdown.tar.gz 1.7M 2022-09-13 05:149 0208-2022-09-13-06-52-65hutdown.tar.gz			
	1.8M 2022-09-12 14:30 0198-2022-09-12-14-30-31-shutdown.tar.gz			

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
0	Basic Management Security Advanced
٥	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.
	<ul> <li>Configuration Management</li> <li>E2E Managed Config Determines whether the controller should manage the node's configuration.</li> </ul>

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



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

	60 GHz cnWave™ ∨5000	
	Configuration Network Nodes	
ß	Q Search	Radio Networking Security Advanced
0	PoP DN	Local IPv4 Management
Ð	R DN	169.254.1.100
٠		Subnet Mask
		255.255.0.0
×		Gateway IP Address 169.254.1.50
t		PoP Configuration
		POP Routing

	60 GHz cnWave™ V5000	
	Configuration Network Nodes	
D	Q Search	Radio Networking Security Advanced
6	Pop DN	Local IPv4 Management
٩	🖗 DN 🔚	169.254.1.200
		Subnet Mask
		255.255.0.0
*		Gateway IP Address
×.		Ethernet Ports
		⊠ Enable Main
		E Enable SFP

# 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.

60 GHz cnWave** v5000							
Configuration Network Nodes							
Q Search	Radio Networki	ng Security Advanced					
Rep DN	Minimum MCS						
ere por bit	2			•			
2 (10 DN	Range - [2, 12]						
1	Maximum MCS			147			
	12 Bange - [2, 12]						
¢	Sector 1						
	Override	Name	Auto Config	Node Config			
		Channel					
		Polarity				5	
	Sector 1 Link (s)	Golay					
	Override	Name	Auto Config (Rx/Tx)	Node Golay Rx	Node Golay Tx		
	No Data						
	Sector 2	Sector 2					
	Override	Name	Auto Config	Node Config			
		Channel	2			~	
		Polarity	Odd Odd			2	
	<ul> <li>Sector 2 Link (s)</li> </ul>	Golay					
	Override	Name	Auto Config (Rx/Tx)	Node Golay Rx	Node Golay Tx		
		link-DN-PoP DN	2/2		~	~	
	Override All						

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

	60 GHz cnWave <sup>ns</sup> V5000	
	Configuration	
Ð	Q Search	Radio Networking Security Advanced
6	Pop DN	Local IPv4 Management
۲	Ø DN	IPv4 Address 169.254.1.200
٩		Subnet Mask
		255.255.0.0 Gateway IP Address
*		169.254.1.10
		Ethernet Ports Enable Main Enable Aux Enable Aux Enable SFP CPE CPE CPE  CPE  CPE interface O Aux O Main O SFP  Disabled Enable Router Advertisements on an interface on the device. Note: Changing this setting requires reboot CPE interface Prefix Overnide prefix on CPE interface, instead of configuring from Io address. Note: Changing this setting requires reboot

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

6	60 GHz cnWave** V5000								ው	Reboot 😑 admin •
	Topology Sites Nodes Links									
0	Q search	0								Add New
۵	Name	MAC Address	IPv6	Туре	Status	Model	Site	PoP Node	Software Version	
	PoP DN	00:04:56:88:31:21	fd00:ceed:8831:2100:1	DN	Online Initiator	V5000	Point A	Yes	1.0-dev12	ê :
	DN DN	00:04:56:88:31:2d	fd00:ceed:8831:2101:1	DN	Online Initiator	V5000	Point E	No	1.0-dev12	8 :
-					D	1 1 10 10 10				
					-0					
*										
10										

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

0	60 GHz cnWave™ VS					Ç	O Disable E2E Controller			U Reboot		8	ıdmin <del>-</del>					
	Statistics Links Ether	net GPS R	adio Performa	nce	BGP											Dov	vnload S	tatistics
3	Link Name	A-Node	Z-Node	RSSI	Link Fade Margin	Rx SNR	Rx MCS	RX PER	RX Scan Beams	TX Power Index	EIRP	Tx MCS	TX PER	TX Scan Beams	RX Errors	RX Frames	TX Errors	TX Frames
2	link-node-V30	12:04:56:88:31:	12:04:56:88:70:	-38	59	32	9	0	57	6	35	10	0	74	20	7540	1195	7101
	link-node-V30	12:04:56:88:70:	12:04:56:88:31:	-37	60	32	9	0	42	6	35	10	0	55	1611	41266	1041	6543
						~~	< 1		» 10 ~	ŝ.								
•																		
×																		
TA																		

6. 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

	60 GHz cnWave** v5000								🖒 Reboot 🕒 admin -
	Statistics								
ō	Links Ethernet GPS	Radio Performance	BGP						
	Device Name	MAC Address	Sync Mode	Channel	Security	Error Association	Channel Last State	RX Throughput	TX Throughput
۵	POP DIN	12:04:56:88:31:21	RF	2	None	0	0	7.86 kbps	1.63 kbps
-	FOF DIN	22:04:56:88:31:21	RF	1	None	0	0	0 kbps	0 kbps
œ	DN	12:04:56:88:31:2d	RF	1	None	0	0	0 kbps	0 kbps
	DN	22:04:56:88:31:2d	RF	2	None	0	0	0.69 kbps	4.66 kbps
					40 4 1 H	+ 10 -		3	
<b>m</b>	1								
1000									
*									
K.									

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

	60 GHz cnWave" V5000							U Rebo	ot 🕒 admin •
	Configuration Network Nodes								
D	Q Search	Radio Network	ing Security Advanced						Submit Cancel
۵	B B-P DN	Minimum MCS							^
~		2			•				
æ	00 DN	Range - (2, 12)							
۵		12			lol				
m		Range - [2, 12]			121				
*		- Sector I							
15		Override	Name	Auto Config	Node Config		10		
-409		u	Channel	2					
			Polarity	Even					
		Sector 1 Link (s)	Golay						
		Override	Name	Auto Config (Rx/Tx)	Node Golay Rx	Node Golay Tx			
			link-DN-PoP DN	2/2		4	0		
		Oreside All							
		Sector 2							
		Override	Name	Auto Config	Node Config				
			Channel						
		-	Charlener				100		
			Polarity						
		E Sector 2 Link (s)	Golay						
	De	Override	Name	Auto Config (Rx/Tx)	Node Golay Rx	Node Golay Tx			
		No Data							
		GPS     Force GPS Dis     When checked, the	able radio will use internal sync rather than	s GPS sync Copyright © 2020 Cambium Netw	rolis, ltd. All rights reserved.   <u>Com</u>	munity   Support			¢

# 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.
- 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:



2. Click Factory Reset and Reboot.

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

Confirm	×
Are you sure you want to reset this device to its factory default configuration?	
Yes	No

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<sup>\*</sup> <u>www.cambiumnetworks.com</u>

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

 $\ensuremath{\textcircled{\sc c}}$  Copyright 2023 Cambium Networks, Ltd. All rights reserved.