Cambium Networks™

OPERATION AND TROUBLESHOOTING GUIDE

cnWave™ 5G Fixed

Release 4.0

Contents

About This Guide

This cnWave™ 5G Fixed Operation and Troubleshooting Guide contains procedures for identifying and correcting faults in a cnWave™ 5G Fixed platform of products in a Lab environment. It also contains a set of operational procedures for managing customer downtime and modifying some parameters such as operational frequencies, bandwidth, and CPE configuration data.

This guide covers the following topics:

- Troubleshooting cnWave™ 5G Fixed Platform of Products
- Operational Procedures for BTS
- General Troubleshooting Procedures

Purpose

Documents specific to the cnWave™ 5G Fixed platform of products are intended to instruct and assist personnel in the operation, installation, and maintenance of the Point-to-Multi-Point (PMP) equipment (Cambium Networks) and ancillary devices of cnWave™ 5G Fixed platform of products. It is recommended that all personnel engaged in such activities be properly trained.

Cambium disclaims all liability whatsoever, implied or express, for any risk of damage, loss or reduction in system performance arising directly or indirectly out of the failure of the customer, or anyone acting on the customer's behalf, to abide by the instructions, system parameters, or recommendations made in this document.

Cross references

References to external publications are shown in italics. Other cross references, emphasized in blue text in electronic versions, are active links to the references.

This document is divided into topics that are divided into sections. Sections are not numbered and are listed in the table of contents.

Feedback

We appreciate feedback from the users of our documents. This includes feedback on the structure, content, accuracy, or completeness of our documents. To provide feedback, visit our support website - https://support.cambiumnetworks.com.

Warnings, cautions, and notes

The following describes how warnings, notes, and cautions are used in this document and in all documents of the Cambium Networks document set.

Warnings

Warnings precede instructions that contain potentially hazardous situations. Warnings are used to alert the reader to possible hazards that could cause loss of life or physical injury. A warning has the following format:

Warning

Warning text and consequence for not following the instructions in the warning.

Cautions

Cautions precede instructions and are used when there is a possibility of damage to systems, software, or individual items of equipment within a system. However, this damage presents no danger to personnel. A caution has the following format:

Caution

Caution text and consequence for not following the instructions in the caution.

Notes

A note means that there is a possibility of an undesirable situation or provides additional information to help the reader understand a topic or concept. A note has the following format:

Note

Note text.

Important regulatory information

The cnWave™ 5G Fixed platform of products are certified as an unlicensed device in frequency bands where it is not allowed to cause interference to licensed services (called primary users of the bands).

Complying with rules for the country of operation

USA specific information

Caution

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operation.

Note

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

Canada specific information

Caution

This device complies with ISEDC 's license-exempt RSSs. Operation is subject to the following two conditions:

- This device may not cause interference.
- This device must accept any interference, including interference that may cause undesired operation of the device. This device must accept any interference, including interference that may cause undesired operation of the device.

Note

Certification note from industry Canada: While this equipment meets the technical requirements for its operation in its rated paired block arrangement, this block arrangement is different than the 40 + 40 MHz block arrangement prescribed in documents RSS-191 and SRSP-324.25. The operation of this equipment IS NOT permitted if the out-of-band and spurious emission limits are not met at the edge of any contiguous licensed spectrum. It should be noted that all current relevant spectrum policies, licensing procedures, and technical requirements are still applicable. For additional information, contact the local Industry Canada office.

Renseignements spécifiques au Canada

Note

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes:

- L'appareil ne doit pas produire d'interférences; et
- L'utilisateur de l'appareil doit accepter toute interférence radioélectrique, même si elle est susceptible d'en compromettre le bon fonctionnement.

European specific information

The cnWave™ 5G Fixed platform of products are compliant with applicable European Directives required for CE marking:

- 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonization of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC; Radio Equipment Directive (RED).
- 2011/65/EU of the European Parliament and of the Council of 8 June 2011 on the restriction of the use of certain hazardous substances in electrical and electronic equipment (RoHS Directive).

EU Declaration of Conformity

Hereby, Cambium Networks declares that the Cambium Networks cnWave™ 5G Fixed Series of Wireless Ethernet Bridge complies with the essential requirements and other relevant provisions of Directive 2014/53/EU. The declaration of conformity may be consulted at https://www.cambiumnetworks.com/.

Application software (firmware)

Download the latest cnWave™ 5G Fixed products family software and install it in the Base Transceiver System (BTS) and Customer Equipment Premise (CPE) before deploying the equipment. Instructions for installing software are provided in the cnWave™ 5G Fixed Planning and Installation Guide (available at https://support.cambiumnetworks.com/files/28cnwave/).

Ethernet networking skills

The installer must have the ability to configure IP addressing on a PC and to set up and control products using a web browser interface.

Lightning protection

To protect outdoor radio installations from the impact of lightning strikes, the installer must be familiar with the normal procedures for site selection, bonding and grounding. Installation guidelines for the cnWave™ 5G Fixed platform family is available in the Lightning Protection Units (LPUs) topic in the cnWave™ 5G Fixed *Planning and Installation Guide.*

Specific expertise and training for professional installers

To ensure that the cnWave™ 5G Fixed series are installed and configured in compliance with the requirements of EU, ISEDC and the FCC, installers must have the radio engineering skills and training described in this section.

Use the Training link to access the technical training program (from Cambium Networks).

Legal and Open-Source Software statements

Refer to the cnWave™ 5G Fixed Legal and Open-Source Guide for:

- Cambium Networks end user license agreement and
- Open-Source Software Notices.

Problems and warranty

Reporting problems

If any problems are encountered when installing or operating this equipment, follow this procedure to investigate and report:

1. Search this document and the software release notes of supported releases.
2. Visit the Support website (Cambium Networks).
3. Ask for assistance from the Cambium Networks product supplier.
4. Gather information from affected units, such as any available diagnostic downloads.
5. Escalate the problem by emailing or telephoning support.

Repair and service

If unit failure is suspected, obtain details of the Return Material Authorization (RMA) process from the Support website.

Hardware warranty

Cambium's standard hardware warranty is for one (1) year from date of shipment from Cambium Networks or a Cambium distributor. Cambium Networks warrants that hardware will conform to the relevant published specifications and will be free from material defects in material and workmanship under normal use and service. Cambium shall within this time, at its own option, either repair or replace the defective product within thirty (30) days of receipt of the defective product. Repaired or replaced products will be subject to the original warranty period but not less than thirty (30) days.

To register the cnWave™ 5G Fixed products or activate warranties, visit the Support website. For warranty assistance, contact the reseller or distributor. The removal of the tamper-evident seal will void the warranty.

Caution

Using non-Cambium parts for repair could damage the equipment or void warranty. Contact Cambium for service and repair instructions.

Portions of Cambium equipment may be damaged from exposure to electrostatic discharge. Use precautions to prevent damage.

Security advice

Cambium Networks systems and equipment provide security parameters that can be configured by the operator based on their particular operating environment. Cambium recommends setting and using these parameters following industry recognized security practices. Security aspects to be considered are protecting the confidentiality, integrity, and availability of information and assets. Assets include the ability to communicate, information about the nature of the communications, and information about the parties involved.

In certain instances Cambium makes specific recommendations regarding security practices, however the implementation of these recommendations and final responsibility for the security of the system lies with the operator of the system.

Caring for the environment

The following information describes national or regional requirements for the disposal of Cambium Networks supplied equipment and for the approved disposal of surplus packaging.

In EU countries

The following information is provided to enable regulatory compliance with the European Union (EU) directives identified and any amendments made to these directives when using Cambium equipment in EU countries.

Disposal of Cambium equipment

European Union (EU) Directive 2012/19/EU Waste Electrical and Electronic Equipment (WEEE).

Do not dispose of Cambium equipment in landfill sites. For disposal instructions, refer to https://www.cambiumnetworks.com/support/compliance/.

Disposal of surplus packaging

Do not dispose of surplus packaging in landfill sites. In the EU, it is the individual recipient's responsibility to ensure that packaging materials are collected and recycled according to the requirements of EU environmental law.

In non-EU countries

In non-EU countries, dispose of Cambium equipment and all surplus packaging in accordance with national and regional regulations.

Troubleshooting cnWave™ 5G Fixed Platform of Products

This section provides basic information about the cnWave™ 5G Fixed platform of products - B1000 Base Transceiver Station (BTS) and C100 Customer Premise Equipment (CPE).

The section explains required configurations that you can use for troubleshooting in a lab environment. This section covers the following topics:

- Basic information about the platform of products
- Troubleshooting in a lab environment

Basic information about the platform of products

The cnWave™ 5G Fixed platform of products requires minimum configuration for installation and normal operation. Apart from configuring parameters such as the operating frequencies, IP addresses, and other networking elements (for example, SNMP and RADIUS) at the B1000 BTS and the C100 CPE, you must confirm that the equipment is operating optimally.

Note

In the later sections of this guide, the term BTS is used to refer to B1000 BTS and the term CPE to refer to C100 CPE.

It is recommended to set up and check that the BTS and/or the CPEs are operational and correctly configured in a lab environment before installing the equipment at the customers' site. This is also known as the staging process. It also provides an opportunity to install updates or specific software or configure specific monitoring parameters.

You may need to troubleshoot either the devices in a lab environment, on a newly installed system, or on an operational system if communication is lost or after a lightning strike. It is assumed that you are familiar with the products and the information that is explained in the following guides:

- *cnWave™ 5G Fixed Planning and Installation Guide*
- *cnWave™ 5G Fixed Configuration Guide*

These guides are available on Cambium Networks Support site.

Troubleshooting in a lab environment

This section describes the key steps required to troubleshoot a BTS, a CPE, and a BTS-CPE link.

It is recommended that you must test both the BTS and the CPE devices prior to installation at a site, as listed:

- BTS and/or the CPE can be powered up.
- Configurations can be checked by accessing the devices' web user interfaces (UI).
- Links can be established between the BTS and the CPEs.

These tasks can be performed when commissioning a BTS or a CPE prior to installation or even on a BTS or a CPE that has been installed and returned due to a failure in the field.

In a lab environment, you must ensure that the following configurations are in place:

- Configuring the management PC
- Connecting the BTS to power
  - Accessing the B1000 UI
- Connecting the CPE to power
  - Accessing the C100 UI
- Establishing a link between a BTS and a CPE
  - Mandatory parameters required for establishing a BTS-CPE link
  - Read-only parameters required for monitoring the link
- Checking the BTS installation using satellite details

Configuring the management PC

It is mandatory to configure a PC or Laptop to access the web UI of the cnWave™ 5G Fixed platform of products (BTS or CPE).

Note

Both the BTS and the CPE are shipped with a default IP address (169.254.1.1) and therefore, the management PC must be configured with an IP address in the same subnet (for example, 169.254.1.100).

You must configure the PC (for example, using Windows PC) or laptop for setting up the IP address (169.254.1.1) for the BTS. This configuration enables the PC to communicate with the BTS and CPEs. For more information on how to connect cables and connect to power, refer to the *cnWave™ 5G Fixed Planning and Installation Guide*.

To configure the PC, perform the following steps:

1. On Windows PC, click **Start** > **Settings** > **Network & Internet**.

   The Network Status page appears with multiple options on the left navigation column.

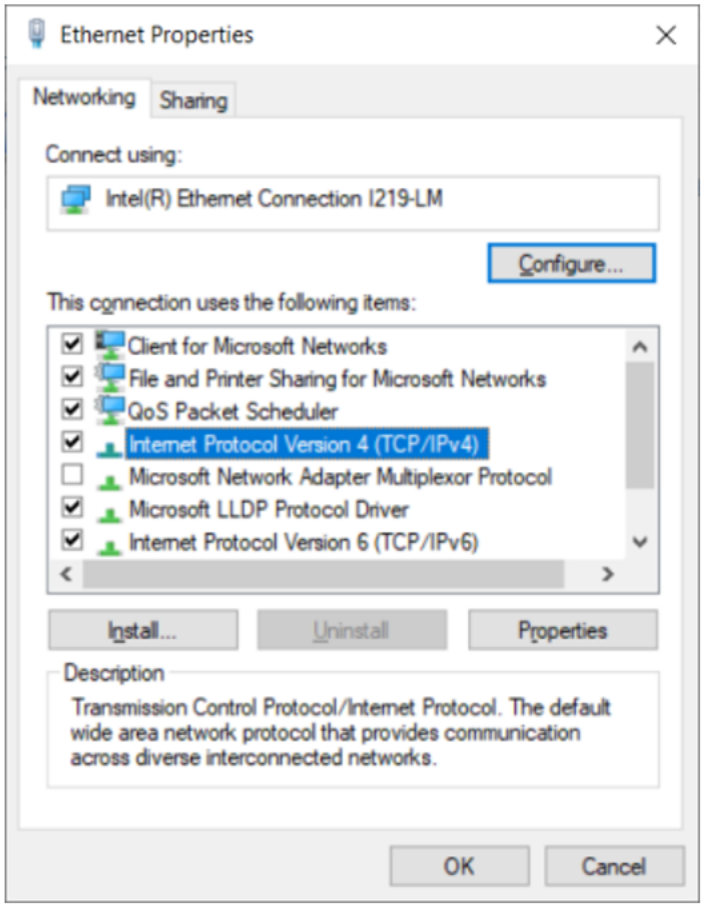
2. Select **Ethernet** > **Change adapter settings**.

   The Network Connections page appears.

3. Select **Ethernet** and right-click to select **Properties**.

   The **Ethernet Properties** dialog box appears with Networking and Sharing tabs, as shown in Figure 1.

Figure 1: *The Ethernet Properties dialog box*

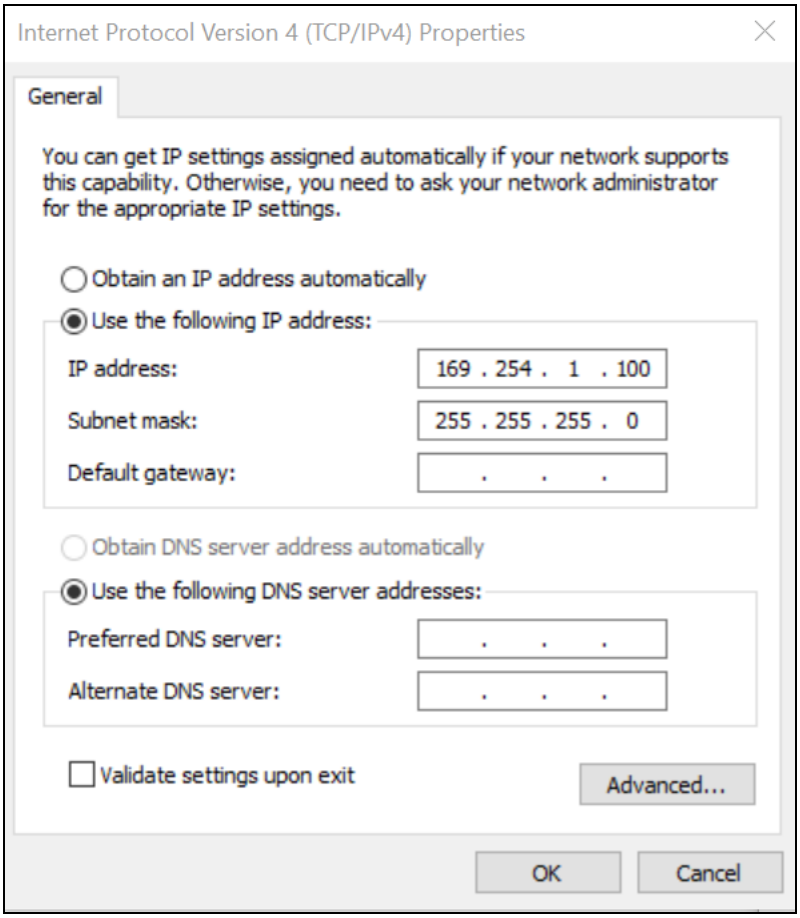


By default, the Networking tab is selected.

4. Select **Internet Protocol Version 4 (TCP/IPv4)** from the available list of connections (as shown in Figure 1).
5. Click **Properties**.

   The **Internet Protocol Version 4 (TCP/IPv4) Properties** dialog box appears, as shown in Figure 2.

Figure 2: *The Internet Protocol Version 4 Properties dialog box*



6. In the **Use the following IP address** section, type an appropriate IP address in the **IP address** text box. Example: 169.254.1.1

   If you are using 169.254.1.1 as the default address, you must avoid using 169.254.0.0 and 169.254.1.1 IP addresses.

7. In the **Subnet mask** text box, type 255.255.255.0.

8. Leave the **Default gateway** text box blank and click **OK**.

   This action must allow you to communicate with the BTS.

9. To verify whether the PC is configured successfully, run a command and type `ipconfig` (on a Windows PC).

10. Check whether the IP address (as shown in Figure 2) is displayed on the command screen, as shown in Figure 3.

    Figure 3 shows the IP address (highlighted in yellow color). If this step fails, you must check or replace the PC until you verify the successful configuration. If the PC configuration is not successful, it is not possible to proceed and troubleshoot the radios.

Figure 3: *Checking the management PC configuration*

```
Command Prompt

C:\Users\qdxb67>ipconfig

Windows IP Configuration


Ethernet adapter Card 3 - Switch:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter Card 2 - cnWave28:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::8cb:3159:10ce:f8a%3
   IPv4 Address. . . . . . . . . . . : 10.10.10.101
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   IPv4 Address. . . . . . . . . . . : 10.10.10.254
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   IPv4 Address. . . . . . . . . . . : 10.10.11.100
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   IPv4 Address. . . . . . . . . . . : 169.254.1.100
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.10.10.1

Ethernet adapter Card 1 - Corporate:

   Connection-specific DNS Suffix  . : CAMNWK.COM
   Link-local IPv6 Address . . . . . : fe80::a0b3:4c7e:b0da:937f%8
   IPv4 Address. . . . . . . . . . . : 10.130.158.9
   Subnet Mask . . . . . . . . . . . : 255.255.254.0
   Default Gateway . . . . . . . . . : 10.130.159.254

C:\Users\qdxb67>_
```

Connecting the BTS to power

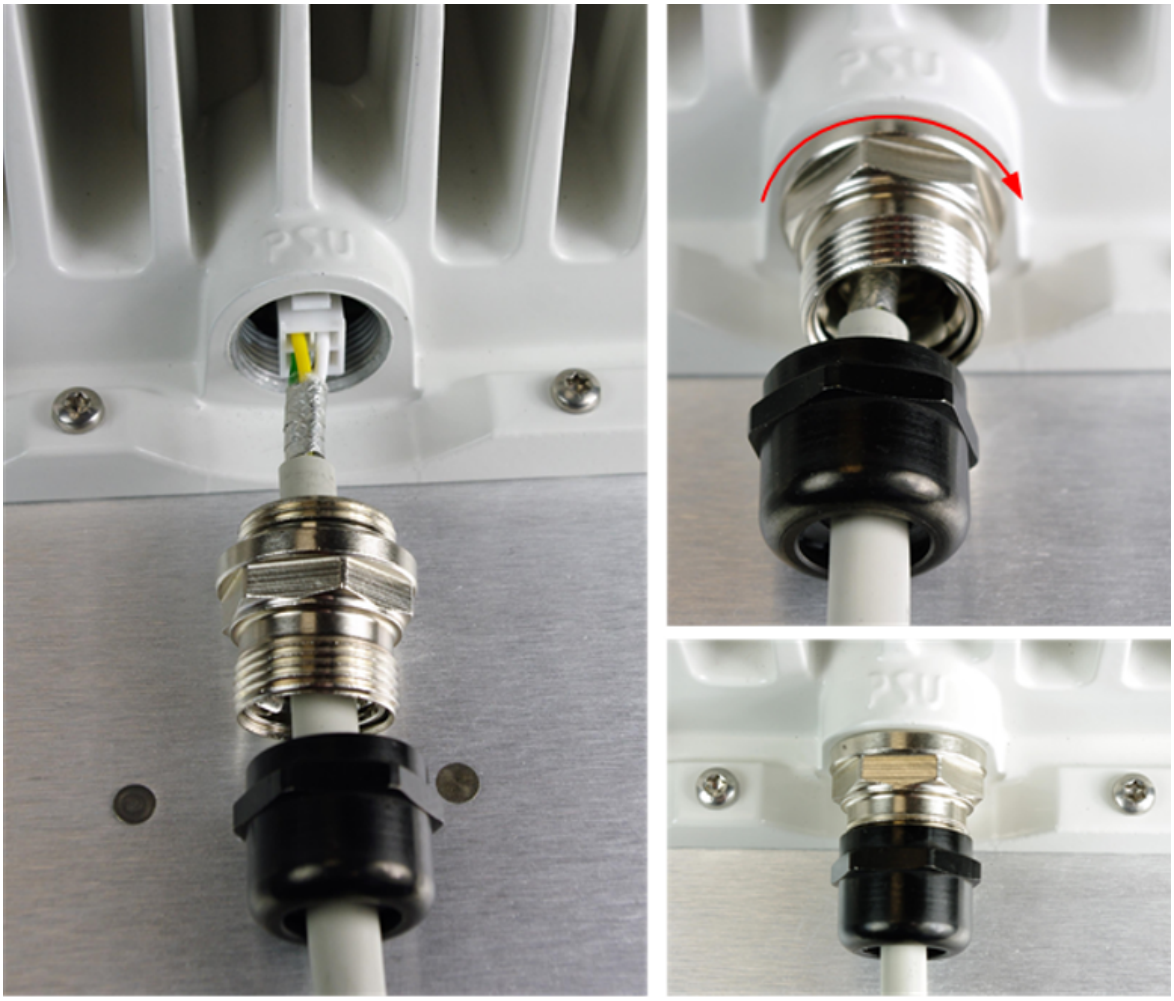
When the management PC is successfully configured with the correct IP address required to communicate with the BTS, you must perform the following tasks:

1. Connect the power and data cables to the BTS (as described here).
2. Power up the BTS (radio module).
3. Access the web UI of the B1000 BTS, as described in the Accessing the B1000 UI section.

To connect the BTS to power, perform the following steps:

1. Connect the input side of the 30W DC Power injector to the BTS, as shown in Figure 4.

   Figure 4: *Connecting the power cable to the BTS*



2. Connect an Ethernet cable (data) between the network port of the PC and the MAIN of the BTS.

   Figure 5 shows the BTS connected with the power and data cables.

Figure 5: *BTS Interface connections*

3. After connecting the BTS to power, ensure that you can communicate with the BTS by running a continuous PING session at a command prompt.

   Example: Run a command prompt and type `Ping -t 169.254.1.1`. If the PING is successful, you can access the login page of B1000 (BTS) UI using the http://169.254.1.1 URL.

For detailed information on how to power up the BTS, refer to the *cnWave™ 5G Fixed Planning and Installation Guide*.

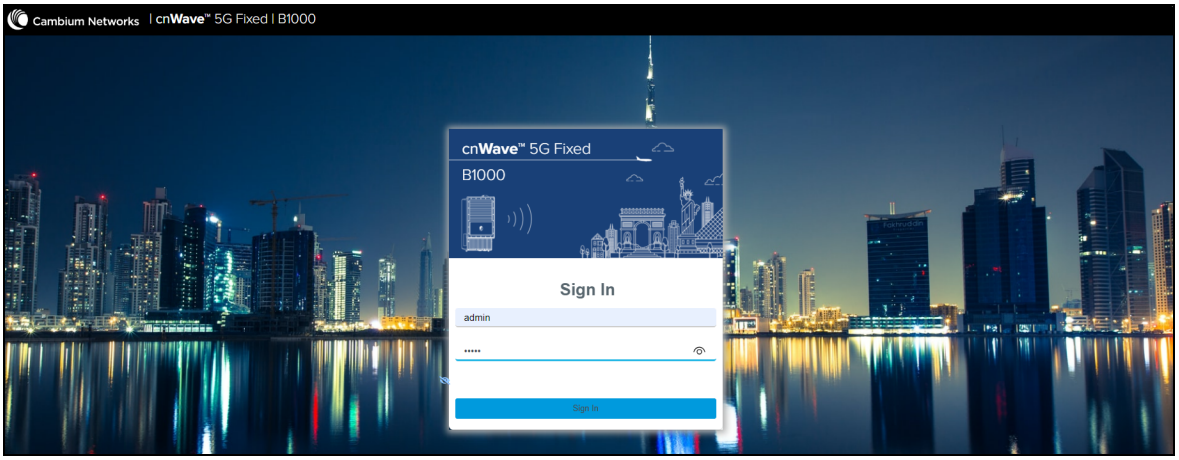
Accessing the B1000 UI

To access the B1000 UI, perform the following steps:

1. Open a web browser and type the URL - http://169.254.1.1 - to access the B1000 UI.

   The **Sign In** page appears, as shown in Figure 6.

   Figure 6: *The Sign In page for B1000 UI (BTS)*



2. Type an appropriate username and password.

   Default username: admin

   Default password: admin

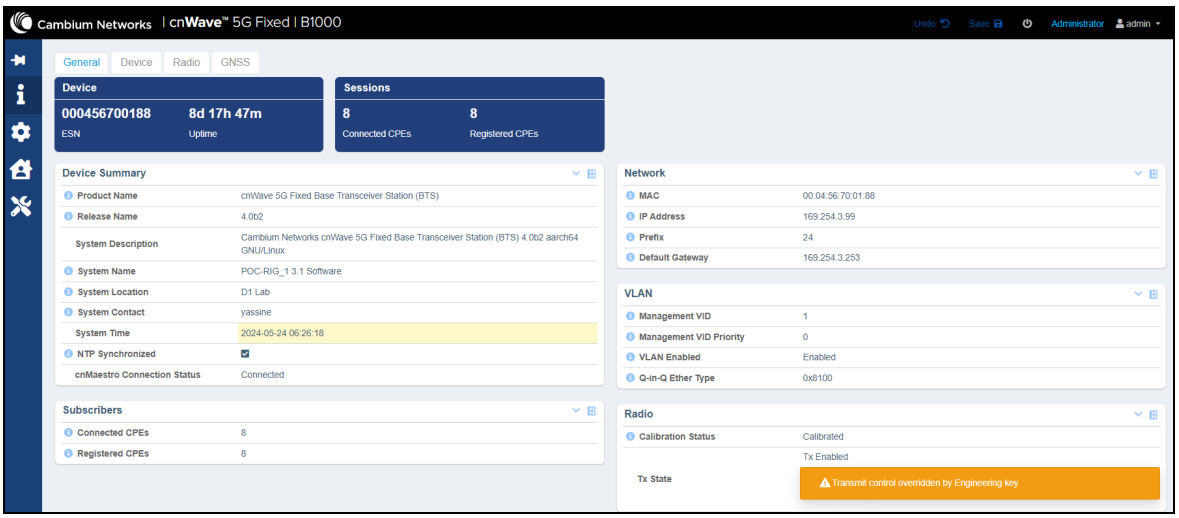
   You can use the show-password eye icon (👁) to view the password characters.

3. Click **Sign In**.

   The Profile page appears. You can use this page to change the password and set your preferences. For more information about the **Profile** page, refer to the *cnWave™ 5G Fixed Configuration Guide*.

   On logging on to the B1000 UI, you must click the icon (Dashboard) icon on the left navigation pane. The main B1000 dashboard page appears, as shown in Figure 7.

   Figure 7: *The main B1000 dashboard page*



   When the B1000 dashboard page appears successfully, you can check default parameters and configure any parameters required for the operation of the BTS.

For detailed information about each B1000 UI configuration pages and associated parameters, refer to the *cnWave™ 5G Fixed Configuration Guide*.

Connecting the CPE to power

You can connect the CPE to power before the BTS but only when the management PC has been successfully configured with the right IP address to communicate with the CPE.

The easiest way to connect the CPE to power is by using a Power over Ethernet (PoE) adapter. It is also possible to power the CPE from a PoE switch port (for example, cnMatrix).

To connect the CPE to power, perform the following steps:

1. Connect the 1 GbE LAN port of the Power injector to the PC or network equipment.

2. Connect the 30 W 56V 1 GbE PoE port of the Power injector to the RJ45 port of the C100 CPE.

   Figure 8 shows how the CPE is connected to the Power Injector.

Figure 8: *Connecting the CPE to power using a PoE*

3. Connect the input side of the 30W DC Power injector to the AC power line.

4. Ensure that you can communicate with the CPE by running a continuous PING session at a command prompt.

   Example: You must run a command prompt and type `Ping -t 169.254.1.1`. If the PING is successful, you can access the login page of C100 UI using the http://169.254.1.1 URL.

For detailed information on how to power up the CPE, refer to the *cnWave™ 5G Fixed Planning and Installation Guide*.

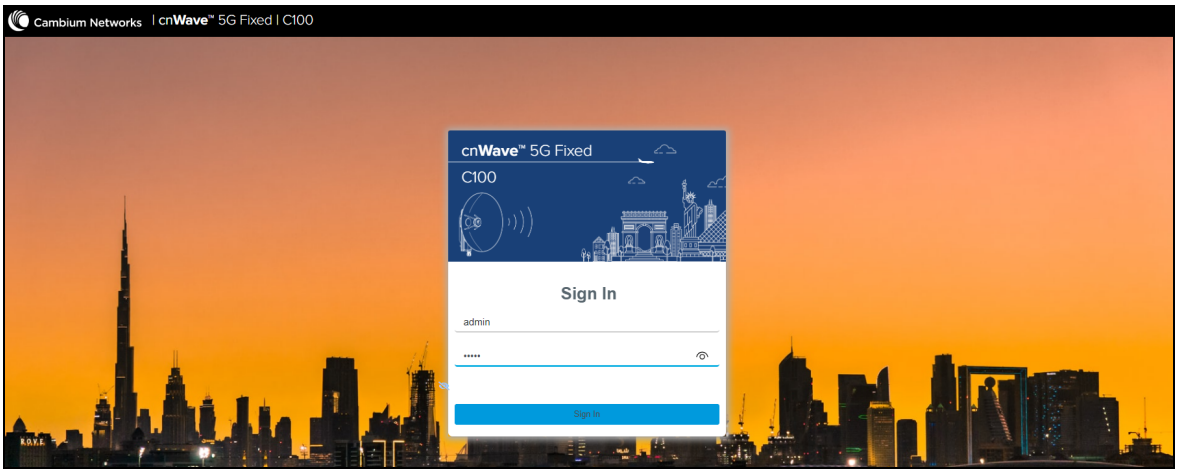
Accessing the C100 UI

To access the C100 (CPE) UI, perform the following steps:

1. Open a web browser and type the URL - http://169.254.1.1 to access the C100 UI.

   The **Sign In** page appears, as shown in Figure 9.

   Figure 9: *The Sign In page for C100 (CPE) UI*



2. Type an appropriate username and password.

   Default username: admin

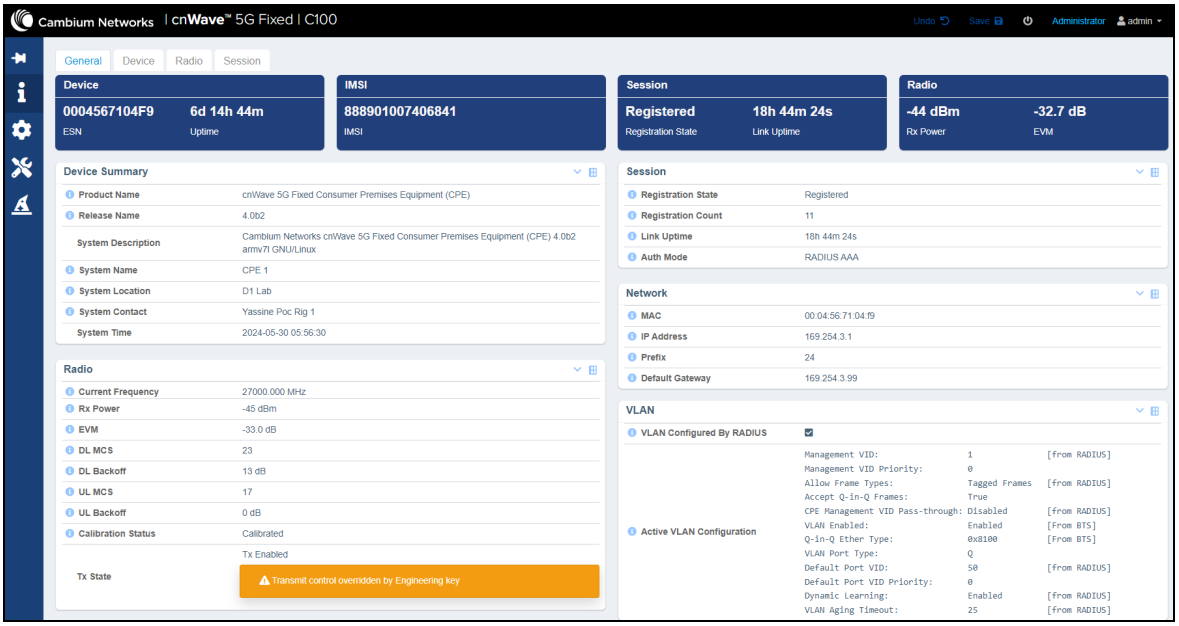
   Default password: admin

   You can use the show-password eye icon (👁) to view the password characters.

3. Click **Sign In**.

   The main C100 dashboard page appears, as shown in Figure 10.

   Figure 10: *The main C100 dashboard page*



When the C100 dashboard page appears successfully, you can check default parameters and configure any other parameters required for the operation of the CPE.

For detailed information about each C100 UI configuration pages and associated parameters, refer to the *cnWave™ 5G Fixed Configuration Guide*.

Establishing a link between a BTS and a CPE

When you can connect to both the BTS and the CPE dashboards (which is a prerequisite to start establishing a radio link), you can repeat the same connection procedure to connect to more than one CPE. This section lists the main parameters that need to be configured for establishing a link (including troubleshooting).

To establish a link between a BTS and a CPE, perform the following steps:

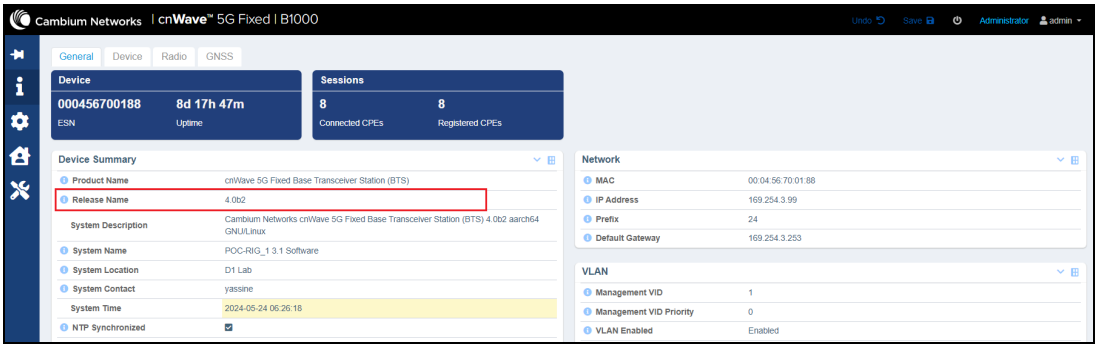
1. Use a pole (ideally) and attach a B1000 BTS using the tilt bracket. For details on how to assemble the tilt brackets, refer to the *cnWave™ 5G Fixed Planning & Installation Guide* (available on Cambium Networks Support site).

2. Power up the BTS and use a PC to access the web interface, as described in Connecting the BTS to power and Accessing the B1000 UI sections, respectively.

3. Check or verify the following main parameters specific to the BTS in the B1000 UI:

- **Release Name** - When you navigate to **Dashboard** > **General** page from the main B1000 dashboard page, the **Release Name** parameter is visible. Note down the operational software version number (as shown in Figure 11).

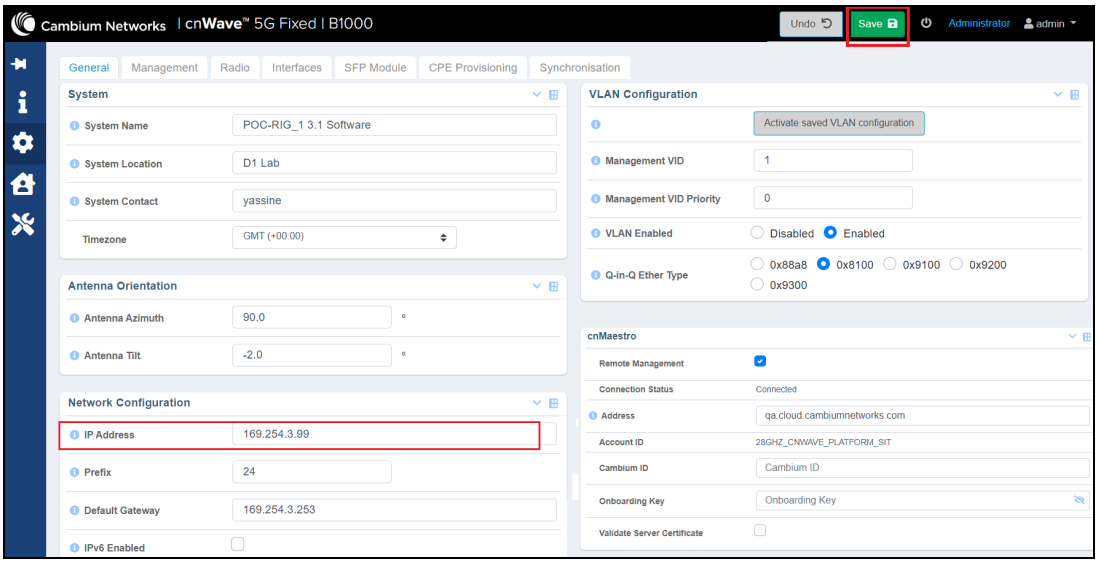
  Figure 11: *The BTS Software Version-specific parameter*



- **IP Address** - When you navigate to **System** > **General** page from the main B1000 dashboard page, the **IP Address** parameter is visible.

  If you change the IP address of the BTS in the UI, you must also change the IP address configured in the management PC accordingly to connect to the BTS after a reboot. On making changes in the UI, you must click **Save** (located on the top right of the page) as shown in Figure 12.

  Figure 12: *The BTS network-related parameters*



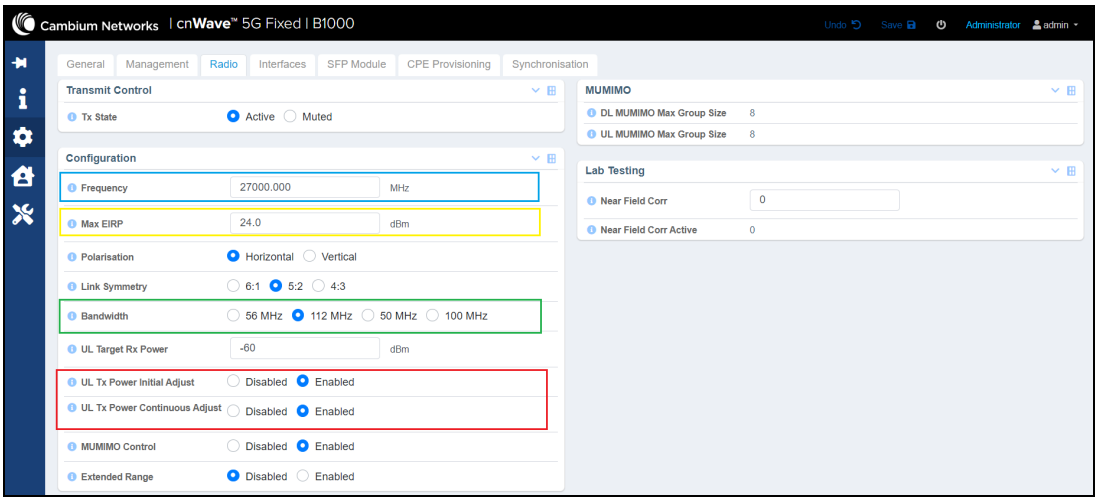
  You must note down the radio-related parameters for the BTS. When you navigate to **System** > **Radio** page from the main B1000 dashboard page, following radio-related parameters are visible as shown in Figure 13:

- **Frequency** - Note down the operating frequency to be used for the lab test. Any frequency in the 26-28 GHz range can be used. The CPE must have this frequency in the Radio Scan Frequencies list (as described in Step 6 in this section).

- **Max EIRP** - This is a parameter that is country regulation specific and the recommended value for a Lab test is 25 dBm (default value is 51 dBm).

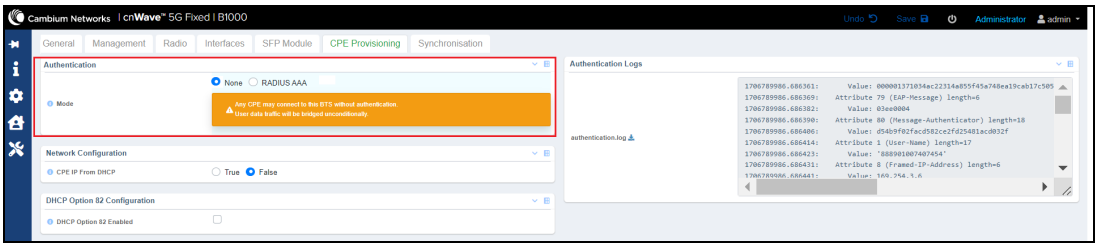
- **Bandwidth** - The value of this parameter must be the same on both BTS and any connected CPE. Following bandwidth values are supported:
    - 50 MHz
    - 56 MHz
    - 100 MHz
    - 112 MHz
- **UL Tx Power Initial Adjust** and **UL Tx Power Continuous Adjust** - Ensure that both parameters are set to **Enabled**. They are used to automatically control the BTS transmission power at the initial connection and continuously after that.

Figure 13: *The BTS Radio parameters*



- **Authentication** - When you navigate to the **System** > **Authentication** page from the main B1000 dashboard page, the **Mode** parameter is visible. To test a BTS-CPE link for the first time or to troubleshoot an existing link, it is recommended to disable the Radius authentication by choosing the **None** option (as shown in Figure 14).

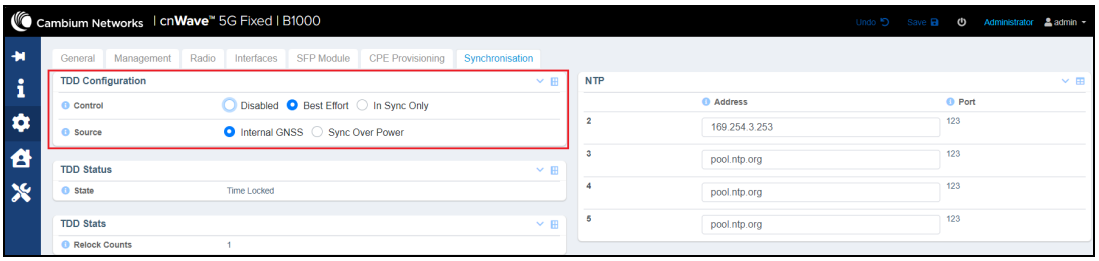
Figure 14: *The Authentication Mode parameter*



- **Synchronisation** - When you navigate to the **System** > **Synchronisation** page from the main B1000 dashboard page, the **TDD Configuration** section is visible with the following parameters (as shown in Figure 15):
    - Control
    - Source

For the initial test, set the **Control** parameter to **Disabled** and use the **Internal GNSS** option as the source (these must be the default parameters) in the **TDD Configuration** section.

Figure 15: *The BTS Synchronisation parameters*



4. Power up the CPE. Ideally, it is recommended to place the CPE upright (without the dish) at a reasonable distance (3-5 meters at least) from the BTS.

5. Use a PC to access the web interface, as described in Connecting the CPE to power and Accessing the C100 UI sections.

> **Note**
>
> If it's a new CPE, the IP address must be set to 169.254.1.1. In this case, it is recommended to change the IP address of the BTS to other than the default address and to access the web interface. Also, note that it is not possible to change the IP address of a CPE.

6. Check or verify the following main parameters specific to CPE in the C100 UI:

   - **Release Name** - When you navigate to **Dashboard** > **General** page from the main C100 dashboard page, the **Release Name** parameter is visible. Take a note of the operational software version number.

     You must note down the radio-related parameters for the BTS. When you navigate to **System** > **Radio** page from the main B1000 dashboard page, following radio-related parameters are visible as shown in Figure 16.

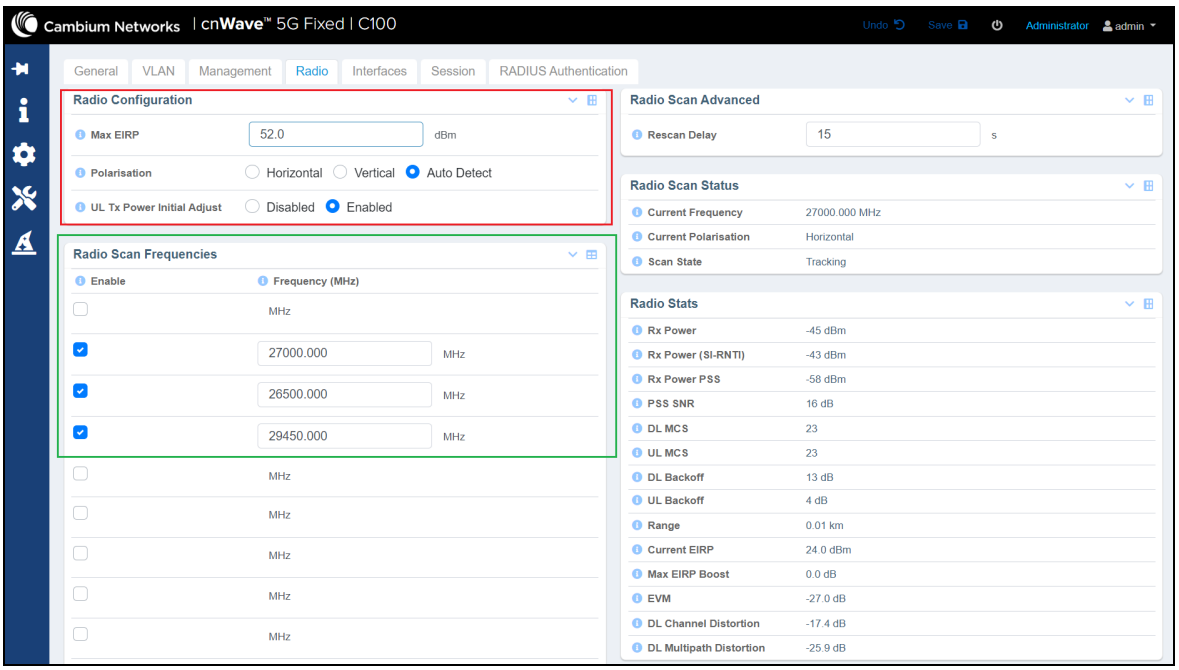
   - **Radio Scan Frequencies** - The CPE must have the operational frequency of BTS listed, and it must be **Enabled**. Figure 16 shows that there are two frequencies in the list and one of them is 27000.000 MHz, which is the same as that of BTS operational frequency (as shown in Figure 13).

   - **Max EIRP** - This is a parameter that is country regulation specific and a recommended value for the Lab test is 30 dBm.

   - **Polarization** - This is a parameter that must be the same as that of the BTS. It is recommended to set it to **Auto Detect** (default value).

   - **Alignment Mode** - For the test, it is recommended not to select this mode. This is a parameter used in the field to align the CPE with a BTS using audible tones.

Figure 16: *The CPE radio parameters*



7. Check that a link has been established between the BTS and the CPE.

   The easiest way is to view the B1000 (BTS) dashboard, which shows the status and number of CPEs connected and registered with BTS (as shown in Figure 17 and Figure 18, respectively).

Figure 17: *Checking the BTS-CPE connection status using the B1000 dashboard*

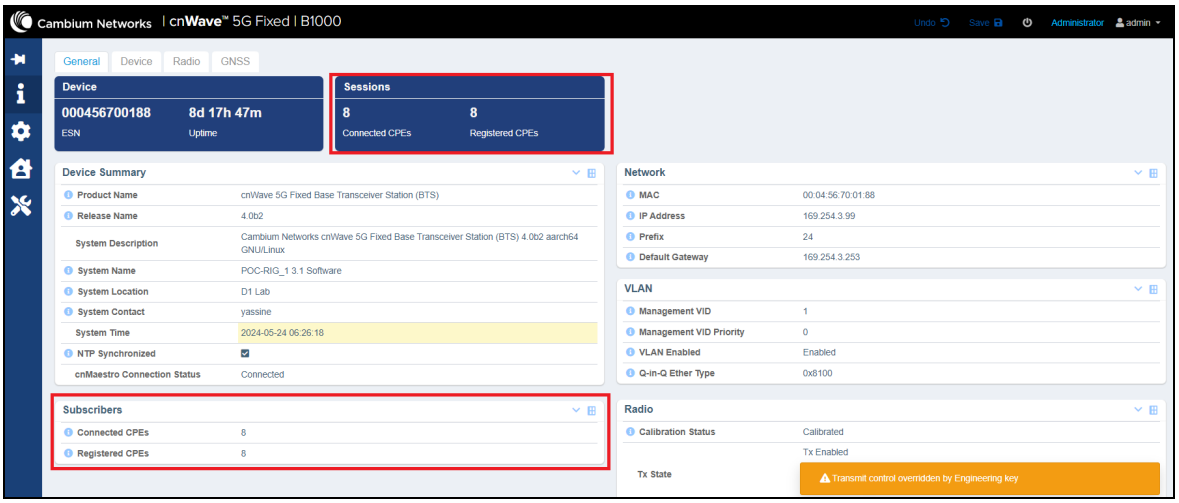
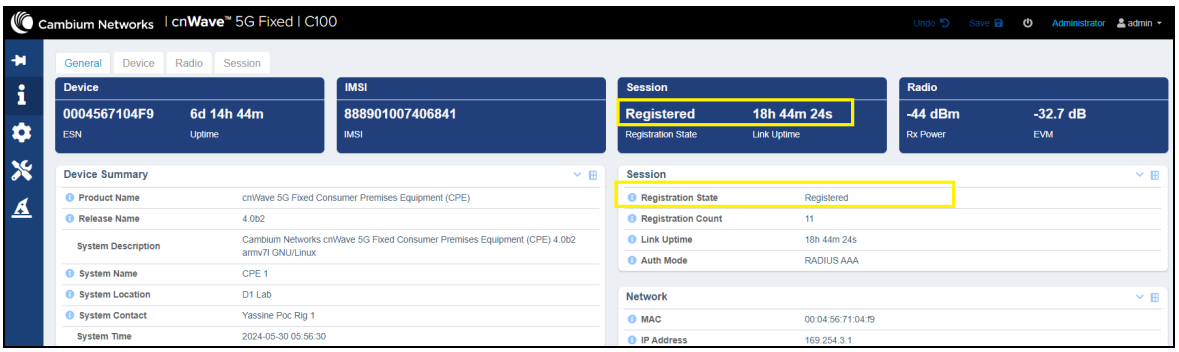
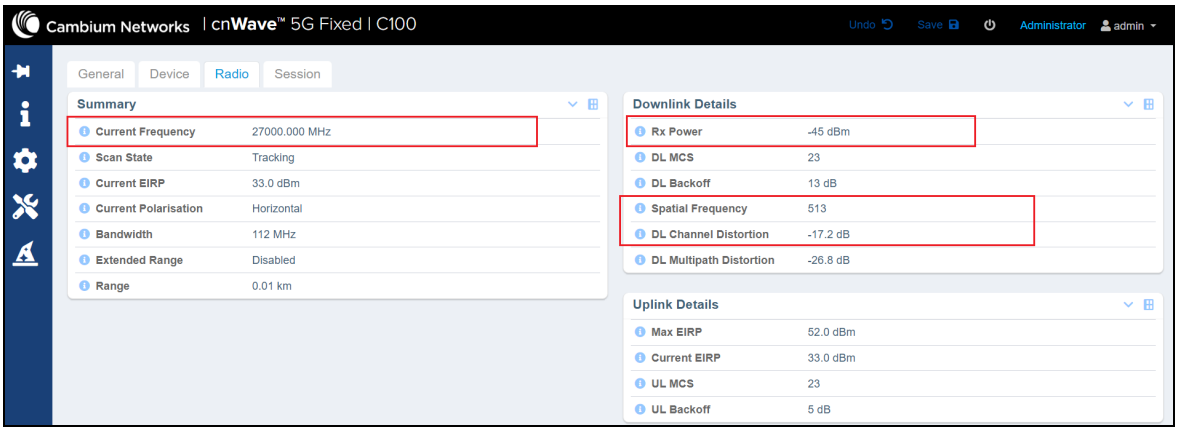


Figure 18: *Checking the BTS-CPE connection status using the C100 dashboard*



8. If the link fails to come up even after following all the above-mentioned steps from 1 to 7, check some of the parameters in the **Radio** page in the main C100 (CPE) dashboard (as shown in Figure 19).

Figure 19: *The CPE Radio page*

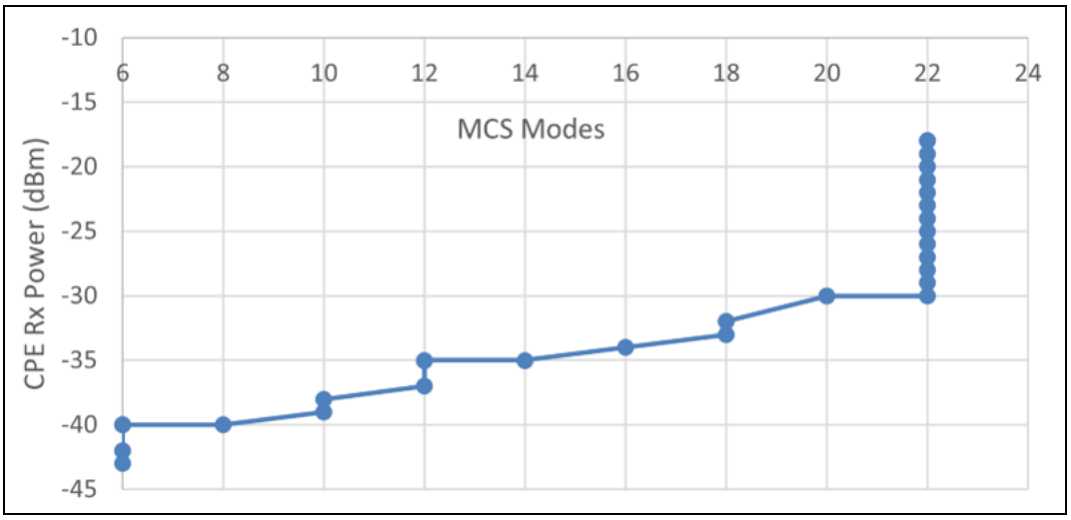


Consider the following details:

- **Rx Power** – if the value shown is -120 dBm (default), then the CPE is not able to find the BTS (wrong frequency or obstacle in the path). Ensure the path between the BTS and the CPE is free of any obstacles. The cnWave™ 5G Fixed platform of products works only in Line of Sight (LoS) environments.

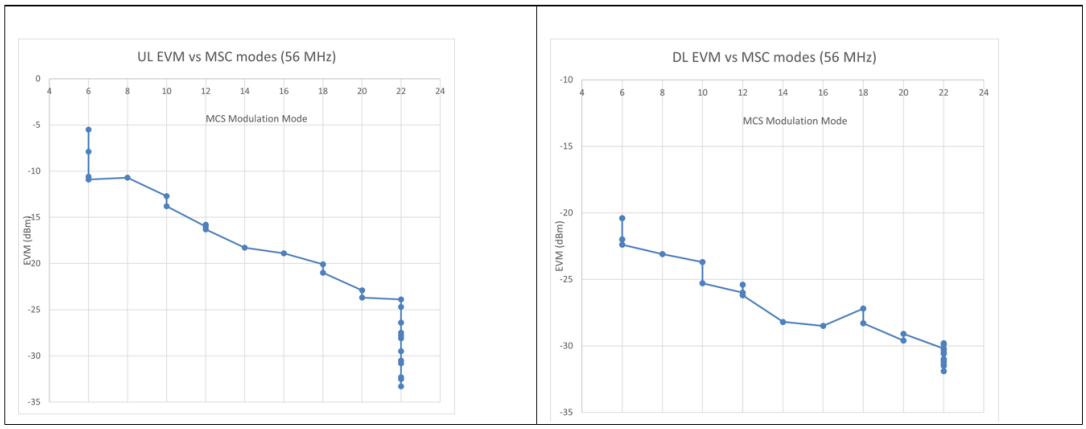
  A good value is around -40 dBm when a BTS-CPE link is well established. This is also dependent on local regulatory requirements (EIRP). Figure 20 shows the relationship between the Modulation and Coding Scheme (MCS) levels and the corresponding value of the CPE Rx Power.

Figure 20: *CPE Rx Power vs MCS modes*



- **Error Vector Magnitude (EVM)** - A good EVM must be in the range of -20/-25 dB. This parameter is dependent on the modulation mode and less on the frequency and bandwidth. You can monitor the changes of this parameter when the CPE is trying to attach. After a little while, you can notice that the value keeps going up and down without settling to the negative twenties value. This means that the CPE cannot see the BTS. That can usually be due to an alignment issue or a frequency issue, but if they have the same frequencies and that the CPE is close and loosely aligned, there is a hardware issue with the CPE (calibration or hardware failure). Figure 21 shows the relationship between the MCS modulation levels and the corresponding EVM value.

Figure 21: *EVM versus MCS modulation Modes (56 MHz)*



- **Transmitted RACH Count** - The Uplink Random Access Channel (RACH) is the uplink channel used by the CPE to initiate a connection request to the BTS. If all is well, the BTS must respond to enable the CPE transmission that results in generating a RACH number.

  With this RACH number, there are also two other counters - **Transmitted SRB** and **Received SRB packets**. These numbers indicate the number of BTS-CPE messages exchanged to attach the CPE. At this point, this means that the CPE can find the BTS, and baring any other radio issues (as shown in Figure 21), the link must establish.

Mandatory parameters required for establishing a BTS-CPE link

Table 1 lists the parameters that must be configured to establish a link between a BTS and one or several CPEs.

Table 1: Parameters required for establishing a link between a BTS and a CPE

Parameter	BTS	CPE	Description
Operational Software	Yes	Yes	It is recommended to have the same label for the operational software. Example: 4.0 label for the 4.0 operation software.
Frequency	Yes	Yes	The CPE must have the same frequency in the Radio Scan Frequencies list as that of the BTS.
Bandwidth	Yes	Yes	Must be the same for both BTS and CPE.
Link Symmetry	Yes	Yes	Must be the same for both BTS and CPE.
Polarization	Yes	Yes	Must be the same for both BTS and CPE or can be set to Auto Detect for the CPE In C100 UI (recommended).

Read-only parameters required for monitoring the link

There are read-only parameters that must be monitored during troubleshooting if a link between a BTS and a CPE cannot be established.

Table 2 lists read-only parameters for the BTS and/or CPE that can be used to troubleshoot if a link cannot be established between a BTS and a CPE. This is a minimal and non-exhaustive list before looking in-depth at the event logs and contacting Cambium Networks Support site for a resolution.

Table 2: Minimal list of read-only parameters

Parameter	BTS	CPE	Description
EVM	No	Yes	The EVM value goes up and down until the CPE finds the BTS and settles to a value in the negative 20s, which indicates a good link. It is important to point out that the higher decibel values represent the best error-free modulation results. Example: An EVM of -40 dB is better than one of -25 dB. In terms of percentage, -40 dB converts to 1% error while -25 dB translates to 5.6% error.
Rx Power	Yes	Yes	The Rx Power level is the strength of the signal that is received from a radio. The Rx Power number is normally represented as a negative value (for example, -41 dBm), It is important to remember that the higher the negative value (further from zero), the transmit signal is weaker. The lower the negative value (closer to zero), the transmit signal is stronger. For troubleshooting, it is recommended to monitor this parameter and compare it with the Rx Signal Level predicted by LINKPlanner at each end of the link. Ideally, the Rx level must be in the range of -18 to -25 dBm. If the Rx level is under -25 dBm, the Signal-to-Noise Ratio (SNR) is likely to decrease, which means that the performance of the link also decreases.

If a link cannot be established (even after following all the procedures described in this section), then there may be a hardware problem. In such a scenario, you can swap the hardware equipment and restart the procedures.

Checking the BTS installation using satellite details

Using the **GNSSS** page in the B1000 UI, you can check whether the BTS device is installed in a clear sky. This action helps you to ensure the BTS installation for optimal GPS synchronisation.

When you complete the installation of the BTS device on Mast, you must install it in a clear sky using the GNSS data (satellite information) available on the B1000 dashboard (UI).

To check and install the BTS device in a clear sky, perform the following steps:

1. Using the B1000 UI (BTS), navigate to the **System** > **Synchronisation** page from the main B1000 Dashboard.

   The **Synchronisation** page appears. Ensure to complete the following configuration steps:

   a. Select **Best Effort** as the **Control** parameter value.

      The **Best Effort** option indicates that the BTS device uses the satellite signal for the reference. Even if all satellites go down, the BTS device uses the reference time for a specific period (for example, 5 minutes) before it loses the reference signal.

   b. Select **Internal GNSS** as the **Source** parameter value.

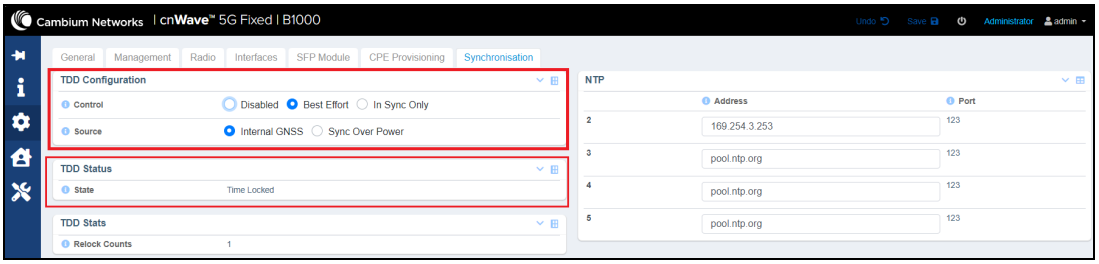
      The **Internal GNSS** option indicates that the BTS device is using an integrated GPS as a reference for the operation of TDD.

   c. Ensure that the value of **State** parameter displays **Time Locked** in the TDD Status section.

      The **Time Locked** state indicates that a pulse per second (PPS) reference signal is detected, the frequency is locked, and the TDD is synchronized.

      Figure 22 is an example of the Synchronisation settings.

      Figure 22: *The Synchronisation page*



2. On the main B1000 dashboard, select the **GNSS** tab.

   The **GNSS** page appears, displaying satellite information.

   To check details of the satellites used by the BTS device, perform the following actions using the GNSS page:

   a. Check the value of **In Use** parameter in the **Satellites** section.

      The **In Use** parameter indicates the number of GNSS satellites that are in use by the device. The value of this parameter must be more than two.

> **Note**
>
> The BTS device relies on minimum three or four satellites.

b. If the value of **In Use** parameter is less than three or four satellites, then check your BTS installation setup, in terms of possible obstructions for the integrated GPS and the BTS device.

   You must check whether the GPS antenna is hidden or blocked by any other radios or metal devices.

c. Check the **Fix Count** value in the **Statistics** section.

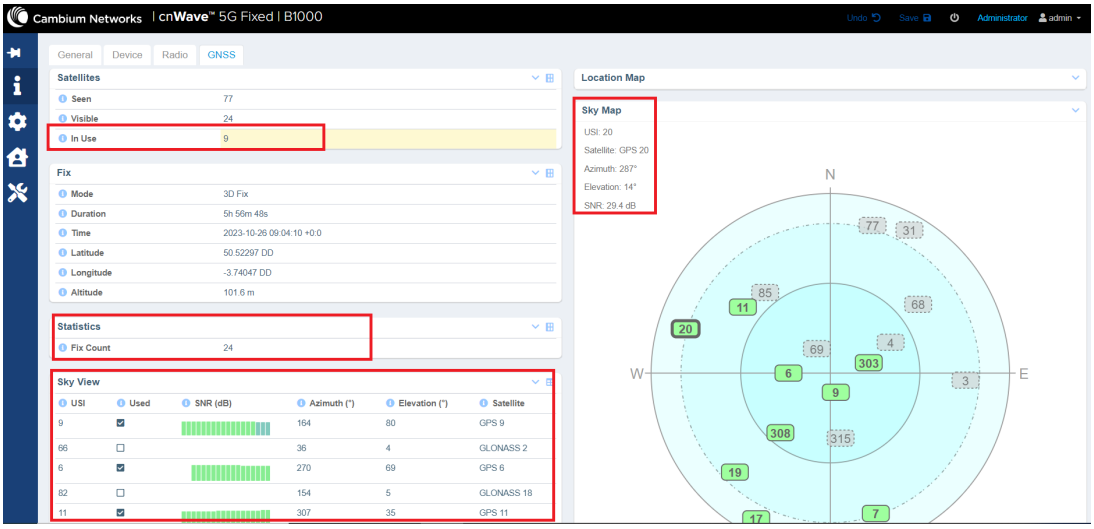
   The fixed count value must not be high, and it must be constant for all the satellites in use.

d. Check SNR, azimuth, and elevation values in the **Sky View** section.

   If the SNR value of any satellite is not optimal (typically, 20 dB and higher), then the BTS device does not use GPs when the signal goes down (below 20). If the SNR value is good (for example, more than 20), the BTS device uses GPS for synchronisation. Figure 23 is an example of the **GNSS** page.

   You can also check the **Sky Map** section for SNR value of each satellite.

   Figure 23: *The GNSS page - B1000 UI (BTS)*



Note

on the **Sky Map** section of the **GNSS** page, green coloured satellites are the ones in use.

With synchronisation and GNSS satellite details, you can ensure that the BTS device is installed in a clear sky and GPS is not hidden.

For more information on using **Synchronisation** and **GNSS** pages in the B1000 UI, refer to the *cnWave 5G Fixed Configuration Guide*.

Operational Procedures for BTS

This section explains some operational procedures for a BTS in the field. Example: Replacing a faulty BTS, changing some key parameters, or performing a software upgrade. The operation procedures help one to understand the time required for reestablishing a connectivity service in the field.

This section covers the following operational scenarios:

Modifying BTS system parameters – No reboot required

The **System** page in the B1000 UI allows you to modify the system parameters for a BTS with no reboot of the system required.

Perform the following steps to modify the system parameters:

1. Log on to the B1000 UI (as described in the Accessing the B1000 UI section).

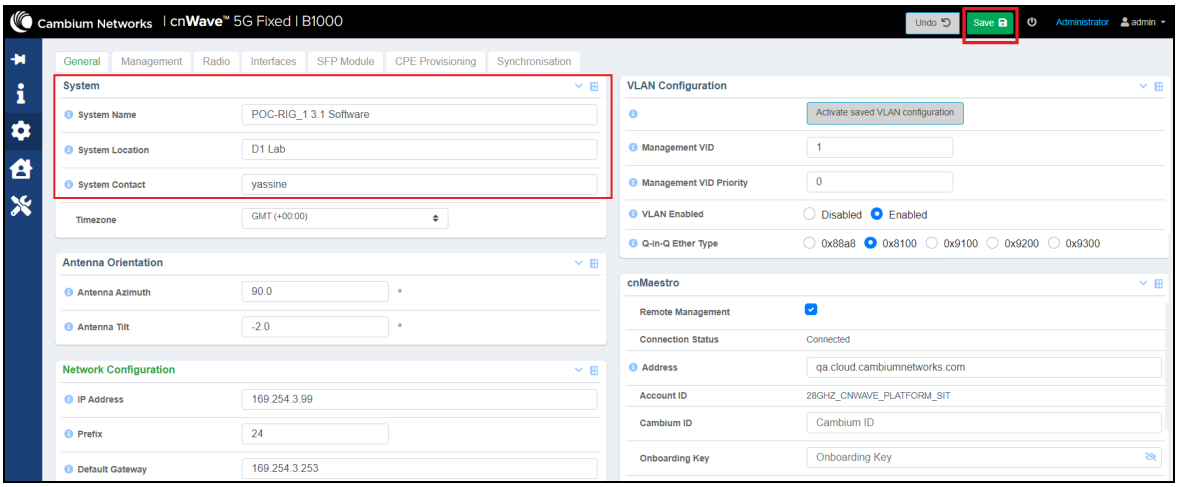
   The main B1000 dashboard page appears (as shown in Figure 7).

2. On the left navigation column, click the **System** icon ( ).

   The **System** page appears with multiple tabs, as shown in Figure 24.

3. Modify the values of **System Name**, **System Location**, and **System Contact**, as shown in Figure 24.

   Figure 24: *The System page - B1000 UI*



4. Click **Save**, as shown in Figure 24.

   The changes are effective, immediately, with no impact on the operation of the system.

For more information about each parameter in the **System** page, refer to the *cnWave™ 5G Fixed Configuration Guide*.

Modifying BTS network parameters - No reboot required

The **Systems** page in the B1000 UI allows you to modify the network-specific parameters for a BTS with no reboot of the system required.

Perform the following steps to modify the parameters specific to the network:

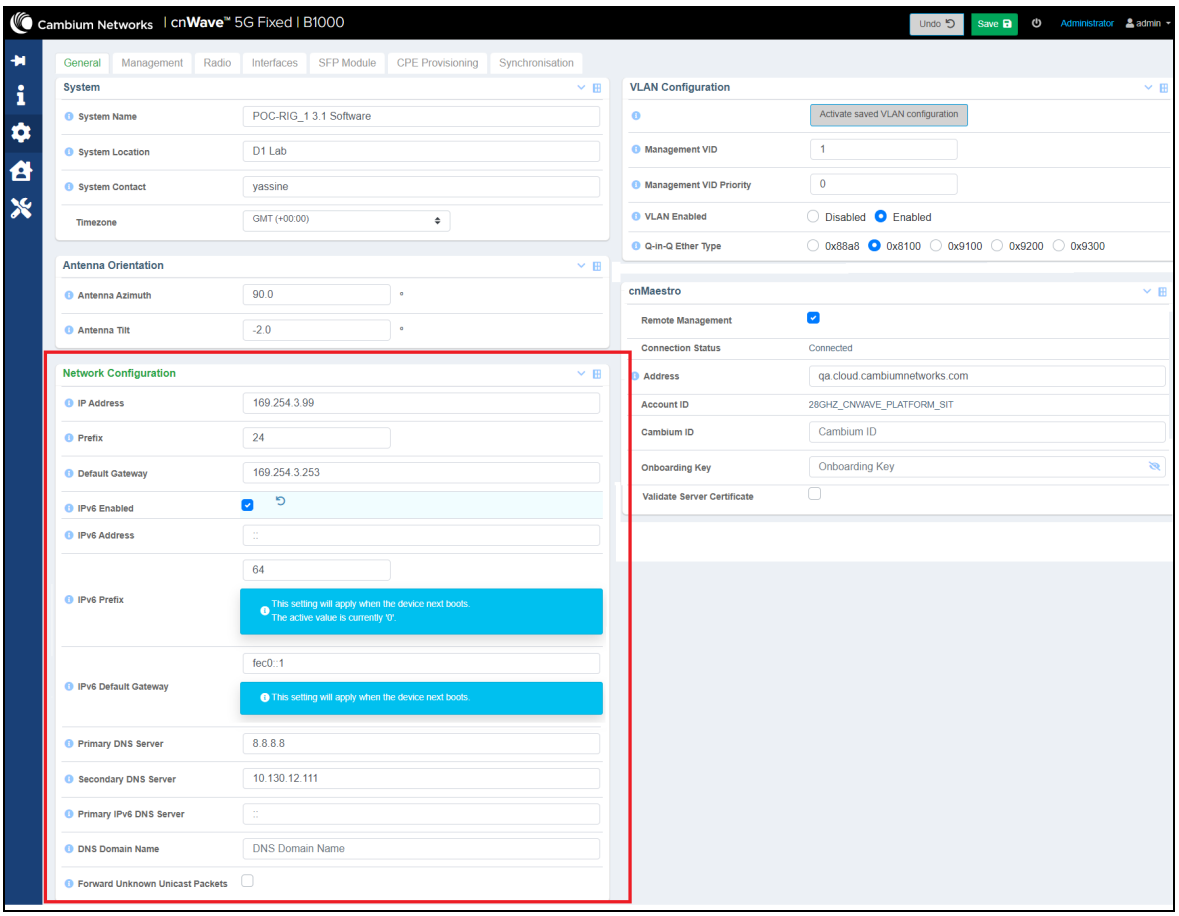
1. From the main B1000 dashboard page, navigate to **System** > **General**.

   The **General** page appears (as shown in Figure 7).

   For information on how to log on to the B1000 UI, refer to the Accessing the B1000 UI section.

2. In the **Network Configuration** section, modify the values of parameters such as IP address, gateways, and DNS (as shown in Figure 25).

Figure 25: *BTS Network parameters in the System page*



3. Click **Save**, as shown in Figure 25.

   The changes are effective, immediately, with no impact on the operation of the system. However, any change made to the **Network Configuration**-specific parameters affects the management of the system. The administrator must ensure that the IP address is compatible with the network and is accessible using SNMP or web UI.

Modifying BTS user accounts - No reboot required

The **Systems** page in the B1000 UI allows you to modify the user account specific parameters with no reboot of the system required.

Perform the following steps to modify the user account specific parameters:

1. From the main B1000 dashboard page, navigate to **System** > **Management**.

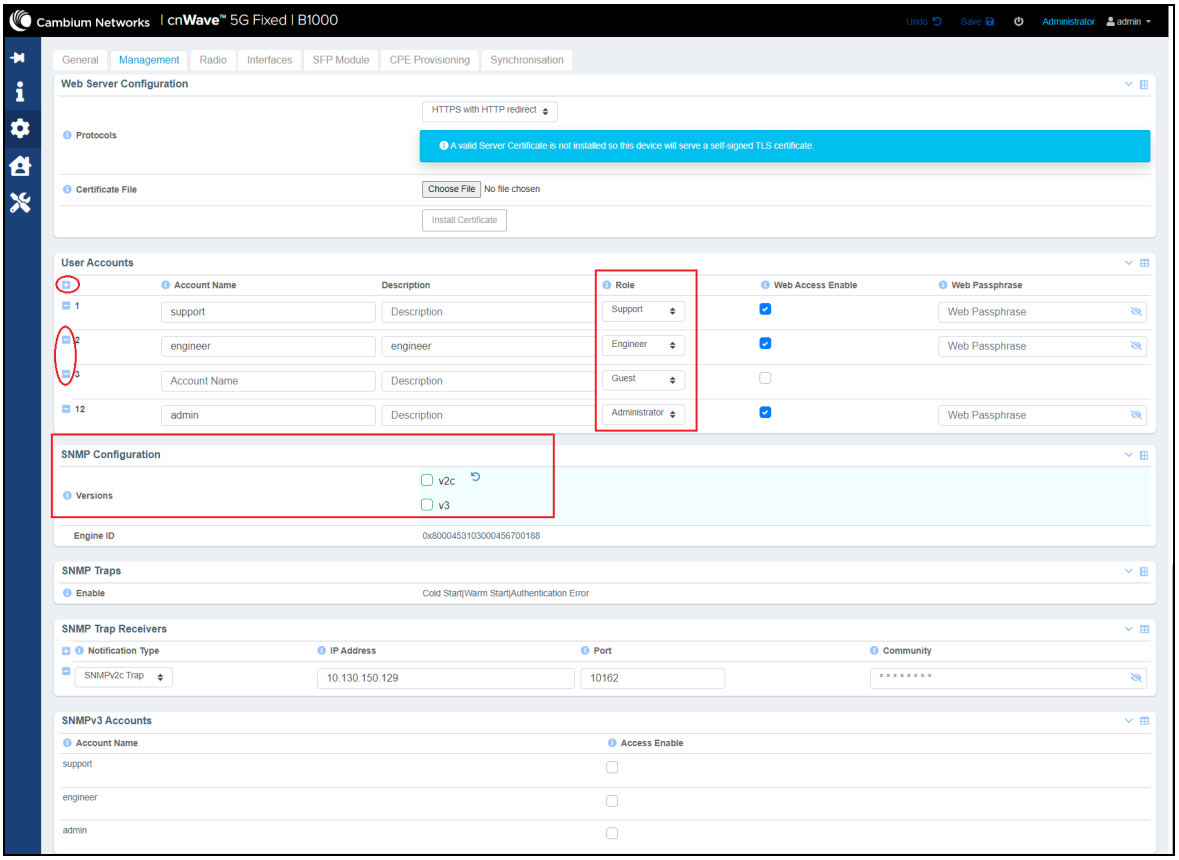
   The **Management** page appears.

   For information on how to log on to the B1000 UI, refer to the Accessing the B1000 UI section.

2. In the **User Accounts** section, add or remove user accounts and set up a role (guest, administrator, user, security, support, engineer, and factory) for each user account, as shown in Figure 26.

You can also select the SNMP Version in the **SNMP Configuration** section if the user needs to manage the system using SNMP. You can also set the notification type in the **SNMP Trap Receivers** section. For details on limitations of each role and configuring SNMP, refer to the *cnWave™ 5G Fixed Configuration Guide*.

Figure 26: *User account parameters in the Management page*



The changes are effective, immediately, with no impact on the operation of the system. However, any change made to the user accounts and SNMP affects the SNMP management and the security of the system (to some extent). The changes are effective on logging back into the system if you are using the web interface.

Modifying the BTS operation frequency - No reboot required

The **Systems** page in the B1000 UI allows you to modify the operating frequency (in MHz) of the radio bearer.

Perform the following steps to modify the frequency specific parameter:

1. From the main B1000 dashboard page, navigate to **System** > **Radio**.

   The **Radio** page appears.

   For information on how to log on to the B1000 UI, refer to the Accessing the B1000 UI section.

2. In the **Frequency** text box, check and modify the value of the operating frequency (in MHz) for the BTS.

   For more information about this parameter, refer to the *cnWave™ 5G Fixed Configuration Guide*.

When you change the value of this parameter, the **Save** button at the top right corner is highlighted (in green color). This indicates that it is necessary to save or apply the configuration change that you made in the **Frequency** text box.

Even though a reboot of the system is not required, the CPEs must have the new frequency in their scan frequency list. Otherwise, CPEs will not connect to the BTS. All the registered CPEs will get disconnected for a short time before they reconnect and re-register to the BTS. It may take longer for some CPEs to reconnect depending on the range and the number of frequencies in their respective scan lists.

Changing the BTS polarization - No reboot required

The **Systems** page in the B1000 UI allows you to change the antenna polarisation settings.

Perform the following steps to modify the parameter specific to polarisation:

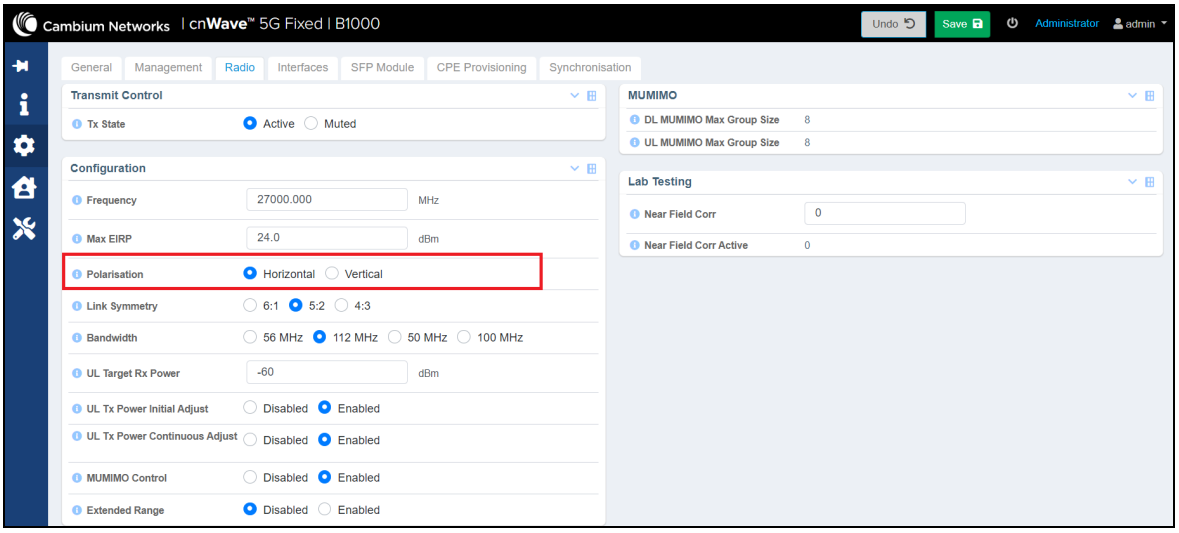
1. From the main B1000 dashboard page, navigate to **System** > **Radio**.

   The **Radio** page appears.

   For information on how to log on to the B1000 UI, refer to the Accessing the B1000 UI section.

2. Select the required polarisation option (Horizontal or Vertical) in the **Polarisation** field, as shown in Figure 27.

   Figure 27: *The polarisation parameter in the Radio page*



3. Click **Save** to apply the change.

   When you change the value of this parameter, the **Save** button at the top right corner is highlighted (in green color). This indicates that it is necessary to save or apply the configuration change that you made in the **Frequency** text box.

   Even though a reboot of the system is not required, the CPEs must have the correct polarization as that of BTS or it is good to set this parameter to **Auto Detect** in the **Radio** page of C1oo UI.

   For more information about the C100 UI settings, refer to the *cnWave™ 5G Fixed Configuration Guide*.

Note

Ensure that there is no disruption to the service on changing the polarisation settings.

Enabling or disabling the RADIUS server - No reboot required

The **Authentication** page in the B1000 UI provides options to configure the RADIUS server for CPEs.

Perform the following steps to modify the parameter specific to the RADIUS server:

1. From the main B1000 dashboard page, navigate to **System** > **Authentication**.

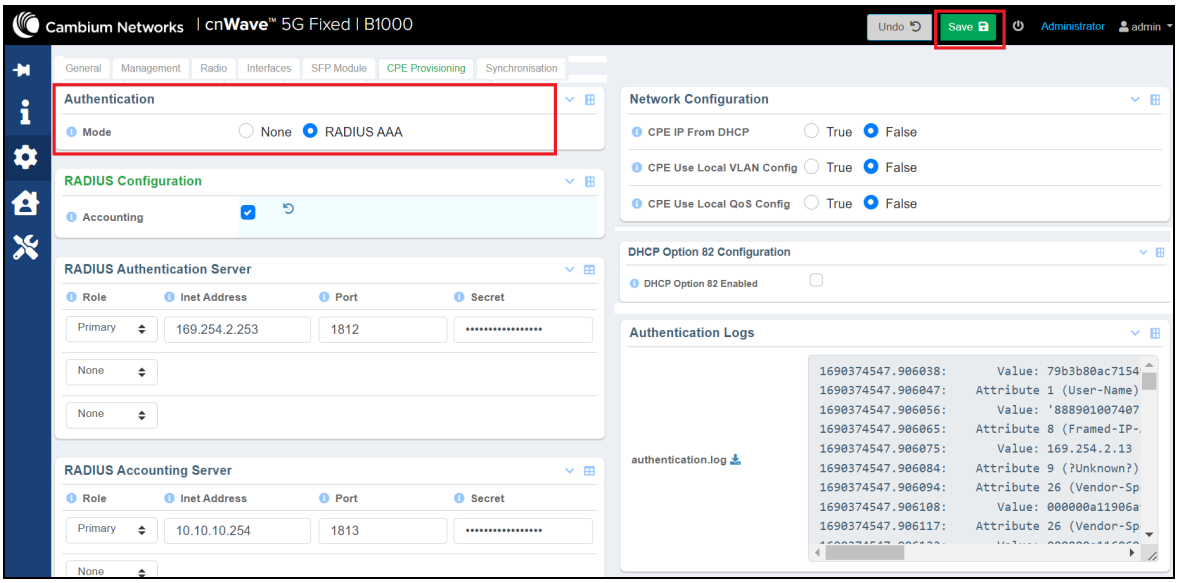
   The **Authentication** page appears.

   For information on how to log on to the B1000 UI, refer to the Accessing the B1000 UI section.

2. To enable the RADIUS authentication, select **RADIUS AAA** in the **Mode** field as shown in Figure 28.

   RADIUS AAA is an accounting parameter used for billing purposes.

   Figure 28: *RADIUS AAA parameter in the Authentication page*



3. Set the IP address (es) of the RADIUS Server(s) and the secret values (or password) that you have configured in the `clients.conf` file in the RADIUS server as shown below:

   ```
   client hawking-auth {
   ipaddr = 10.10.10.150/24
   secret = phn_shared_secret
   shortname = hawking_auth
   ```

   If any CPE is already connected to and registered with BTS, then they must be rebooted to consider the new RADIUS configuration that may include VLANs and other QoS parameters. This change implies that the service will be interrupted until the CPEs reconnect and re-register. The overall downtime depends on the number of CPEs, but each CPE's loss of service must not exceed 2 minutes.

   For more information about the RADIUS server configuration and related parameters, refer to the *cnWave™ 5G Fixed Configuration Guide*.

Testing MU MIMO performance - No reboot required

Multi-user multi-input multi-output (MU MIMO) is used to multiply the capacity of a wireless connection with no need for additional spectrum.

If you have deployed MU MIMO at your site, you can test its performance in a lab environment using one of the following methods:

- Web user interface (UI) of BTS
- Linux setup - iPerf server

> **Note**
>
> For information on maximum MU MIMO throughput for all TDD symmetry and channel sizes, refer to the Maximum MU MIMO throughput section.

Before testing the MU MIMO performance, make sure that your lab environment contains 1 x BTS and at least 2 x CPEs (which are installed such that the spatial frequency is at least 128).

Following sections describe the methods used for testing the MU MIMO performance in a lab environment.

Web UI of BTS

You can run a link capacity test using the **Tools** page of the B1000 UI. Determine the **MU MIMO Control** mode (enabled or disabled) for CPEs before running the link capacity test.

To run the link capacity test for the required CPEs, perform the following steps:

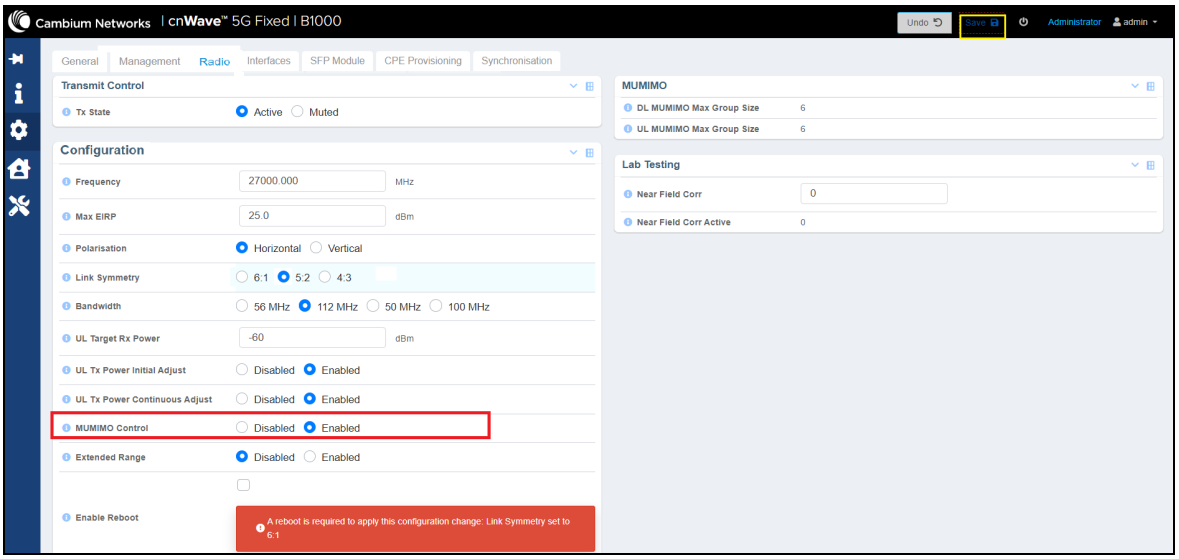
1. From the main B1000 dashboard page, navigate to **System** > **Radio**.

   The **Radio** page appears.

2. In the **MUMIMO Control** field, select **Disabled** as shown in Figure 29.

   By default, this parameter is enabled. 112 MHz is selected as an example for bandwidth.

   Figure 29: *The MUMIMO Control parameter*

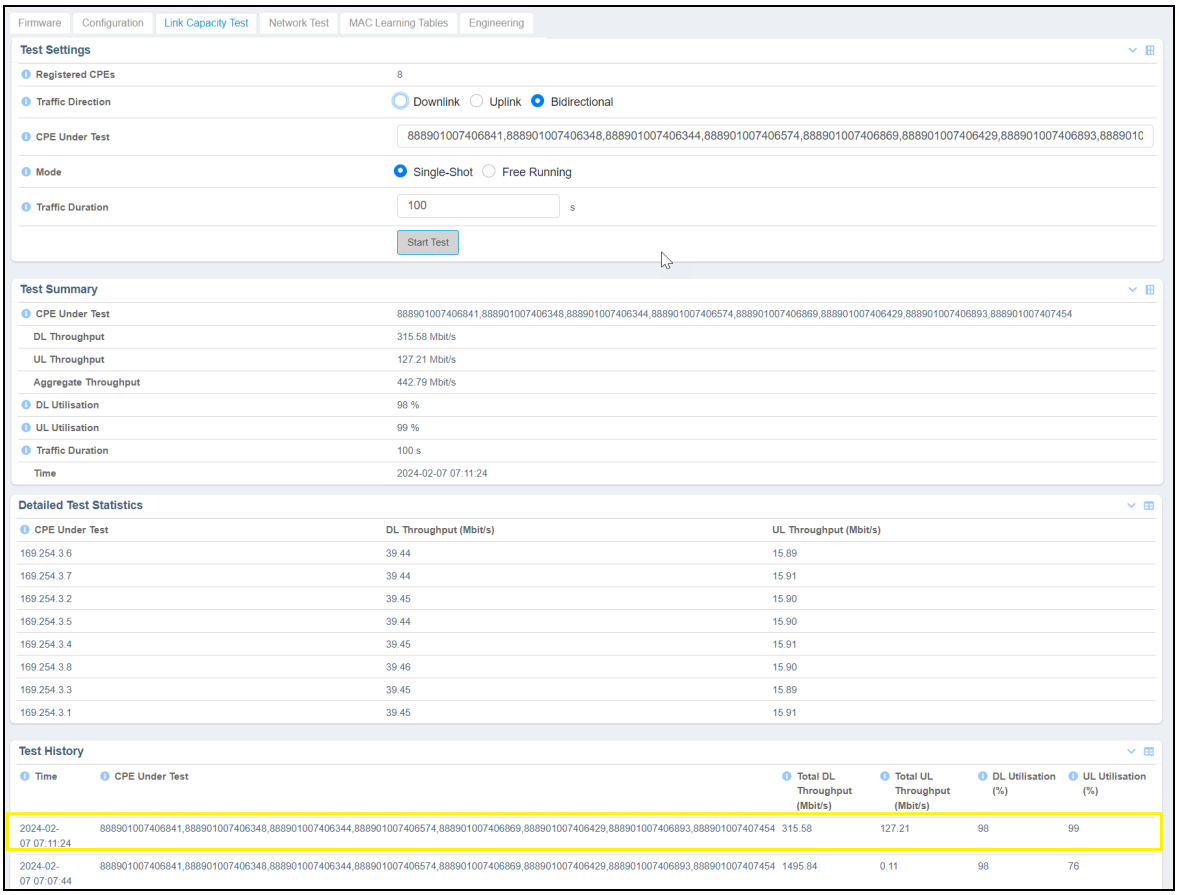


3. Navigate to **Tools** > **Link Capacity Test** page.

Using multiple IMSIs or IP addresses (of CPEs), you must run the test for the required duration (in seconds).

Figure 30 is an example of the link capacity test. For the 112 MHz bandwidth, you can see a maximum of 300 Mbps, which is the maximum downlink performance as if there was a single CPE. In other words, the group size for MU MIMO is 1.

Figure 30: *Link capacity test with MUMIMO disabled*

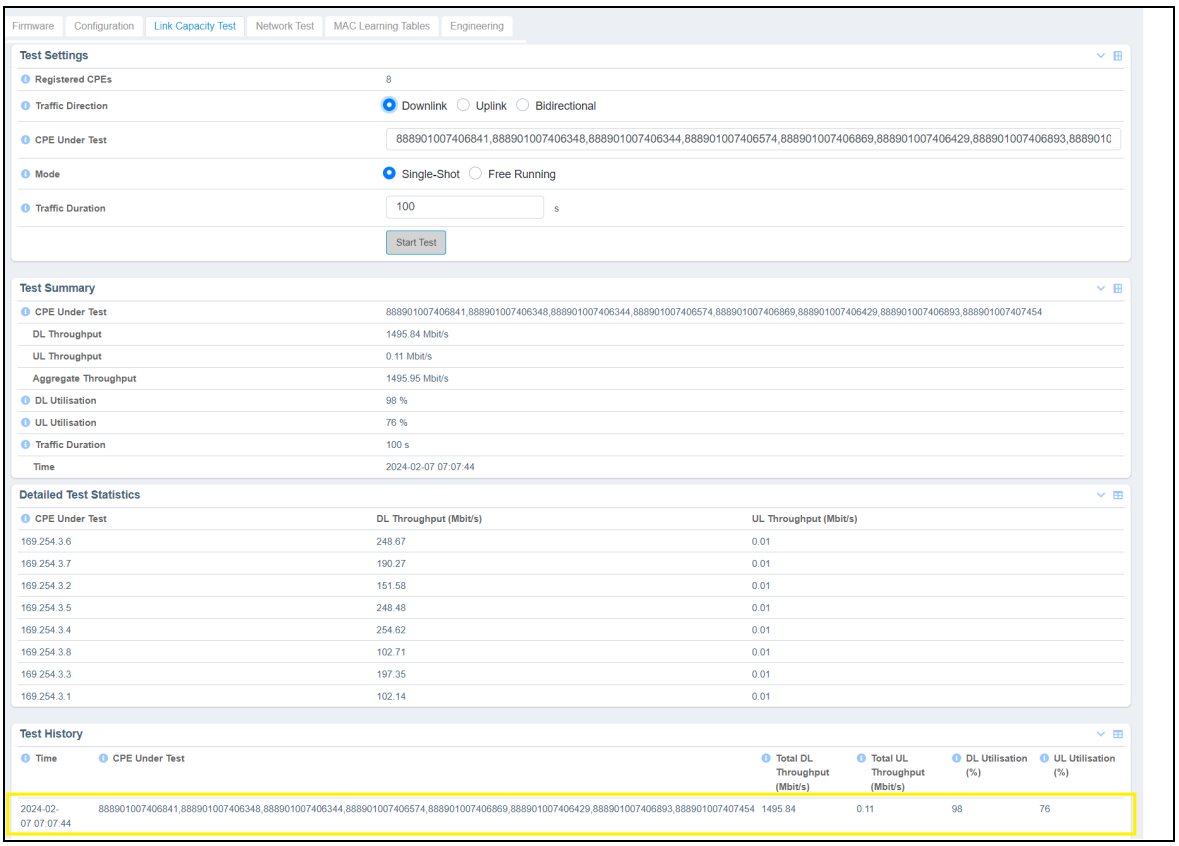


4. Select **Enabled** in the **MUMIMO Control** field in the System > Radio page of B1000 dashboard.

5. Redo the same test using the **Tools** > **Link Capacity Test** page.

   For the 112 MHz bandwidth (used as an example), you can notice that the performance has quadrupled (current release limitation of downlink MU-MIMO with group size =8) as shown in Figure 31.

Figure 31: *Link capacity test with MUMIMO enabled*



For more information about each parameter in the **Link Capacity Test** page, refer to the *cnWave™ 5G Fixed Configuration Guide*.

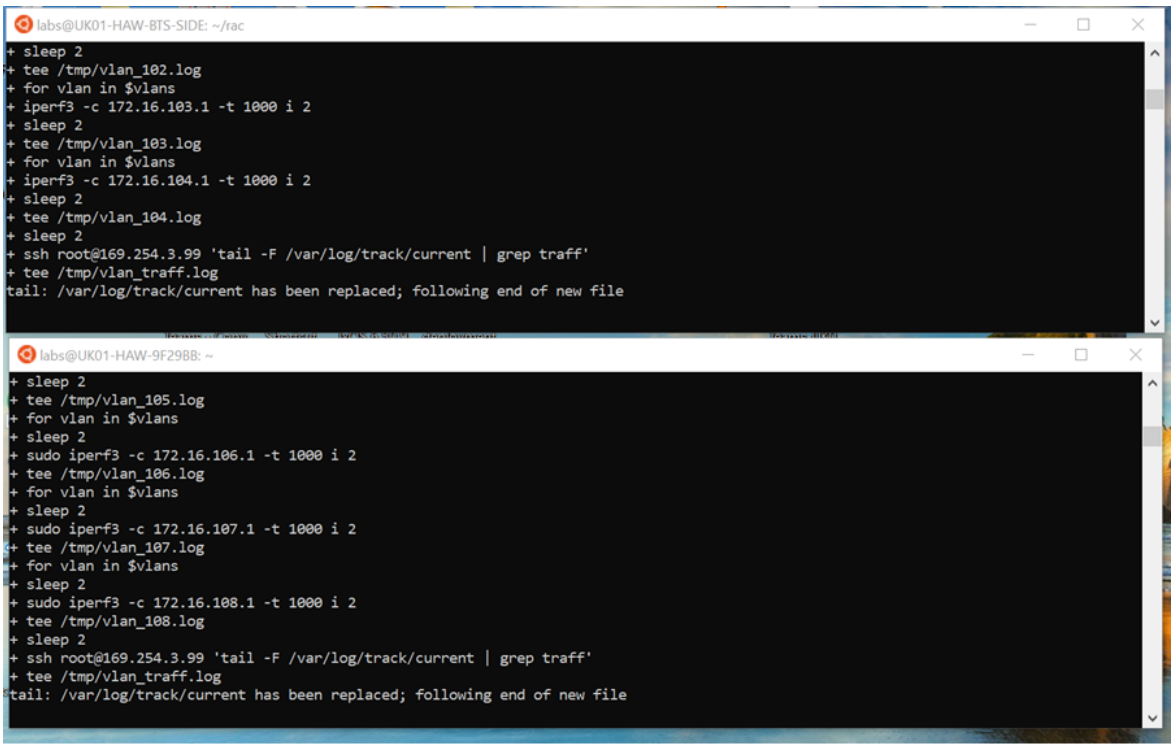
Linux setup - iPerf server

Testing the MUMIMO performance on a Linux setup using the iPerf server is an alternative method. Perform the following steps to test the MUMIMO performance in a lab environment:

1. On each CPE c4000, set up an iPerf server: `iperf3 -s`
2. On the BTS c4000, run a script that sets concurrent iPerf clients to the CPEs (in this case 8 streams, as described about eight CPEs in the previous section).

   Figure 32 is an example of running the iPerf flood traffic scripts from BTS to all CPEs, simultaneously.

Figure 32: *Running the iPerf flood traffic scripts*



3. Run the following command for each stream.

```
iperf3 -c 172.16.$(VLAN).1 -t 1000 -i 2
```

As an output, each stream creates a log file, as shown in Figure 33 and Figure 34.

4. Inspect the traffic log on the BTS to view the number of grouping-size during the tests.

Figure 33 and Figure 34 are the sample results (examples) of max grouping size (4) and throughput on the BTS log for both 56 MHz and 112 MHz bandwidth.

Figure 33: *Example of an output - the traffic log for 56 MHz*

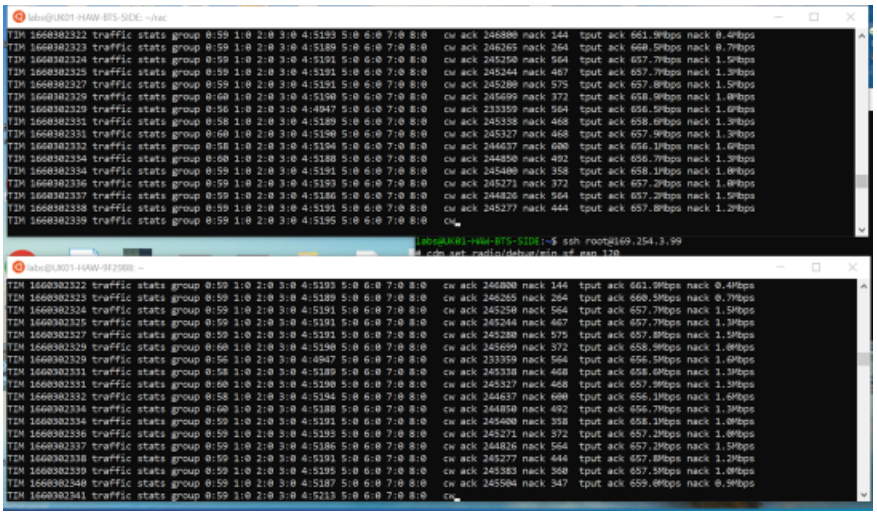


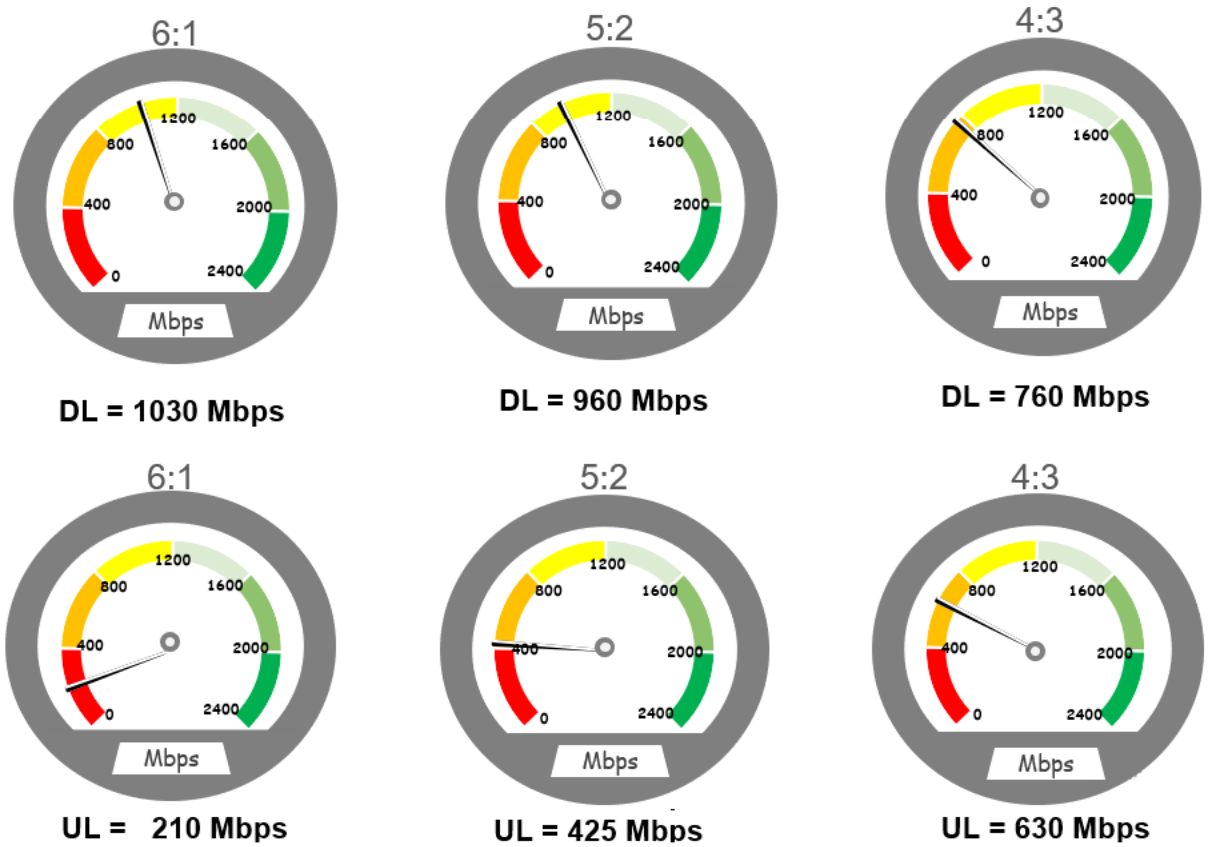
Figure 34: *Example of the output - the traffic log for 112 MHz*

```
labs@UK01-HAW-BTS-SIDE: ~/rac
TIM 1660302322 traffic stats group 0:59 1:0 2:0 3:0 4:5193 5:0 6:0 7:0 8:0   cw ack 246800 nack 144  tput ack 661.9Mbps nack 0.4Mbps
TIM 1660302323 traffic stats group 0:59 1:0 2:0 3:0 4:5189 5:0 6:0 7:0 8:0   cw ack 246265 nack 264  tput ack 660.5Mbps nack 0.7Mbps
TIM 1660302324 traffic stats group 0:59 1:0 2:0 3:0 4:5191 5:0 6:0 7:0 8:0   cw ack 245250 nack 564  tput ack 657.7Mbps nack 1.5Mbps
TIM 1660302325 traffic stats group 0:59 1:0 2:0 3:0 4:5191 5:0 6:0 7:0 8:0   cw ack 245244 nack 467  tput ack 657.7Mbps nack 1.3Mbps
TIM 1660302327 traffic stats group 0:59 1:0 2:0 3:0 4:5191 5:0 6:0 7:0 8:0   cw ack 245280 nack 575  tput ack 657.8Mbps nack 1.5Mbps
TIM 1660302329 traffic stats group 0:60 1:0 2:0 3:0 4:5190 5:0 6:0 7:0 8:0   cw ack 245699 nack 372  tput ack 658.9Mbps nack 1.0Mbps
TIM 1660302329 traffic stats group 0:56 1:0 2:0 3:0 4:4947 5:0 6:0 7:0 8:0   cw ack 233359 nack 564  tput ack 656.5Mbps nack 1.6Mbps
TIM 1660302331 traffic stats group 0:58 1:0 2:0 3:0 4:5189 5:0 6:0 7:0 8:0   cw ack 245338 nack 468  tput ack 658.6Mbps nack 1.3Mbps
TIM 1660302331 traffic stats group 0:60 1:0 2:0 3:0 4:5190 5:0 6:0 7:0 8:0   cw ack 245327 nack 468  tput ack 657.9Mbps nack 1.3Mbps
TIM 1660302332 traffic stats group 0:58 1:0 2:0 3:0 4:5194 5:0 6:0 7:0 8:0   cw ack 244637 nack 600  tput ack 656.1Mbps nack 1.6Mbps
TIM 1660302334 traffic stats group 0:60 1:0 2:0 3:0 4:5188 5:0 6:0 7:0 8:0   cw ack 244850 nack 492  tput ack 656.7Mbps nack 1.3Mbps
TIM 1660302334 traffic stats group 0:59 1:0 2:0 3:0 4:5191 5:0 6:0 7:0 8:0   cw ack 245400 nack 358  tput ack 658.1Mbps nack 1.0Mbps
TIM 1660302336 traffic stats group 0:59 1:0 2:0 3:0 4:5193 5:0 6:0 7:0 8:0   cw ack 245271 nack 372  tput ack 657.2Mbps nack 1.0Mbps
TIM 1660302337 traffic stats group 0:59 1:0 2:0 3:0 4:5186 5:0 6:0 7:0 8:0   cw ack 244826 nack 564  tput ack 657.2Mbps nack 1.5Mbps
TIM 1660302338 traffic stats group 0:59 1:0 2:0 3:0 4:5191 5:0 6:0 7:0 8:0   cw ack 245277 nack 444  tput ack 657.8Mbps nack 1.2Mbps
TIM 1660302339 traffic stats group 0:59 1:0 2:0 3:0 4:5195 5:0 6:0 7:0 8:0   cw_
labs@UK01-HAW-BTS-SIDE:~$ ssh root@169.254.3.99
# cdm set radio/debug/min_sf_gap 120
labs@UK01-HAW-9F298B: ~
TIM 1660302322 traffic stats group 0:59 1:0 2:0 3:0 4:5193 5:0 6:0 7:0 8:0   cw ack 246800 nack 144  tput ack 661.9Mbps nack 0.4Mbps
TIM 1660302323 traffic stats group 0:59 1:0 2:0 3:0 4:5189 5:0 6:0 7:0 8:0   cw ack 246265 nack 264  tput ack 660.5Mbps nack 0.7Mbps
TIM 1660302324 traffic stats group 0:59 1:0 2:0 3:0 4:5191 5:0 6:0 7:0 8:0   cw ack 245250 nack 564  tput ack 657.7Mbps nack 1.5Mbps
TIM 1660302325 traffic stats group 0:59 1:0 2:0 3:0 4:5191 5:0 6:0 7:0 8:0   cw ack 245244 nack 467  tput ack 657.7Mbps nack 1.3Mbps
TIM 1660302327 traffic stats group 0:59 1:0 2:0 3:0 4:5191 5:0 6:0 7:0 8:0   cw ack 245280 nack 575  tput ack 657.8Mbps nack 1.5Mbps
TIM 1660302329 traffic stats group 0:60 1:0 2:0 3:0 4:5190 5:0 6:0 7:0 8:0   cw ack 245699 nack 372  tput ack 658.9Mbps nack 1.0Mbps
TIM 1660302329 traffic stats group 0:56 1:0 2:0 3:0 4:4947 5:0 6:0 7:0 8:0   cw ack 233359 nack 564  tput ack 656.5Mbps nack 1.6Mbps
TIM 1660302331 traffic stats group 0:58 1:0 2:0 3:0 4:5189 5:0 6:0 7:0 8:0   cw ack 245338 nack 468  tput ack 658.6Mbps nack 1.3Mbps
TIM 1660302331 traffic stats group 0:60 1:0 2:0 3:0 4:5190 5:0 6:0 7:0 8:0   cw ack 245327 nack 468  tput ack 657.9Mbps nack 1.3Mbps
TIM 1660302332 traffic stats group 0:58 1:0 2:0 3:0 4:5194 5:0 6:0 7:0 8:0   cw ack 244637 nack 600  tput ack 656.1Mbps nack 1.6Mbps
TIM 1660302334 traffic stats group 0:60 1:0 2:0 3:0 4:5188 5:0 6:0 7:0 8:0   cw ack 244850 nack 492  tput ack 656.7Mbps nack 1.3Mbps
TIM 1660302334 traffic stats group 0:59 1:0 2:0 3:0 4:5191 5:0 6:0 7:0 8:0   cw ack 245400 nack 358  tput ack 658.1Mbps nack 1.0Mbps
TIM 1660302336 traffic stats group 0:59 1:0 2:0 3:0 4:5193 5:0 6:0 7:0 8:0   cw ack 245271 nack 372  tput ack 657.2Mbps nack 1.0Mbps
TIM 1660302337 traffic stats group 0:59 1:0 2:0 3:0 4:5186 5:0 6:0 7:0 8:0   cw ack 244826 nack 564  tput ack 657.2Mbps nack 1.5Mbps
TIM 1660302338 traffic stats group 0:59 1:0 2:0 3:0 4:5191 5:0 6:0 7:0 8:0   cw ack 245277 nack 444  tput ack 657.8Mbps nack 1.2Mbps
TIM 1660302339 traffic stats group 0:59 1:0 2:0 3:0 4:5195 5:0 6:0 7:0 8:0   cw ack 245383 nack 360  tput ack 657.5Mbps nack 1.0Mbps
TIM 1660302340 traffic stats group 0:59 1:0 2:0 3:0 4:5187 5:0 6:0 7:0 8:0   cw ack 245504 nack 347  tput ack 659.0Mbps nack 0.9Mbps
TIM 1660302341 traffic stats group 0:59 1:0 2:0 3:0 4:5213 5:0 6:0 7:0 8:0   cw_
```

Maximum MU MIMO throughput

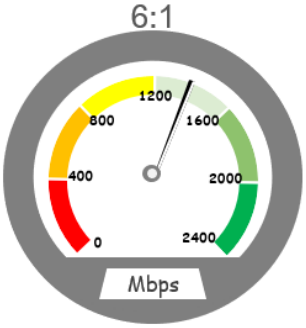
The following charts demonstrate the MU-MIMO performance (8x8) in both DL and UL directions for all the supported channel sizes and link symmetry ratios (6.1, 5.2, and 4.3):

50 MHz



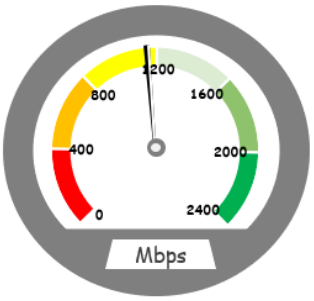
56 MHz

6:1



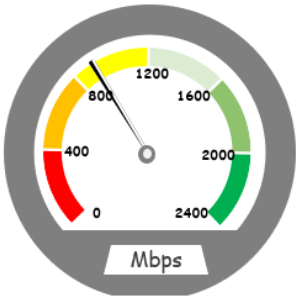
DL = 1230 Mbps

5:2



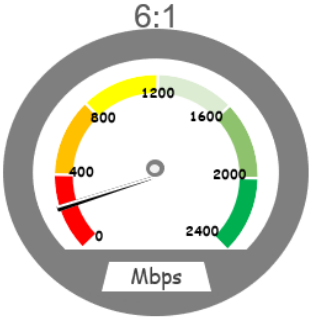
DL = 1150 Mbps

4:3



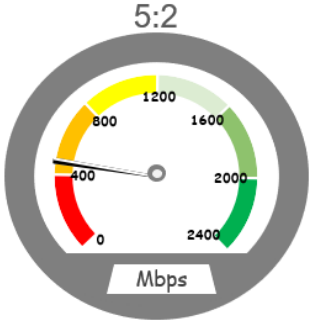
DL = 910 Mbps

6:1



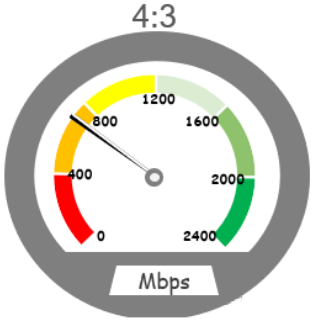
UL = 230 Mbps

5:2



UL = 470 Mbps

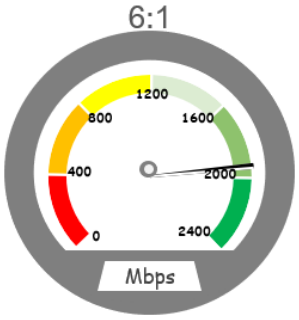
4:3



UL = 710 Mbps

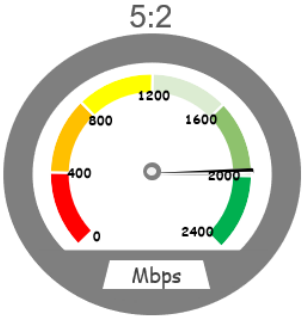
100 MHz

6:1



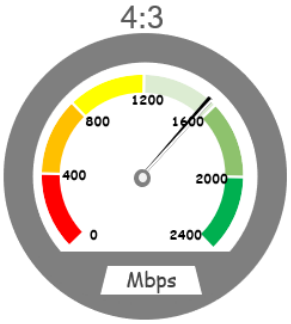
DL = 1940 Mbps

5:2



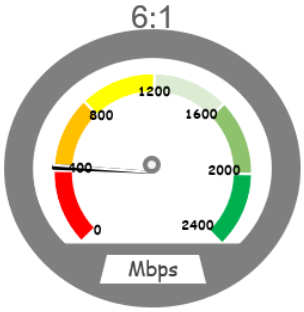
DL = 1975 Mbps

4:3



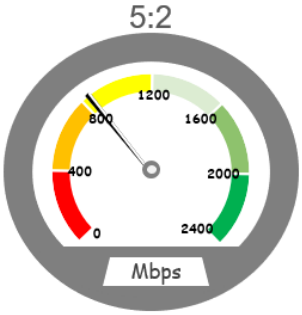
DL = 1560 Mbps

6:1



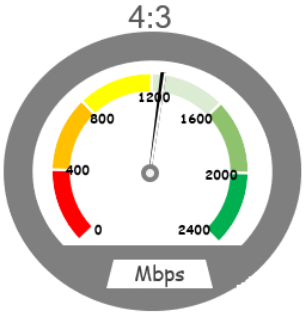
UL = 420 Mbps

5:2



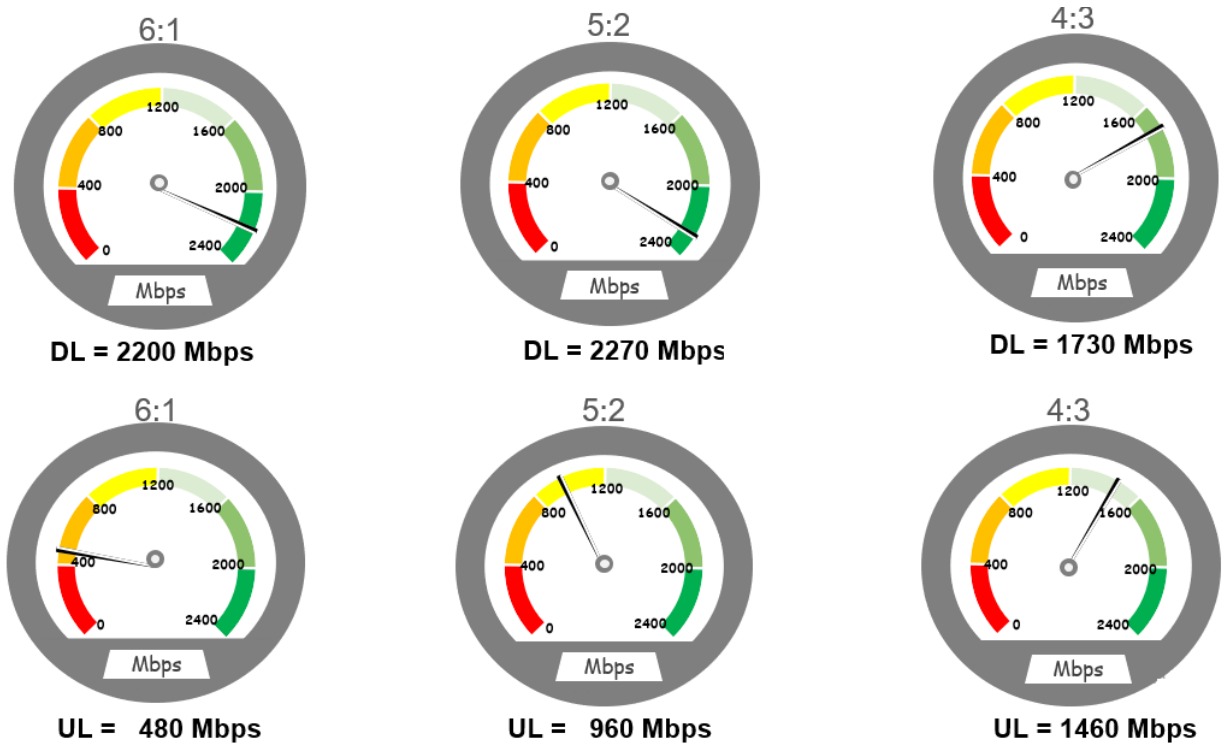
UL = 845 Mbps

4:3



UL = 1260 Mbps

112 MHz



Updating a BTS firmware - Reboot required

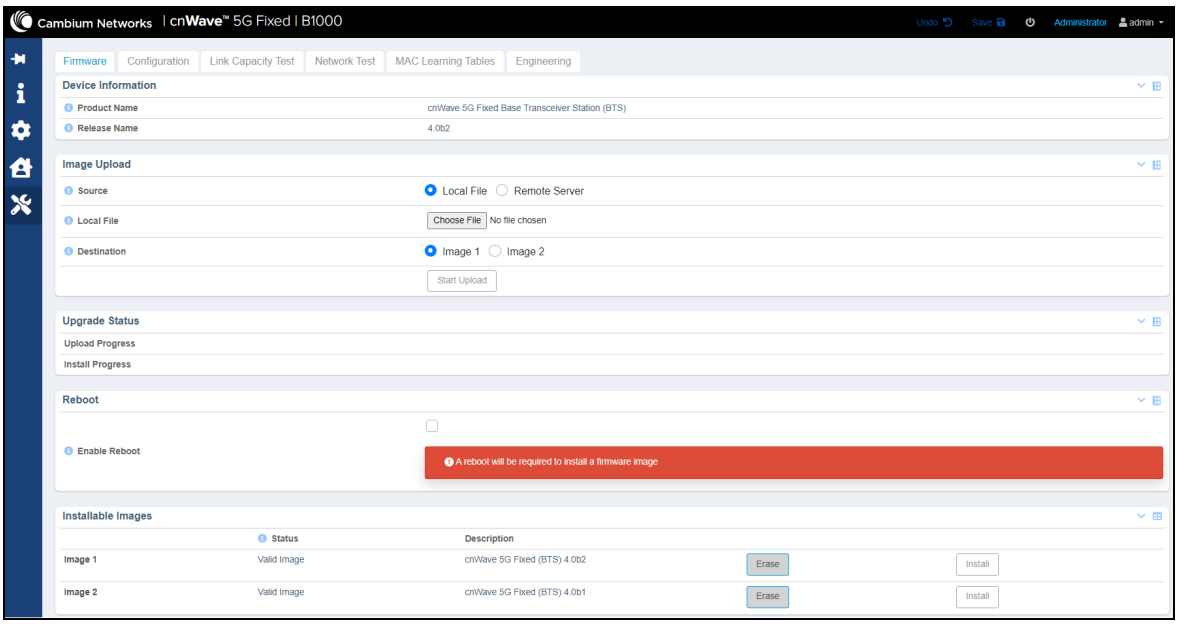
The **Tools** page in the B1000 UI allows you to update firmware (software).

Perform the following steps to update the firmware on the **Tools** page:

1. On the left navigation column in the B1000 UI, click the **Tools** icon ( ).

   The **Tools** page appears with multiple tabs, as shown in Figure 35. By default, the **Firmware** tab is selected.

Figure 35: *The Firmware page*



2. Select the **Enable Reboot** check box in the **Reboot** section of the **Firmware** page.

   This action indicates that the BTS performs a reboot after the installation of a new firmware.

3. Click **Choose File** to select a new firmware either from a local PC or a remote server.

4. Browse the image file that you want to replace.

   By default, Image 1 is selected.

5. Click **Start Upload** and monitor the upload status in the **Upload Progress** field in the **Upgrade Status** section of the **Firmware** page. If the uploading is successful, the **Upload Progress** section displays the same.

   The BTS has room for two uploaded images and the user can select the newly updated one. and click onto install.

6. Click **Install** to update the uploaded image file.

   The BTS reboots and all registered CPEs get disconnected for at least two minutes before they reconnect to and re-register with the BTS. Some CPEs may take a longer period to reconnect depending on the range.For more information about each parameter on the **Firmware** page, refer to the *cnWave™ 5G Fixed Configuration Guide*.

Note

In each release, it is recommended that the CPEs must be upgraded with the same firmware version as that of the BTS for the system to reconnect. For information on the upgrade requirements, refer to the *Requirements for firmware version upgrade or downgrade* section in the cnWave™ 5G Fixed Configuration Guide.

Changing the bandwidth - Reboot required

The **Radio** page in the B1000 UI allows you to modify or change the bandwidth (in MHz) of the radio channel spacing.

Perform the following steps to modify the parameter specific to bandwidth:

1. From the main B1000 dashboard page, navigate to **System** > **Radio**.

   The **Radio** page appears.

   For information on how to log on to the B1000 UI, refer to the Accessing the B1000 UI section.

2. In the **Bandwidth** field, select the required value(in MHz).

   When you change the bandwidth value, a warning message appears. This warning message indicates that a reboot is necessary to apply the configuration change.

   When the **Enable Reboot** check box is selected, the BTS reboots. All the registered CPEs get disconnected for at least two minutes before they reconnect and register back with the BTS. Some CPEs may take a longer period to reconnect depending on the range.

Changing the Uplink Tx Power initial or continuous control - Reboot required

The **Radio** page in the B1000 UI allows you to change the uplink (UL) initial or continuous transmit power control. This action allows you to:

- reach the BTS target receive power before starting transmission and
- keep the transmit power control constant, for CPEs, during a session and use the initial transmit power control level, respectively.

If the **UL Tx Power Initial Adjust** and the **UL Tx Power Continuous Adjust** parameters in the **Radio** page are set to **Disabled**, the CPE uses its configured maximum transmit power.

Perform the following steps to change the parameters specific to UL Tx power initial or continuous control:

1. From the main B1000 dashboard page, navigate to **System** > **Radio**.

   The **Radio** page appears.

   For information on how to log on to the B1000 UI, refer to the Accessing the B1000 UI section.

2. Set the following parameters to either **Disabled** or **Enabled**:

   - **UL Tx Power Initial Adjust**, which determines the initial power adjust mode of CPEs.
   - **UL Tx Power Continuous Adjust**, which determines the continuous power adjust mode of CPEs.

   For more information about these parameters, refer to the *cnWave™ 5G Fixed Configuration Guide*.

When you change the uplink Tx power initial or continuous control value, a warning message appears. This warning message indicates that a reboot is necessary to apply the configuration change.

When the **Enable Reboot** check box is selected, the BTS reboots. All the registered CPEs get disconnected for at least two minutes before they reconnect and register back with the BTS. Some CPEs may take a longer period to reconnect depending on the range.

Resetting BTS to factory default configuration - Reboot required

The **Configuration** tab on the **Tools** page of the B1000 UI allows you to reset the BTS to factory default settings. Using the B1000 UI, you can perform the following configurations:

- Reset the BTS configuration to factory defaults with no change to the local management IP address, as described here.
- Reset the BTS configuration to factory defaults including the local management IP address, as described here.

Reset BTS to factory defaults with no change to the IP address

To reset the BTS to factory defaults with no changes to the IP address, perform the following steps:

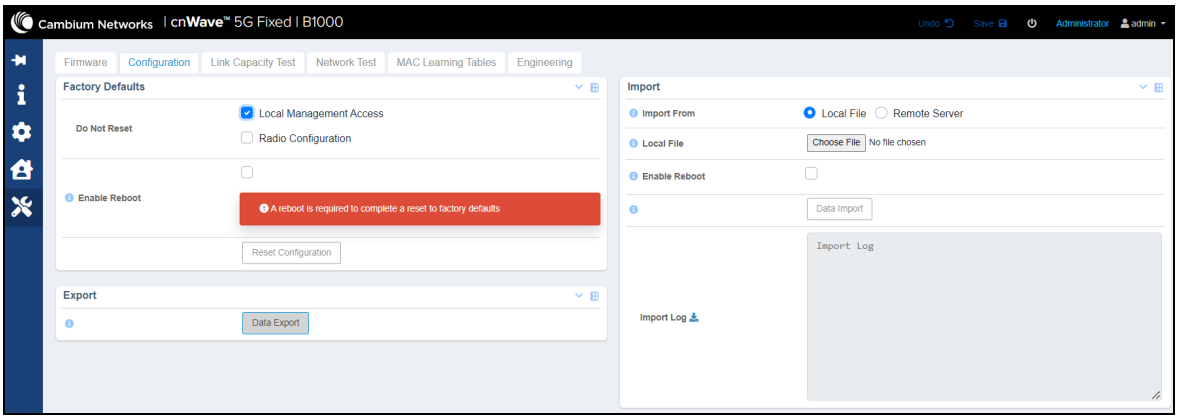
1. From the main B1000 dashboard page, navigate to **Tools** > **Configuration**.

   The **Configuration** page appears. If the **Local Management Access** parameter is ticked, then all the BTS configurations are reset to factory defaults except for the local management IP address.

2. Select the **Enable Reboot** check box.

   A warning message appears as shown in Figure 36. This warning message indicates that a reboot is necessary to apply the configuration change. The BTS then reboots.

   Figure 36: *BTS factory defaults specific parameters*



   It is necessary to reconfigure the main parameters (as listed in Table 1) for the BTS to reconnect to all the CPEs.

   When the reconfiguration of parameters is done, all the registered CPEs must reconnect and register back with the BTS. This operation may take several minutes to complete. Some CPEs may take a longer period to reconnect depending on the range.

Reset BTS to factory defaults including the IP address

To reset the BTS to factory defaults including the IP address, perform the following steps:

1. From the main B1000 dashboard page, navigate to **Tools** > **Configuration**.

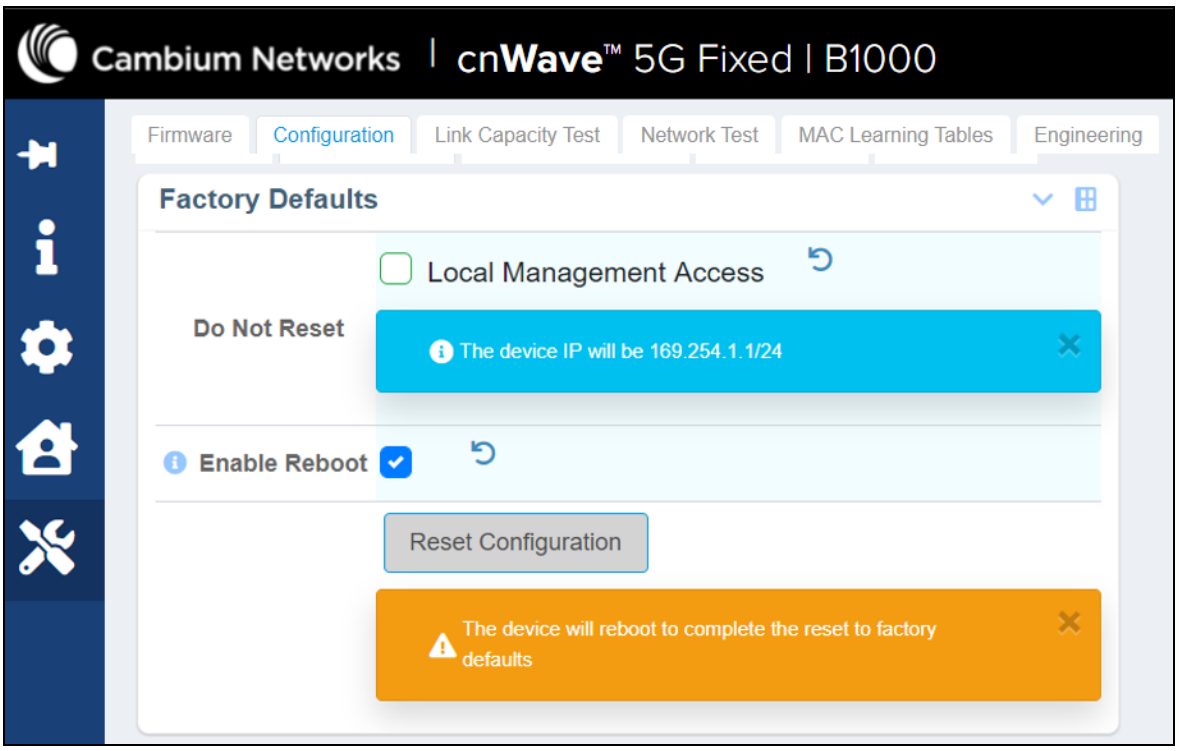
   The **Configuration** page appears.

2. Deselect the **Local Management Access** check box in the **Do Not Reset** parameter.

   This action implies that all the BTS configurations are reset to factory defaults including the local management IP address.

   When this check box is deselected, a warning message appears as shown in Figure 37. This warning message indicates that the local management IP address will be set to the default 192.254.1.1/24 following the reboot. When the **Enable Reboot** check box is selected, the BTS reboots.

Figure 37: *Factory defaults specific parameters*



It is necessary to reconfigure the main parameters (as listed in Table 1) for the BTS to reconnect to all the CPEs.

When the reconfiguration of parameters is done, all the registered CPEs must reconnect and register back with the BTS. This operation may take several minutes to complete. Some CPEs may take a longer period to reconnect depending on the range.

Note

You must also reconfigure the local management IP address to use SNMP and manage the system.

Resetting CPE to factory default configuration - Reboot required

The **Configuration** tab on the **Tools** page of the C100 UI allows you to reset the CPE to factory default settings. Using the C100 UI, you can perform the following configurations:

- Reset the CPE configuration to factory defaults with no change to the local management IP address, as described here.
- Reset the CPE configuration to factory defaults including the local management IP address, as described here.

Reset CPE to factory defaults with no change to the IP address

To reset the CPE to factory defaults with no changes to the IP address, perform the following steps:

1. From the main C100 dashboard page, navigate to **Tools** > **Configuration**.

   The **Configuration** page appears.

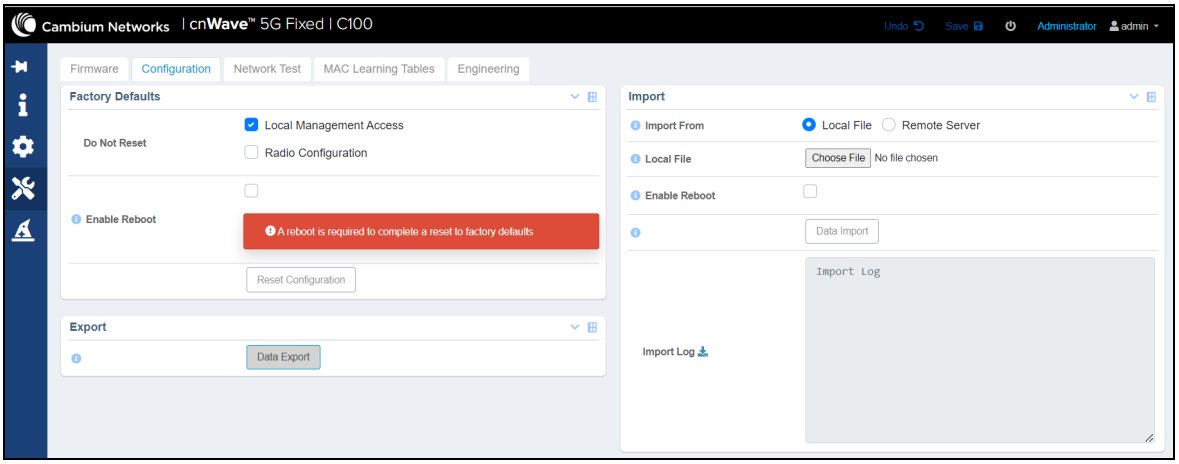
For more information on logging in to the C100 UI, refer to the Accessing the C100 UI section.

If the **Local Management Access** parameter is ticked, then all the CPE configurations are reset to factory defaults except for the local management IP address.

2. Select the **Enable Reboot** check box.

   A warning message appears as shown in Figure 38. This warning message indicates that a reboot is necessary to apply the configuration change. Then, the CPE reboots.

   Figure 38: *CPE factory defaults specific parameters*



It is necessary to reconfigure the operating frequency list (as listed in Table 1) for the CPE to reconnect.

When the reconfiguration of parameters is done, the CPE must reconnect and register back with the BTS. This operation may take a few minutes to complete.

> **Note**
>
> The Radius server must be running for the CPE to get its entire configuration.

Reset CPE to factory defaults including the IP address

To reset the CPE to factory defaults including the IP address, perform the following steps:

1. From the main C100 dashboard page, navigate to **Tools** > **Configuration**.

   The **Configuration** page appears.

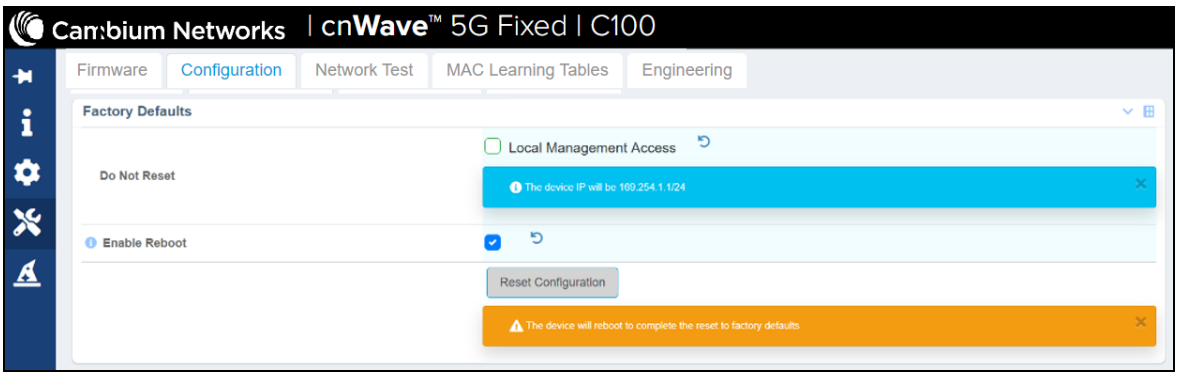
   For more information on logging in to the C100 UI, refer to the Accessing the C100 UI section.

2. Deselect the **Local Management Access** check box in the **Do Not Reset** parameter.

   This action implies that all the CPE configurations are reset to factory defaults including the local management IP address.

   When this check box is deselected (unticked), a warning message appears as shown in Figure 39. This warning message indicates that the local management IP address will be set to the default 192.254.1.1/24 following the reboot. When the **Enable Reboot** check box is selected, the CPE reboots.

Figure 39: *Factory defaults specific CPE parameters*



It is necessary to reconfigure the list of operating frequencies (as listed in Table 1) for the CPE to reconnect with the BTS.

When the reconfiguration of parameters is done, the CPE must reconnect and register back with the BTS. This operation may take a few minutes to complete.

Note

The Radius server must be running for the CPE to get its entire configuration.

Importing or exporting configuration - No reboot required

The **Configuration** page in the B1000 UI allows you to import a saved configuration or export a BTS configuration for backup (restore). This Import feature exports or imports the date model configuration (and/or status) in a JSON file.

Perform the following steps to configure the Import feature:

1. From the main B1000 dashboard page, navigate to **Tools** > **Configuration**.

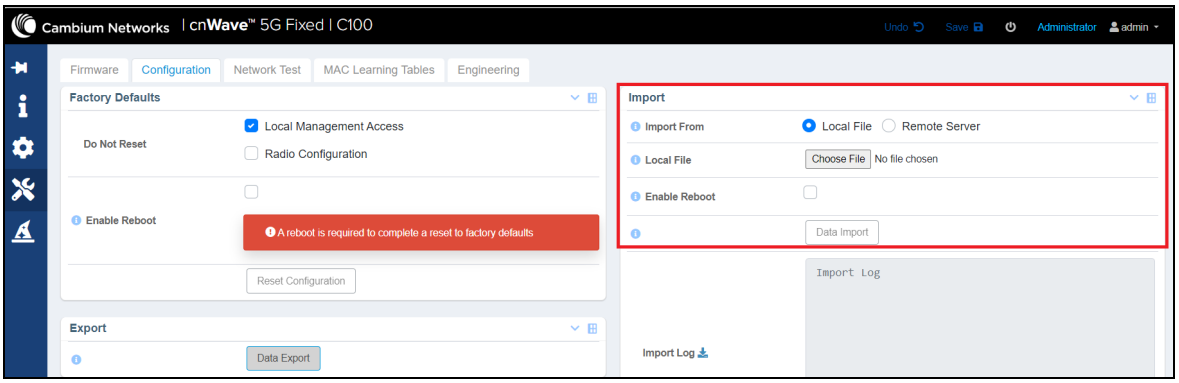
   The **Configuration** page appears.

   For information on how to log on to the B1000 UI, refer to the Accessing the B1000 UI section.

2. To export the current configuration, click on **Data Export** in the **Import** section as shown in Figure 40.

   The `_cdm-export.json_` file is saved in the **Downloads** folder, by default.

   Figure 40: *Exporting the current configuration*



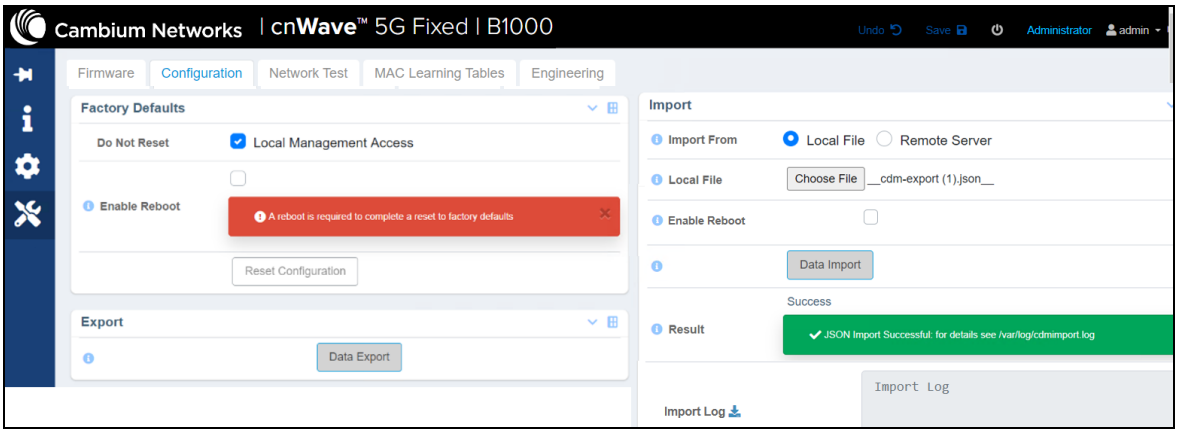
> **Note**
>
> For security reasons, the configuration export functionality does not contain any password settings. As a result, accounts are not fully restored when a configuration is restored. You have to set the accounts and passwords manually.

3. To import a configuration file, choose an import option (Local File or Remote Server) from the **Import From** parameter.

4. Click **Data Import**.

   A message appears indicating that the JSON import is successful, as shown in Figure 41.

   Figure 41: *Importing a configuration file*

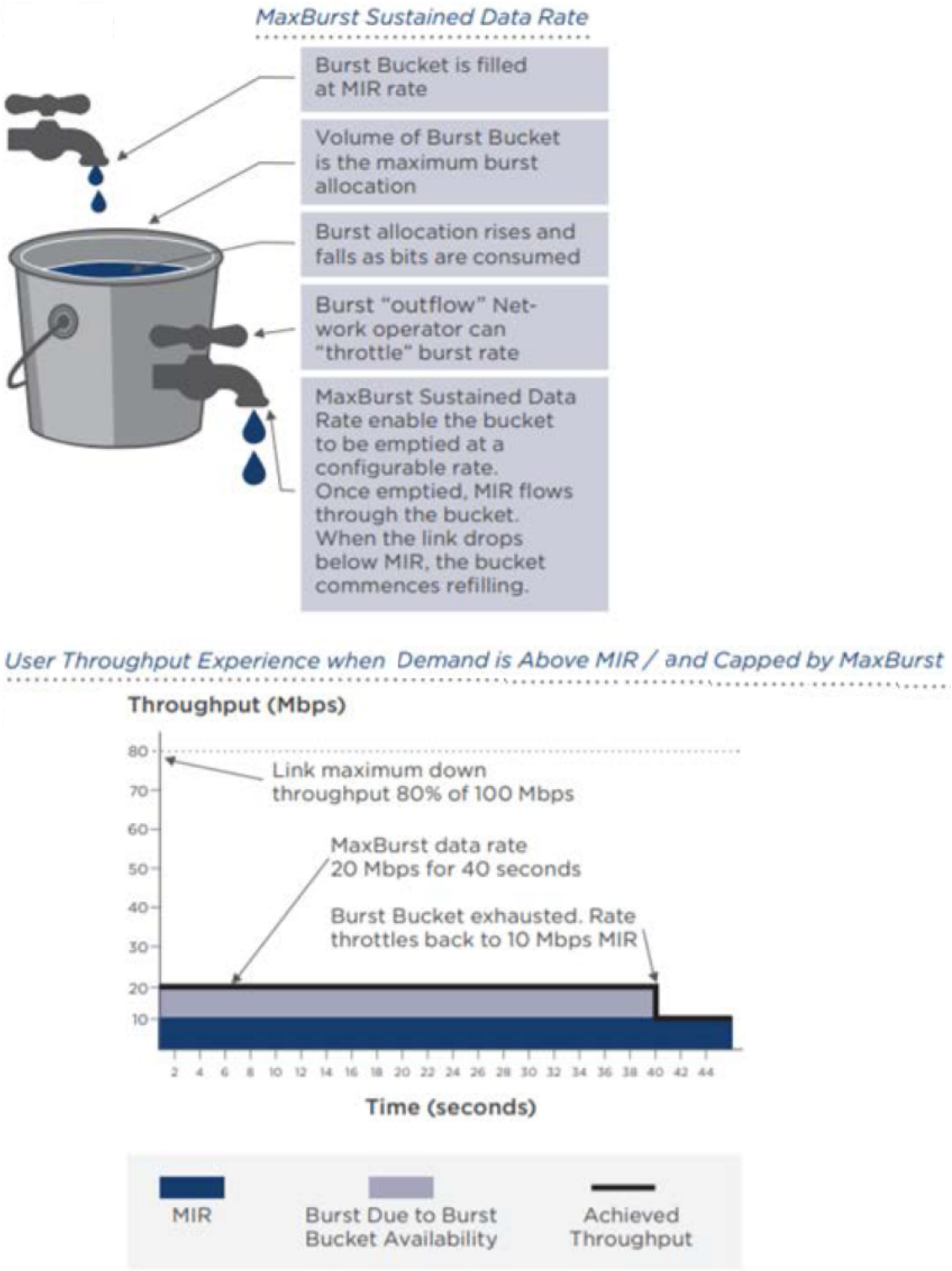


Testing MIR - No reboot required

Maximum Information Rate (MIR) is a functionality that provides a mechanism to limit the rate at which data traffic can be received or sent to a station over its wireless interface. This MIR functionality is required for managing various services for different customers.

To meet the huge bandwidth demands, Cambium Networks introduced the MIR functionality by considering the Burst Bucket concept (as shown in Figure 42). The purpose is to set limits on how much data can be sent to and received from a CPE.

Figure 42: *The Burst Bucket Concept and MIR*



For MIR testing, you must modify the following parameters in the `authorize` file (a Radius Server file):

- **ULBR**: The uplink bit rate or sustained uplink rate (in kbps) at which each CPE has registered with the BTS. The BTS is replenished with credits for transmission.
- **ULBL**: The uplink bit limit or uplink burst allocation (in kbits). Indicates the maximum amount of data that each CPE is allowed to transmit before being recharged at the sustained uplink data rate (in kbps).
- **DLBR**: The downlink bit rate or sustained downlink rate (in kbps) at which the BTS is replenished with credits (tokens) for transmission to each of the CPEs in its sector.
- **DLBL**: The downlink bit limit or downlink burst allocation (in kbits). Indicates the maximum amount of data that the BTS is allowed to transmit to any registered CPE before it is replenished with the transmission credits at the sustained downlink data rate (in kbps).

For more information about these MIR-specific parameters, refer to the *cnWave™ 5G Fixed Configuration Guide*.

To test MIR, perform the following tasks:

- Modifying the MIR parameters on the Radius Server
- Running the MIR test

Modifying the MIR parameters on the Radius Server

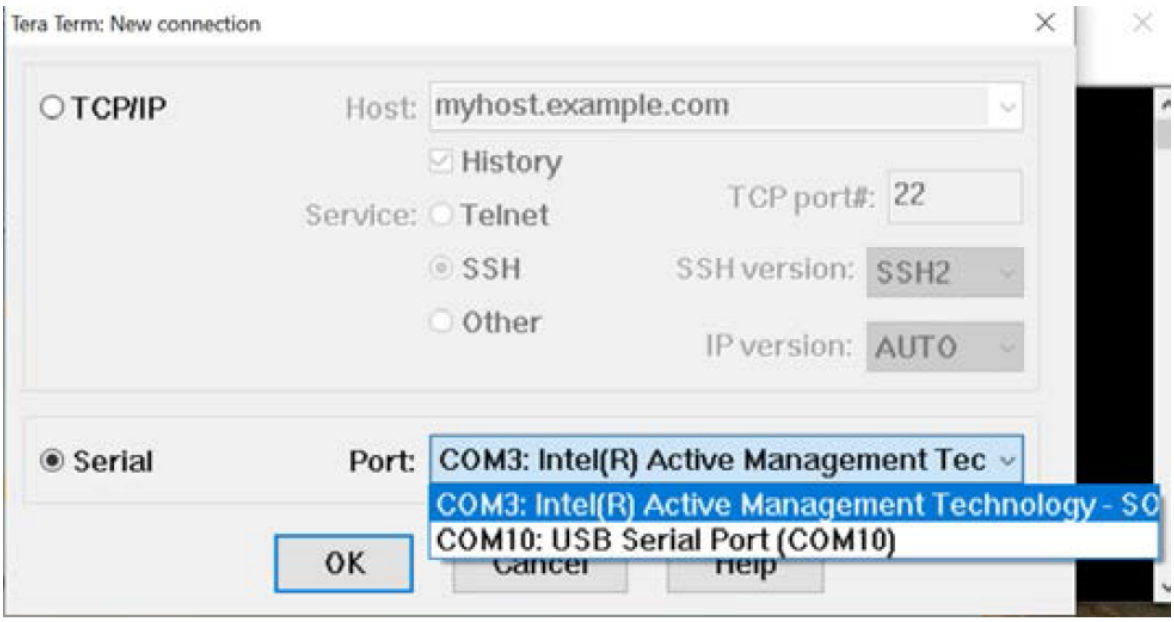
To configure the MIR functionality, you must modify MIR -specific parameters in the `authorize` file (a Radius Server file). This file contains all the CPE parameters passed onto the CPEs during the registration process.

To modify the MIR-specific parameters, perform the following steps:

1. Log on to the Radius Server C4000 using a serial cable that is connected between the Console Port and a USB port on the PC.
2. Use any Terminal program (for example, Tera Term) to select the PC port and log on to the Radius Server C4000.

   The **Tera Term New Connection** screen appears.
3. In the **Tera Term New Connection** screen, choose **Serial** and select the correct PC Port from the drop-down list (for example, COM10 in this case as shown in Figure 43).

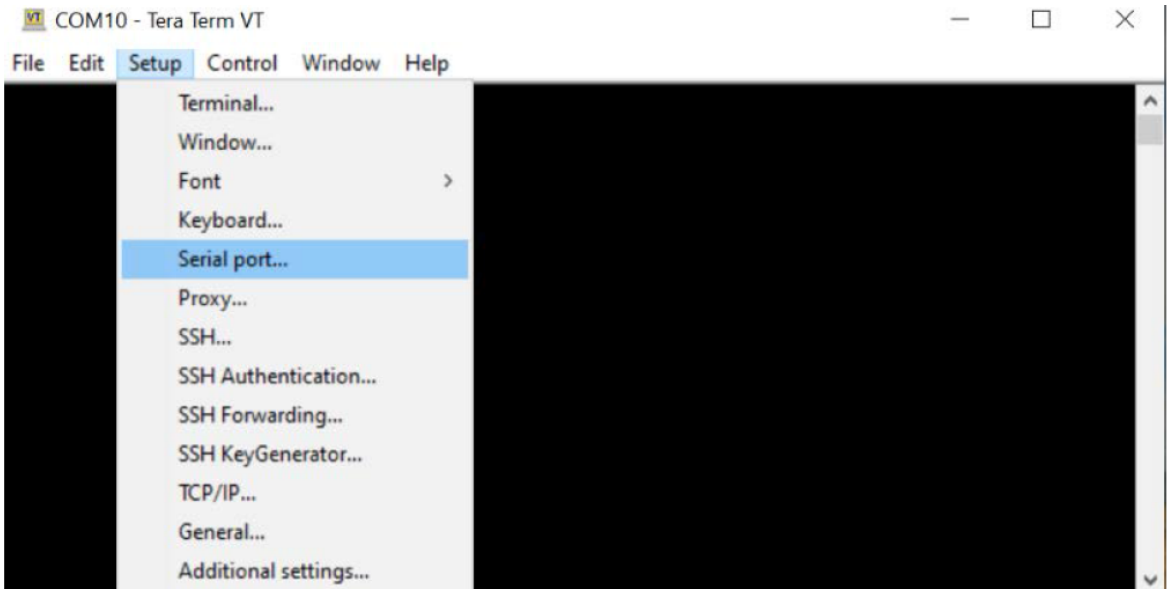
Figure 43: *Selecting the PC Port to log in to the Radius Server C4000*



4. Click **OK**.

5. Open the Tera Term vi Editor screen and navigate to **Setup** > **Serial Port**, as shown in Figure 44.

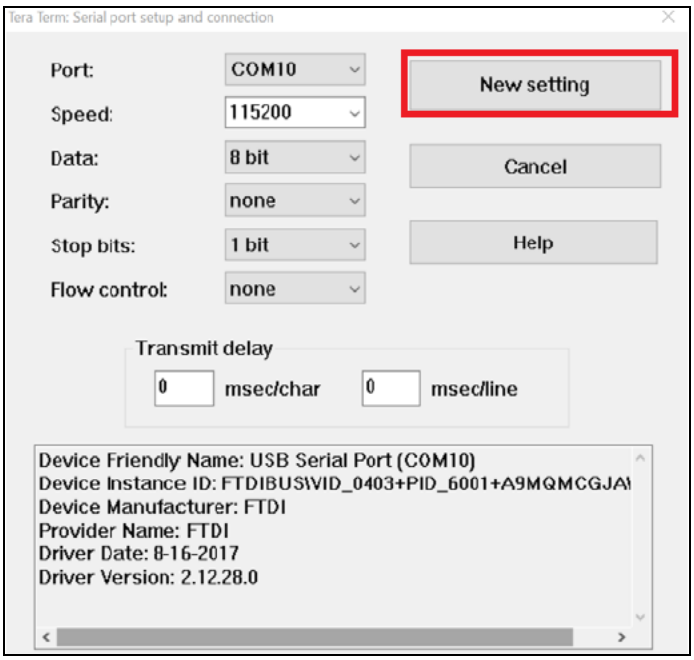
   Figure 44: *Selecting the serial port*



   The **Serial port setup and connection** screen appears.

6. In the **Serial port setup and connection** screen, set the serial port parameters and click **New Setting** (as shown in Figure 45) .

Figure 45: *Configuring serial port settings*

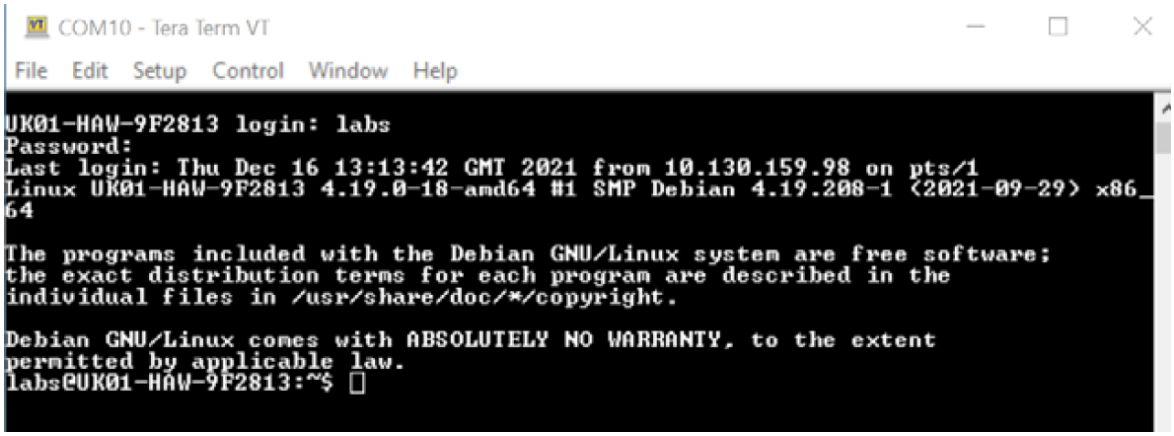


7. Touch any one of the keys on your keyboard.

   The login screen of Radius Server C4000 appears. You must use the following credentials to log on (as shown in Figure 46):

   - Username: labs
   - Password: phn

   Figure 46: *The log in screen of Radius Server C400*



8. Edit the authorize file using the vi Editor.

   You may need to familiarize yourself with the Editor by using the main command such as the following:

   $ sudo vi /etc/freeradius/3.0/mods-config/file/authorize

9. In the `authorize` file, locate and modify the MIR parameters for the CPE that is under test.

The value of MIR parameters (ULBR, ULBL, DLBR, and DLBL) is `0` (zero), which indicates that there are no limits on the CPE data traffic size.

Figure 47: *MIR Parameters set with no limits*

```
# Fixed IMSIs for test rigs
888901007405870 Cleartext-Password := "networks"
        Framed-IP-Address          = "169.254.1.11",
        Framed-IP-Netmask          = 255.255.255.0,
        Cambium-Canopy-Gateway     = 169.254.1.0,
        Cambium-Canopy-VLMGVID     = 1,
        Cambium-Canopy-VLSMMGPASS  = 0,
        Cambium-Canopy-HPENABLE    = 0,
        Cambium-Canopy-ULBR        = 0,
        Cambium-Canopy-ULBL        = 0,
        Cambium-Canopy-DLBR        = 0,
        Cambium-Canopy-DLBL        = 0,
        Cambium-Canopy-BCASTMIR    = 100,
        Cambium-Canopy-ULMB        = 6144,
        Cambium-Canopy-DLMB        = 61440,
        Cambium-Canopy-LPULCIR     = 1000,
```

For the test purpose, you can set (for instance) ULBL and ULBR to 20000 kbps (maximum 20 Mbits/s). You can set DLBL and DLBR to 50000 kbps (maximum 50 Mbps).

Figure 48: *MIR Parameters set with limits*

```
# Hawking CPEs 1-8
# Fixed IMSIs for test rigs
888901007405870 Cleartext-Password := "networks"
        Framed-IP-Address          = "169.254.1.11",
        Framed-IP-Netmask          = 255.255.255.0,
        Cambium-Canopy-Gateway     = 169.254.1.0,
        Cambium-Canopy-VLMGVID     = 1,
        Cambium-Canopy-VLSMMGPASS  = 0,
        Cambium-Canopy-HPENABLE    = 0,
        Cambium-Canopy-ULBR        = 20000,
        Cambium-Canopy-ULBL        = 20000,
        Cambium-Canopy-DLBR        = 50000,
        Cambium-Canopy-DLBL        = 50000,
        Cambium-Canopy-BCASTMIR    = 100,
        Cambium-Canopy-ULMB        = 6144,
        Cambium-Canopy-DLMB        = 61440,
        Cambium-Canopy-LPULCIR     = 1000,
        Cambium-Canopy-HPULCIR     = 100,
```

10. To apply the changes that you made in the `authorize` file, perform the following steps:

    a. Stop the Radius Server by running the following command:

    $ sudo systemctl stop freeradius

b. Restart the Radius Server by running the following command:

   $ sudo systemctl start freeradius

c. Reboot the CPE for which the MIR parameters are modified in the `authorize` file.

   Either repower the CPE manually or go to the C100 UI and press the **Reboot** button (located at the top right corner of the UI). Wait for the CPE(s) to get re-connected and re-registered before doing the throughput tests.

Running the MIR test

On modifying the MIR-specific parameters in the `authorize` file for the required CPE, you must run the test.

To complete the MIR testing, perform the following steps:

1. Ensure that all the other CPEs are powered off, except for the one under test.

   Only one CPE is enough to demonstrate the MIR functionality. Ensure that the Radius Server is restarted, and the CPE (under test) is rebooted after modifying the MIR-specific parameters. For more information, refer to the Modifying the MIR parameters on the Radius Server section.

2. Check the B1000 UI dashboard (BTS) to confirm that only one CPE is connected and registered.

3. Run the link capacity test using the **Tools > Link Capacity Test** page of B1000 UI.

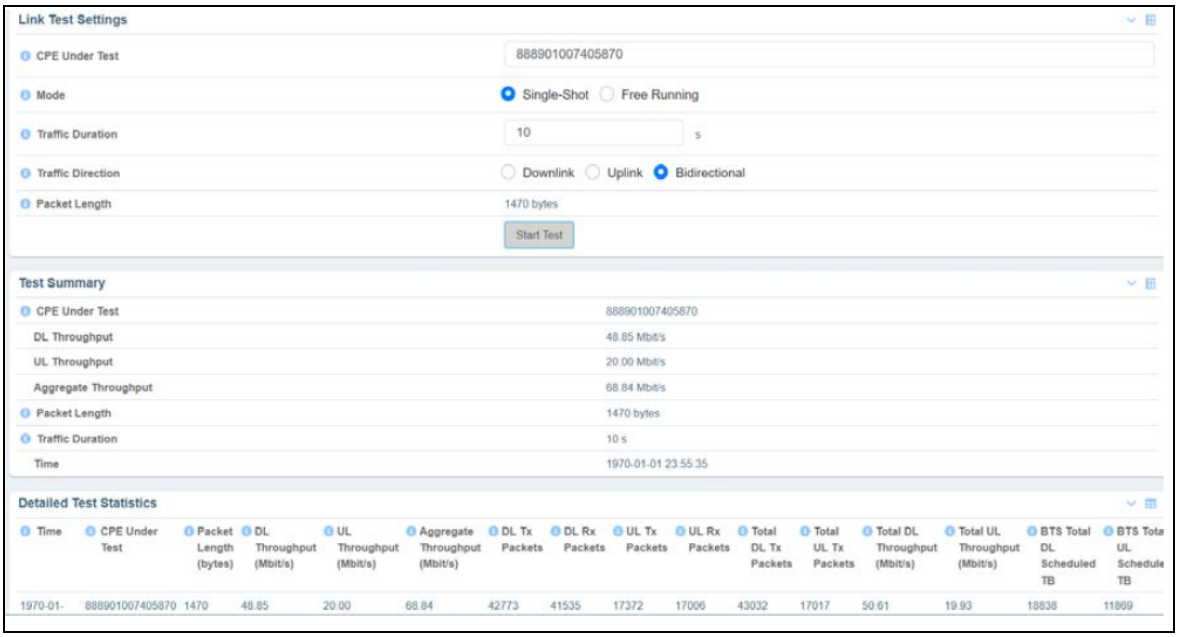
   You must run this test using a single shot 30s bidirectional traffic setting.

4. Configure MKTK on the BTS side and the CPE side for throughput measurements.

5. Run the tests and record the results.

   Check the throughput, which must show that the maximum downlink throughput does not exceed 50 Mbps and that the uplink throughput does not exceed 20 Mbps (as shown in Figure 49).

   Figure 49: *An example of Link Capacity Test using MIR settings DL 50/UL 20*

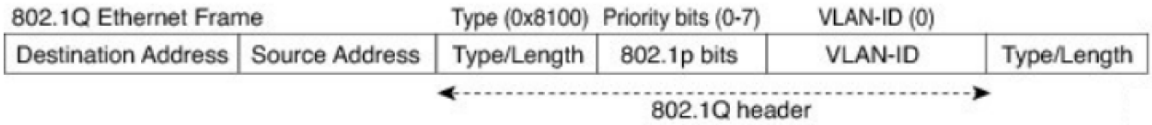


Testing CIR - No reboot required

Committed information rate (CIR) is a functionality that supports the data traffic for managing different services with committed rates for different customers (using phones as well).

Similar to Canopy (PMP450), cnWave™ 5G Fixed has four priority levels. These four priority levels are mapped using the priority bits. Packet classification is done on the p-bits field of the VLAN header.

Figure 50: *802.1Q Ethernet frame*



The CnWave™ 5G Fixed scheduler uses a round-robin scheme at each priority level. Everything is scheduled at each level until the queues at that level are empty.

In addition to MIR, Cambium Networks provides a CIR per priority level. The CIR priority levels support in delivering up to an allotted amount of data, provided capacity exists, while considering the priority constraints. CIR protects and guarantees the allocated data rates even under overload.

The four priority levels start at the highest level and work down to the lowest level. This implies that a high-priority level traffic is scheduled ahead of any low-priority level traffic (which is pending). Following are the four priority levels, which are listed in the priority order from highest to lowest:

- Ultra High Priority (802.1p-bit priority 6 or 7)
- High Priority (802.1p-bit priority 5 or 6)
- Medium Priority (802.1p-bit priority 4 or 3)
- Low Priority (802.1p-bit priority 2 or 1)

Consider the following example for the CIR priority levels:

In a sector with no other traffic and which is capable of sustaining an excess of 40 Mbps, apply UDP traffic to all priorities. Each priority is sufficient to saturate the sector capacity. You can observe the following:

- The High Priority bearer is carried to 10 Mbps.
- The Low Priority bearer is carried to 30 Mbps.
- The Ultra High Priority bearer uses up what remains of the sector capacity due to the second scheduling round.

In this way, CIR has the allocated data rates even under overload.

For CIR testing, you must modify the following parameters in the `authorize` file (a Radius Server file):

- **LPULCIR**: The minimum rate (in kbps) at which a low priority traffic is sent over the uplink (unless CIR is oversubscribed or the RF link quality is degraded).
- *MPULCIR*: The minimum rate (in kbps) at which a medium priority traffic is sent over the uplink (unless CIR is oversubscribed or the RF link quality is degraded).
- **HPULCIR**: The minimum rate (in kbps) at which a high priority traffic is sent over the uplink (unless CIR is oversubscribed or the RF link quality is degraded).

- **UHPULCIR**: The minimum rate (in kbps) at which an ultra-high priority traffic is sent over the uplink (unless CIR is oversubscribed or the RF link quality is degraded).
- **LPDLCIR**: The minimum rate (in kbps) at which a low priority traffic is sent over the downlink (unless CIR is oversubscribed or the RF link quality is degraded).
- **MPDLCIR**: The minimum rate (in kbps) at which a medium priority traffic is sent over the downlink (unless CIR is oversubscribed or the RF link quality is degraded).
- **HPDLCIR**: The minimum rate (in kbps) at which a high priority traffic is sent over the downlink (unless CIR is oversubscribed or the RF link quality is degraded).
- **UHPDLCIR**: The minimum rate (in kbps) at which an ultra-high priority traffic is sent over the downlink (unless CIR is oversubscribed or the RF link quality is degraded).

For more information about these CIR-specific parameters, refer to the *cnWave™ 5G Fixed Configuration Guide*.

To test CIR, perform the following tasks:

- Modifying the CIR parameters on the Radius Server
- Running the CIR test

Modifying the CIR parameters on the Radius Server

To configure the CIR functionality, you must modify CIR-specific parameters in the `authorize` file (a Radius Server file). This file contains all the CPE parameters passed onto the CPEs during the registration process.

To modify the CIR-specific parameters, perform the following steps:

1. Log on to the Radius Server C4000 using a serial cable that is connected between the Console Port and a USB port on the PC.
2. To set the serial port and access the login page of the Radius Server C4000, follow the steps from 2 to 8 described in the Modifying the MIR parameters on the Radius Server section.
3. In the `authorize` file, locate and modify the CIR parameters for the CPE that is under test.

   For the test purpose, you can set (for instance) ULBL and ULBR to 20000 kbps (maximum 20 Mbits/s). You can set the D BL and DLBR to 250000 kbps (maximum 250 Mbps). Now, you can set LPDLCIR (50000), MPDLCIR (70000), HPDLCIR (90000), and UHPDLCIR (150000).

Figure 51: *An example of CIR Parameter settings*

```
# Hawking CPEs 1-8
# Fixed IMSIs for test rigs
888901007406841 Cleartext-Password := "networks"
    Framed-IP-Address          = "169.254.3.1",
    Framed-IP-Netmask          = 255.255.255.0,
    Cambium-Canopy-Gateway     = 169.254.3.99,
    Cambium-Canopy-VLMGVID     = 1,
    Cambium-Canopy-VLSMMGPASS  = 0,
    Cambium-Canopy-HPENABLE    = 1,
    Cambium-Canopy-ULBR        = 0,
    Cambium-Canopy-ULBL        = 0,
    Cambium-Canopy-DLBR        = 310000,
    Cambium-Canopy-DLBL        = 0,
    Cambium-Canopy-BCASTMIR    = 100,
    Cambium-Canopy-ULMB        = 6144,
    Cambium-Canopy-DLMB        = 61440,
    Cambium-Canopy-LPULCIR     = 0,
    Cambium-Canopy-MPULCIR     = 0,
    Cambium-Canopy-HPULCIR     = 0,
    Cambium-Canopy-UHPULCIR    = 0,
    Cambium-Canopy-LPDLCIR     = 20000,
    Cambium-Canopy-MPDLCIR     = 40000,
    Cambium-Canopy-HPDLCIR     = 60000,
    Cambium-Canopy-UHPDLCIR    = 80000,
    Cambium-Canopy-VLLEARNEN   = 1,
    Cambium-Canopy-VLIGVID     = 50,
    Cambium-Canopy-VLFRAMES    = 1,
    Cambium-Canopy-VLIDSET     = 101,
    Cambium-Canopy-VLIDSET     = 141,
```

4. To apply the changes that you made in the `authorize` file, perform the following steps:

   a. Stop the Radius Server by running the following command:

      $ sudo systemctl stop freeradius

   b. Restart the Radius Server by running the following command:

      $ sudo systemctl start freeradius

   c. Reboot the CPE for which the MIR parameters are modified in the `authorize` file.

      Either repower the CPE manually or go to the C100 UI and press the **Reboot** button (located at the top right corner of the UI). Wait for the CPE(s) to get re-connected and re-registered before doing the throughput tests.

Running the CIR test

On modifying the CIR-specific parameters in the `authorize` file for the required CPE, you must run the test.

To complete the CIR testing, perform the following steps:

1. Ensure that all the other CPEs are powered off, except for the one under test.

   Only one CPE is enough to demonstrate the CIR functionality. Ensure that the Radius Server is restarted, and the CPE (under test) is rebooted after modifying the CIR-specific parameters. For more information, refer to the Modifying the CIR parameters on the Radius Server section.

2. Check the B1000 UI dashboard (BTS) to confirm that only one CPE is connected and registered.

3. Run the link capacity test using the **Tools > Link Capacity Test** page of B1000 UI.

   You must run this test using a single shot 30s bidirectional traffic setting. Check the throughput, which must show that the maximum downlink throughput doesn't exceed 50 Mbps and that the uplink throughput doesn't exceed 20 Mbps (as shown in Figure 49).

4. Edit the **authorize** file of the Radius to add four (4) VLANs, with each VLAN corresponding to a priority.

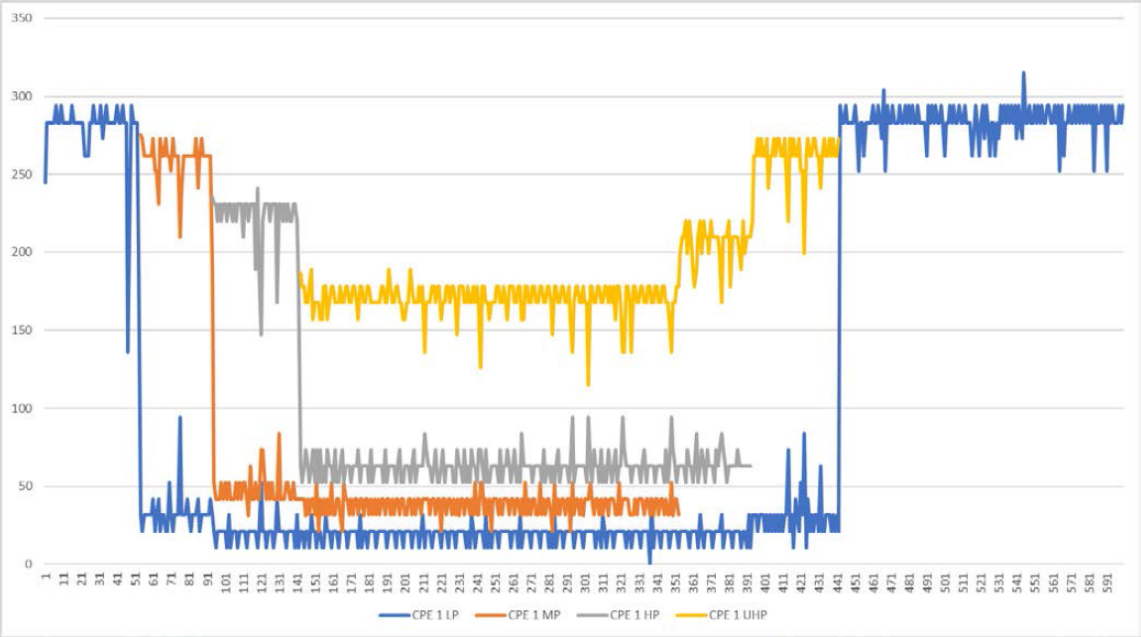
5. Set up the p-bit priority bits on the machines that you are using to send traffic.

   Example: If you are using a Linux PC, use the following scripts to set up Ultra High priority (VLAN ID = 241) on both sides:

   ```
   sudo ip link set enp1s0.241 type vlan id 241 egress-qos-map 0:7 1:7 2:7 3:7 4:7
   5:7 6:7 7:7 ingress-qos-map 0:7 1:7 2:7 3:7 4:7 5:7 6:7 7:7
   ```

   You can experiment the four priorities, but you must run four (4) concurrent iperf client sessions from the BTS side and ensure that the CPE side is running an iPerf server. Otherwise, you can use one priority level to test the CIR. An example of four priorities is shown in Figure 52.

   Figure 52: *An example of CIR test with four priority levels*



6. Run the tests and record the results.

Verify that the CPE throughput is as expected for each bandwidth (all sample results summarized in Table 3 for reference). The test can be repeated with more than one CPE, if needed (as described in Using QoS priority levels for testing).

Table 3: A sample of eighth Scenario Results - CIR (with MIR)

Active Radio	Test	Set up in Radius	Microtik or else Reading (DL Mbps)	LCT (Expected) Reading (DL/UP Mbps)
POP_0 CPE 1	MIR	DL Burst Rate = 250 Mbps DL Limit Max = 350 Mbps		250 Mbps
POP_0 CPE 1	CIR	LPDLCIR = 50 Mbps MPDLCIR = 70 Mbps HPDLCIR= 90 Mbps UHPDLCIR = 150 Mbps (Refer to the Radius Configuration in the cnWave™ 5G Fixed Configuration Guide)		Verify the iPerf results and check limits of each priority in line with what is set and the MIR limit.

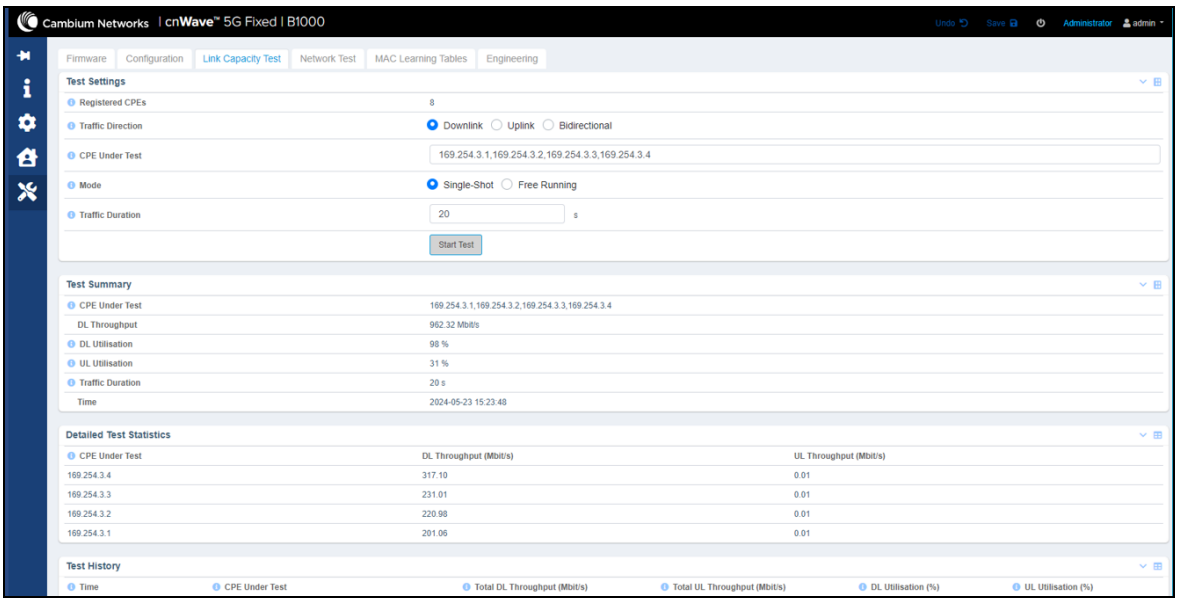
Using QoS priority levels for testing

You can use the QoS priority levels to test MIR and CIR. Consider the following example of CPE configuration (CPE-1, CPE-2, CPE-3, ad CPE-4) with MIR and CIR settings, and running tests:

1. Configure the four CPEs with the following settings:
   - **CPE-1**:
     - MIR Setting - 200 Mbps
     - CIR Settings:
       - Low priority (LP) CIR - 20 Mbps
       - Medium priority (MP) CIR - 40 Mbps
       - High priority (HP) CIR - 60 Mbps
       - Ultra-high priority (UHP) CIR - 80 Mbps
   - **CPE-2, CPE-3, and CPE-4**:
     - MIR Setting: 220 Mbps and 230 Mbps
     - CIR Settings: None (LP CIR - 0 Mbps, MP CIR - 0 Mbps, HP CIR - 0 Mbps, and UHP CIR - 0 Mbps)
2. Run the LCT tool for the four CPEs using the **Tools** > **Link Capacity Test** page of B1000 UI (as shown in Figure 53).

   When the LCT tool is carried out using the downlink traffic direction, the four CPEs (CPE-1 to CPE-4) give the maximum throughput. Note that CPE-1, CPE-2 and CPE-3 are all limited by their respective MIR settings.

Figure 53: *Example of running LCT for four CPEs using downlink traffic*

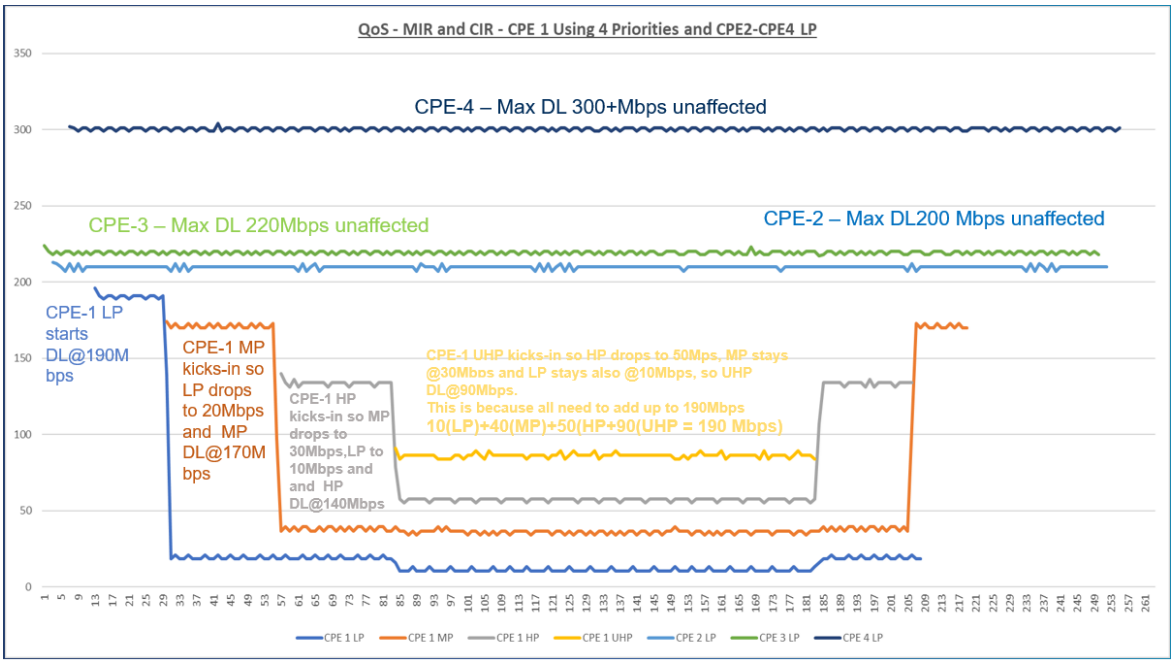


The LCT results (downlink) are (as shown in Figure 54):

- CPE-1 - 200 Mbps (MIR limited)
- CPE-2 - 220 Mbps (MIR limited)
- CPE-3 - 230 Mbps (MIR limited)
- CPE-4 - 317 Mbps (Unlimited)

Figure 54 is an annotation of CIR and MIR tests using four CPEs and their service priority levels.

Figure 54: *Annotation for CIR and MIR tests*



General Troubleshooting Procedures

This section provides information about operational procedures for a BTS and a CPE in the field. For instance, replacing a faulty BTS, changing some key parameters, or performing a software upgrade.

If the cnWave™ 5G Fixed system has already been installed in the field, then additional troubleshooting will be required on all components of the system (for example, power supply, cables, LPUs, networks, and others).

The cnWave™ 5G Fixed platform of products is a Point-to-Multipoint (PMP) system and you must be aware of the following main issues that require troubleshooting:

- Loss of connectivity between a BTS and one or more CPEs.
- Loss of performance of a sector in either the downlink or uplink direction.
- Loss of synchronization if more than one BTS is installed.

This section explains some troubleshooting techniques to deal with the above main issues. In all cases, effective troubleshooting depends on measures you take before experiencing any problem or trouble) in your network. Hence, Cambium Networks recommends the following measures for each site:

- Identify the troubleshooting tools that are available at your site (such as a protocol analyzer).
- Identify commands and other sources that can capture baseline data for the site. These commands and sources may include:
    - Ping
    - Link Capacity Test results
    - Throughput data
    - Data captured in the **Configuration** UI page
    - Data captured in the **Interface** UI page
    - Session logs
    - Web browser used
- Start a log for the site.
- Include the following information in the log:
    - Operating procedures
    - Site-specific configuration records
    - Network topology
    - Software releases, boot versions and FPGA firmware versions
    - Types of hardware deployed
    - Site-specific troubleshooting processes
    - Escalation procedures
- Capture baseline data into the log from the sources, as listed here.

This section covers the following troubleshooting topics:

What is the general fault isolation process?

Effective troubleshooting also requires an effective fault isolation methodology that includes the following:

- Attempting to isolate the problem to the level of a system, subsystem, or link, such as the following:
    - BTS or CPE
    - Sector (GPS Synchronization)
    - Backhaul
    - Network
    - Power
- Searching for event logs of the involved equipment.
- Interpreting messages in the event log.
- Answering the questions listed in the How to isolate the problem? section.
- Reversing the last previous corrective attempt before proceeding to the next.
- Performing only one corrective attempt at a time.

How to isolate the problem?

When a problem occurs, you must take primary steps to isolate the problem. Attempt to answer the following frequently asked questions (FAQs):

- What is the history of the problem?
    - Have you changed something recently?
    - Have you seen any other symptoms before this?
- How widespread is the symptom?
    - Is the problem only with a single CPE? (If so, focus on that CPE.)
    - Is the problem with multiple CPEs? If so, think of the following:
        - Is the problem with one BTS in the cluster? (If so, focus on that BTS)
        - Is the problem with multiple, but not all, BTS devices in the cluster? (If so, focus on those BTS devices)
        - Is the problem with all BTS devices in the cluster? (If so, focus on the synchronization and GPS signal.)
- What data does the event log contain?
    - Does the problem correlate to external hard resets with no Watchdog timers? (If so, this indicates a loss of power. Correct the power-related problem.)
    - Is intermittent connectivity indicated? (If so, verify your configuration, power level, cables and connections, and the symmetry of both ends of the link).
    - Does the problem correlate to loss-of-sync events?
- Are connections made via shielded cables?
- Does the BTS GPS antenna have an unobstructed view of the entire horizon?
- Has the site grounding been verified?

What are the secondary steps to isolate the problem?

On completing the preliminary fault isolation steps (as described in the How to isolate the problem? section), perform the following tasks:

- Check the knowledge base information (available on the Cambium Networks portal) to find whether other network operators have encountered a similar problem.
- Proceed to any appropriate set of diagnostic steps that are organized, as follows:
    - The radio has lost or does not establish connectivity (as described in the Troubleshooting a loss of connectivity section).
    - The CPE with DHCP configuration has lost or does not establish connectivity (as described in the Troubleshooting a loss of Ethernet connectivity section).
    - The CPE does not register with a BTS (as described in the Troubleshooting when CPE fails to register with a BTS section).

- The radio does not establish Ethernet connectivity (as described in the Troubleshooting a loss of Ethernet connectivity section).
- The radio's software cannot be upgraded.
- The radio functions properly, except for the web interface that is inaccessible (as described in How to hardware reset a BTS to factory default? and How to hardware reset a CPE to factory default? sections).

Troubleshooting a loss of connectivity

When the radio has lost connectivity or does not establish the connectivity, perform the following steps to troubleshoot the loss of connectivity:

1. Isolate the end user or CPE from peripheral equipment and variables such as routers, switches, and firewalls.
2. Set up the minimal amount of equipment (for example, removal of any additional or testing equipment).
3. On each end of the link, perform the following tasks:
    - Check the cables and connections.
    - Verify that the cable or connection scheme – straight through or crossover – is correct.
    - Access the **Dashboard** tab on the home page of B1000 UI (BTS).
    - Verify that the dashboard shows the connected and registered CPE information.
    - Verify that the Received Power is -87 dBm or higher.
    - Verify that the Error Vector Magnitude (EVM) does not contain a value greater than zero.
    - Verify that the IP addresses match and are in the configured subnets.
    - If the RADIUS authentication is configured, ensure that the RADIUS server is operational.
4. At the CPE end of the link, perform the following tasks:
    - Verify that the PC, connected to the CPE, is correctly configured to obtain an IP address through DHCP or a static address in the same subnet of the CPE.
    - Execute the `ipconfig` (Windows) or `ifconfig` (Linux) command.
    - Verify that the PC has been assigned with an IP address.
5. On each end of the link, perform the following tasks:
    - Access the **Dashboard** UI page of each device (radio).
    - Verify that the polarity matches the BTS polarity or the polarity is set to Auto Detect in the UI.
    - Verify that the setting for symmetry matches that of the other radio.
    - Access the **Radio** tab on the **Dashboard** page of B1000 or C100 UI.
    - Verify that the radio frequency carrier setting of the BTS is checked in the **Frequency Scan Selection List** for the CPE in the C100 UI.

- Access the browser LAN settings (for example, navigate to **Tools** > **Internet Options** > **Connections** > **LAN Settings** in the browser).
- Verify that none of the settings are selected.
- Access the **Link Capacity Test** tab on the **Tools** page of the B1000 UI (BTS).
- Perform a link test.
- Verify that the link test results show efficiency that is greater than 90% in both uplink and downlink.
- Execute a Ping command.
- Verify that no packet loss was experienced.
- Verify that the response periods are not significantly greater than:
  - 15 ms from CPE to BTS.
  - 4 ms from BTS to CPE.
- Replace any cables that you suspect OF causing the problem.

6. After connectivity has been re-established, reinstall network elements and variables that you removed earlier (in Step 1).
7. If all the above-mentioned steps fail, then start the process of advanced troubleshooting as described in the How to troubleshoot BTS? Section.

Troubleshooting a loss of Ethernet connectivity

When the CPE does not establish the Ethernet connectivity, perform the following steps to troubleshoot the loss of Ethernet connectivity:

1. Verify that the connector crimps on the Ethernet cable are not loose.
2. Verify that the Ethernet cable is not damaged.
3. If the Ethernet cable connects the radio to a network interface card (NIC), verify that the cable is pinned out as a straight-through cable.
4. If the Ethernet cable connects the radio to a hub, switch, or router, verify that the cable is pinned out as a crossover cable.
5. Verify that the Ethernet port, to which the cable connects the radio, is set to auto-negotiate speed.
6. Verify the VLAN configuration in the network, which may cause loss of radio access if the access (of a device) is on a separate VLAN from the radio.
7. Power cycle the radio module.

   Approximately 60 seconds after the power cycle, the **Dashboard** UI page must indicate that the link has been established. If the EVM doesn't stabilize at around -25 dBm or the Dashboard page shows scanning, then the radio is in the alignment mode due to the radio module's failure to establish the link.
8. If the radio has encountered no customer-inflicted damage, then request an RMA for the radio module.

Troubleshooting when CPE fails to register with a BTS

When a CPE fails to register with a BTS, perform the following steps:

1. If Radius is used, verify that the Radius Server is enabled on the BTS.
2. Verify that the Radius Server is running and responding to a Ping to its IP address.
3. Verify that IMSI of the CPE is configured in the Radius Server's `Authorize` file.
4. Verify that the BTS shows the connection possibilities to the CPE, but the authentication fails.
5. Verify that the CPE has the correct certificate.
6. Power cycle the radio module.

   Approximately 60 seconds after the power cycle, the **Dashboard** UI page must indicate that the link has been established. If the module's dashboard shows that CPE is not registered after few minutes, the BTS shows that the authentication still failed to complete.
7. Run the Radius Server in **Debug** mode and note any errors displayed when the CPE is attempting authentication.
8. Report the error and act accordingly. Otherwise, request an RMA for the radio module.

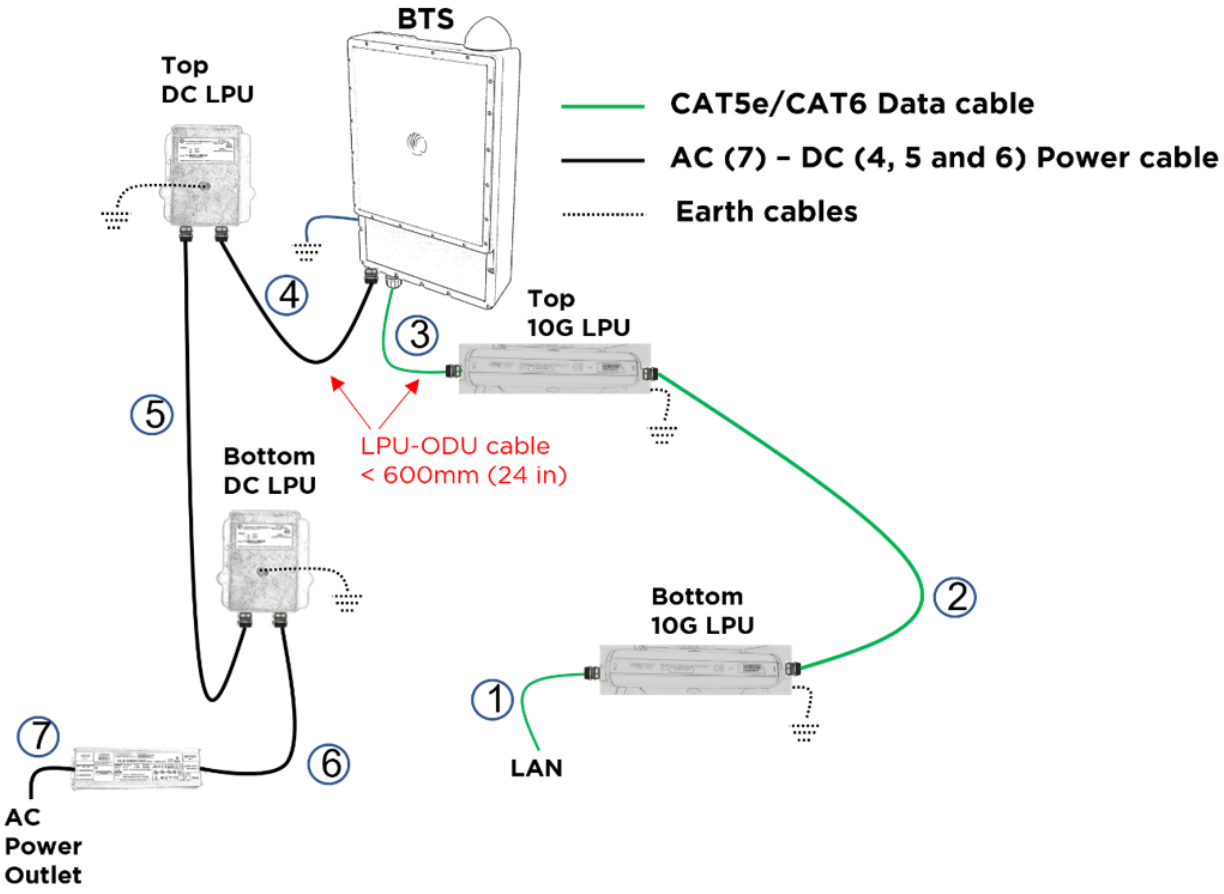
How to troubleshoot BTS?

If a BTS is faulty at a deployment site, then all the customers in the sector will experience a loss of service until the BTS is fixed or replaced (in some cases). This operation can take several minutes or hours due to the physical installation process.

A simple diagram of a BTS installation is shown in Figure 55 and following the steps above, we want to diagnose and eliminate any cabling issues.

A simple ping process can be used to test the connectivity to the BTS. For more detailed troubleshooting, an ohmmeter can be used to measure cable resistance values in case there is connectivity to the BTS, but data errors are observed.

Figure 55: *An example of the BTS cabling*



As shown in Figure 55, multiple things can go wrong with the cables or the surge suppressors before suspecting the BTS.

The following sections provide some steps on how to isolate the issue before troubleshooting the BTS and replace any faulty cables, faulty surge suppressor, or ultimately a faulty BTS:

- Troubleshooting the power cable (black)
    - Power cable connections
    - Power supply
    - Testing
    - Testing resistance of the power cable
    - Testing the Cable (6)
- Troubleshooting the BTS data cable (green)
    - Testing BTS connectivity using Ping
- Troubleshooting BTS using Resistors Table
    - Pre-power testing

Troubleshooting the power cable (black)

This issue must be determined rapidly as you must verify that the BTS is being powered up correctly. Sometimes, multiple things can go wrong including the cables. Therefore, it is recommended to prepare all the cables before the installation.

For details on preparing the power cables, refer to the *cnWave™ 5G Fixed Planning and Installation Guide*.

> **Note**
>
> When preparing the power cable connectors, fit the gland nut, seal, and cage over the wire. It is important to do this task before fitting the plug body.

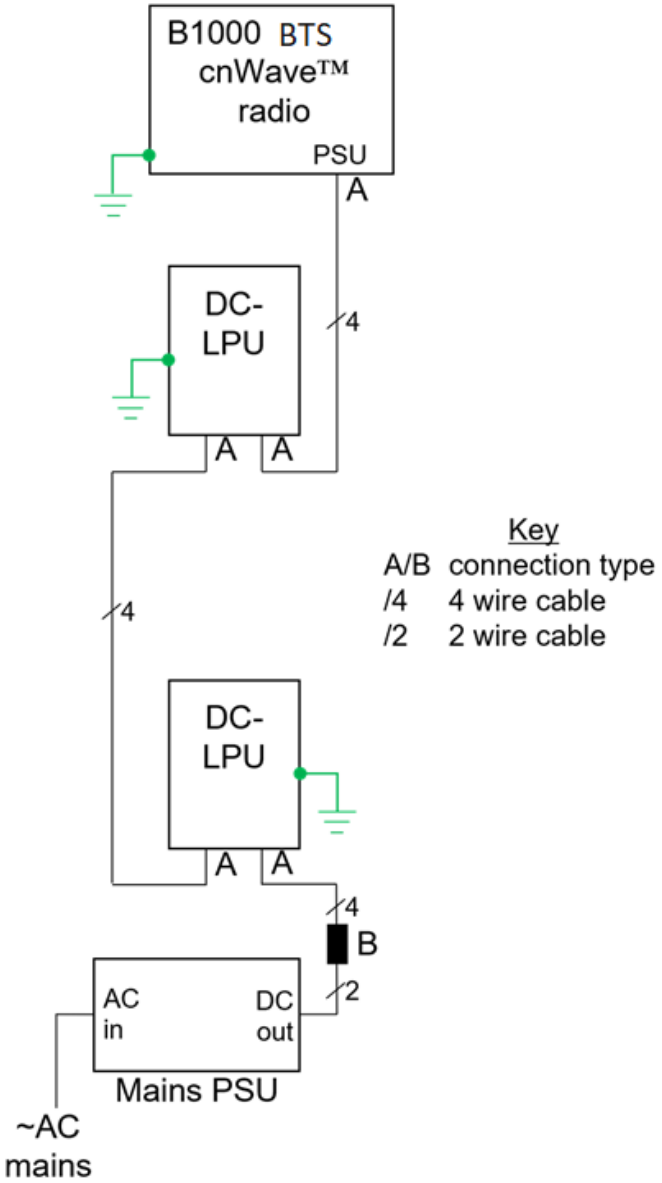
It is good practice to test the resistance in the BTS (as described in the Power cable connections section) and keep doing it at each section of the cable, as shown in Figure 55.

Power cable connections

A typical installation includes a mains power supply, DC-lightning protection units (LPUs) and the radio (as illustrated in Figure 56).

> **Note**
>
> In Figure 56, data cables are not shown. This document is not a substitute for the LPU Installation Guide. Significant installation and grounding details are omitted for clarity in this document.

Figure 56: *Typical DC installation*



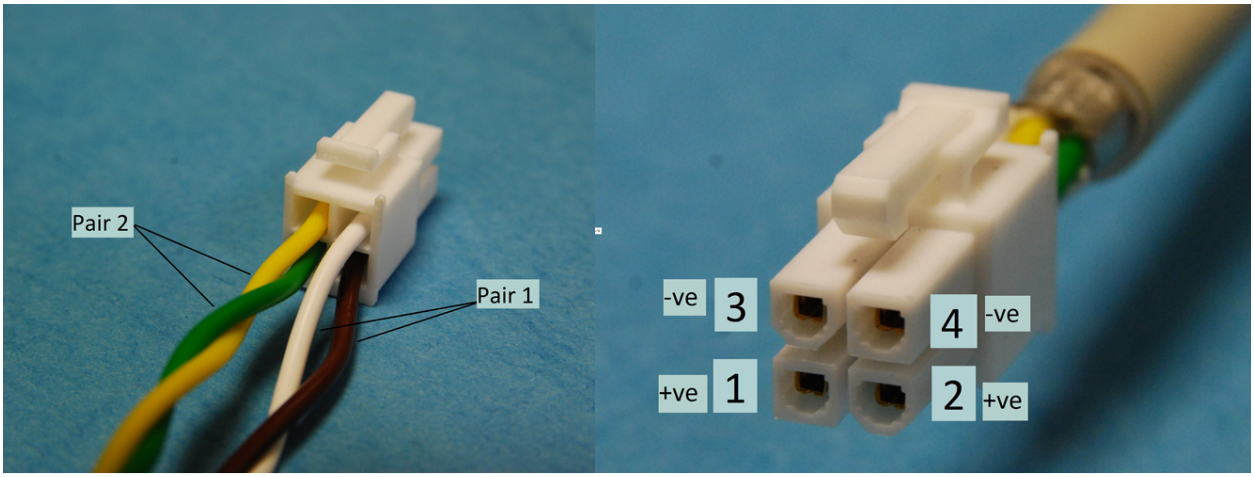
In Figure 56, there are two types of connection:

- **Type A – At the cnWave™ 5G Fixed BTS and at the DC-LPUs**: 4-wire cable to 4-pin plug, as described and illustrated in cnWave™ 5G Fixed BTS radio and DC LPU connections (type A).
- **Type B – At the PSU**: 4-wire cable to 2-wire cable, as described and illustrated in Power supply connection (type B).

cnWave™ 5G Fixed BTS radio and DC LPU connections (type A)

The recommended cable is connected, as shown in Figure 57, using the parts in the 4-pin connector kits (N000000L123A and N000000L124A). The plug body (as shown in Figure 57 for illustration) may be either black or white.

Figure 57: *Cable to B1000/LPU wiring*



Details of pin numbers, wire colors (when using the recommended cable), and power supply polarities are given in Table 4.

Table 4: Details of pin number, wire color, and DC polarity

Pin number	Wire color	DC Polarity	Notes
1	Brown	Positive (+ve)	
2	Green	Positive (+ve)	
3	White	Negative (-ve)	Negative pins are closest to the plug latch.
4	Yellow	Negative (-ve)	

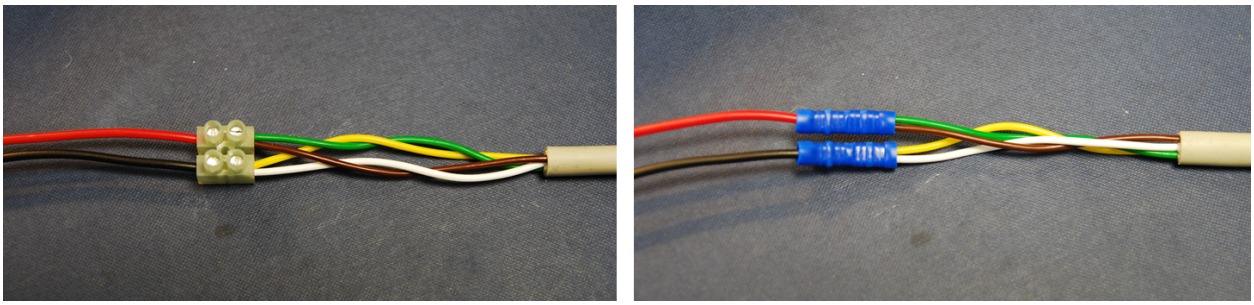
Power supply connection (type B)

Ensure to review the cable testing section before making the connections to the power supply.

The connection between the four wires of the drop cable and the two wires of the power supply must be made, as shown in Figure 58.

In Figure 58, two examples are shown using a terminal block and using crimps. Cambium Networks do not supply this connector. The installer must use any similar suitable means that fits the site installation.

Figure 58: *Cable to PSU wiring, terminal block (left), crimps (right)*



Details of wire colors (when using the recommended cable) and power supply polarities are given in Table 5.

Table 5: Details of pin number, wire color, and DC polarity

450m Wire color	PSU Wire color	DC Polarity	Notes
Brown	Red	Positive (+ve)	
Green		Positive (+ve)	
White	Black	Negative (-ve)	Negative wires are closest to the B1000 plug latch.
Yellow		Negative (-ve)	

Note

1. If the power supply wire strands are consolidated with solder, then snip the soldered part off. Soldered strands must not be used in screwed or crimped connections.
2. When using a screw-terminal connector (as shown in Figure 58), make sure that the wire strands are protected from the terminal screw. Use a terminal block with wire protectors, such as leaf springs or a rising cage type, to fit crimp sleeves to the conductor strands.

Power supply

The recommended power supply from Meanwell has a default output voltage of about 54 V. It can be adjusted over a limited range using the trimmer under the black sealing bung labelled - Vo ADJ - on the top face. It is recommended, particularly, for longer cable runs, or installations with an Auxiliary port PoE load, to trim the output voltage up to between 57 V and 58 V. Gently prise the bung out, use a small screwdriver with a DMM (meter) to set the voltage, and replace the bung before use.

If a different power supply is used, it must be fitted with fold-back current limiting means such as a hiccup mode or fuse.

Testing

It is recommended that the wiring to the LPUs and radio be tested before making the connections to the power supply. Use a meter, ideally a DMM (digital multi-multimeter) with a diode test range, to check the following measurements. The LPUs and the radio must be connected, the power supply must not be connected.

Table 6: Details of cable testing

Test number	Meter positive	Meter negative	Approximate value	Notes
1	Brown (pin 1)	Green (pin 2)	0.6 ohms per 10 m cable 8 ohms maximum	Proportionate to cable length
2	White (pin 3)	Yellow (pin 4)		
3	Brown+Green (pins 1+2)	White+Yellow (pins 3+4)	10 K (kohms) minimum or 2 V minimum	Ohms test range or Diode test range
4	White (pin 3)	Brown (pin 1)	0.7 V typical	Diode test range (note)
5	Yellow (pin 4)	Green (pin 2)		
6	White+Yellow (pins 3+4)	Brown+Green (pins 1+2)		

Note

The cnWave™ 5G Fixed B1000 radio includes a reverse-polarity protection diode wire across the supply. Tests 4, 5, and 6 (as listed above in Table 6) sense this diode and help confirm the correct wiring.

Testing resistance of the power cable

Before connecting the bottom end of the power cable to the PSU, measure the resistance between pins. If any of the tests fail, examine the power cable for wiring faults. Table 4 provides the expected resistances from the bottom of the cable up to the ODU (which must be connected) and back again. It must be the same with or without DC-LPUs fitted.

Table 7: Details of the expected resistances

Cable length		Approximate resistance (O hm), using 0.75 mm^2 cable		
Ft	m	Between pins 1 and 2 Between pins 3 and 4	Between pins 1 and 3 and Between pins 2 and 4	Between any pin and the cable shield
0	0	0.5	>10K (all cable lengths)	> 100K (all cable lengths)
33	10	1.0		
66	20	1.5		
99	30	2.0		
131	40	2.5		
164	50	3.0		
197	60	3.5		
230	70	4.0		
262	80	4.5		
295	90	5.0		
328	100	5.5		

Note

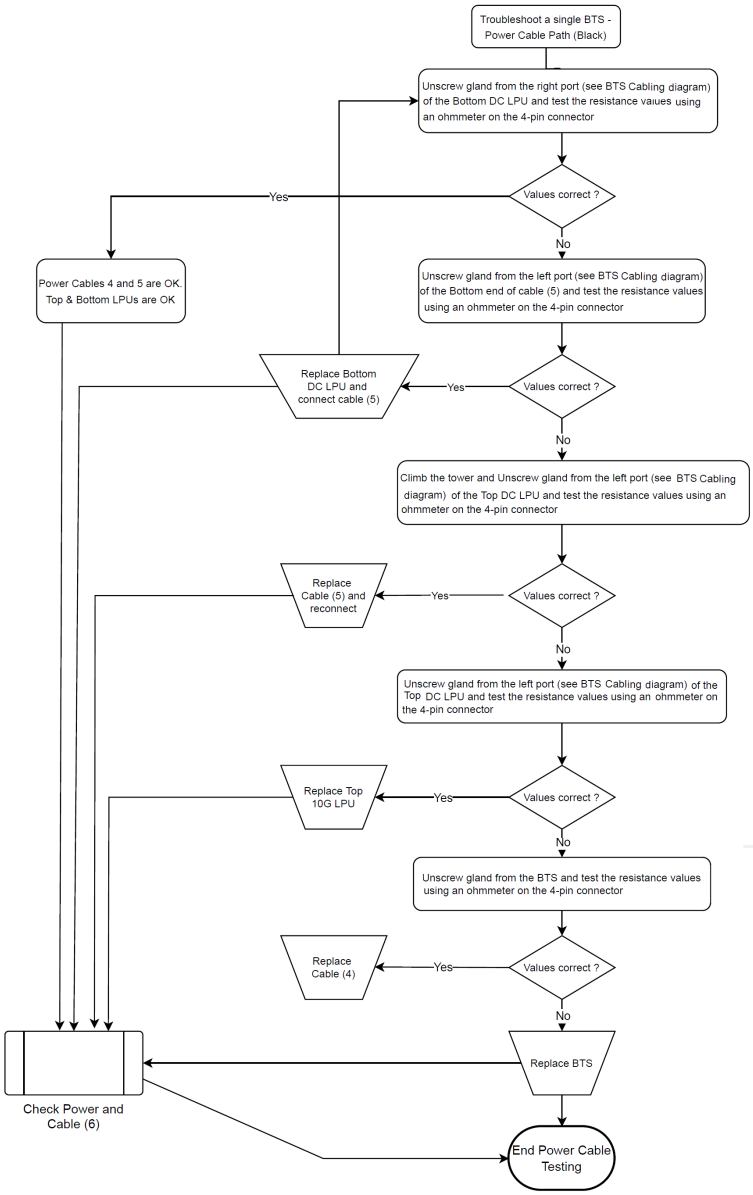
Ensure that the 1-2 and 3-4 resistances are within 10% of each other by multiplying the lower resistance by 1.1. If the other resistance is greater than this, the test has failed.

In Figure 59, we show some simple steps to diagnose any part of the data cable and surge suppressors that may be faulty. The first stage is done at the site and the second stage would require a tower climb.

Note

The cable numbering (for example, cable 5) and color (for example, Black) in Figure 59 are used with reference to the Figure 55An example of the BTS cabling diagram (for better understanding).

Figure 59: *BTS Power cable troubleshooting*



Testing the Cable (6)

It is difficult to test the Cable (6) using the resistance measurement as it is connected directly to the AC/DC power block. It is recommended to replace the cable if the test fails, as indicated in Figure 59.

Troubleshooting the BTS data cable (green)

Figure 60 and Figure 61 show simple steps to diagnose any part of the data cable and surge suppressors that may be faulty. The first stage is done at the site and the second stage requires a tower climb.

Note

The cable numbering (for example, cable 1) and color (for example, Green) in Figure 60 and Figure 61 are used with reference to Figure 55 (for better understanding).

Figure 60: *BTS Data cable troubleshooting - Part 1*

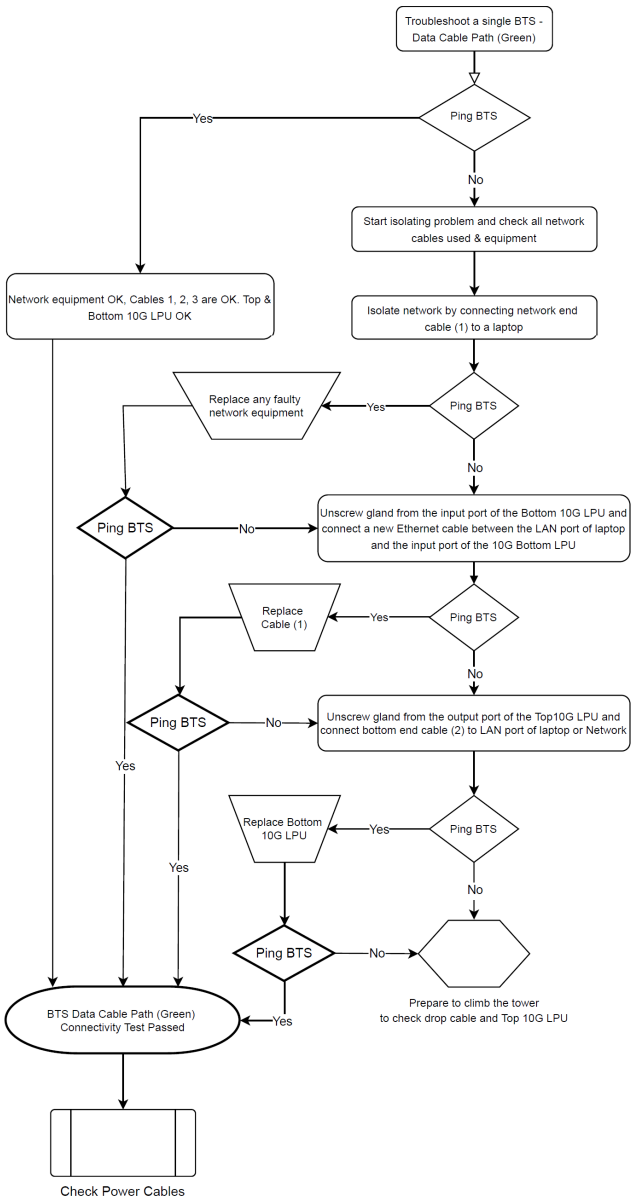
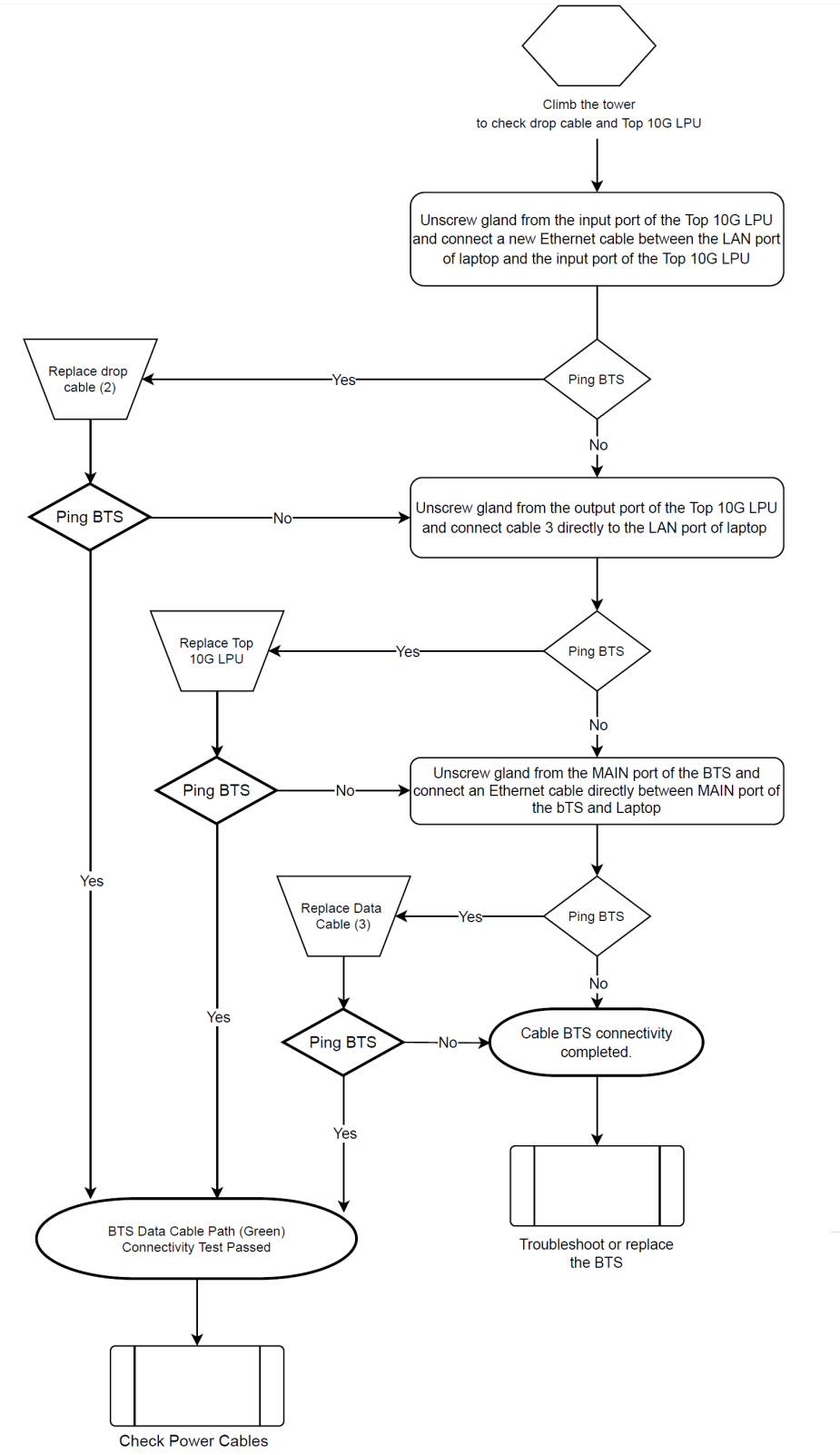


Figure 61: *BTS Data cable troubleshooting - Part 2*



Testing BTS connectivity using Ping

If a customer cannot access the web interface of the BTS or fails to ping it, then it is likely that there is an issue with the cables. This is a test that is recommended during initial installation to ensure that the BTS can be powered and started to operate.

Troubleshooting BTS using Resistors Table

The process of using the Resistors Table must be executed during the pre-installation process of the radios. In this process, the resistance values of the radio RJ45 port transformers are used to check whether the cables between the radio and LPUs are correctly wired.

However, it can also be used for general troubleshooting before deciding to bring the BTS down from the tower and cause service disruption to all customers in that sector.

Pre-power testing

Before plugging the RJ45 cable from the lower LPU (or if not fitted the BTS or CPE) into the switch or router, check the following resistances at the RJ45 cable (as listed in Table 8):

Table 8: Details of resistances for the RJ45 cable (for reference only)

Cable length (in meters)	Resistance pins 1&2, 3&6, 4&5 and 7&8 ohms	Resistance pins 1&2, 3&6, 4&5 and 7&8 ohms	Resistance between pins 4&7 ohm
0	0.8	1.0	1.6
10	2.5	2.7	3.3
20	4.2	4.4	5.0
30	5.9	6.1	6.7
40	7.6	7.8	8.4
50	9.3	9.5	10.1
60	11.0	11.2	11.8
70	12.7	12.9	13.5
80	14.4	14.6	15.2
90	16.1	16.3	16.9
100	17.8	18	18.6

Consider the following points for the pre-power testing:

- Check the cable resistance between pins 1&2, 3&6, 4&5, and 7&8 at the RJ45. Check against column 2 in Table 8.
- Resistances for each pair must be within 1 ohm of each other.
- Check the resistance between pins 1&3 and 4&7 at the RJ45. Check against columns 3 and 4 in Table 8.
- Ensure that there is greater than 100K ohms between pins 1&8 for all cable lengths.
- Ensure that there is greater than 100K ohms between pins 1&8 for all cable lengths.

It is useful to record the following information in the event of a requirement to contact Cambium Networks Support or to identify changes in the installation at a later period:

- IP Address
- Link name
- MAC Address
- Measured resistance between pins (such as for the following):
    - 1&2
    - 3&6
    - 4&5
    - 7&8
    - 1&3
    - 4&7
    - 1&8
    - 1&ODU Ground
    - 8&ODU Ground

Figure 62: *Identifying pin 1*

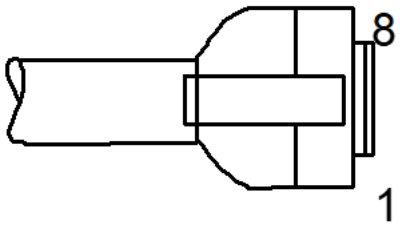
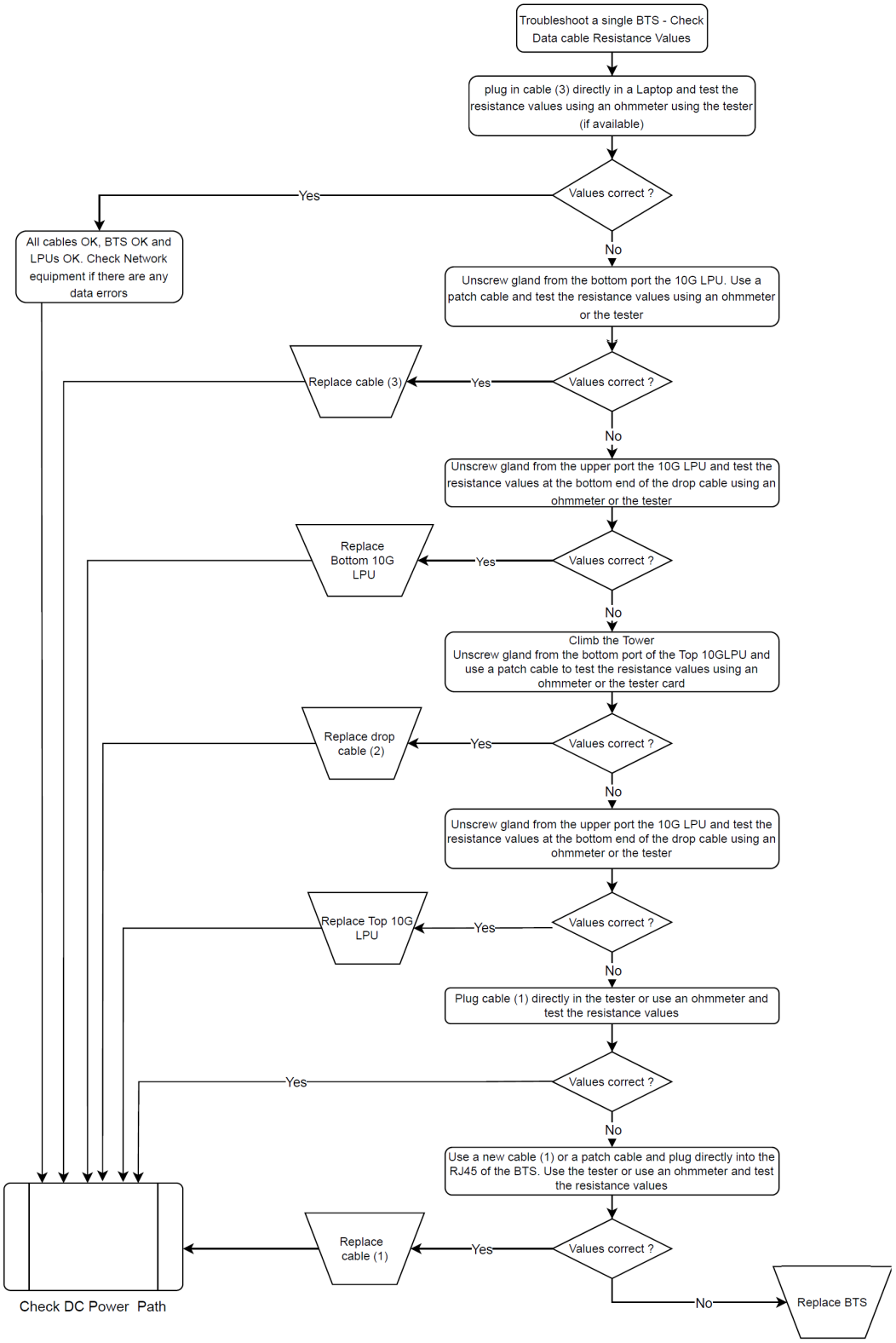


Figure 63 shows the flow chart to check the resistance for the BTS data cable.

Note

The cable numbering in Figure 63 (for example, cable 3) is used with reference to Figure 55 (for better understanding).

Figure 63: *BTS Data cable - Resistance checking*



How to hardware reset a BTS to factory default?

If the BTS fails in a field (site) and if it is not possible to access the BTS using the web interface due to loss of IP address or other reasons, then you must execute a process to recover the BTS. The process offers several options on which part of the configuration can be kept or the entire BTS can be reset to factory defaults.

To reset the BTS to factory defaults, perform the following steps:

1. Execute a short power cycle of the BTS. At the power source, you must do a simultaneous power OFF and power ON.

2. Using a PC, open a web browser and access the default IP address `192.254.1.1` to view the **Radio Recovery Console** page of the BTS (for example, as shown in Figure 64).

   Figure 64: *The Radio Recovery Console page - BTS*

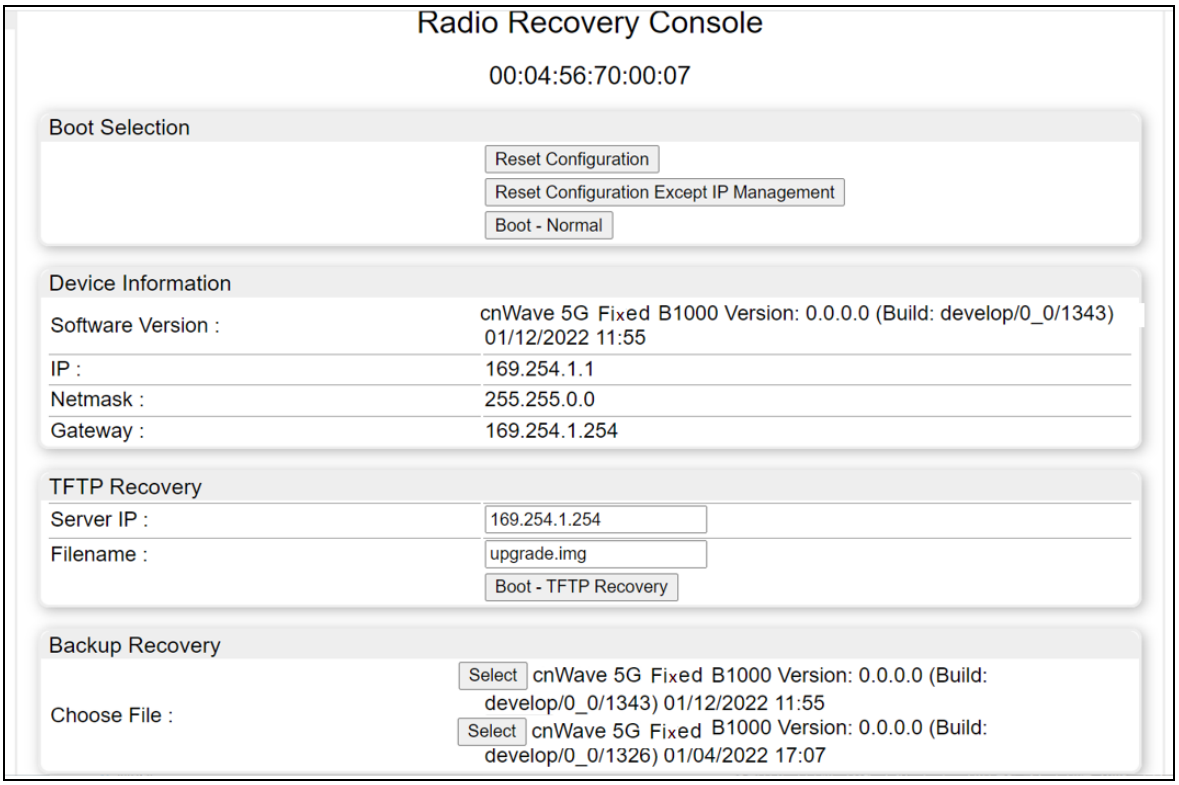


Table 9 lists and describes the parameters required for resetting the BTS to factory defaults.

Table 9: Parameters in the Radio Recovery Console page for BTS

Parameter	Description
Boot Selection	
Reset Configuration	Resets the entire BTS configuration back to default settings. This implies that you must reconfigure all the parameters for the BTS, including the IP address. **Note**: This is an option that you can use in case of loss of the IP address.

Parameter	Description
Reset Configuration Except IP Management	Resets the BTS configuration parameters except for the IP address. This is an option that can be used to reconfigure a BTS from scratch, but it will not reset the IP address. Therefore, you can use the web interface or SNMP to replay a saved configuration if needed. When you select this option, the **Radio Recover Console** page appears with the following details: • Default Mode - Keep IP Management • BTS rebooting information
Boot - Normal	An option, which is equivalent to a normal booting process and keeps all the configurations unchanged.
TFTP Recovery	
Server IP	Indicates the IP address of a TFTP server that must be installed and executed for the BTS. This configuration enables the BTS to use the image file uploaded in the **Filename** parameter for booting the BTS. To complete the action, you must click **Boot – TFTP Recovery**. This option can be used if the BTS image has been corrupted and cannot therefore start the application. **Note**: The image that is loaded using the **Filename** parameter must be the one stored in the TFTP directory. You must always keep a copy of the operating software in that directory.
Backup Recovery	
Choose File	An option used to reload one of the two BTS images available to restart the BTS.

How to hardware reset a CPE to factory default?

If the CPE fails in a field (site) and if it is not possible to access the CPE using the web interface due to loss of IP address or any reason, then you must execute a process to recover the CPE. The process offers several options on which part of the configuration can be kept or the entire CPE can be reset to factory defaults.

Note

The CPE also gets its IP address from the Radius Server. Therefore, the IP address must be available in the Radius Server.

To reset the CPE to factory defaults, perform the following steps:

1. Execute a short power cycle of the CPE. At the power source, you must do a simultaneous power OFF and power ON.

2. Using a PC, open a web browser and access the default IP address `192.254.1.1` to view the **Radio Recovery Console** page for the CPE (for example, as shown in Figure 65).

Figure 65: *The Radio Recovery Console page - CPE*

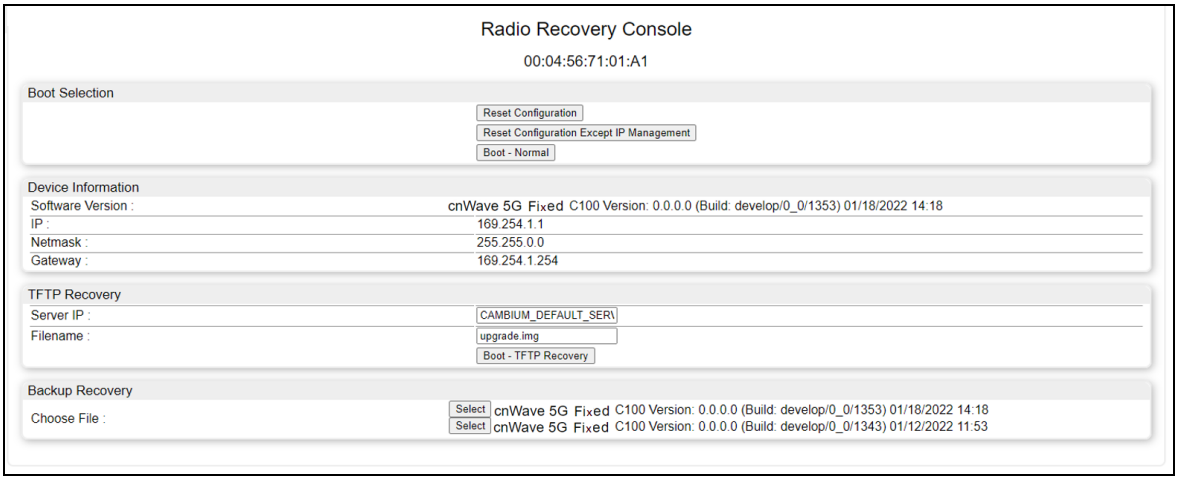


Table 10 lists and describes the parameters required for resetting the CPE to factory defaults.

Table 10: Parameters in the Recovery Image Console page for CPE

Parameter	Description
Boot Selection	
Reset Configuration	Resets the entire CPE configuration back to default settings. This implies that you must reconfigure all the parameters for the CPE, including the IP address. **Note**: This is an option that you can use in case of loss of the IP address.
Reset Configuration Except IP Management	Resets the CPE configuration parameters except for the IP address. This is an option that can be used to reconfigure a CPE from scratch, but it will not reset the IP address. Therefore, you can use the web interface or SNMP to replay a saved configuration if needed. When you select this option, the **Radio Recover Console** page appears with the following details: • Default Mode - Keep IP Management • CPE Reboot information
Boot - Normal	An option, which is equivalent to a normal booting process and keeps all the configurations unchanged.
TFTP Recovery	
Server IP	Indicates the IP address of a TFTP server that must be installed and executed for the CPE. This configuration enables the CPE to use the image file uploaded in the **Filename** parameter for booting the CPE.

Parameter	Description
	To complete the action, you must click **Boot – TFTP Recovery**. This option can be used if the CPE image has been corrupted and cannot therefore start the application. **Note**: The image that is loaded using the **Filename** parameter must be the one stored in the TFTP directory. You must always keep a copy of the operating software in that directory.
Backup Recovery	
Choose File	An option used to reload one of the two CPE images available to restart the CPE.

Appendix 1: Sensitivity Figures for All Bandwidths

This topic lists the sensitivity figures (in dB) for all uplink and downlink bandwidths for cnWave 5G Fixed products.

BTS

Sensitivity figures for 50MHz uplink:

Table 11: 50MHz Uplink (BTS)

MCS	H (Average across all frequencies)	V (Average across all frequencies)
MCS-22 / CW-10	-85.0	-84.6
MCS-20 / CW-9	-86.7	-86.3
MCS-18 / CW-8	-89.8	-89.5
MCS-16 / CW-7	-91.1	-90.6
MCS-13 / CW-6	-92.7	-92.3
MCS-11 / CW-5	-96.7	-96.4
MCS-9 / CW-4	-97.7	-97.4
MCS-7 / CW-3	-100.0	-99.5
MCS-4 / CW-2	-104.7	-104.5

Sensitivity figures for 56MHz uplink:

Table 12: 56MHz Uplink (BTS)

MCS	H (Average across all frequencies)	V (Average across all frequencies)
MCS-22 / CW-11	-84.8	-84.4
MCS-20 / CW-10	-86.4	-85.9
MCS-18 / CW-9	-89.1	-88.6
MCS-16 / CW-8	-90.6	-90.2
MCS-14 / CW-7	-91.7	-91.1
MCS-12 / CW-6	-94.5	-93.9
MCS-10 / CW-5	-96.7	-96.3
MCS-8 / CW-4	-97.9	-97.4
MCS-6 / CW-3	-103.8	-103.6

Sensitivity figures for 100MHz uplink:

Table 13: 100MHz Uplink (BTS)

MCS	H (Average across all frequencies)	V (Average across all frequencies)
MCS-22 / CW-20	-82.4	-82.2
MCS-21 / CW-19	-83.2	-82.8
MCS-20 / CW-18	-84.1	-83.7
MCS-19 / CW-17	-85.3	-84.9
MCS-18 / CW-16	-87.4	-87.2
MCS-17 / CW-15	-88.3	-88.0
MCS-16 / CW-14	-88.8	-88.6
MCS-15 / CW-13	-89.4	-88.8
MCS-13 / CW-12	-90.0	-89.6
MCS-12 / CW-11	-91.8	-91.3
MCS-11 / CW-10	-94.3	-94.1
MCS-10 / CW-9	-94.7	-94.7
MCS-9 / CW-8	-95.6	-95.0
MCS-8 / CW-7	-96.0	-95.6
MCS-7 / CW-6	-97.7	-97.5
MCS-6 / CW-5	-102.7	-102.4

Sensitivity figures for 112MHz uplink:

Table 14: 112MHz Uplink (BTS)

MCS	H (Average across all frequencies)	V (Average across all frequencies)
MCS-23 / CW-23	-81.6	-81.2
MCS-22 / CW-22	-82.3	-81.9
MCS-21 / CW-21	-82.8	-82.5
MCS-20 / CW-20	-83.6	-83.2
MCS-19 / CW-19	-84.6	-84.3
MCS-18 / CW-18	-86.5	-86.0
MCS-17 / CW-17	-87.7	-87.2
MCS-16 / CW-16	-88.1	-87.8
MCS-15 / CW-15	-88.6	-88.2
MCS-14 / CW-14	-89.1	-88.7
MCS-13 / CW-13	-89.8	-89.4

MCS	H (Average across all frequencies)	V (Average across all frequencies)
MCS-12 / CW-12	-92.0	-91.4
MCS-11 / CW-11	-93.9	-93.4
MCS-10 / CW-10	-94.6	-94.1
MCS-9 / CW-9	-94.9	-94.4
MCS-8 / CW-8	-95.4	-94.9
MCS-7 / CW-7	-96.4	-96.0
MCS-6 / CW-6	-101.0	-101.0

CPE

Sensitivity figures for 50MHz downlink:

Table 15: 50MHz Downlink (CPE)

MCS	H (Average across all frequencies)	V (Average across all frequencies)
MCS-22 / CW-10	-61.0	-60.3
MCS-20 / CW-9	-62.6	-62.4
MCS-18 / CW-8	-63.6	-63.6
MCS-16 / CW-7	-66.8	-65.6
MCS-13 / CW-6	-69.4	-68.7
MCS-11 / CW-5	-71.2	-70.4
MCS-9 / CW-4	-73.7	-73.0
MCS-7 / CW-3	-75.2	-74.8
MCS-4 / CW-2	-77.3	-77.6

Sensitivity figures for 56MHz downlink:

Table 16: 56MHz Downlink (CPE)

MCS	H (Average across all frequencies)	V (Average across all frequencies)
MCS-24 / CW-12	-59.3	-58.8
MCS-22 / CW-11	-61.4	-60.7
MCS-20 / CW-10	-62.8	-62.2
MCS-18 / CW-9	-64.2	-63.4
MCS-16 / CW-8	-66.1	-65.0
MCS-14 / CW-7	-68.5	-67.9
MCS-12 / CW-6	-69.8	-69.1

MCS	H (Average across all frequencies)	V (Average across all frequencies)
MCS-10 / CW-5	-72.4	-71.1
MCS-8 / CW-4	-74.2	-73.6
MCS-6 / CW-3	-76.3	-76.3

Sensitivity figures for 100MHz downlink:

Table 17: 100MHz Downlink (CPE)

MCS	H (Average across all frequencies)	V (Average across all frequencies)
MCS-22 / CW-20	-57.8	-57.3
MCS-21 / CW-19	-59.2	-58.7
MCS-20 / CW-18	-60.1	-59.8
MCS-19 / CW-17	-60.6	-60.7
MCS-18 / CW-16	-62.0	-61.4
MCS-17 / CW-15	-62.4	-62.0
MCS-16 / CW-14	-63.8	-63.0
MCS-15 / CW-13	-64.9	-64.3
MCS-13 / CW-12	-66.6	-66.0
MCS-12 / CW-11	-67.3	-67.2
MCS-11 / CW-10	-68.2	-67.8
MCS-10 / CW-9	-68.9	-68.4
MCS-9 / CW-8	-69.8	-69.6
MCS-8 / CW-7	-70.6	-70.3
MCS-7 / CW-6	-70.6	-70.8
MCS-6 / CW-5	-73.9	-74.2

Sensitivity figures for 112MHz downlink:

Table 18: 112MHz Downlink (CPE)

MCS	H (Average across all frequencies)	V (Average across all frequencies)
MCS-23 / CW-23	-56.6	-56.2
MCS-22 / CW-22	-57.8	-57.2
MCS-21 / CW-21	-58.9	-58.5
MCS-20 / CW-20	-60.0	-59.6
MCS-19 / CW-19	-60.7	-60.2
MCS-18 / CW-18	-61.7	-61.2

MCS	H (Average across all frequencies)	V (Average across all frequencies)
MCS-17 / CW-17	-61.8	-61.5
MCS-16 / CW-16	-62.4	-61.9
MCS-15 / CW-15	-63.8	-63.1
MCS-14 / CW-14	-65.4	-64.5
MCS-13 / CW-13	-66.7	-65.6
MCS-12 / CW-12	-66.9	-66.4
MCS-11 / CW-11	-67.7	-67.2
MCS-10 / CW-10	-68.2	-68.0
MCS-9 / CW-9	-68.5	-68.6
MCS-8 / CW-8	-68.7	-69.0
MCS-7 / CW-7	-68.6	-69.1
MCS-6 / CW-6	-73.3	-72.4

Appendix 2: Acronyms and Abbreviations

Table 19 lists the terms that are used in this guide.

Table 19: List of acronyms and abbreviations

Term	Definition
5G NR	5G New Radio (From Release 15, the 3GPP consortium refers to the air interface as 5G New Radio)
BTS	Base Transceiver Station
C-RNTI	Call-Radio Network Temporary Identifier
CIR	Committed information rate
CPE	Customer Premise Equipment
dBm	Decibel relative to a milliwatt
DNS	Domain Name System
DL	Downlink
EIRP	Effective Isotropic Radiated Power
ESN	Electronic Serial Number
EVM	Error Vector Magnitude
GHz	Gigahertz
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
LoS	Line of Sight
LPU	Lightning Protection Unit
MAC	Media access control
MCS	Modulation and Coding Scheme
MHz	megahertz
MU-MIMO	Multi- user multi-input-multi-output (MU-MIMO)
ms	Millisecond
MSN	Mechanical Serial Number
NTP	Network Time Protocol
OFDMA	Orthogonal Frequency Division Multiple Access
ODU	Outdoor Unit
PC	Personal computer
PDCCH	Physical Downlink Control Channel
PMP	Point-to-MultiPoint

Term	Definition
POC	Proof of Concept
PoE	Power over Ethernet
PPS	Pulse Per Second
PSU	Power Supply Unit
QAM	Quadrature Amplitude Modulation
QoS	Quality of Service
QPSK	Quadrature Phase Shift Keying
RF	Radio Frequency
RADIUS	Remote Authentication Dial-In Service
RSSI	Receiver Signal Strength Indication
RACH	Random Access Channel
SFP	Small form-factor pluggable (transceiver)
SIM	Subscriber Identification Module
SI-RNTI	System Information-Radio Network Temporary Identifier
SNR	Signal-to-Noise Ratio
SKU	Stock Keeping Unit
SNMP	Simple Network Management Protocol
TDD	Time Division Duplexing
UI	User Interface
UL	Uplink
VLAN	Virtual Local Area Network

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 Configuration 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™

www.cambiumnetworks.com