G1 Administration Guide

18-0028-001 rev 1.3

September 6, 2024

Table of Contents

Supported Releases

This guide supports these current G1 and G6 models:

Model	Supported Hardware
RN 5GHz	G1RN5ASI002, G1RN5ASI012, G1RN5ASI012
RN CBRS (Cat B)	G1RN3ASI001, G1RN3ASI011
BN 5GHz	G1BN5ASI002
BN CBRS (Cat B)	G1BN3ASI001
RN 6GHz	G1RN6AHB012
BN 6GHz	G1BN6ASI002

Intended Audience

This document is intended for system administrators and engineers interested in the design, daily management, operations, and troubleshooting of Tarana G1 networks including base nodes, remote nodes, and Tarana Cloud Suite (TCS).

To benefit from this document, the reader must have a good working knowledge of radio frequency (RF), wireless systems, and networking concepts.

G1 products are designed to be installed and used by trained professionals and require that such professionals adhere to all relevant regulatory, safety, and telecom industry best practice guidelines for outdoor radios. This document assumes that the Tarana G1 base node and remote nodes are installed onsite and are connected to TCS.

NOTE

The release version for TCS is now simply the date in yyyy-mm-dd format, which is the actual date that the version was released. The publication date of the release notes is also provided. Revisions of the release notes for a particular version have an updated publication date and revision number, but an unchanged version.

Documentation and Support

For information about base node installation, see the Base Node Installation Guide:

- https://www.taranawireless.com/bn_manual

For information about remote node installation, refer to the Remote Node Installation Guide:

- https://www.taranawireless.com/rn_manual

For information about using the Tarana mobile app to install remote nodes, refer to the relevant version of the Mobile Installation App Guide:

- https://support.taranawireless.com/s/global-search/ig-mobileapp

For information about network planning, refer to the Network Planning and Deployment Guide:

- https://support.taranawireless.com/s/article/Network-Planning-and-Deployment-Guide

To view or search additional support resources, or to open a support ticket, visit the Tarana Support site:

- https://support.taranawireless.com/

G1 Network Architecture

The G1 network architecture consists of the following elements:

- Tarana Base Node (BN): Base nodes are deployed at the site tower, elevated to provide coverage and line-of-sight advantages to remote nodes.
- Tarana Remote Node (RN): Remote nodes are deployed at the subscriber site and do not require line-of-sight coverage from the base node.
- Tarana Cloud Suite (TCS): TCS is the cloud-based management and monitoring platform. Because it is cloud-based, administrators can access it from any Internet-connected device.
- Tarana API: Administrators can use APIs to access TCS data and make it available to third-party portals and support systems.

Planning and deploying a Tarana G1 network is straightforward. When you connect base nodes to power and a backhaul path, they automatically contact and register with the TCS management platform over an encrypted connection. With a frequency reuse of 1, you can install multiple base nodes on the same frequency in an array formation (referred to as a cell). A collection of cells at a single location is called a site. There can be multiple cells at a site. When operating in a licensed spectrum, deploying a single-channel cell can reduce licensing fees.

When you connect a remote node to a power source, it automatically finds the base node with the best link quality and generates a list of alternate base nodes within range, called a neighbor list. After discovering and connecting to the appropriate base node, the remote node uses beamforming to optimize its signal path to its associated base node. Beamforming creates a main RF lobe that points toward the receiving antenna and creates RF nulls in the direction of interference sources. Interference sources can include self-interference from the operator's equipment or other nearby devices. After the remote node and base node adjust the RF link power and signal, the remote node registers and authenticates with the network.

After you deploy the base and remote node, the pair monitor and adjust the link parameters to maintain a high quality link in both directions while rejecting interference from interference sources.

When you deploy a single base node, it can support up to 256 concurrent remote node connections. When you deploy a cell of four base nodes, the cell can support up to 1024 remote nodes distributed evenly at 250 per base node.

For more information on planning and deployment, see the Network Planning and Deployment Guide.

Tarana Cloud Suite (TCS) Overview

The Tarana Cloud Suite (TCS) is a cloud-hosted system to monitor, manage, and troubleshoot Tarana base nodes and remote nodes. TCS makes it easy to plan, install, provision, and manage Tarana radio network infrastructure. TCS provides network management, business operations, and control-plane functions. As a cloud-based offering, TCS takes advantage of cloud architecture, including high availability and redundancy, data security, and auto (cloud) scaling.

TCS supports multiple levels of access and privilege that allow operators to manage business operations.

The TCS northbound interfaces connect to the operator's OSS / BSS systems through APIs for tight integration with existing infrastructure and maximum flexibility.

Log In To TCS

Chrome is the supported and tested browser for TCS.

1. From a laptop with internet connectivity, open a tab in Chrome:
   For 5 GHz and 6 GHz, use https://cloud.taranawireless.com.
   For 3 GHz devices, use https://portal.trial.cloud.taranawireless.com.
2. Enter the username and password provided by the TCS system administrator.

If you have only 3 GHz (CBRS) currently deployed, use https://portal.trial.cloud.taranawireless.com.

If you have deployed both 5 GHz and 3 GHz (CBRS) devices, use https://portal.trial.cloud.taranawireless.com. It supports mixed mode (5 and 3 GHz devices) deployment.

If you haven't deployed any Tarana devices yet, 6 GHz devices are onboarded to https://portal.trial.cloud.taranawireless.com so you should use that URL.

Terms of Service

When a user logs in to TCS for the first time, TCS displays a link to the terms of service and asks the user to accept them. Once the user has done that, they see the default screen.

Existing users are prompted to accept the terms of service when their token expires.

User Roles

TCS allows secure user access and network management using a role-based access control (RBAC) approach. Each user role defines what the user is allowed to see and do from TCS. Three user roles are available:

- NOC L1 User: Network Operation Center Level 1. This role can view TCS display pages and can run diagnostic tests.
- NOC Operator: Network Operator. This role can view TCS pages and run diagnostic tests. It can use the Web UI interface and make configuration changes.
- OP Admin: Administrator. This role can view all TCS pages and perform all actions.

Menu items and functionality are different depending on the user role assigned to the account logged in to TCS.

These roles are defined as follows:

Action	NOC L1 User	NOC Operator	OP Admin
View Dashboard Page	Yes	Yes	Yes
View Map Page	Yes	Yes	Yes
View Performance Page	Yes	Yes	Yes
View Devices Page	Yes	Yes	Yes
View Alarms Page	Yes	Yes	Yes
View Events Page	Yes	Yes	Yes
View Single Device Pages	Yes	Yes	Yes
Edit Profile Information (Self)	Yes	Yes	Yes
Edit Profile Information (Others)	No	No	OP Admin can change only the name, phone number, and role. They can't change the email address. They can force a password reset but not set the password.
Upgrade software	No	Yes	Yes
Save Snapshots	No	Yes	Yes
Reboot Device	No	Yes	Yes
Create and Configure Networks	No	No	Yes
Add and Configure Network Policies	No	No	Yes
Add and Configure Users	No	No	Yes
Assign User Roles	No	No	Yes
Perform Speed Test	Yes	Yes	Yes
Perform DNS Lookup	Yes	Yes	Yes
Configure Installation Parameters	No	Yes	Yes
Configure Network Parameters	No	Yes	Yes

Action	NOC L1 User	NOC Operator	OP Admin
Configure Primary Base Node	No	Yes	Yes
Reset Telemetry Data	No	Yes	Yes
Use Device Web UI	No	Yes	Yes
View Performance Page	Yes	Yes	Yes
Add or Modify Device Notes	No	Yes	Yes
View Device Notes	Yes	Yes	Yes
Reconnect Device to Network	No	Yes	Yes

There are three user roles that support multi-tenancy for retailers. Roles and permissions are similar to existing TCS User Profiles and Roles. User roles for multi-tenancy are:

- **Retailer Viewer:** Read-only access to their devices (remote nodes)
- **Retailer Operator:** Both read and write access to their devices. This allows the user to make configuration changes, reboot a remote node, and upgrade software on their remote node.
- **Retailer Admin:** All the privileges as Retailer Operator plus the ability to add users for their organization (Retailer).

There is also a Radio Installer role for users who install remote nodes using Tarana's mobile app. This role had no access to anything on the TCS portal.

Login Security

TCS provides protection against brute force attacks with these features:

- Strong password rules.
- Users must change their password every 6 months.
- User is notified when an attempt is made to log in from a new device or location.
- User account is locked after multiple failed attempts.
- Accounts that are inactive for more than 90 days are automatically disabled. The OP Admin can re-activate them, if needed.
- Multi Factor Authentication is required.

MFA Support

TCS supports MFA (multi-factor authentication), an authentication process that implements additional layers of access security beyond the standard user name and password, and protects TCS from brute force attacks. The TCS MFA implementation includes the user name and password as the first layer, followed by a time-based one-time password (TOTP) method using commonly available authenticator apps, such as Google

Authenticator or Duo Mobile, which must be installed on a mobile devices beforehand, as the second layer.

Within TCS a user with Op Admin privileges can activate or deactivate MFA using Admin > User Management. Select **Enable MFA** in the upper left corner. This activates MFA for all users. By default, MFA is deactivated.

Admin events, visible only to OP Admin users, are generated for all MFA related events. This includes events where a user tries to log on using an incorrect MFA code.

After MFA is activated, the first time a user logs in they must follow these steps to map their device to TCS:

1. Enter username and password on TCS login screen.
2. TCS prompts the user to scan a QR code to implement MFA on a mobile device.
3. The QR code maps the user to their ID using the MFA app the user has installed, then pairs the app to TCS using a time-based one-time code (OTP).
4. TCS prompts the user to log in again using the username and password, plus the time-based one-time password.
5. TCS allows user access to the platform.

Once MFA is set up on the user's mobile device, they follow these steps to log in:

1. Enter username and password on TCS login screen.
2. Enter OTP from authenticator app on the mobile device.
3. TCS allows user access to the platform.

Activate MFA

To activate MFA, do the following:

1. Log in to TCS.
2. Navigate to **Admin > User Management**.
3. Select **Enable MFA** to activate the feature.
4. To acknowledge that you want to activate MFA for all users in the operator account, select **Yes**.

Deactivate MFA

To deactivate MFA, do the following:

1. Log in to TCS.
2. Navigate to **Admin > User Management**.
3. Clear **Enable MFA** to deactivate the feature.
4. To acknowledge that you want to deactivate MFA for all users in the operator account, select **Yes**.

If a user loses or changes their mobile device, the OP Admin must reset MFA for the user and the user must repeat the steps to pair their mobile device with MFA.

To reset MFA, do the following:

1. Log in to TCS.
2. Navigate to **Admin > User Management**.
3. Select the three dots by the user's table entry and select **Reset MFA**.

Single Sign-On With OAuth

For stronger login security, administrators can configure Single Sign-On with OAuth, which adds an option to log on with company credentials to the portal logon screen. The first time a user logs on with company credentials, they enter their corporate email and a password. The next time they use company credentials to log on, they enter email but don't need to enter the password.

To enable single sign on, the Operator Admin user must configure OAuth. Under Admin in the navigation pane, select **Login Security** (formerly User Management). You now see two tabs, User Management (the default) and Identity Provider.

On the Identity Provider tab, select **Add OAuth Configuration**.

Enter OIDC Parameters:

Client ID: Client ID you received from identity provider.

Client Secret: Client secret you received from identity provider.

Auth Scopes: Scopes to define which groups of user attributes (such as email) that you application will request from your provider. Email, OpenID, and Profile are included by default.

Domain Identifiers: Domain names supported for user federation.

Choose Attribute Request Method, **POST** or **GET**, depending upon what is supported by the IDP.

Set the OIDC endpoint by entering the Issuer URL, the base URL for the OIDC endpoint.

Configure Attribute Mapping between Tarana and your IDP:

Email: Standard attribute for user email.

Name: Standard attribute for user's display name.

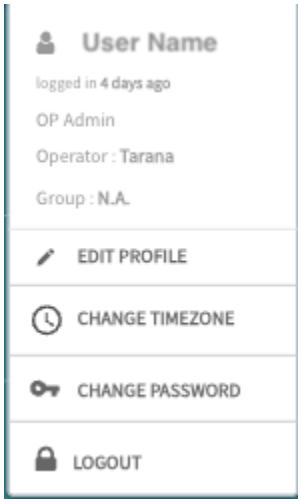
Roles: Custom attribute used to specify user roles or security groups.

Retailer ID: Custom attribute used only if retailer configuration exists.

If you want to use this feature and encounter any issues, contact Support for assistance.

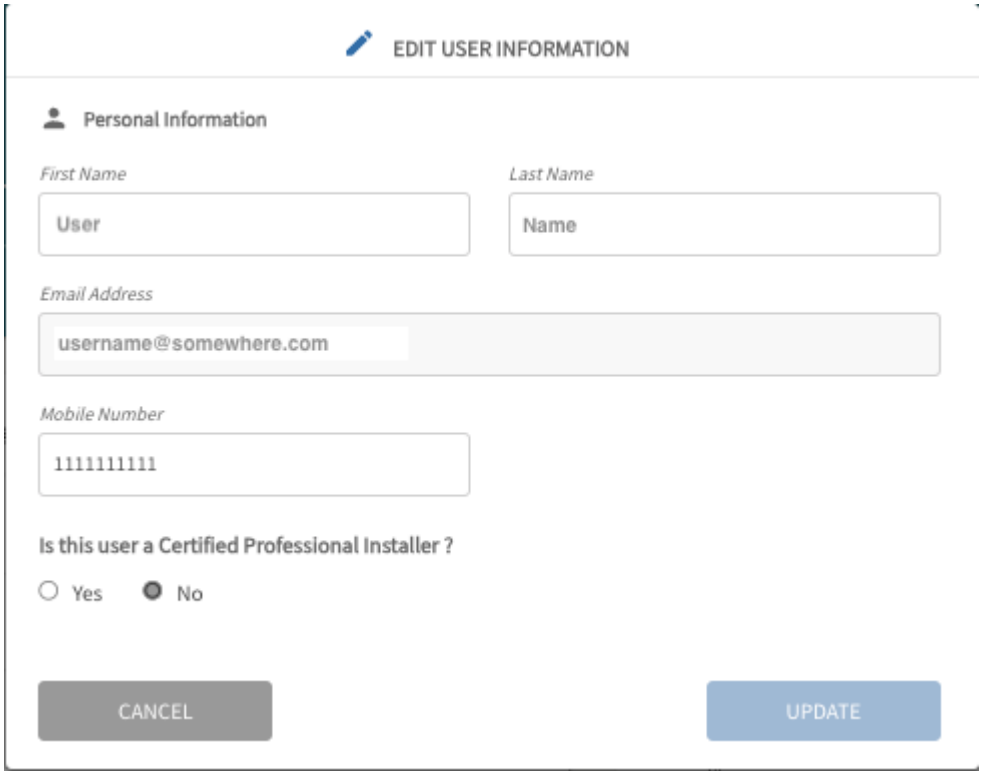
User Profile

Users can view and edit their profile information by selecting the **user profile icon** (E) at the top right of the dashboard. Users can change their own profile information, time zone, or password.



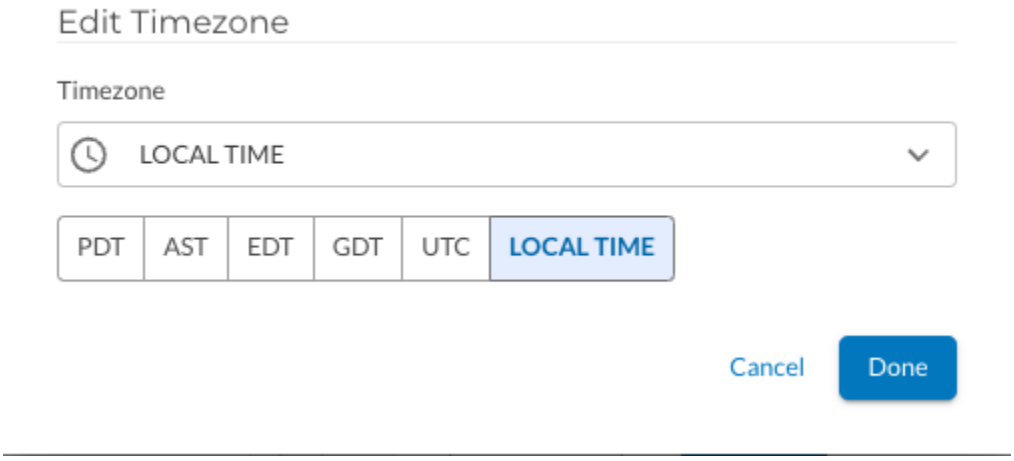
User Profile Information

To edit the profile, select **Edit Profile** and enter first name, last name, and mobile number. Select **Submit**. Users can't change their email address. If they need to change their email, an Admin must add a new account and delete the old one.



Edit User Information

To change the timezone, select **Change Timezone** and choose a new timezone from the dropdown or the list of timezones, then select **Done**. Local time is pulled from the time on the user's computer.

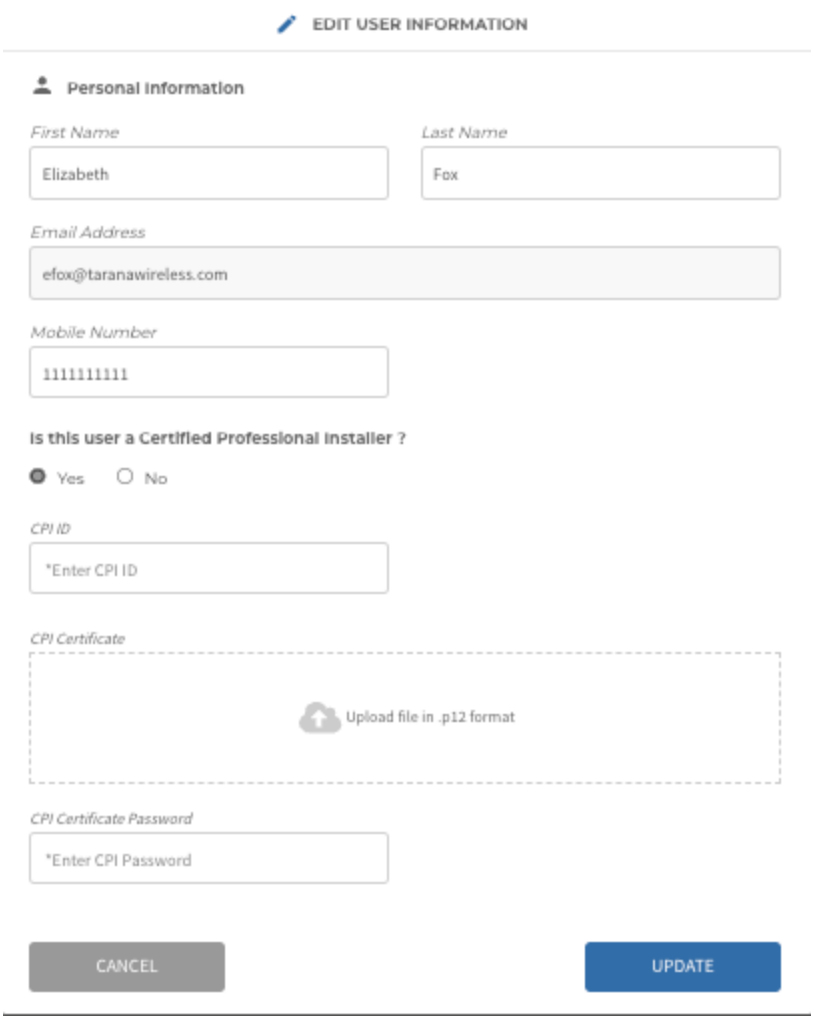


Edit Timezone

For CBRS installations, a certified professional installer (CPI) is required to sign off on the installation parameters.

To enter CPI credentials, users should follow these steps:

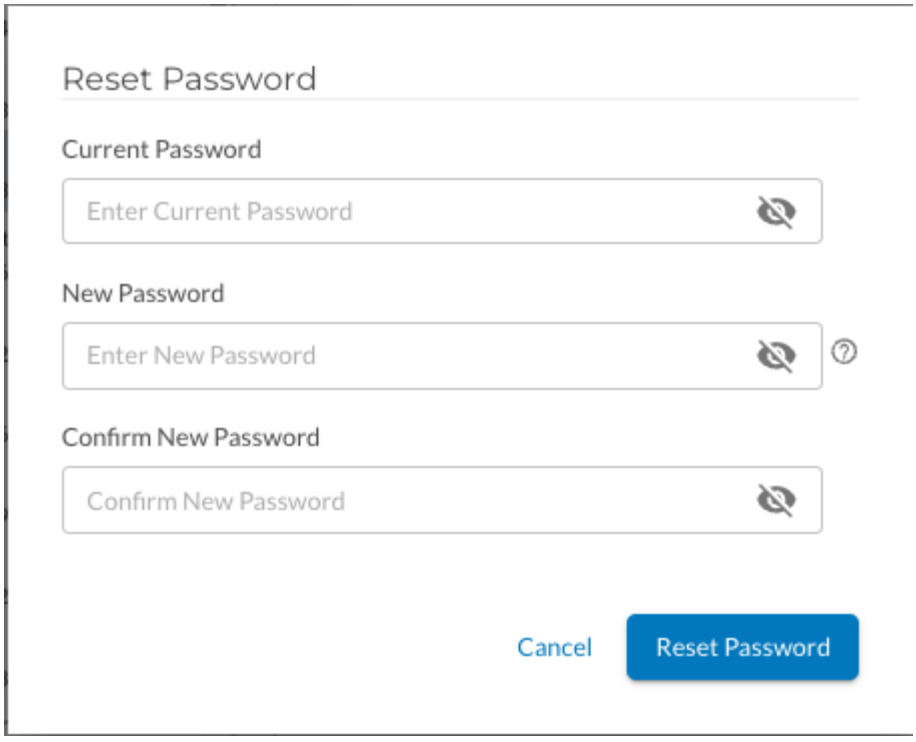
1. Log in to TCS.
2. Navigate to **User Profile** > **Edit Profile**.
3. Enter contact information in the Personal Information section. The first and last name must match the name in the CPI certificate.
4. Select **Yes** to indicate that the user is a certified professional installer.
5. Enter CPI ID.
6. Upload CPI certificate in .p12 format.
7. Enter CPI certificate password.
8. Select **Update**.



Enter CPI ID and Certificate

When an administrator removes a CPI from TCS, TCS retains the CPI credentials for existing CBRS installations that require it.

To change the user profile password, select **Change Password**. Enter the current password, then the new password. It must have at least 8 characters and include at least one number, one uppercase letter, one lowercase letter, and one special character. Select **Update Password**.



Change Password

Password Policy

TCS enforces the following password policy for all users:

- The password must contain between 8 and 40 characters.
- The password must be different from the previous five passwords.
- The password must be changed at least every six months.
- The password cannot contain whitespace characters.
- The password must contain at least one uppercase, one lowercase, one numerical, and one special character.
- The password cannot contain any of the following:
  - First name
  - Last name
  - User email address
  - White space
  - Alphabetical sequences five or more characters long
  - Numerical sequences five or more characters long

- QWERTY sequences five or more characters long

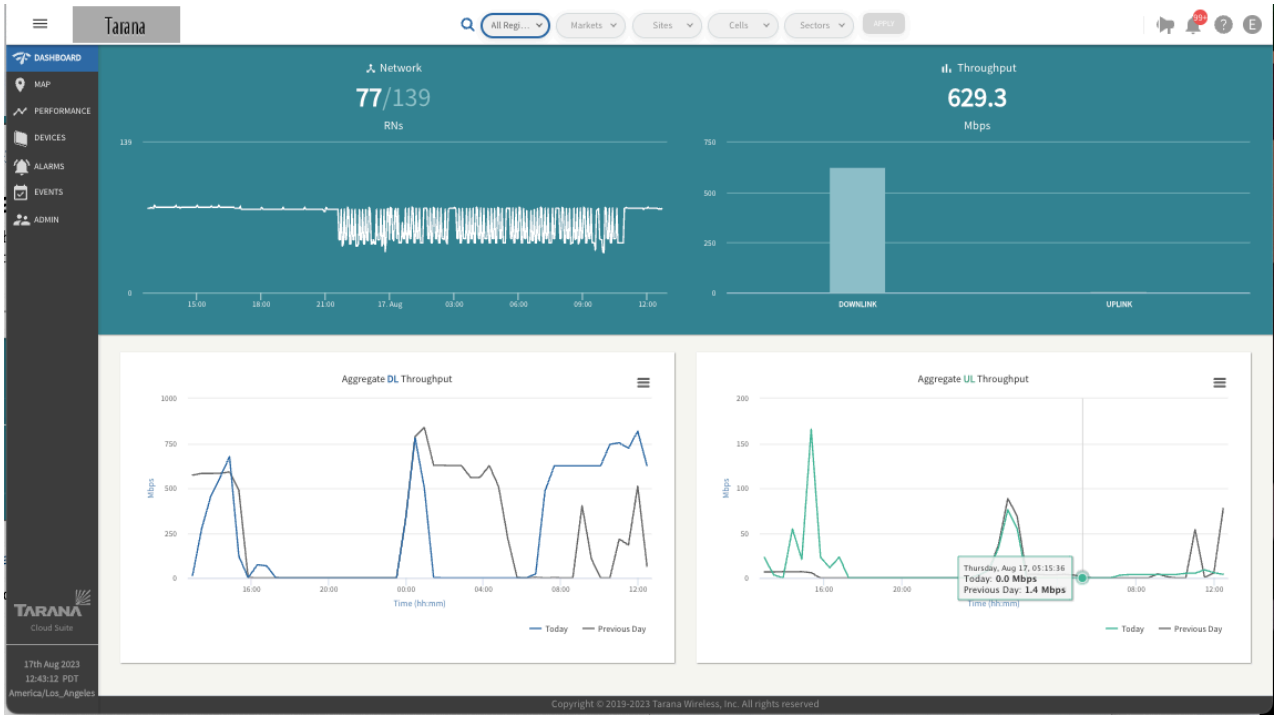
- Weak passwords commonly used on test or lab systems, such as Test@123 and Password@123 cannot be used, even if all other requirements are met.

Reset Password

To reset a forgotten password, go to the TCS login screen and select **Forgot Password ?**. Enter the email address of the account registered with TCS and select **Submit**. The system sends an email to this address with a one-time OTP verification code and a link to reset the password.

TCS Layout

TCS displays the dashboard after you log in. You see a high-level display of network performance and you can select various display options.



TCS Dashboard

The menu in the upper left shows or hides the navigation pane. The navigation pane on the left has these display options:

- **Dashboard:** Widgets containing information such as the number of remote nodes, real time throughput, and aggregate downlink and uplink throughput for the last 24 hours. Some widgets are interactive. Throughput in the upper right corner is in real time.
- **Map:** Devices displayed based on latitude and longitude values configured for each device. You can search for and select devices by hostname, IP address, or serial number.

A filter widget (first icon on the upper right hand corner) allows you to filter a range on 7 parameters.

- **Performance:** Customizable widget that shows KPIs (key performance indicators) such as downlink (DL) rate, uplink (UL) rate, number of active connections, DL capacity, and UL capacity, depending on how you have filtered network entities. You can compare KPIs on a single device or compare against other devices and overlay events across the same timespan and entities chosen. You can select the time domain to view a specific timespan of the view.
- **Devices:** Customizable table of devices showing important status, environment, and performance information. Base nodes and remote nodes are displayed in separate views. You can see either by selecting the appropriate device type.
- **Alarms:** Device and system alarm information, categorized by device type (base node, remote node, or TCS), criticality (critical, major, minor, or warning), or system (operational, equipment, communication, QoS, security, or environmental). You can view and filter the table of all alarms.
- **Events:** Table of events, filterable by event type (network, alarm, operations, spectrum, or other). Admin events track user activity.
- **Admin:** Configuration landing page that you use to add or modify network entities in the network hierarchy, alerts, user accounts, and webhooks. You can also view software inventory.

At the top right side of the dashboard are four icons:

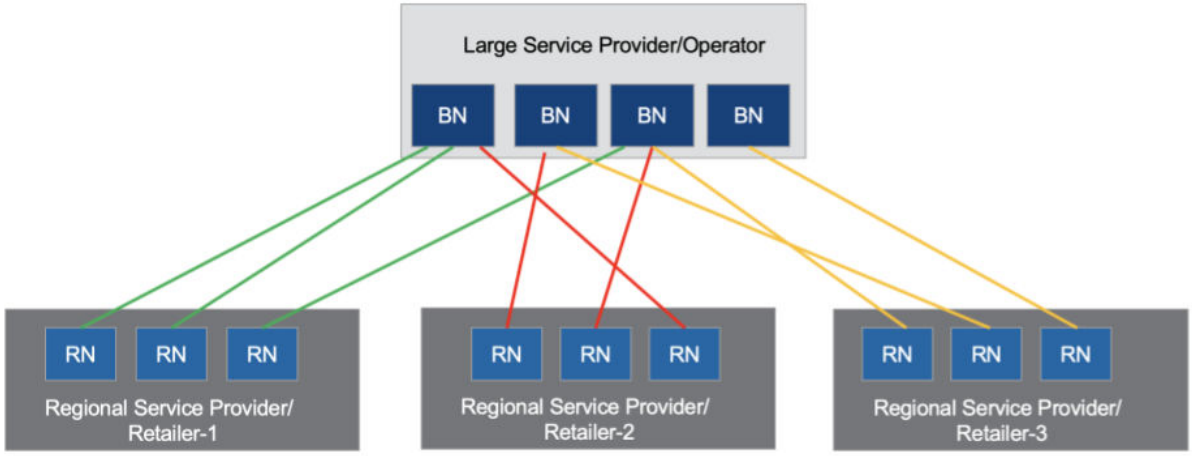
Notification, Alarm, Support, User Profile icons

- Notifications ( ): Links to recent release notes. If there are new unread release notes, you also see this badge:
- Alarms ( ): Number of active alarms. If there are new alarms, you see a red circle with the number of alarms: 22+. Selecting the icon shows a popup with the number of alarms for each criticality. These are hyperlinks that take you to the alarms page with those alarms filtered.
- Support ( ): Opens Tarana support page in a new tab.
- User Profile ( ): Access to user account information. The User Profile icon is a colored circle that shows the user's first initial. For more about managing a user account, see User Profile (page 16).

Multi-Tenant Support for Retailers

Large service providers (SPs) can deploy and own the network infrastructure down to the base node level and allow different retailers to acquire subscribers. Those retailers can then install and manage their own remote nodes associated to the service provider base node. In this application:

- Base nodes are owned and operated by a large service provider. Each base node may have connected remote nodes belonging to different retailers.
- Retailers are smaller regional service providers providing internet service to their subscribers.
  - Remote nodes are owned and operated by these regional service providers / retailers.
  - Remote nodes from different retailers may connect to the same base node.



Large Service Provider / Operator

This feature applies only to operators that run wholesale networks. To discuss implementing this feature, contact your Tarana representative.

Sectors (base nodes and connected remote nodes) can be shared across multiple retailers; that is, the remote nodes connected to a base node may not all belong to the same retailer. The base node is owned by the large service provider (using its operator id and default retailer id), while remote nodes have their own retailer ids (but use the operator id of the large service provider).

Retailers need to be able to manage their respective remote nodes and have read-only visibility of the base nodes their remote nodes are associated to in the network.

- Large service providers configure and manage the TCS hierarchy and their base nodes.
- Retailer operators provision and manage the remote nodes in their own network.

- Base nodes that belong to the large service provider are visible to retailers, with limited information. Retailer users can't perform any device operations, such as rebooting a base node, making configuration changes, or performing software upgrades.
- A Northbound API supports adding remote nodes under a specific Retailer:
  For 5 GHz and 6 GHz devices: https://portal.cloud.taranawireless.com/northbound/swagger-ui.html
- For 3 GHz devices: https://portal.trial.cloud.taranawireless.com/northbound/swagger-ui.html

A remote node's configuration includes a Retailer Name parameter, shown in the Device view under Planning Metrics.

Three user roles support multi-tenancy for retailers. A user with OP Admin rights can add and define new user accounts by going to Admin and selecting User Management. Roles and permissions are similar to existing TCS User Profiles and Roles (page 12). User roles for multi-tenancy are:

- **Retailer Viewer:** Read-only access to their devices (remote nodes)
- **Retailer Operator:** Both read and write access to their devices. This allows the user to make configuration changes, reboot a remote node, and upgrade software on their remote node.
- **Retailer Admin:** All the privileges as Retailer Operator plus the ability to add users for their organization (Retailer).

Each of these user roles has limited read-only access to the base nodes associated to their remote nodes.

For this feature, Tarana adds Retailers on behalf of the large service provider operators with wholesale networks. The operator is then able to assign remote nodes under those retailers using a BULK PATCH API. See Swagger API Documentation (page 135) for details.

Network Entities Overview

A Tarana G1 network may include thousands of devices: up to 250 remote nodes per base node (1000 per cell). Deployed devices are grouped in TCS under various entities. In general, these entities pertain to the geography of deployments. Each entity assigns particular attributes to all deployed devices within that group, from highest to lowest in hierarchy at the top of the dashboard.

Understanding the structure of network entities is vital because this is how TCS determines which devices or networks to display or operate on. If a network entity contains more than 2048 devices, TCS doesn't display them unless you filter at the next level down.

Network entities consist of this hierarchy, highest to lowest:

- Region
- Market
- Site
- Cell
- Sector

To add entities, go to the Admin > Network Configuration section of TCS. After you add each entity, you assign or edit related attributes, as needed.

See the Network Configuration (page 103) section for descriptions of these entities and information about configuring them. You must have OP Admin rights for configuration.

Region

A Region is a geographical area under the jurisdiction of a regulatory domain, such as the United States Federal Communication Commission (FCC). It can be an entire country or part of one, such as a state, province, or canton.

Market

A Market is an arbitrary area within a Region. It can include a city's metropolitan area, but that's not required.

Site

A Site is a single geographical point within a Market. This is typically a vertical asset such as a tower where a single base node or a base node cluster (multiple base nodes) are installed. A Market can contain numerous sites.

Cell

A Cell is an array of four base nodes that service a group of remote nodes within proximity to a Site. The 4 base nodes in the same cell must be on the same band, but they don't have to be on the same frequencies. There can be multiple cells at a single site if needed in a particularly dense deployment. Cells on the same tower should have a minimum vertical separation of 4 meters.

Multiple cells can exist at a single site. When you configure a base node, it uses a Planning ID with the format `<setID><cellID><sectorID>`. See Base Node Planning Metrics (page 62) for more information.

Sector

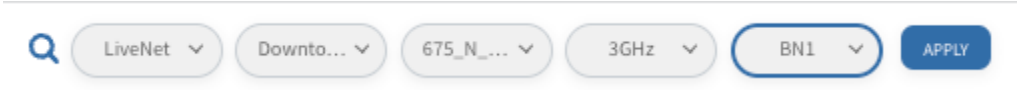
A Sector is an individual base node and all of its connected remote nodes, though a base node doesn't define a Sector. Use TCS to add a Sector as an abstract. This allows a base node and remote nodes to be swapped out of a Sector while the Sector name and attributes stay the same, though the actual hardware has changed. The Sector ID is set by TCS in the order that the Sector is created under a Cell. The first is 0, the second is 1, and so on. There can be up to four sectors per cell, so the sector ID has a range of 0 - 3.

Filter Network Entities

A Region can contain multiple Markets, Markets can include multiple Sites, and Cells can include multiple Sectors, depending on the specific deployment requirements. Each hierarchical entity assigns attributes to all deployed devices in the hierarchy beneath it.

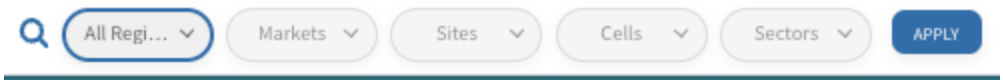
The drop-down menu selections at the top of the screen allow you to select a specific network entity based on Region, Market, Site, Cell, and Sector. Make a selection and select **Apply** to change the information displayed in any of the navigation page windows, except Admin.

To define the most granular filter for network devices, select individual entities from Region through Sector and select **Apply**.



Granular Filter of Network Entities

To define the least granular view, select **All Regions**. and select **Apply**.

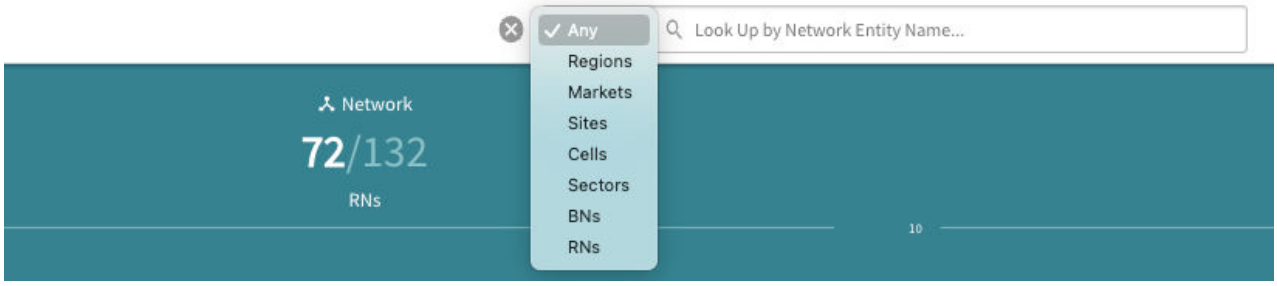


All Network Entities

NOTE
For any one network area, only 2048 entities can be shown. For a very large deployment, you may not be able to see all remote nodes under All Regions. You might need to add more granular filters.

Search Network Entities

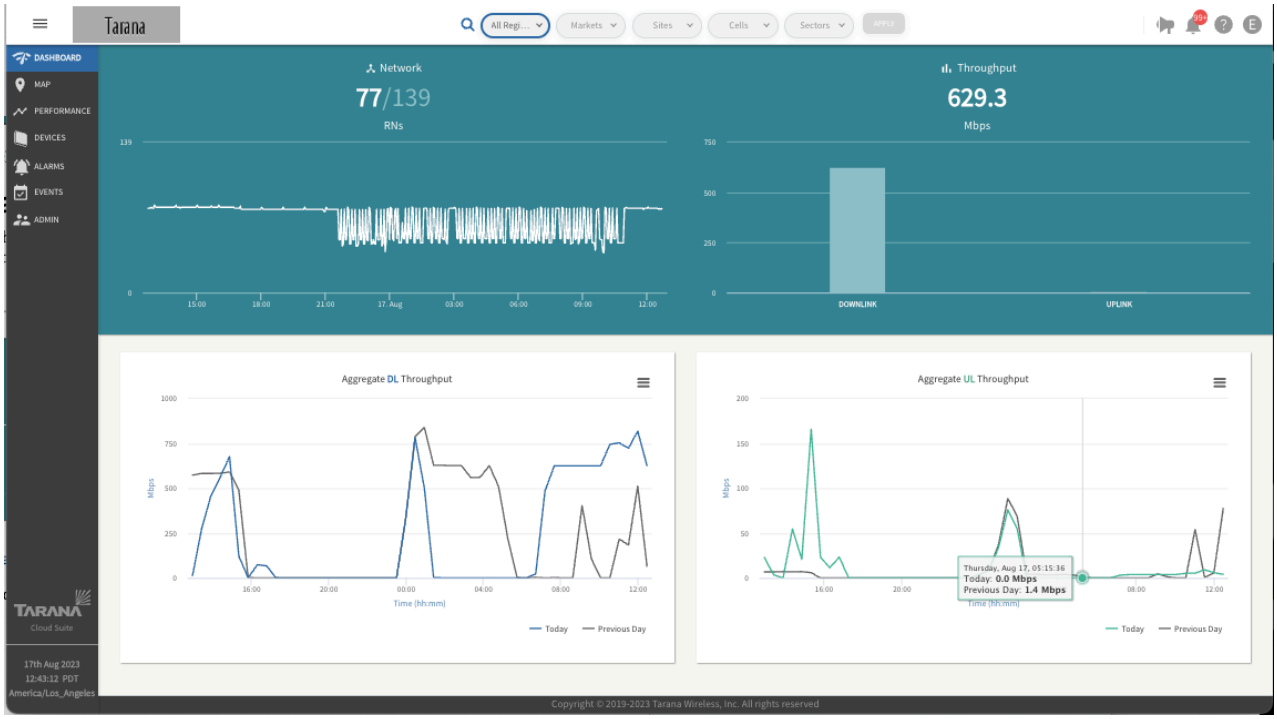
The global search option allows for a quick search based on network hierarchy name, device name, or serial number. Select the **Search** icon (🔍) to activate the global search bar. When you select any entity from the global search bar, it filters the network entities appropriately and this filter persists across any of the navigation page windows, except in Admin.



Global Search Bar

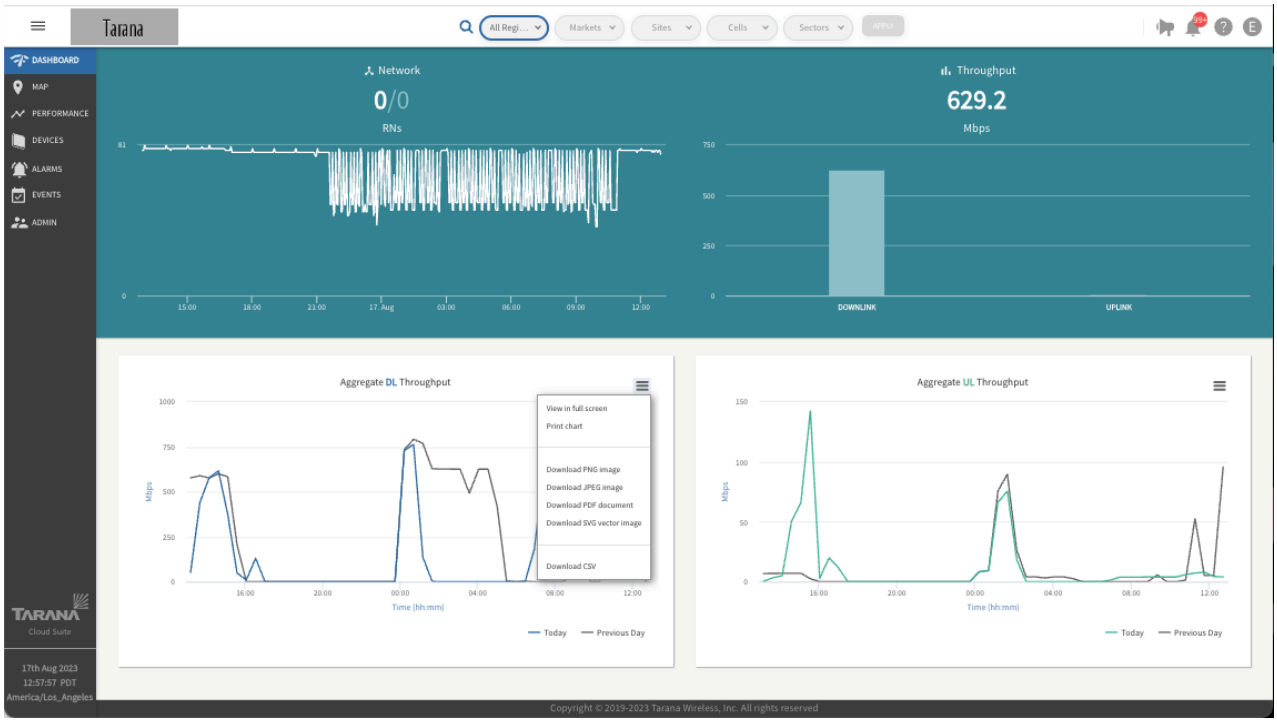
Dashboard

The dashboard is a high-level display of overall network performance. The top tiles display information about the network, like the number of devices connected or disconnected and throughput statistics. The bottom tiles display aggregate DL and UL throughput.



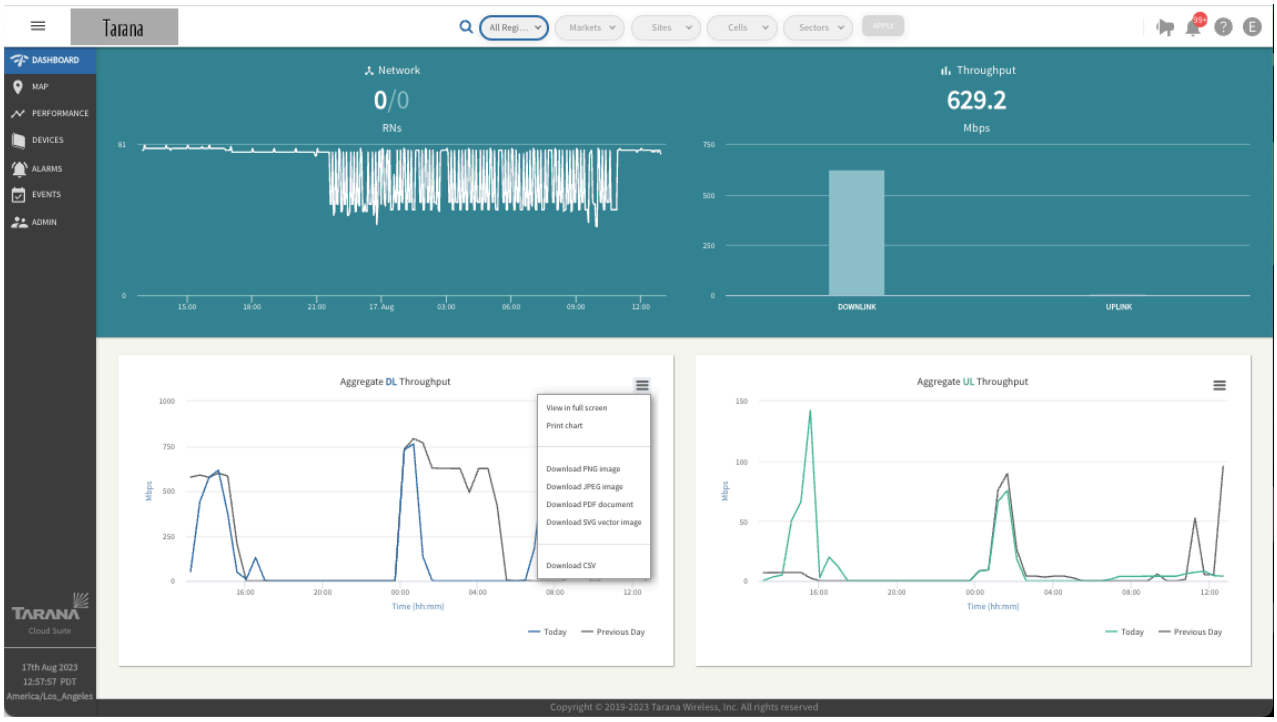
TCS Dashboard

Hover your cursor over each tile to display information about that specific data point.



Data Points

To view the data displayed on the individual tiles in full screen or to download the displayed data, select the chart context menu icon (☰) in the upper right corner of each information tile. You can download the data as PNG, JPEG, PDF, SVG, or CSV.



Download Dashboard Data

The DL Peak Throughput Distribution shown in the example above reflects actual throughput and not capacity.

Subscriber MAC Address Lookup

Remote nodes learn the MAC addresses that attach to the LAN port and report up to five subscriber MAC addresses to TCS. TCS allows you to search for subscriber devices by MAC address.

Operators can identify problematic traffic source, such as those involved in DDoS attacks, and then use the search function to identify the remote node and mitigate the problem. Likewise, if a subscriber reports traffic issues to the operator, the operator can use the MAC search function to begin troubleshooting and correcting the issue.

You can also search subscriber device MAC addresses using the Northbound API:

API Call: `/v1/network/radios/search`

To search for a subscriber device by MAC address, do the following:

1. Log in to TCS.
2. Select Search ( ) from the top network navigation bar.
3. Select either Any or Subscriber MAC from the drop-down list, and then enter the MAC address of the device you are trying to locate.

   NOTE
   The MAC address must be in colon-separated format:

   12:34:56:78:90:AB

   As you type, the look-ahead search begins to pre-populate results.
4. Select the matching result from the search results.

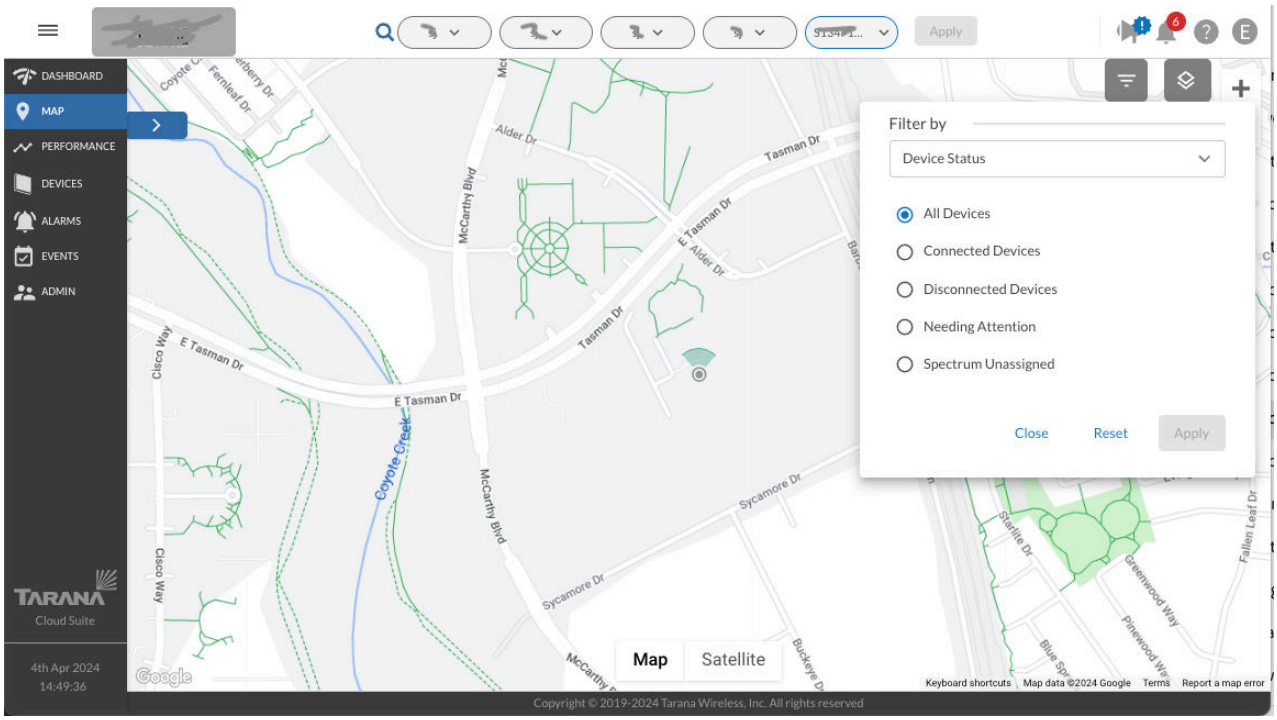
Map View

To display a map showing the location of each deployed Tarana device that appears in TCS and information about it, select **Map** in the left side navigation pane.

Make sure that you've chosen the correct network entity from the drop-down menus at the top. This filters the network down to the granularity you need. Because the menus are hierarchical, start by selecting the Region, then Market, Site, Cell, and Sector, as needed.

By default, any devices associated to this network are displayed on a street map. You can add terrain to the street view or switch to satellite view.

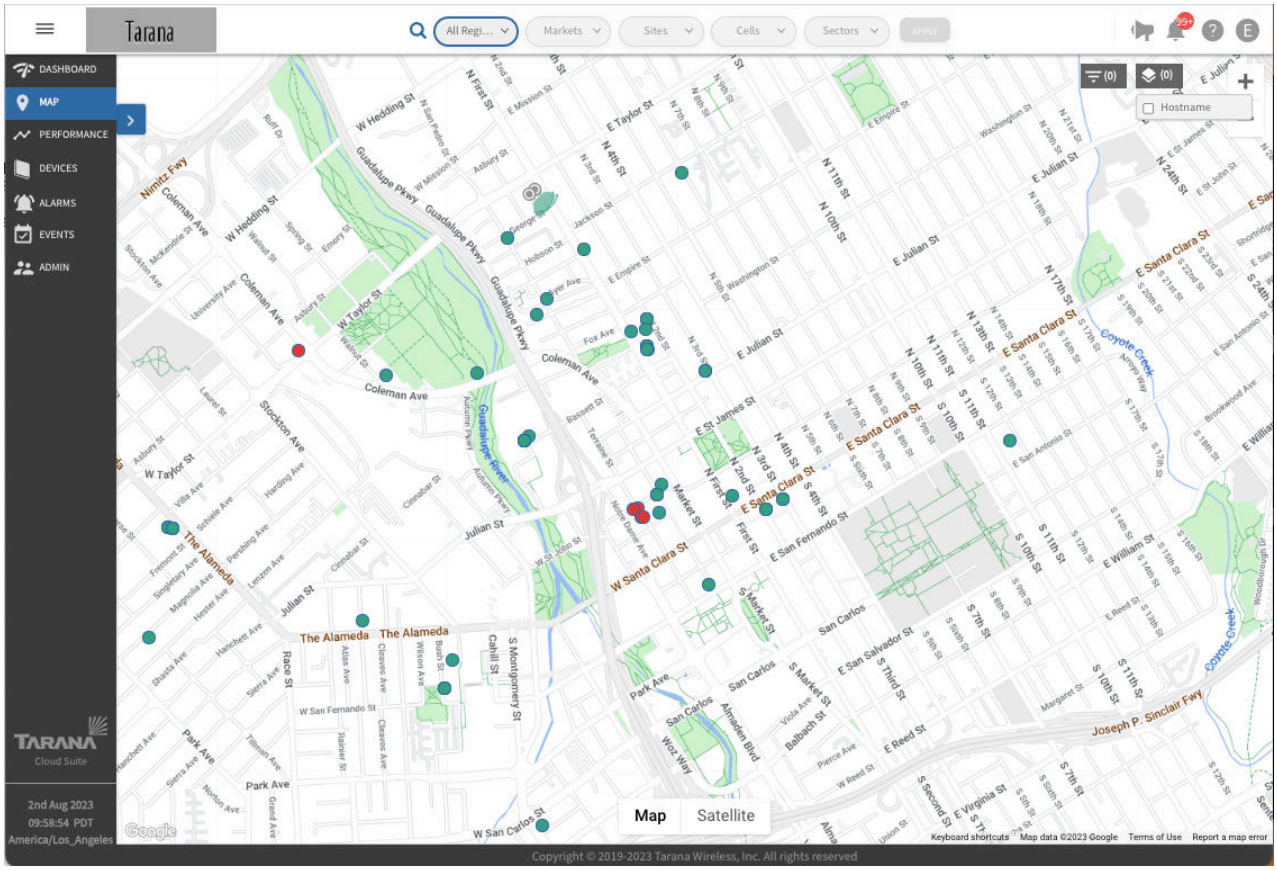
You can filter devices on the map by status using a drop down: All Devices, Connected Devices, Disconnected Devices, Needing Attention, or Spectrum Unassigned.



Map View

Base nodes are shown as circles with an antenna signal pointing in the direction of the configured azimuth. Remote nodes are shown as plain circles. When you select a remote node to view its details, the remote node icon displays an arrow that points in the direction of the configured azimuth. A line also appears indicating the link path back to the base node.

Devices that are connected and communicating with TCS are shown in green. Devices that had previously been connected to TCS but are currently disconnected are shown in red.



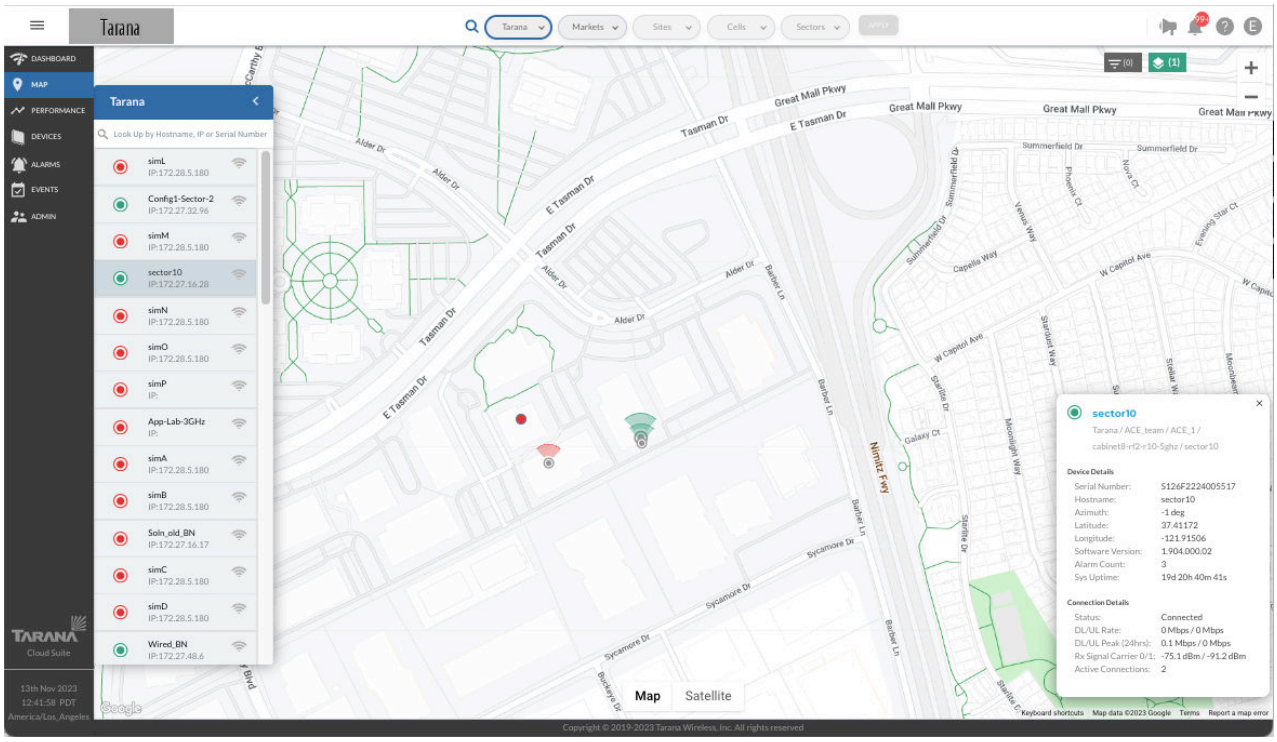
Map View of Base Nodes and Remote Nodes

When you zoom out on the map, the device icons can become dense on the page. You can collapse the group into a single icon that indicates the number of remote nodes in that location. Select **Layers**, then select **Cluster**.

Map View Device Details

The pop-out search bar next to Map shows a list of all devices the network selected. To open or close it, select the right or left arrow. Base nodes are shown as a circle with an antenna signal and remote nodes are shown as a plain circle.

To zoom to a device's location on the map, select any of the devices by clicking its name. The selected device is centered in the window and a pop-up window with device details appears on the right side of the window.



Map View of Base Node with Device Details

Information displayed in the Device Details window for a base node includes:

Device Details

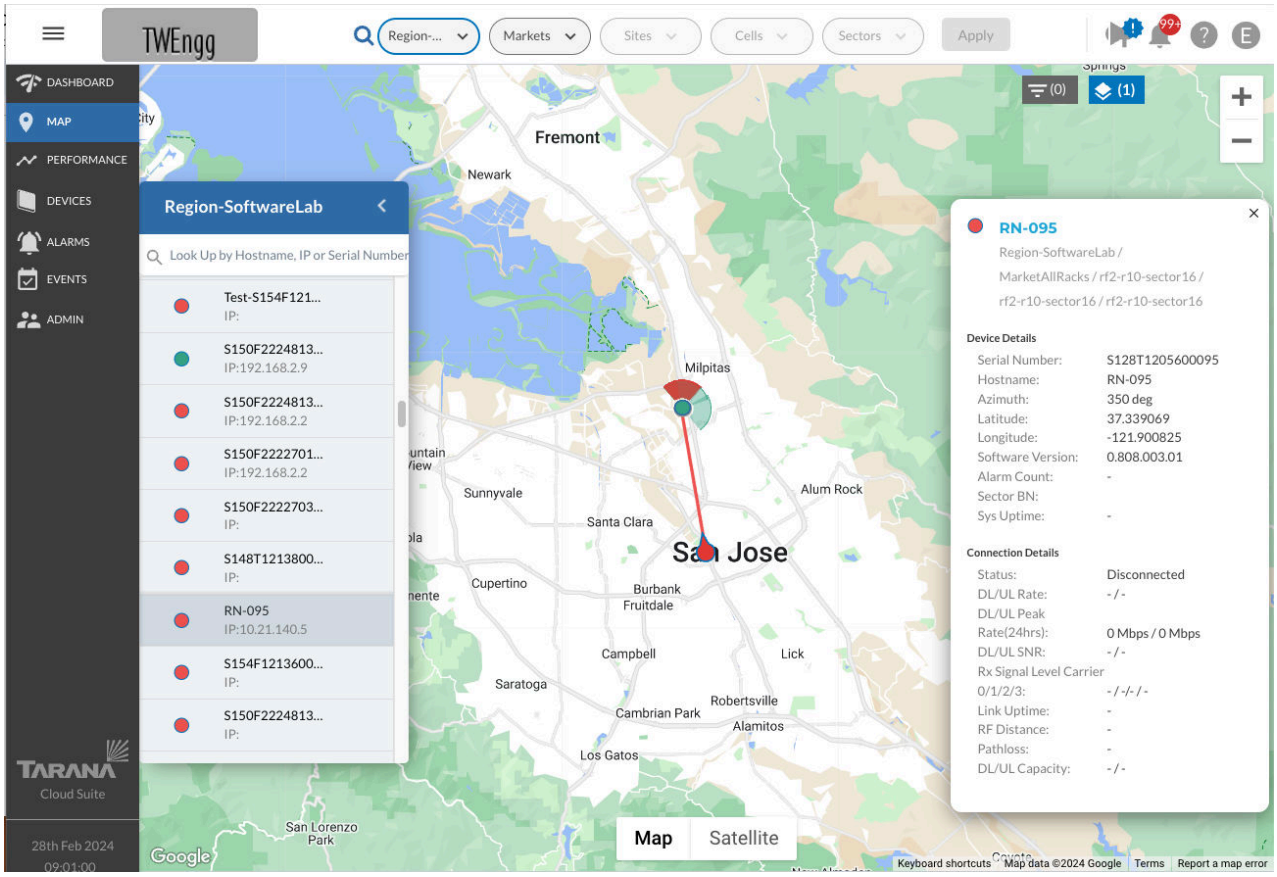
- Region / Market / Site / Cell / Sector
- Serial Number
- Hostname
- Latitude
- Longitude
- Software Version
- Alarm Count
- System Uptime

Connection Details

- Connection Status
- DL / UL Rate (Mbps)
- DL / UL Peak (for 24 hour period)

- Rx Signal Carrier
- Active Connections

When you select a remote node from the list of devices in the map, TCS shows a line from the remote node to its base node. If the remote node is currently connected to the base node, the line and devices are shown in green. If the remote node is currently disconnected, it's shown in red.



Map View of Remote Node with Device Details

Information displayed in the Device Details window for a remote node includes:

Device Details

- Region / Market / Site / Cell / Sector
- Serial Number
- Hostname
- Latitude
- Longitude

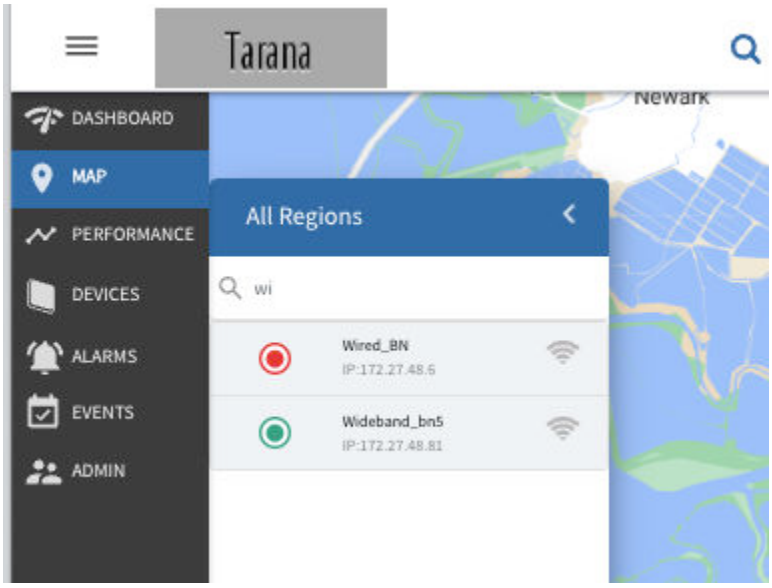
- Software Version
- Alarm Count
- Sector BN
- System Uptime

Connection Details

- Connection Status
- DL / UL Rate in Mbps
- DL / UL Peak (over 24 hours)
- DL / UL SNR
- Rx Signal Carrier
- Link Uptime
- RF Distance
- Pathloss
- DL / UL Capacity

Map View Search Bar

You can use the pop-out search bar in the upper left side of the screen to search for a specific device by Hostname, IP, or Serial Number. This action is dynamic and the list shows filtered results immediately.



Map View Search Bar

Map Overlay

On the TCS map, you can see a color-coded overlay of up to four sectors' base node-remote node associations where you can see which remote nodes are connected to which base nodes.

To display the overlay, select up to 4 base nodes by selecting **Show Coverage** ( ) next to its name. In order of selection, the coverage symbols by the device's name and coverage graphics on the map next to the base node are colored:

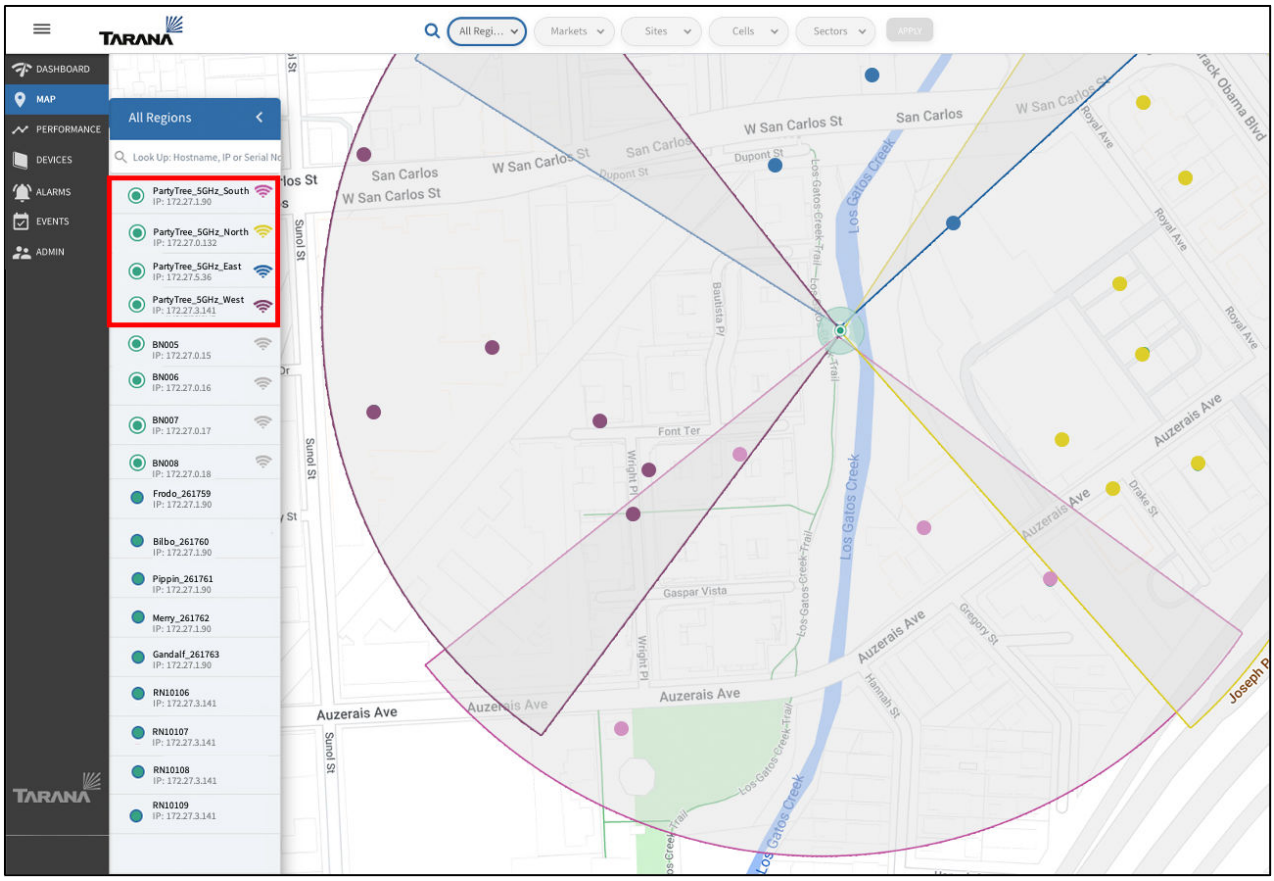
- Pink
- Yellow
- Blue
- Purple

Each base node has a colored arc on the map that corresponds to these colors. All remote nodes associated to that base node are shaded according to this scheme. You can select a disconnected base node, represented by a circle shaded with its base node color and an X in the middle.

In this example, four base nodes have been selected (shown in the red box). In the device list, the first base node selected (BN0002) has a pink antenna signal and a pink shaded arc on the map shows that base node coverage graphic. All remote nodes associated to that base node are shaded pink.

The second base node selected (BN0004) has a yellow antenna signal and a yellow shaded arc on the map shows that base node coverage graphic. All remote nodes associated to that base node are shaded yellow. The third and fourth base nodes are similarly colored.

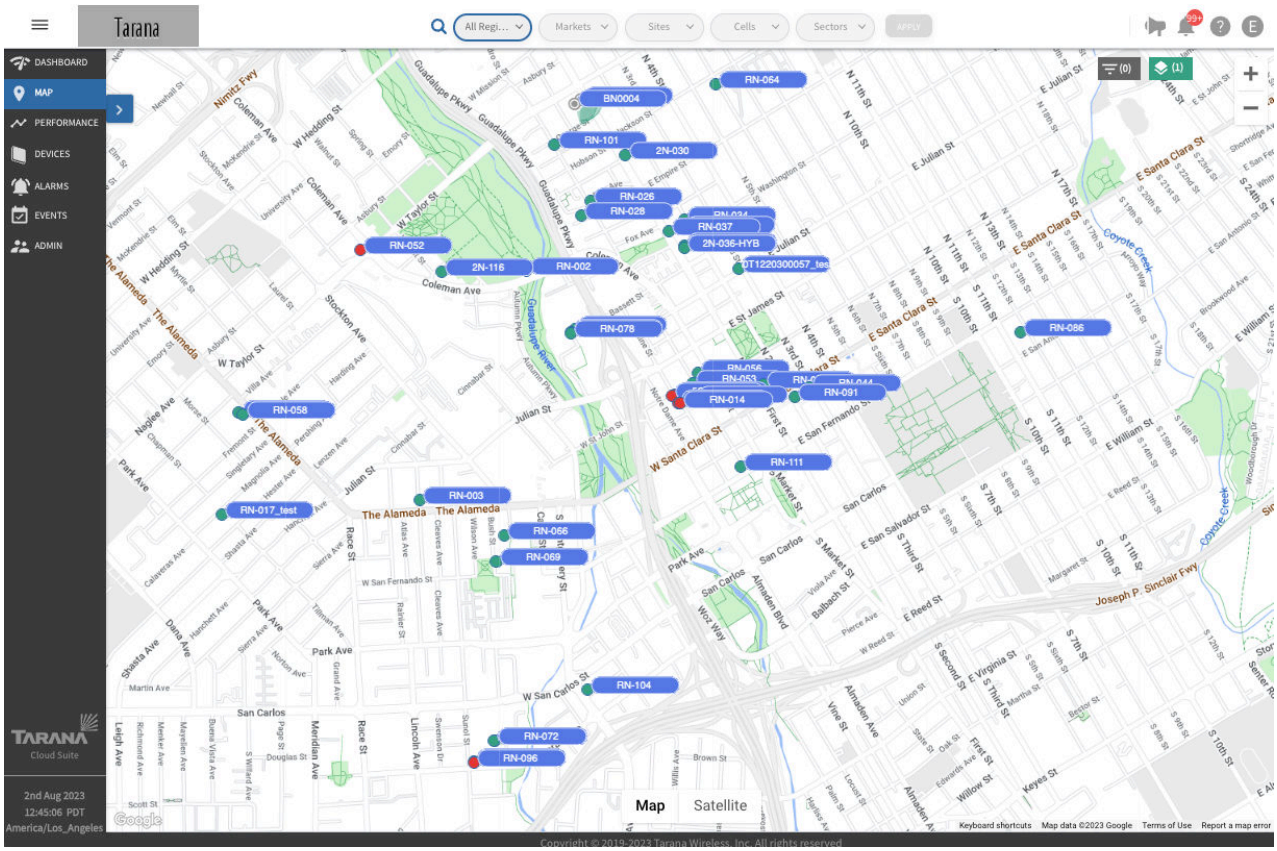
Even when one base node coverage graphic overlaps another base node area, it's easy to see which remote nodes are associated to a particular base node.



Select for Overlay

Display Device Hostnames

To display device hostnames on the map, select the **Layers** icon ( ) in the top right corner and check **Hostname**.

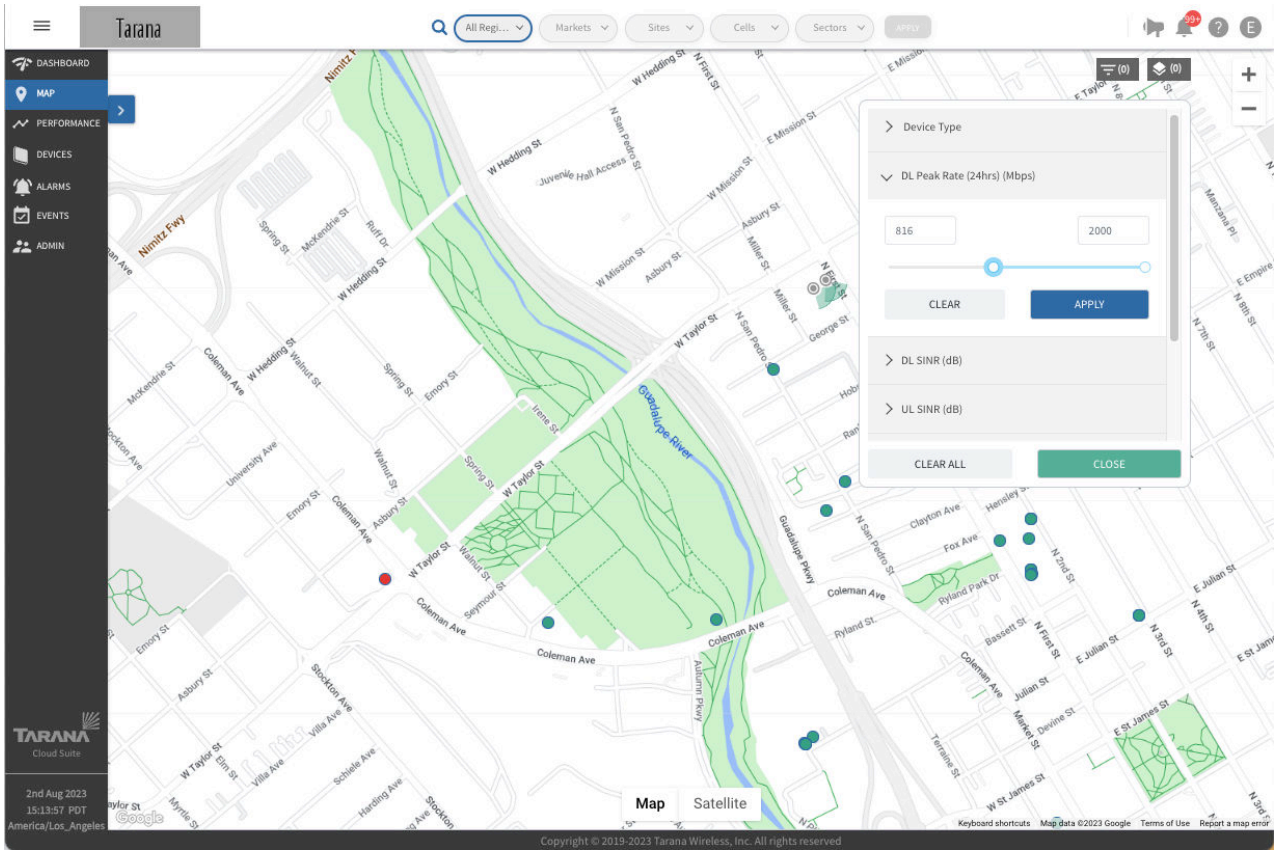


Display Device Hostnames

To remove the hostname display, uncheck **Hostnames**.

Filter Map by Metrics

To filter devices based on metrics, select the filter icon (⚌) in the top right corner.



Filter the Map by Metrics

Use the slider bars to adjust between specific values for these categories:

- **Device Type:** Toggle between all nodes or base nodes only.
- **DL Peak Rate (24 hours):** Highest downlink rate, in Mbps, recorded within the last 24 hours.

  Adjust the slider to select a value between 1 and 2000.
- **DL SINR**: Average downlink signal-to-interference-and-noise ratio (SINR), in dB, for a link. This value is measured at the time traffic is transmitted.

  Adjust the slider to select a value between -99 and 35.
- **UL SINR**: The average uplink signal-to-interference and noise ratio (SINR), in dB, for a link. This value is measured at the time traffic is transmitted.

  Adjust the slider to select a value between -99 and 35.
- **Path Loss**: Attenuation of the RF signal, in dB, between the base node antenna and the remote node antenna, excluding antenna gains. Values higher than that calculated by free space pathloss typically indicate some type of degradation of the signal such as as an obstacle (near- or non-line-of-sight).

Adjust the slider to select a value between 75 and 165.

- **DL Tonnage (24hrs)**: Amount of data sent in the downlink direction in the last 24 hours, in gigabytes.

  Adjust the slider to select a value between 0 and 100.

- **UL Tonnage (24hrs)**: Amount of data sent in the uplink direction in the last 24 hours, in gigabytes.

  Adjust the slider to select a value between 0 and 100.

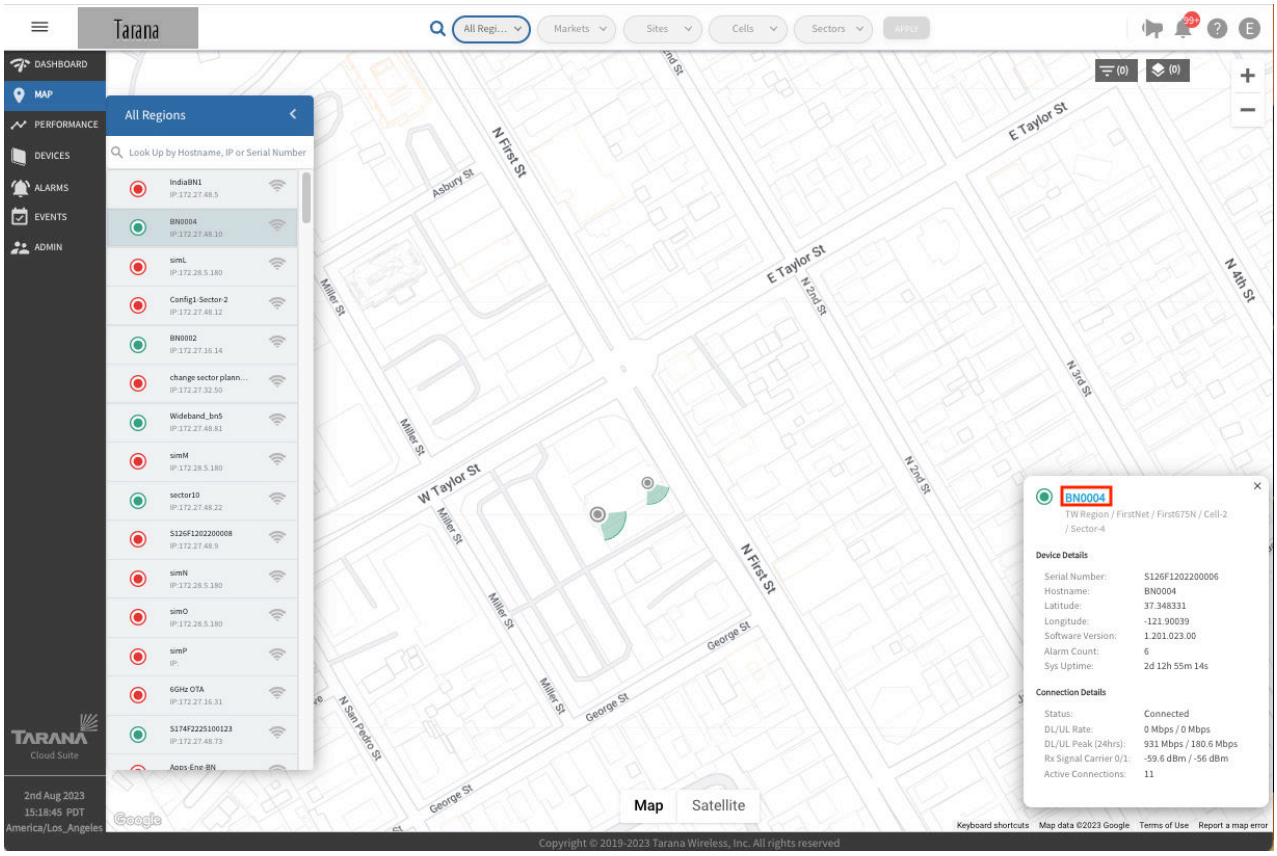
Select **Apply** to save the filter and apply it to the map view. Select **Clear** to reset the filter to its default values.

Select **Clear All** to clear the filters from the display and **Close** to close the filter dialog box.

View an Individual Device Dashboard

You can view a separate dashboard for individual devices that shows status and configuration information.

From the Device Details pop-up display in the Map view, select the device name hyperlink at the top. See Individual Device Dashboard (page 66) for details.



View Individual Device Dashboard from Map

Performance Metrics

Performance metrics are a valuable troubleshooting tool for individual devices or to compare multiple devices. To see performance metrics for a device, select the **Performance** icon (📈) from the top of the page. Use the toggle to set metrics to **Compare KPIs** or **Compare Entities**.

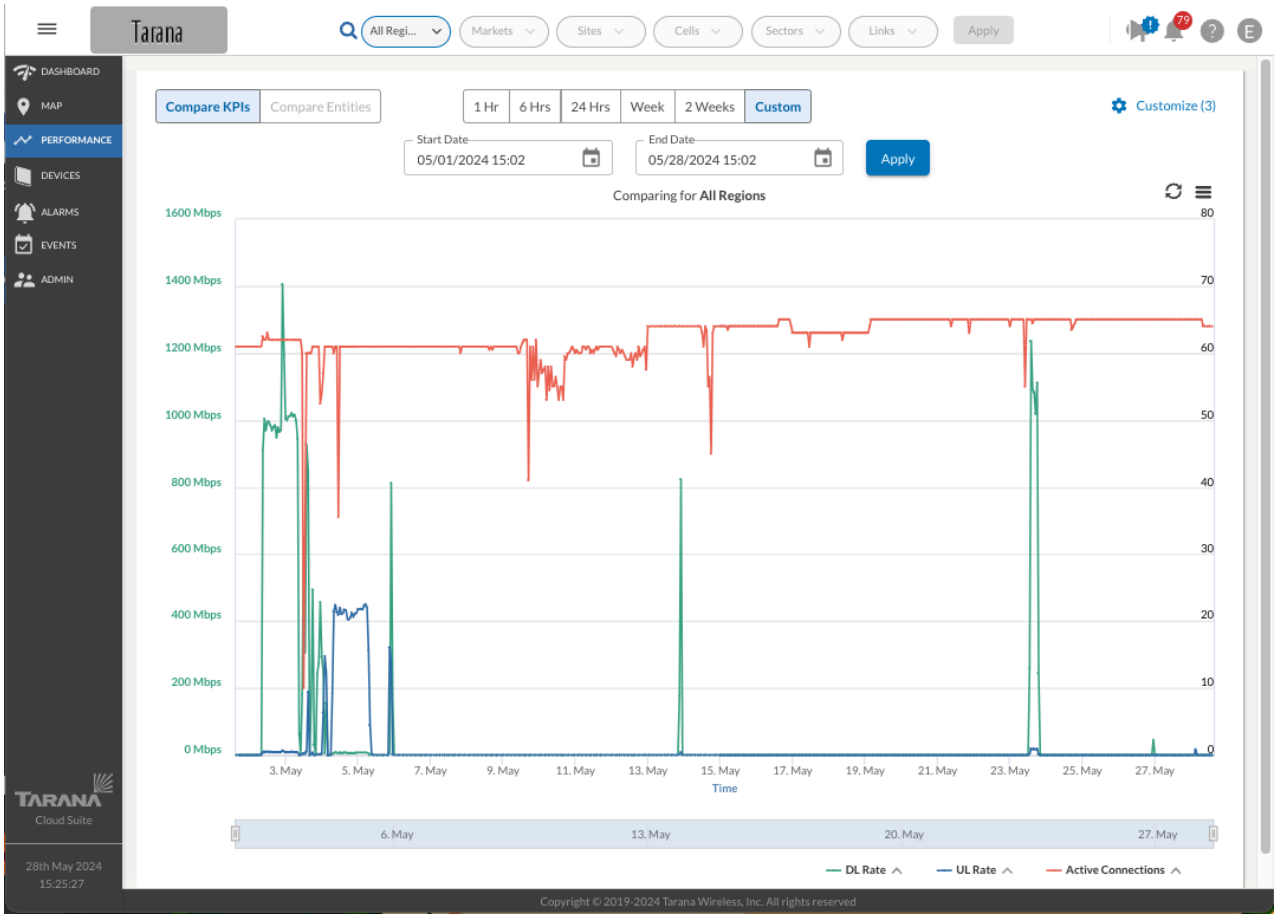
Metrics (Analytics)

Select individual entities from Region through Links and select **Apply**.

Make sure that you've chosen the correct network entity from the drop-down menus at the top. This filters the network down to the granularity you need. Because the menus are hierarchical, start by selecting the Region, then Market, Site, Cell, and Sector, as needed.

The Sector option represents the selection of the Sector's base node. The Links option includes a drop-down box showing all remote nodes connected to the selected base node under Sector. Select a specific remote node under Links to see metrics for that remote node.

It's important to remember which network entity you've selected because the performance metrics account only for that entity and for devices within that entity.



Performance Monitoring

You can limit the display to a time period: Last 1 hour, last 24 hours, last 1 week, last 2 weeks, or a custom time period.

If you select 1 hour, the graph updates automatically every 30 seconds. If you select any other time period, you must select the refresh icon in the upper right corner to update the graph.

Use the Start and End Date fields to set a time period, then select **Apply**.

Click and drag the mouse to zoom in on the graph. The display shows you the lowest granularity for that time period, down to 60 seconds. As you zoom out, the granularity increases. Click anywhere to zoom out.

TCS stores KPI data for three months. When you select recent data, the first month is the most granular. As you select data further in the past, it's summarized in a larger time period.

Compare KPIs

Set the toggle at the upper left corner of the Performance window to **Compare KPIs**. This setting lets you compare KPIs on a single network entity.

Select the **Customize** icon (⚙) on the top right to open a selection box of available KPIs for the network entity that's selected. This selection box lets you choose to display KPIs or Events.

Choose the KPIs for the device that you want to graph. Select **Done** to apply these values to the graphical display. For any network entity selected from Region down to Cell level of granularity, available KPIs are Active Connections, DL Rate, and UL Rate. This allows you to chart the UL and DL rates for a region, market, site, or cell compared to the number of active connections.

For selected Sectors (individual base nodes) and Links (individual remote node), available KPIs are:

- **Temperature**: Internal temperature, at board level, reported by the device. The maximum internal temperature for devices is 199 degrees Fahrenheit (95 degrees Celsius).

NOTE
Temperature as defined here is distinct from the temperature listed in the data sheet, which describes the ambient operating temperature range.

- **CPU Utilization:** Percentage of CPU utilized on the device.
- **Memory Utilization**: The percentage of memory currently in use. This value is typically within the range of 30 to 90 percent.
- **DL Rate**: The latest downlink rate, in Mbps, as sampled once every 30 seconds.
- **UL Rate**: The latest uplink rate, in Mbps, as sampled once every 30 seconds.
- **DL Peak Rate**: Highest downlink rate, in Mbps, recorded within the last 150 seconds.
- **UL Peak Rate**: The highest uplink rate, in Mbps, recorded within the last 150 seconds.
- **Frequency Carrier *n***: The administrator-selected operating center frequency of the carrier, where n is the number of the carrier (0 – 3). The value is hardware-dependent and based on the device model.
- **Bandwidth Carrier *n***: Bandwidth of the carrier, where n is the number of the carrier (0 – 3).
- **Intf. Noise Ratio Max Carriers *n*:** The maximum interference-to-noise ratio detected on any of the subcarriers of carrier n, where n is the carrier number (0 - 3), as sampled over

a 30-second period. The detected interference might overlap the entire carrier or just a portion of it, which influences link performance.

- **Sensitivity Loss Max Carrier *n*:** Loss in sensitivity on carrier n, in dB, due to very high received signal strength, where n is the carrier number (0 – 3). A device that reports a non-zero value is likely experiencing high interference levels. In the case of remote nodes, this typically correlates with a low path loss number for the link. Calculate expected performance of a link by summing the sensitivity loss with measured path loss.
- **Rx Signal Level Carrier *n*:** The received signal strength for carrier *n* in dBm, where n is the carrier number (0 – 3). Received signal strength includes both the signal of interest and interference. This value is typically lower when there is no traffic passing on the link, at which point the number indicates the amount of interference noise on the link.

For a selected Sector (individual base node), additional available KPIs are:

- **RF Utilization:** The number of available resource blocks that are consumed by traffic, including management, control, and data traffic, expressed as a percentage. Low utilization means that more resource blocks are available for devices to gain access to the medium to transmit and receive data. If the utilization is too low to render accurately, a hyphen (-) appears in the table.

NOTE
Because different MCS indices have different resource requirements, resource blocks might not be uniformly sized.

- **GPS SINR:** GPS Signal to Interference Noise Ratio.
- **GPS Lock Status**: Indicates if the base node has successfully acquired enough satellites to determine its location. A base node must have a GPS lock before it can transmit.
- **Satellites:** Number of GPS satellites (0 - 30) visible to this base node. Minimum number for GPS lock is 3.
- **Active Connections**: Number of remote nodes that are currently connected to a base node.
- **Input Voltage:** Input DC voltage to the base node.
- **Power Consumption**: Power consumed by the base node in watts.

For a selected Link (individual remote node), additional available KPIs are:

- **Path Loss**: Attenuation of the RF signal, in dB, between the base node antenna and the remote node antenna, excluding antenna gains. Values higher than that calculated by free space pathloss typically indicate some type of degradation of the signal such as as an obstacle (near- or non-line-of-sight).

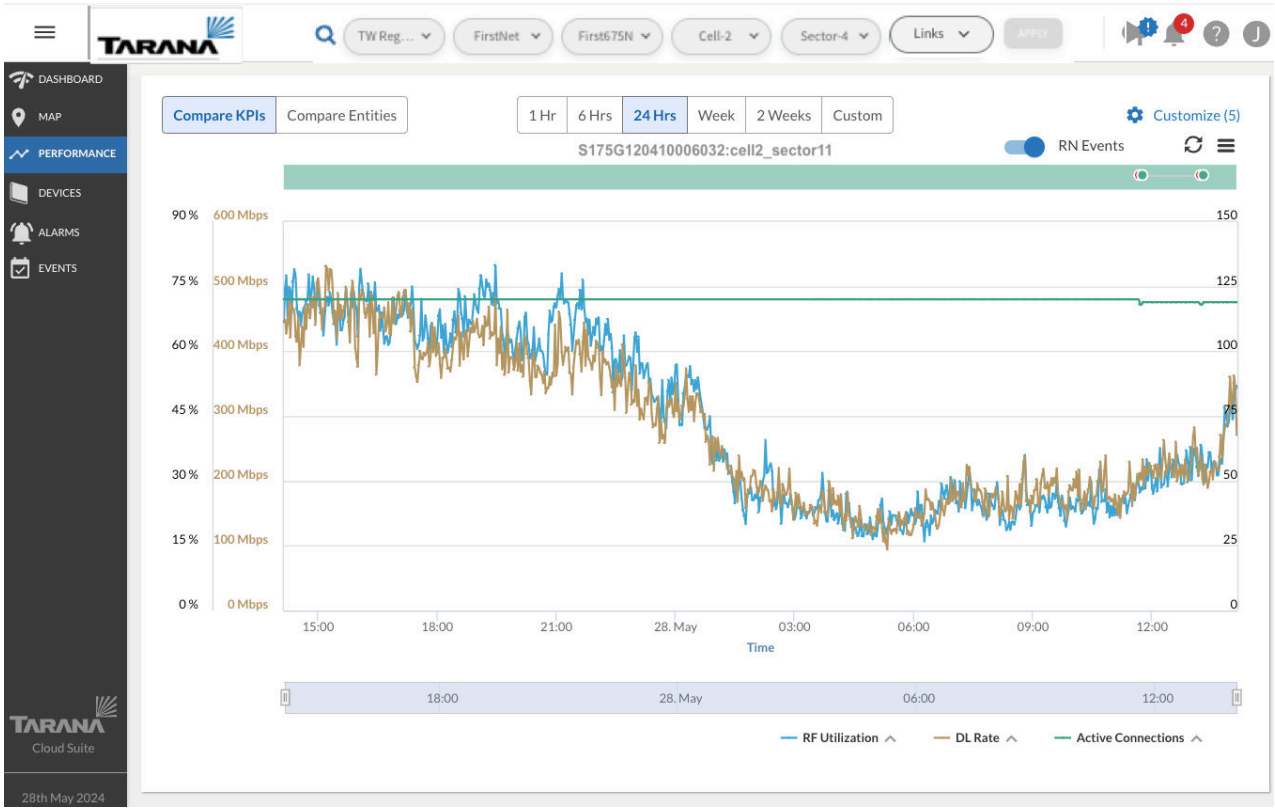
- **RF Distance (RF Range)**: Estimated distance traveled by the signal between the base node and the remote node, in meters. This differs from LoS distance in that it accounts for reflections and diffractions. In general, the RF range will be equal to, or slightly greater than, LoS distance.
- **DL SINR**: Average downlink signal-to-interference-and-noise ratio (SINR), in dB, for a link. This value is measured at the time traffic is transmitted.
- **UL SINR**: The average uplink signal-to-interference and noise ratio (SINR), in dB, for a link. This value is measured at the time traffic is transmitted.
- **DL PER**: The downlink packet error rate after accounting for ARQ retransmissions. Acceptable values are typically in the range of 0% to 1%. A value of 1% to 10% indicates moderate degradation of the link while values greater than 10% are considered detrimental to link performance. In general, the higher the peak rate of a link, the lower the acceptable PER value.
- **UL PER**: The uplink packet error rate after accounting for ARQ retransmissions. Acceptable values are typically in the range of 0% to 1%. A value of 1% to 10% indicates moderate degradation of the link while values greater than 10% are considered detrimental to link performance. In general, the higher the peak rate of a link, the lower the acceptable PER value.

You can plot KPI metrics for an individual base node or remote node against a timeline of operation events. Follow these steps:

1. Select the Customize icon and choose **Events**.
2. Enable the toggle for Events.
3. Choose the event types of interest and select **Done**.

Events are displayed in the green band at the top of the graph. Gray on the bar indicates the device was disconnected. Hover your mouse over the events in the green band to see details.

This example shows KPIs for an individual Link with RF utilization, DL rate, and Active Connections compared.



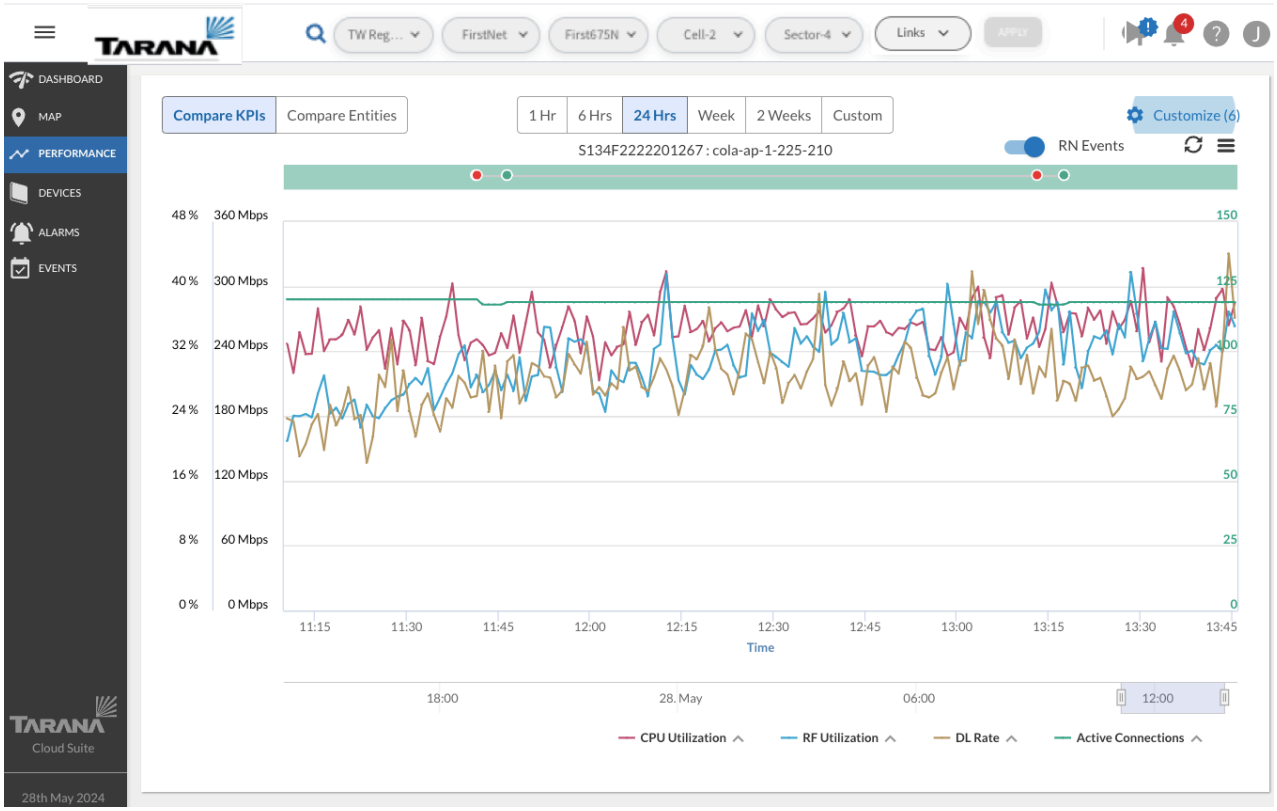
Overlay Events on a KPI Metric

If there are too many events to display, TCS displays a message "Showing latest 100 events only. Reason: too many events" along with a link to open the Events page. The time range you set on the Performance page carries over to the Events page.

Hover the mouse to see a listing of the values for a specific point in time. This example is a close-up of a specific point in time.

Hover Mouse to See Timestamp

Click and drag the mouse to zoom in on the graph.



Zoomed in area

Click anywhere to reset the graph to the selected time frame. Use the chart context menu icon (☰) in the upper right to view the graph in full screen, print the chart, or download the chart as an image (PNG, JPEG, PDF, or SVG) or CSV file.

Compare Entities

Comparing entities or KPIs is a valuable troubleshooting tool.

Set the toggle at the upper left corner of the Performance window to **Compare Entities**. Select the **Customize** icon on the top right to open a selection box of available KPIs for the network entity that's selected. You can also choose between KPIs and Events.

It's important to keep in mind which entity you've selected when doing comparisons. Selecting an entity (Region, Market, Cell, etc.) accounts for all devices within that entity. Selecting individual Links accounts for only the remote node involved in the selected link.

Compare Entities

To select specific KPIs to compare between selected entities, use Settings to select a KPI. Then select another entity from the Compare list. Select **Done** to return to the graph and see the comparison.

Entities compared

In this example, filtering has been set down to a specific link (a remote node), so only remote nodes connected to the same base node are available to compare. The entity names are listed at the bottom of the page. The comparison is for DL Rate over a 24 hour period.

By filtering down to a specific sector (base node), you can compare any base nodes in the same cell.

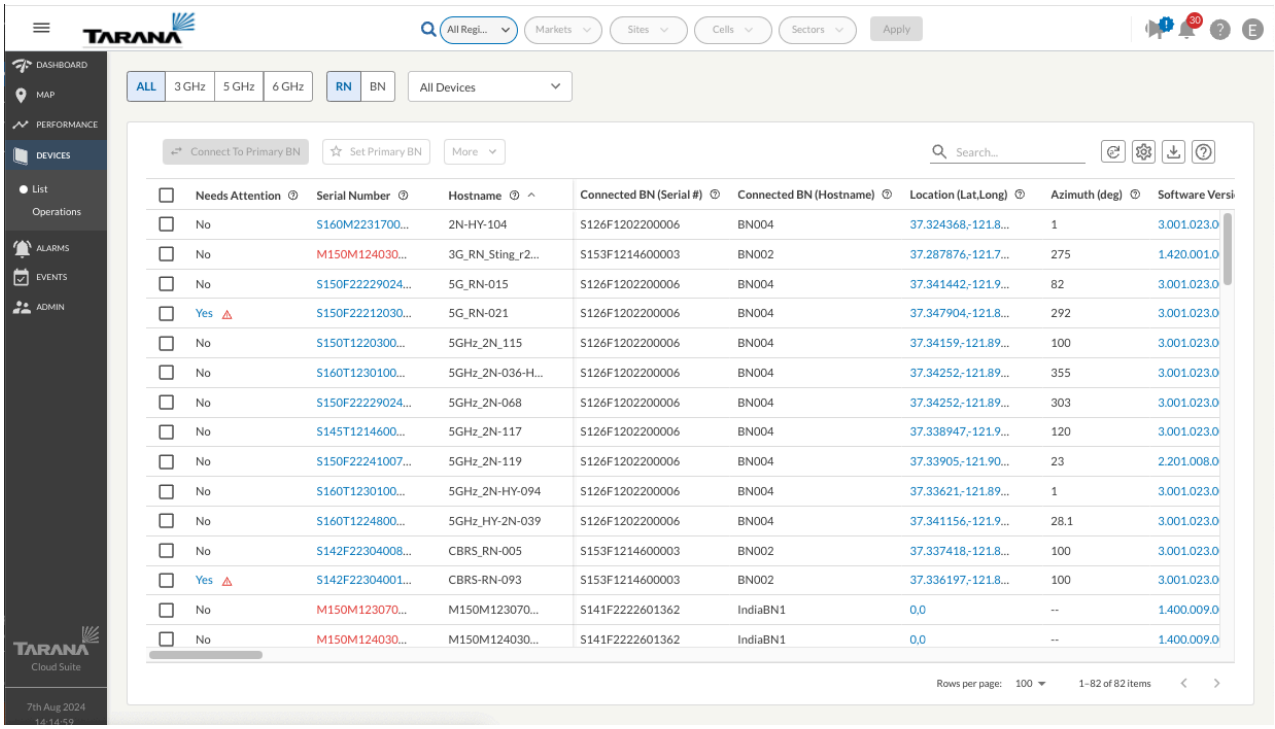
If there are too many events to display, TCS displays a message "Showing latest 100 events only. Reason: too many events" along with a link to open the Events page. The time range you set on the Performance page carries over to the Events page.

Devices View

To see a network-wide view of devices, select **Devices** in the navigation pane. Two views are available, List and Operations.

Device List View

To see detailed information about a particular device, select **Devices** from the navigation pane. You see device information in a table, by type. At the top, use the filters to select a specific network. You can also filter devices based on band or mode, and select either remote nodes or base nodes.



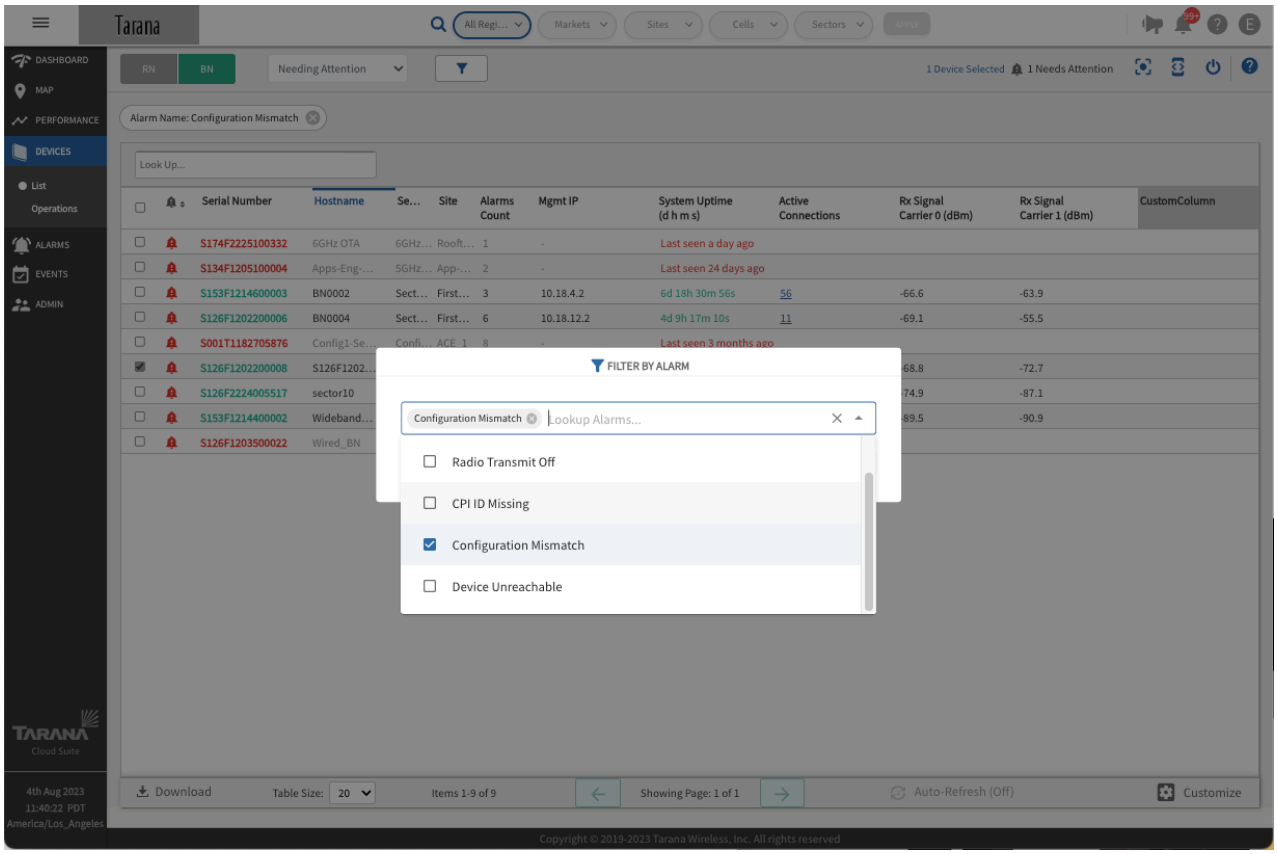
Device List View

To go to an individual device dashboard, select the serial number hyperlink. See Individual Device Dashboard (page 66) for details.

Serial numbers for devices that are up and connected are shown in green. Disconnected devices are shown in red. Devices that need attention are marked with a red triangle.

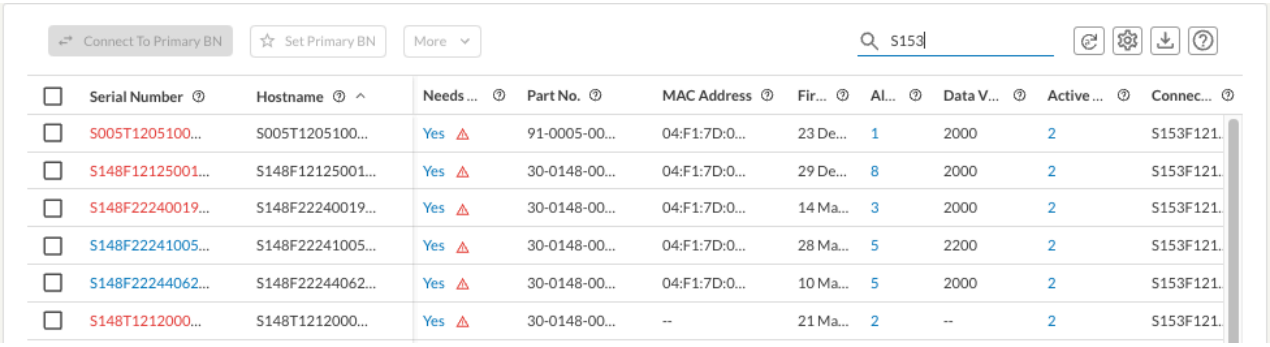
Filter the list with the Device Status dropdown. You can show All Devices, Connected Devices, Disconnected Devices, Needing Attention, or Spectrum Unassigned. The default is Needing Attention.

If you filter the list with Needing Attention, you can use the filter icon ( ) to select from various alarm conditions. Use the check box to select one or more then select **Apply**.



Filter by Alarm

Remove filters by clearing the check box and selecting **Apply**.

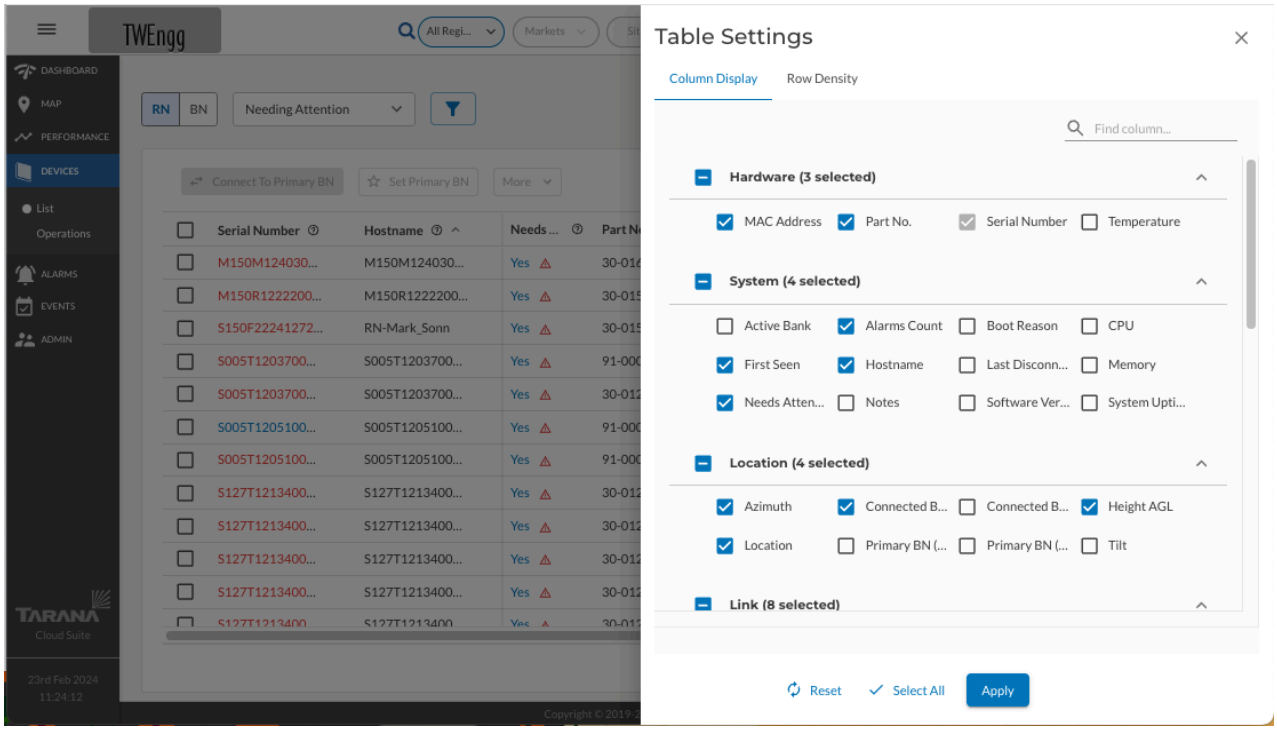


Enter any value in the Search... box. If it appears in any of the fields, the rows are filtered to show only those rows.

Icons at the top of the table let you control refresh rate, change settings, download data, or view information about KPIs.

The data displayed for each column doesn't refresh automatically. To change this behavior, select the **Auto-Refresh icon** (). It remains on for your user account even after you log out. Select it again to turn off Auto-Refresh.

Column categories are dependent on the device type and you can customize them by selecting the Settings icon (). Select the fields you want to display, then **Apply**. These changes remain for your user account even after you log out. Use **Reset** to clear your selection.



You can download up to 10,000 events data in CSV format. The download is context sensitive depending on the filters and column topics chosen under Customize. To download, select the checkbox next to the devices then select the Download () icon. Navigate to the folder on your local device where you want to save the file.

For information about metrics, select the **Support** icon () in the upper right corner.

To sort in ascending or descending order, select the column heading.

Select and drag column headings to reposition that column in the table.

Use the drop down at the bottom to control rows per page, and use the arrows to move between pages.

To resize columns, put your cursor between column headings. Click and drag the resize tool to widen or narrow the column width.

You can copy data in several of the columns by hovering over the field until you see a **Copy** icon. Select it to copy.

If your role is NOC Operator or OP Admin, you can issue operational commands against individual devices. Select the check box next to the device, then select **Snapshot**, **Software Install**, or **Reboot** in the upper right corner. For remote nodes, you can also perform **Network Action** (Set Primary BN, Reconnect to Network, or Connect to Primary BN) or **Remove**. To remove a remote node, that node must be disconnected (its serial number is shown in red).

For details about operational commands, see Device Dashboard Action Icons (page 81).

You can remove only disconnected remote nodes. If you select **Remove**, TCS displays a message that lists any connected devices that will be excluded. You can only close the message.

If the device isn't connected, TCS shows a popup where you select **Cancel** or **Proceed**. If you select **Proceed**, the device is removed from TCS.

Use the check box to select one or more then select **Apply**.

Link Metrics

Link metrics provide measured operational information about the device link between the base node and remote node. These metrics are common to both nodes:

- **Availability (month)**: For a base node, the amount of time it was available during the calendar month, excluding power loss, reboot, manually muted radios, or backhaul outages. For a remote node, the amount of time it was up during the calendar month, excluding power loss and reboot. If the node was down due to a software issue, availability time is reduced accordingly.
- **DL Peak Rate**: Highest downlink rate, in Mbps, recorded within the last 150 seconds.
- **Intf. Noise Ratio Max Carriers *n***: The maximum interference-to-noise ratio detected on any of the subcarriers of carrier n, where n is the carrier number (0 - 3), as sampled over a 30-second period. The detected interference might overlap the entire carrier or just a portion of it, which influences link performance.
- **Life Time DL Peak Rate**: The highest downlink rate recorded, in Mbps, since the device was first seen in TCS, or since the last reset of this KPI.
- **Life Time UL Peak Rate**: The highest uplink rate recorded, in Mbps, since the device was first seen in TCS, or since the last reset of this KPI.

- **Rx Signal Level Carrier *n*:** The received signal strength for carrier *n* in dBm, where n is the carrier number (0 – 3). Received signal strength includes both the signal of interest and interference. This value is typically lower when there is no traffic passing on the link, at which point the number indicates the amount of interference noise on the link.
- **Sensitivity Loss Max Carrier *n*:** Loss in sensitivity on carrier n, in dB, due to very high received signal strength, where n is the carrier number (0 – 3). A device that reports a non-zero value is likely experiencing high interference levels. In the case of remote nodes, this typically correlates with a low path loss number for the link. Calculate expected performance of a link by summing the sensitivity loss with measured path loss.
- **Spectrum Status:** Status of the CBRS grants that are issued to the device by a SAS (Spectrum Access System). When a device is removed from TCS, TCS relinquishes the grant that was held by the device band with the highest frequency.
- **Spectrum Reason:** Reason for the spectrum status.

Base Node Link Metrics

- **Active Connections**: Number of remote nodes that are currently connected to a base node.
- **RF Utilization:** The number of available resource blocks that are consumed by traffic, including management, control, and data traffic, expressed as a percentage. Low utilization means that more resource blocks are available for devices to gain access to the medium to transmit and receive data. If the utilization is too low to render accurately, a hyphen (-) appears in the table.

NOTE
Because different MCS indices have different resource requirements, resource blocks might not be uniformly sized.

Remote Node Link Metrics

- **DL PER**: The downlink packet error rate after accounting for ARQ retransmissions. Acceptable values are typically in the range of 0% to 1%. A value of 1% to 10% indicates moderate degradation of the link while values greater than 10% are considered detrimental to link performance. In general, the higher the peak rate of a link, the lower the acceptable PER value.
- **DL Peak Rate (24 hours)**: Highest downlink rate, in Mbps, recorded within the last 24 hours.
- **DL Rate**: The latest downlink rate, in Mbps, as sampled once every 30 seconds.

- **DL SINR**: Average downlink signal-to-interference-and-noise ratio (SINR), in dB, for a link. This value is measured at the time traffic is transmitted.
- **DL Tonnage (24hrs)**: Amount of data sent in the downlink direction in the last 24 hours, in gigabytes.
- **DL Tonnage (month)**: Amount of data sent in the downlink direction in the last month, in gigabytes.
- **Link Uptime**: Elapsed time (in days, hours, minutes, and seconds) since an active link was established.
- **Network Entry Time**: The amount of time a remote node took to establish a link to the base node. This value resets each time the remote node reestablishes the link.
- **Path Loss**: Attenuation of the RF signal, in dB, between the base node antenna and the remote node antenna, excluding antenna gains. Values higher than that calculated by free space pathloss typically indicate some type of degradation of the signal such as as an obstacle (near- or non-line-of-sight).
- **RF Distance (RF Range)**: Estimated distance traveled by the signal between the base node and the remote node, in meters. This differs from LoS distance in that it accounts for reflections and diffractions. In general, the RF range will be equal to, or slightly greater than, LoS distance.
- **UL PER**: The uplink packet error rate after accounting for ARQ retransmissions. Acceptable values are typically in the range of 0% to 1%. A value of 1% to 10% indicates moderate degradation of the link while values greater than 10% are considered detrimental to link performance. In general, the higher the peak rate of a link, the lower the acceptable PER value.
- **UL Peak Rate**: The highest uplink rate, in Mbps, recorded within the last 150 seconds.
- **UL Peak Rate (24hrs)**: The highest uplink rate, in Mbps, recorded within the last 24 hours.
- **UL Rate**: The latest uplink rate, in Mbps, as sampled once every 30 seconds.
- **UL SINR**: The average uplink signal-to-interference and noise ratio (SINR), in dB, for a link. This value is measured at the time traffic is transmitted.
- **UL Tonnage (24hrs)**: Amount of data sent in the uplink direction in the last 24 hours, in gigabytes.
- **UL Tonnage (month)**: Amount of data sent in the uplink direction in the last month, in gigabytes.

System Metrics

System metrics provide non-hardware-specific information about the device. These are common to both nodes:

- **Active Bank**: The software bank that holds the currently running software.
- **Alarms Count**: Number of currently raised alarms for a device.
- **Boot Reason**: Reason reported by the device for the most recent reboot. Possible reasons include a cold reboot due to power interruption, a warm reboot prompted by the software, or a Watchdog reboot initiated when the system detects an unrecoverable condition.
- **CA1:** Custom Attribute set with an API.
- **CPU**: The percentage of CPU actively in use. This value is typically within the range of 30 to 90 percent.
- **First Seen:** Time when the device first connected to TCS.
- **Hostname**: Identifier used to distinguish the device on a network. By default, hostname is the device serial number.
- **Memory**: The percentage of memory currently in use. This value is typically within the range of 30 to 90 percent.
- **Needs Attention:** Device has alarms indicating that it needs attention.
- **Notes**: A text field for useful details about the device. Notes can be added by an administrator or NOC operator. The maximum length is 1024 characters.
- **Region**: The Region to which this device belongs.
- **Region**: The Region to which this device belongs.
- **Software Version**: The software version the device is running.
- **System Uptime**: Time since the device last booted, in days, hours, minutes, and seconds.

Base Node System Metrics

- **Cell**: The Cell to which this device belongs.
- **Mgmt IP**: IP address assigned by customer's network for device management.
- **Market**: The Market to which this device belongs.
- **Radio Uptime**: Uptime in days, hours, minutes, and seconds.
- **Sector**: Name of the Sector to which the remote node is connected.

- **Site**: The Site to which this device belongs.

Remote Node System Metrics

Last Disconnect Reason: The reason for the last link disconnect between a base node and a remote node.

Hardware Metrics

Hardware metrics include information relevant to device identification or environment.

- **MAC Address**: The physical hardware address of the device.
- **Part Number**: System part number based on the hardware SKU.
- **Serial Number**: A string that uniquely identifies a device or component. Displayed by default.
- **Temperature**: Internal temperature, at board level, reported by the device. The maximum internal temperature for devices is 199 degrees Fahrenheit (95 degrees Celsius).

NOTE
Temperature as defined here is distinct from the temperature listed in the data sheet, which describes the ambient operating temperature range.

- **Voltage**: The input power supply voltage as reported by the base node. Nominally, this is 48VDC, but the base node can safely function when the voltage is between 44VDC and 58VDC. Lower voltage may cause the device to power down.

NOTE
If the input voltage to the base node falls below -40 V, it may power down.

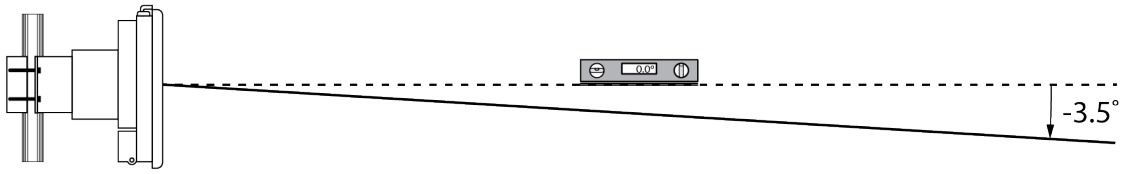
Location Metrics

Location Metrics provide device installation information. These values are common to both nodes:

- **Azimuth**: Horizontal angle of the device aim measured clockwise from true north.
- **Height (AGL)**: Installed height of the device above ground level (AGL).
- **Location**: Comma delimited latitude and longitude of the device in decimal degrees. For a base node, this is obtained from the GPS module. For a remote node, it's user-configured.

- **Tilt**: The vertical angle, measured in degrees relative to the true (horizontally level) horizon. 5 GHz base nodes that are tilted down have a positive tilt (0 through 180 degrees), while those that are tilted up have a negative tilt (0 through -180 degrees).

  3 GHz base nodes have a 3.5 degree electrical downtilt (towards the ground) in addition to the value reported on TCS. To conform with the CBRS standard, the antenna downtilt for a 3 GHz CBRS base node is reported as negative while an upward tilt is reported as positive.



Base Node Location Metrics

Height (AMSL): Height of the device Above Mean Seal Level (AMSL).

Remote Node Location Metrics

- **Azimuth**: Horizontal angle of the device aim measured clockwise from true north.
- **Connected BN (Hostname)**: Hostname of the base node to which the remote node is connected.
- **Connected BN (Serial #)**: Serial number of the base node to which the remote node is connected.
- **Height (AGL)**: Installed height of the device above ground level (AGL).
- **Location**: Comma delimited latitude and longitude of the device in decimal degrees. For a base node, this is obtained from the GPS module. For a remote node, it's user-configured.
- **Primary BN (Hostname)**: As defined in the network, hostname of the Primary base node that can provide the best connectivity to this remote node.
- **Primary BN (Serial #)**: As defined in the network, serial number of the Primary base node that can provide the best connectivity to this remote node.

For remote nodes, you can edit the location metrics from the Configuration action on the device page, or by using the Web UI.

For 6 GHz remote nodes the latitude and longitude are provided automatically with a GPS module. You can edit tilt and can configure azimuth and height AGL both in the remote

node's web UI at the time of install or from the base node's Configuration action icon (under Configure Installation Parameters).

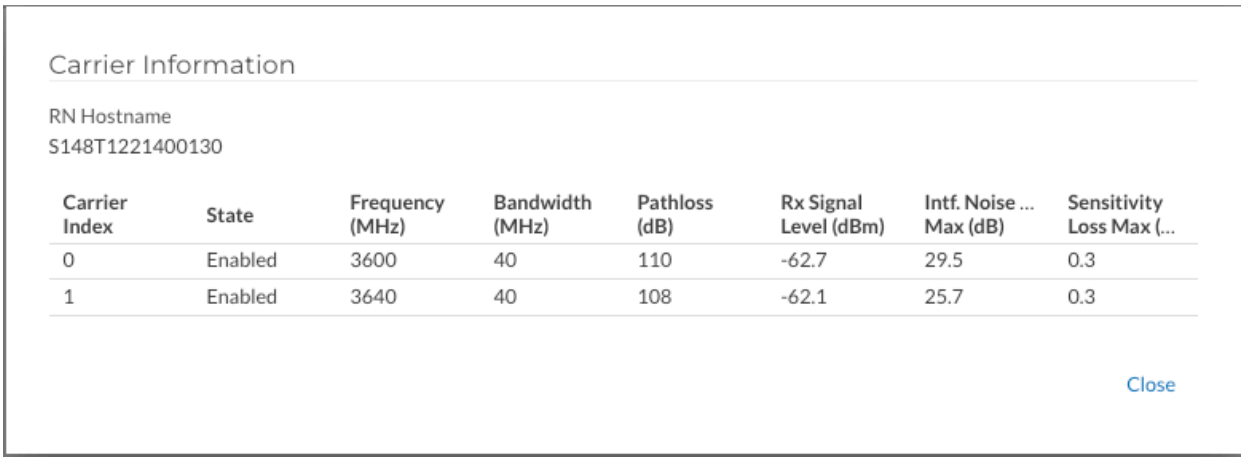
For 5 GHz remote nodes, latitude and longitude are necessary only for accurate Map View (page 32). Height, Tilt, and Azimuth are optional, but recommended.

For CBRS remote nodes, all of these parameters are required.

Planning Metrics

Planning metrics describe device radio configuration information. These values are common to both nodes:

- **Active Carriers:** The number of carriers that are currently in use for the device. The Active Carriers column is visible by default and contains the number of active carriers for the selected device as a link. You can select the link to display the Carrier Information table, which appears as a modal window over the Devices table:



  The columns in the Carrier Information table are fixed and always visible, so you don't have to customize the table.

- **Frequency Carrier *n***: The administrator-selected operating center frequency of the carrier, where n is the number of the carrier (0 – 3). The value is hardware-dependent and based on the device model.
- **Operational Bandwidth**: The amount of operational spectrum, in MHz, available for use by a sector or link.

Base Node Planning Metrics

- VLAN ID for in-band management.
- **Network Profile**: Defines the overall ratio of downlink throughput to uplink throughput and link distance. All cells with overlapping coverage and frequencies must use the same

network profile to avoid unnecessary interference. The network profile is configured at the cell and market levels.

Network Profile	Maximum Cell Range	Downlink (DL) Symbols	Uplink (UL) Symbols	DL:UL Ratio
1	15 km	36	8	4.5:1
2	30 km	32	8	4:1
5	15 km	32	12	2.67:1
6	15 km	28	16	1.75:1

- **Planning ID**: An identifier for the base node that uses the format `<setID><cellID><sectorID>`. Cell ID [BN] is an identifier for the cell and a group of 4 sectors forms a cell. An administrator can customize the Set ID (range 0 - 5) and Cell ID (range 0 - 23) in TCS at the cell level. TCS sets the Sector ID based on the order each base node is added to a cell. This results in 576 possible planning IDs.

  The planning ID is used by remote nodes to distinguish between base node and is also used in the remote node's Web UI to see the primary base node. If a remote node detects multiple base nodes with the same Planning ID, that can cause a longer search time. The remote node may not be able to accurately calibrate to its intended base node, which can affect performance, or it may connect to the wrong base node (based on the remote node’s Primary base node setting).

  For these reasons, it’s important that all base nodes in a given area have unique Planning IDs. The distribution of Planning IDs is geographically dependent and has been predetermined by Tarana. To implement proper Planning IDs in your deployment, open a ticket with Tarana Support.

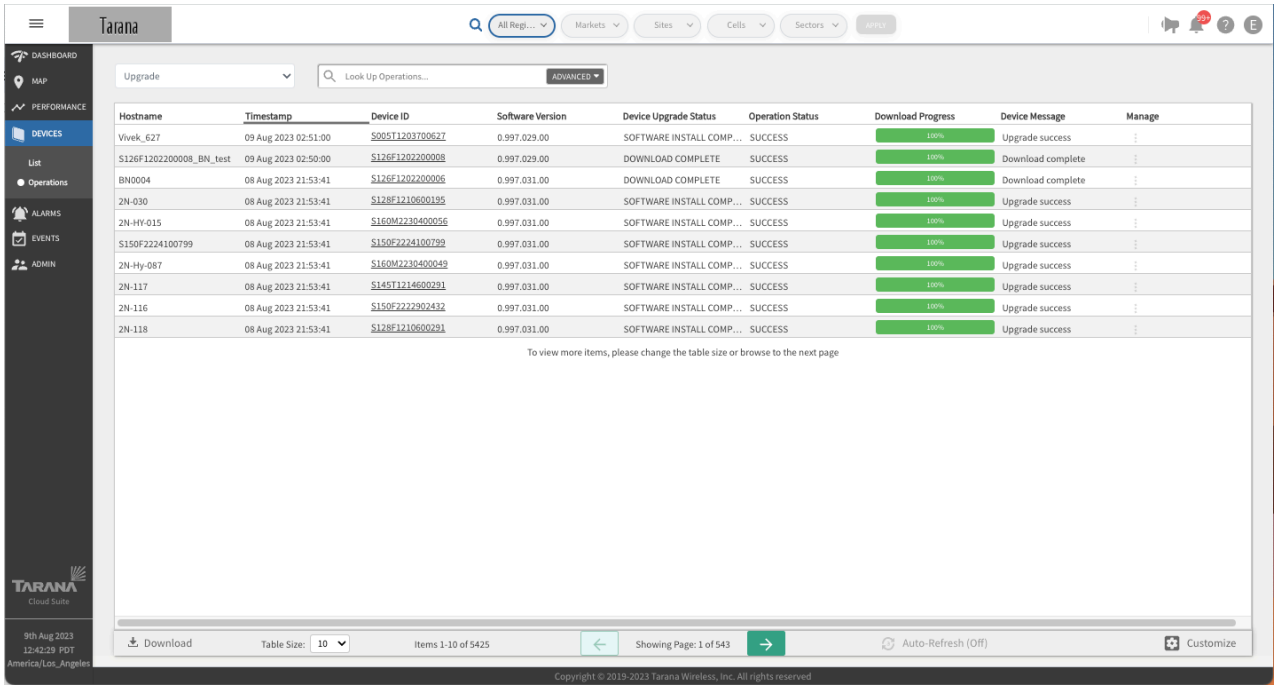
- **Data VLAN**: An optional VLAN setting that overrides the VLAN setting on the base node (the remote node doesn't tag or untag frames).

Remote Node Planning Metrics

- **Data VLAN**: An optional VLAN setting that overrides the VLAN setting on the base node (the remote node doesn't tag or untag frames).
- **Retailer Name**: Name of the retailer operator in wholesale deployment model.
- **SLA Profile**: The service level agreement (SLA) on each remote node, applied to both uplink and downlink traffic.

Device Operations View

To display operational information about base nodes and remote nodes, select **Devices** from the navigation pane, then **Operations**. The screen shows a table of operations that have been performed on the device.



Device Operations View

To view operations by type, select Upgrade, Snapshot, or Reboot from the drop-down menu on the top left.

You can limit the display to a time period: Last 1 hour, last 24 hours, last 1 week, last 2 weeks, or a custom time period.

Enter any value in the Search... box. If it appears in any of the fields, the rows are filtered to show only those rows.

Icons at the top of the table let you control refresh rate, change settings, or download data.

Select the Filter icon ( ) to filter the data by event type, event details, hostname or serial number, or email ID.

The data displayed for each column doesn't refresh automatically. To change this behavior, select the **Auto-Refresh icon** ( ). It remains on for your user account even after you log out. Select it again to turn off Auto-Refresh.

Column categories are dependent on the device type and you can customize them by selecting the Settings icon ( ). Select the fields you want to display, then **Apply**. These changes remain for your user account even after you log out. Use **Reset** to clear your selection.

You can download up to 10,000 events data in CSV format. The download is context sensitive depending on the filters and column topics chosen with Settings. Select the

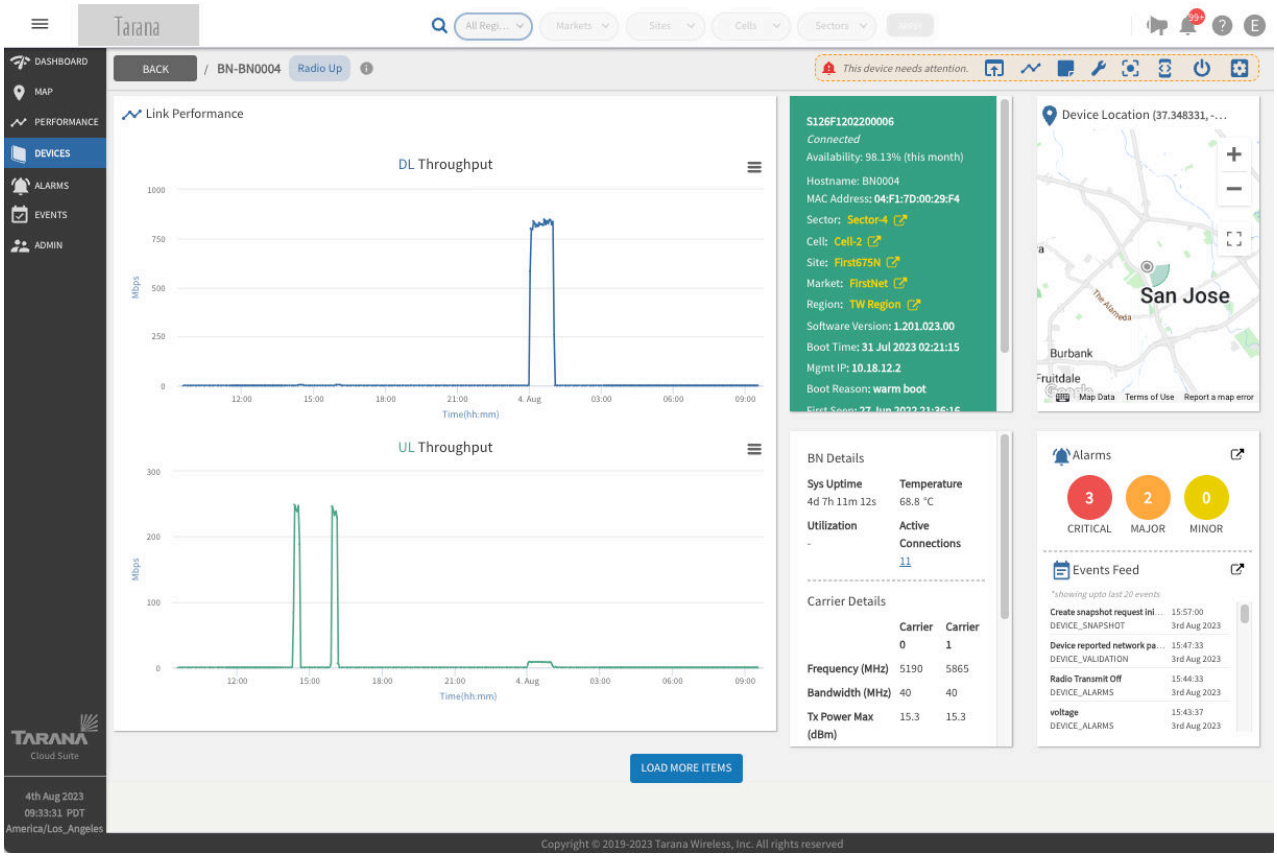
download icon (⭳) and navigate to the folder on your local device where you want to save the file.

Individual Device Dashboard

Navigate to a device individual dashboard by selecting **Devices** in the left side Navigation pane, then select the device serial number. Make sure you've selected the correct network entity for the device you want to display, and check that you've selected the correct device type (remote node or base node).

TCS displays several panes with details about the device.

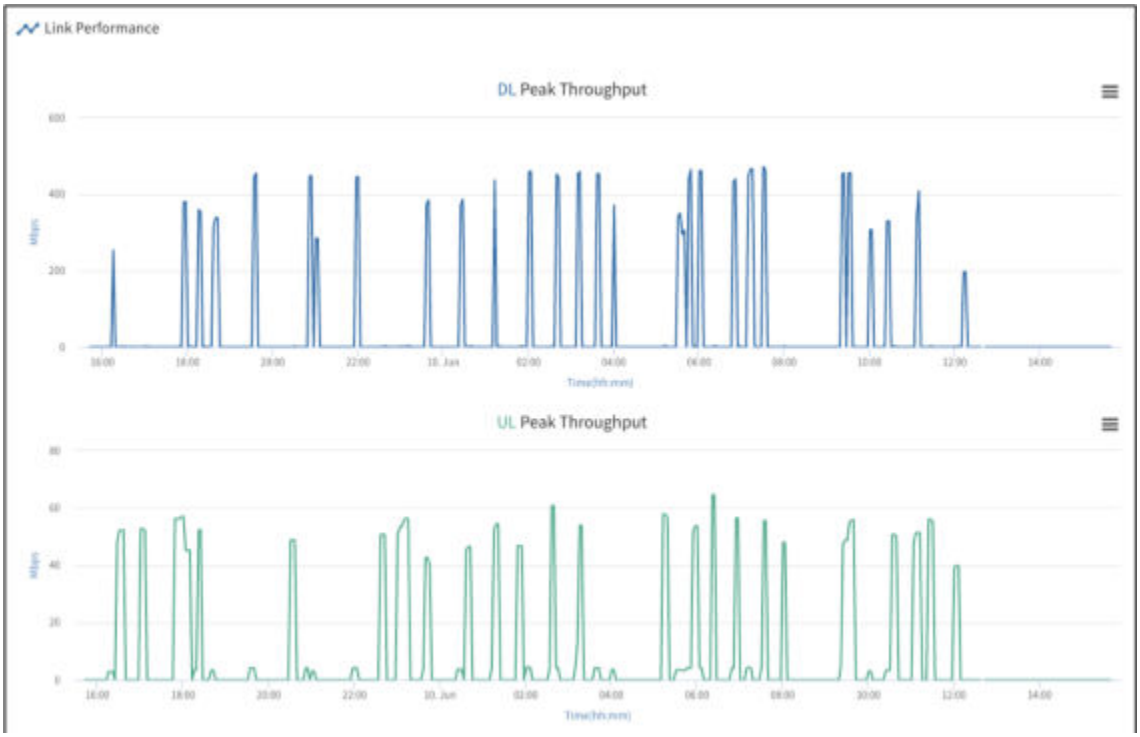
If your user role is NOC Operator or OP Admin, you can use the action icons at the top of the page to perform device management functions. For details, see Device Dashboard Action Icons (page 81).



Individual Device List Dashboard

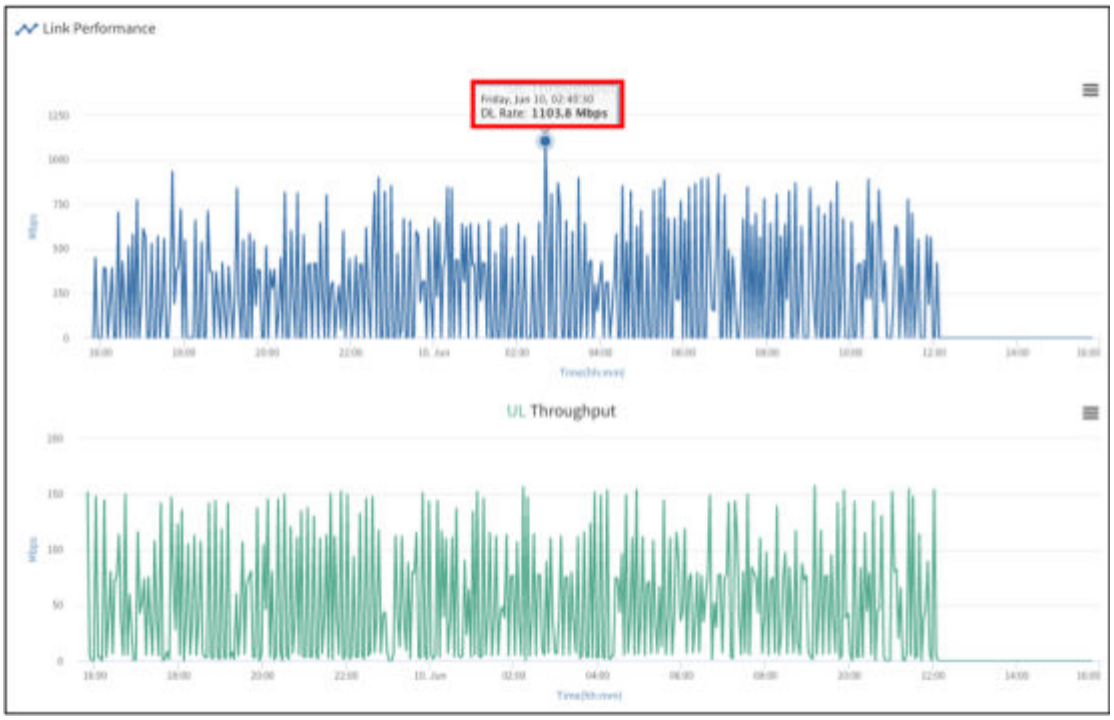
Link Performance

The individual device box for both remote nodes and base nodes is divided into several sections. Link performance is in the upper left quadrant. For a remote node, the graphs show the DL and UL peak throughput over the past 24 hours.



Remote Node Device Dashboard (Link Performance)

For a base node, the graphs show the DL and UL throughput over the past 24 hours. For either device type, mouse over any part of the chart to see the throughput and timestamp. Select the mini menu for any of the link performance parameters to view the chart in full screen, print it, or download the chart as an image (PNG, JPEG, or SVG), PDF, or CSV file.



Base Node Device Dashboard (Link Performance)

Device Summary

The summary box displays some high-level information about the device. A connected device is shown as green. Disconnected devices are shown as gray. Sector, Cell, Site, Market, and Region parameter values are hyperlinks that link to the Performance page for that network entity.

The base node device summary includes the management VLAN IDs and the Air Interface Protocol number.

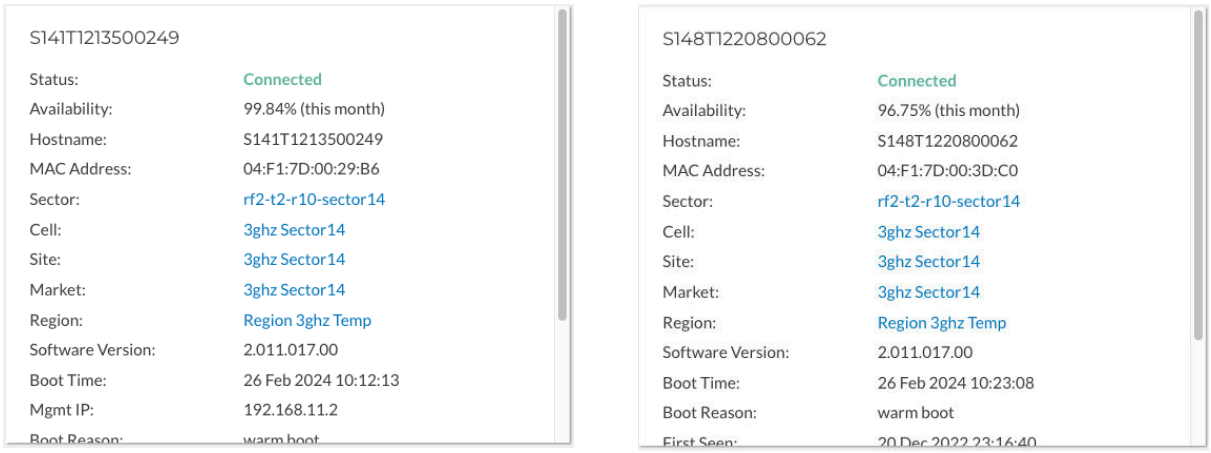
NOTE
By default, the base node is configured with a Data VLAN of 2000. Both the management and Data VLANs are optional. If you use a management VLAN, it must be on a separate VLAN from the Data VLAN. For both VLANs, 4092, 4093, and 4094 are reserved.

The remote node device summary includes the SLA profile and Data VLAN.

NOC L1 NOC OP OP ADMIN

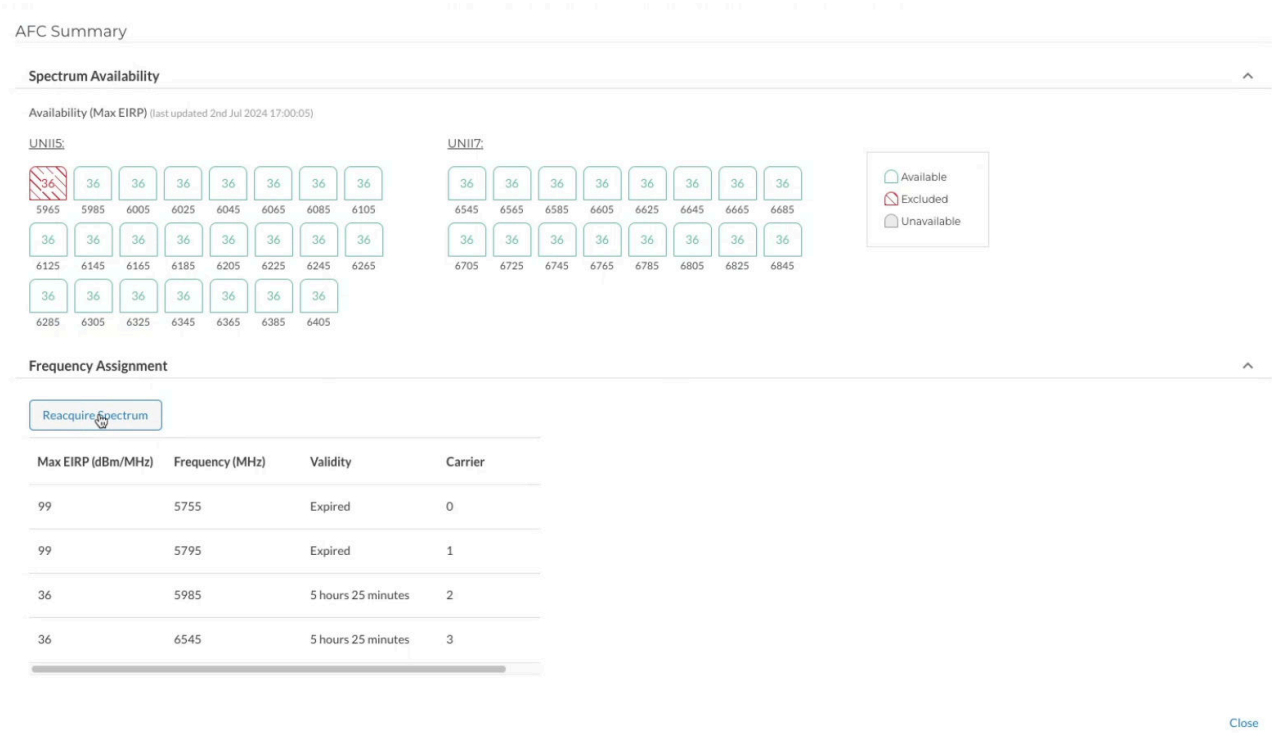
If your role is NOC Operator or OP Admin, you can use the Configuration action icon ( ) to select **Configure Network Parameters** and edit these values.

NOTE
The Data VLAN always exists between the base node and the upstream router. Defining a Data VLAN on the remote node overrides only what the base node uses for that remote node's traffic.



Device Summary (Base Node and Remote Node)

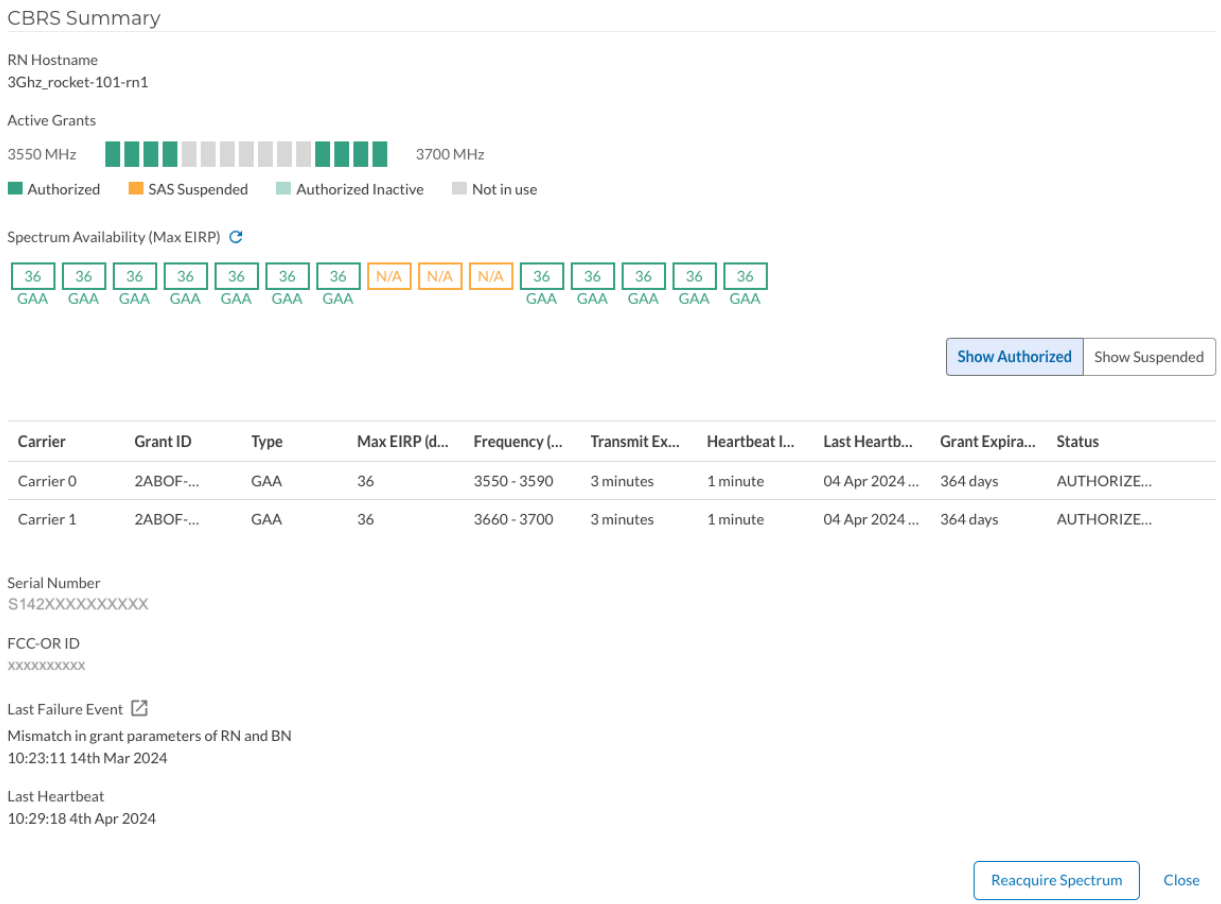
For 6 GHz devices, you can see a display of available channels and corresponding maximum EIRP values by selecting **AFC** from the top of the Device Summary card. You see this screen:



Spectrum Availability

You can reacquire spectrum from this screen (instead of changing an install parameter or waiting for renewal time) by choosing **Reacquire Spectrum** from that screen. Be aware that this affects service.

You can find additional information about CBRS installations by selecting **CBRS** at the top of the Device Summary card. If there are any error conditions such as registration or grant failures, the button turns red to alert you.



CBRS Summary

Tarana devices support Priority Access License (PAL) frequencies. Operators who have purchased PAL licenses and have them enabled with the SAS vendor are able to receive PAL grants. PAL grants in the CBRS band have a higher priority than General Authorized Access (GAA) grants. PAL grants are 10 - 40 MHz wide channels in 10 MHz increments (10, 20, 30, 40) within the 3550 - 3650 MHz portion of the CBRS band.

The CBRS Spectrum Access System (SAS) used by the Operator verifies that the Citizens Broadband Radio Service Device (CBSD) is properly registered for the PAL frequencies and authorizes and assigns their use. The SAS also ensures proper interference protection from GAA users in areas where there are PAL grants.

TCS chooses the CBRS band in this order:

1. Prioritize the band with the highest transmit power allowance. The first consideration is the allowed transmit power. Of all available channels, TCS chooses the channel with the highest transmit power; if more than one channel is allowed the same high transmit power, TCS prioritizes them, then considers the grant license.

2. Prioritize the bands that are PAL bands. If only one PAL band is available, TCS selects it; if there are multiple PAL bands available, TCS prioritizes them, and then considers the frequency. If there are only GAA bands, TCS considers the frequency.
3. Choose the band with the highest frequency. Of the remaining prioritized bands, TCS selects the band with the highest frequency.

When TCS receives a heartbeat message from a CBRS device, the message includes a field that contains the power available for the device to use. TCS increases the transmit power of devices when the SAS increases the power allocation for the device.

Rather than send CBRS grant heartbeats at fixed intervals, TCS uses this criteria to determine the most appropriate heartbeat interval:

- SAS provider
- Operating frequency
- Geographic location

SAS servers synchronize their information during the Coordinated Periodic Activities among SASs (CPAS) time, which occurs every day between 0700 and 1000 UTC. The SAS doesn't approve grant requests during CPAS, so to prevent unplanned network disconnections in CBRS networks, TCS queues CBRS grant requests during CPAS, then sends the queued requests after CPAS.

You can see the assigned PAL grants by going into the base or remote node's individual device page and selecting CBRS in the green information card. The actual grants allocated to the device are at the top of the window under Active Grants. Details about available PAL vs. GAA grants, including the maximum EIRP of each, are under Spectrum Availability and are labeled either PAL or GAA.

If a Dynamic Protected Area (DPA) is activated, the Tarana Domain proxy (DP) automatically requests new grants for the affected devices. This solution typically affects only one of the device's two carriers, which ensures continuous connectivity during a DPA event, but with lower performance than before or after the DPA event. A DPA event is limited to the top 50MHz of the CBRS band. If the device uses 2x40MHz of the spectrum, at least 30MHz of spectrum is not affected.

If you change the frequencies for the Sector, you must reacquire the frequencies spectrum. Select **Reacquire Spectrum** in the CBRS Summary window. Any associated remote notes will lose their connection until the base node reacquires spectrum. The new grants will be visible on this card after 30 seconds. You can use Reacquire Spectrum for either base nodes or remote nodes to request new grants in case of any grant failures.

Remote Node SLA

The remote node service level agreement (SLA) box shows supported SLA profiles. The SLA is set on a per-remote node basis.

If your role is NOC Operator or OP Admin, you can use the Configuration action icon (⚙) to select **Configure Network Parameters** and edit it.

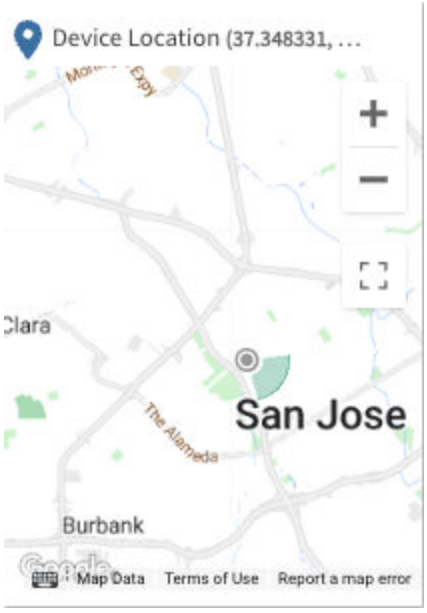
NOTE
The SLA is applied to downlink and uplink traffic.

- Min SLA – 1 Mbps
- SLA 5 – 5 Mbps
- SLA 10 – 10 Mbps
- SLA 20 – 20 Mbps
- SLA 25 – 25 Mbps
- SLA 50 – 50 Mbps
- SLA 100 – 100 Mbps
- SLA 150 – 150 Mbps
- SLA 200 – 200 Mbps
- SLA 250 – 250 Mbps
- SLA 300 – 300 Mbps
- SLA 400 – 400 Mbps
- SLA 500 – 500 Mbps
- SLA 600 – 600 Mbps
- SLA 1000 – 1,000 Mbps
- Max SLA – unlimited (no restrictions)

Device Location

Device Location shows a zoomed-in view of the device plotted on a map. You can adjust the zoom level or show the map in full screen.

You can also view device installation parameters.



Device Location Map

NOC L1 NOC OP OP ADMIN

If your role is NOC Operator or OP Admin you can use the Configuration action icon (⚙) to select **Configure Network Parameters** and edit some device installation parameters on this page.

Operating Information

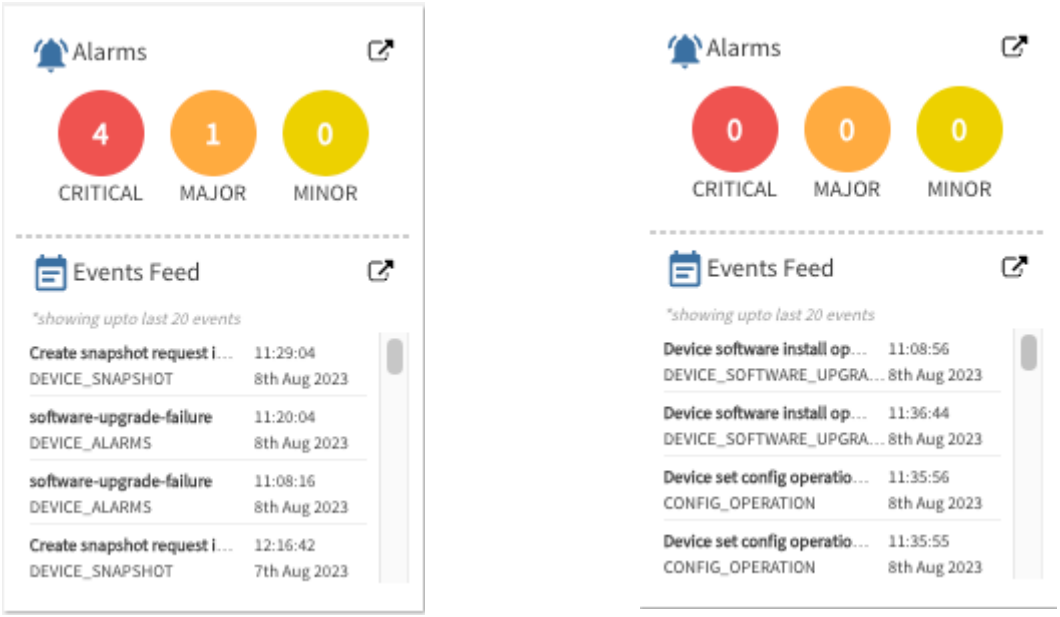
The operating information box displays system information including system uptime, configured radio frequency and bandwidth, utilization, and active connections. The display is different for base nodes and remote nodes.

Operating Information (Base Node and Remote Node)

Alarms Feed

The Alarms Feed box shows a high-level summary of critical, major, and minor alarms. Below that is a real-time feed of events for this device.

The Open in New Tab icon in the upper right of each window opens the Alarms or the Events window for this device.



Device Dashboard: Alarms and Events Feed (Base Node and Remote Node)

Interface Summary

The interface summary box displays important information about network interfaces on the device in a table. This list varies depending on the device type.

NOTE
Cloud Internal indicates the device connection to TCS.

Interface Summary

Interfaces	Admin Status	Data Status	Operational Status	Speed	Duplex	VLAN	IP Address	DHCP Client
Data1 - 10G	Enabled	Enabled	On	10GB	Full	3000	-	-
Data2 - 10G	Disab...	Disab...	Off	UNKN...	Half	0	-	-
Data3 - 1G	Disab...	Disab...	Off	UNKN...	Half	0	-	-
Cloud Int...	Enabled	Disab...	On	-	-	0	-	Disab...
OOB	Enabled	Disab...	On	100MB	Full	0	-	Disab...
Inband M...	Enabled	Disab...	On	-	-	0	-	Disab...

Interface Summary - Base Node

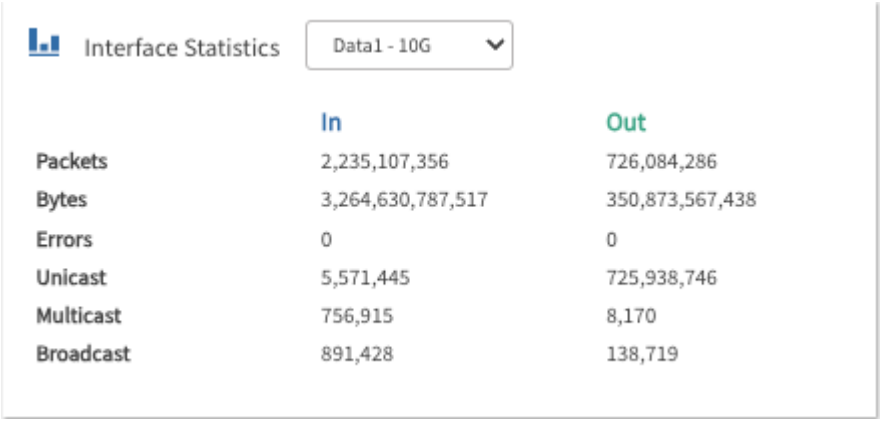
Interface Summary

Interfaces	Admin Status	Data Status	Operational Status	Speed	Duplex	VLAN	IP Address	DHCP Client
Subscrib…	Enabled	-	On	1GB	Full	-	-	-
Cloud Int…	Enabled	-	On	-	-	-	-	-

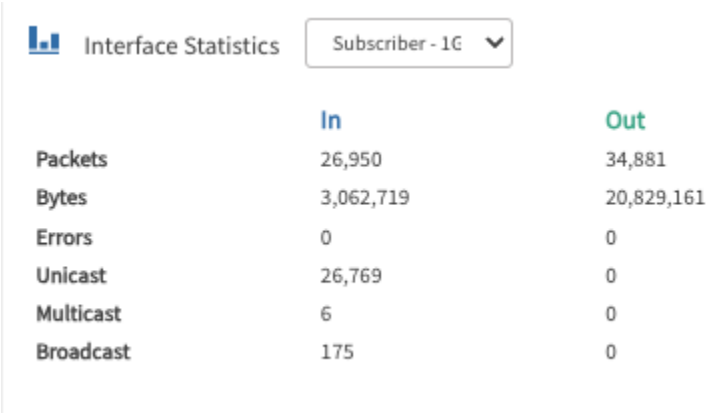
Interface Summary - Remote Node

Interface Statistics

This box displays network packet statistics, listed by packet type as well as ingress or egress. Use the drop-down menu to switch between different network interfaces.



Network Interface Statistics - Base Node



Network Interface Statistics - Remote Node

Alignment Metric

The alignment metric tool provides a visual display of the base-node-to-remote-node alignment. You can use this tool to align the remote node to the base node during installation. A single alignment session is three minutes. When you start an alignment session, a three-minute timer appears so that you are aware of the session progress. As you adjust the tilt and azimuth, the signal meter updates every three seconds, so deliberate adjustments result in quicker alignment. The widget includes:

- Start Button: Visible only when the widget is not actively monitoring the signal strength. When an active session ends, the Start button reappears, and you can start a new alignment session.
- Alignment Meter: Monitors the alignment and updates every three seconds. The meter is arc-shaped and ranges from 0 to 30 with no units; the dark green portion of the arc indicates the degree of alignment with a greater portion of green indicating a greater alignment. It's based on multiple factors, not any one metric.
- Numeric Alignment Display: Below the graphical meter is the numerical representation of the alignment, from 0 to 30.
- Max Alignment Display: As the live signal alignment indicators change and fluctuate, the peak value is recorded. You can reset the max value indicator by selecting the **Refresh** button.
- Minimum Recommended Value: The reliability of a signal is strongly correlated to the signal strength. The Alignment Metric widget displays a recommended minimum value of 12.
- Time Remaining: When you start a session, the Time Remaining value begins to count down from three minutes, indicating how much time is left before the session ends. When the alignment session ends after three minutes, the metric indicators become unavailable and the Start button appears.

To run the alignment metric from the individual device page, select **Start** to begin the three minute alignment session. Adjust the tilt and azimuth of the remote node until the signal meter is at a peak value and moving the remote node in any direction reduces the signal value. If the session expires, you can restart another three-minute session. This is a useful diagnostic tool and is available to all user roles.

MAC Table

This shows the MAC addresses for the CPU, data port, and radios on the remote node and devices connected to the remote node.

Software Banks

Multiple banks allow you to use one bank for operation while newer software versions are loaded on the other bank for use at a later time.

The Software Banks box shows three versions of software:

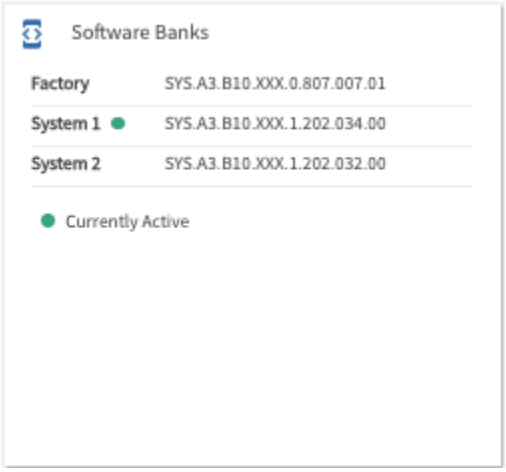
Factory: Software version loaded to factory defaults

System 1: Bank used to house software version

System 2: Redundant bank used to house software version

Either System 1 or System 2 can be the active bank.

The green dot indicates the currently active software version.



Software Banks

Speed Test for Remote Node

Shows information about recent speed tests for a remote node. You can set a baseline for the node from this window.

Base Node Disconnects

The Base Node Disconnects box shows recent disconnects with the date, time connected, duration of disconnect, and software version.

BN Disconnects (5)

Time Disconnected	Time Connected	Duration of Disconnect (hh:mm:ss)	Software Version
06 Sep 2023 11:11:57	06 Sep 2023 11:12:08	00:00:10	SYS.A3.B10.XXX.1.202.034.00
06 Sep 2023 10:49:44	06 Sep 2023 10:51:11	00:01:27	SYS.A3.B10.XXX.1.202.034.00
06 Sep 2023 10:35:41	06 Sep 2023 10:37:47	00:02:06	SYS.A3.B10.XXX.1.202.034.00
31 Aug 2023 19:41:18	31 Aug 2023 19:41:19	00:00:01	SYS.A3.B10.XXX.1.202.034.00
30 Aug 2023 23:46:12	30 Aug 2023 23:46:13	00:00:01	SYS.A3.B10.XXX.1.202.032.00

5 Records Available

BN Disconnects

Remote Node Disconnects

The Remote Node Disconnects box shows recent disconnects with the date, time connected, duration of disconnect, and software version.

RN Disconnects (6)

Time Disconnected	Time Connected	Duration of Disconnect (hh:mm:ss)	Software Version
05 Sep 2023 20:30:52	05 Sep 2023 20:37:22	00:06:30	SYS.A3.R10.XXX.1.202.035.00
05 Sep 2023 20:24:10	05 Sep 2023 20:30:44	00:06:34	SYS.A3.R10.XXX.1.202.035.00
01 Sep 2023 07:54:03	01 Sep 2023 08:00:22	00:06:19	SYS.A3.R10.XXX.1.202.035.00
31 Aug 2023 18:40:52	31 Aug 2023 18:46:45	00:05:52	SYS.A3.R10.XXX.1.202.035.00
31 Aug 2023 18:10:24	31 Aug 2023 18:16:23	00:05:59	SYS.A3.R10.XXX.1.202.035.00
31 Aug 2023 15:15:18	31 Aug 2023 15:20:03	00:04:44	SYS.A3.R10.XXX.1.202.035.00

6 Records Available

RN Disconnects

Device Dashboard Action Icons

The upper right corner of individual device boxes show a set of icons that link to device pages or to actions you can take with the device. If your role is NOC L1 you see only icons for performance, notes, and diagnostics. The actions are:

- Log In to the Web UI (page 81)
- See Performance Page
- Add or View Notes (page 82)
- Diagnostics Operations (page 83)
- Network Operations (Remote Node Only) (page 82)
- Snapshot (page 87)
- Manage Port (page 87)
- Software Install (page 88)
- Reboot Operations (page 90)
- Device Configuration (page 90)

Hover over each icon to see a description.

Log In to the Web UI

If your role is NOC Operator or OP Admin and you have login / password information for the device, you can proxy into it from TCS. Select the **Web UI** icon ( ) to open a new browser window to the login page for the device Web UI. This UI is the same interface that you see if you directly connect through the management port on the device, though you can't upgrade device software from the Web UI if you used TCS to proxy in. See Device Web UI (page 144) for details.

WARNING
Use the Web UI only for initial configuration and setup. TCS settings overwrite web UI settings. To avoid misconfiguration, always use TCS once the device is registered and reachable. TCS flags configuration mismatches with an alarm.

Performance Metrics

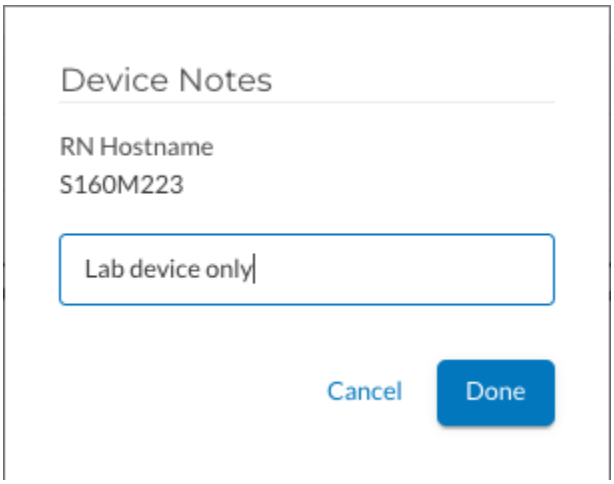
Performance metrics are a valuable troubleshooting tool for individual devices or to compare multiple devices. To see performance metrics for a device, select the **Performance** icon (~) from the top of the page. Use the toggle to set metrics to **Compare KPIs** or **Compare Entities**.

Add or View Notes

NOC L1 NOC OP OP ADMIN

If your role is NOC Operator or OP Admin, you can use Notes to add additional information to a device, such as comments or descriptions. NOC L1 users have read-only access to Notes.

To add or view a note, select the **Note** icon ( ) on the top right of the Device Dashboard screen. Enter your text and select **Update**.



Add Device Note

Network Operations (Remote Node Only)

Select the **Network Operations** icon ((•)) to perform various network actions. Select from the drop down list.

If you selected this option from the remote node's individual device page, only Reconnect to Network is available. This affects service because the remote node will drop its RF link to its current base node and start a new search.

If you selected this option from the Devices List table, you can also set or connect to the primary base node (if enabled by the network admin).

Diagnostics Operations

Select the **Diagnostics** icon (🔧) to perform diagnostics operations. You can select **Speed Test** or **Troubleshoot**.

Speed Test

Before you perform a speed test, ensure that the link you want to test is an active link with a base node and a remote node that can communicate, can send and receive data, and are visible in TCS as active devices. The speed test suspends normal traffic and can disrupt the current active network traffic. Ensure that affected subscribers or network users are aware that the speed test is scheduled.

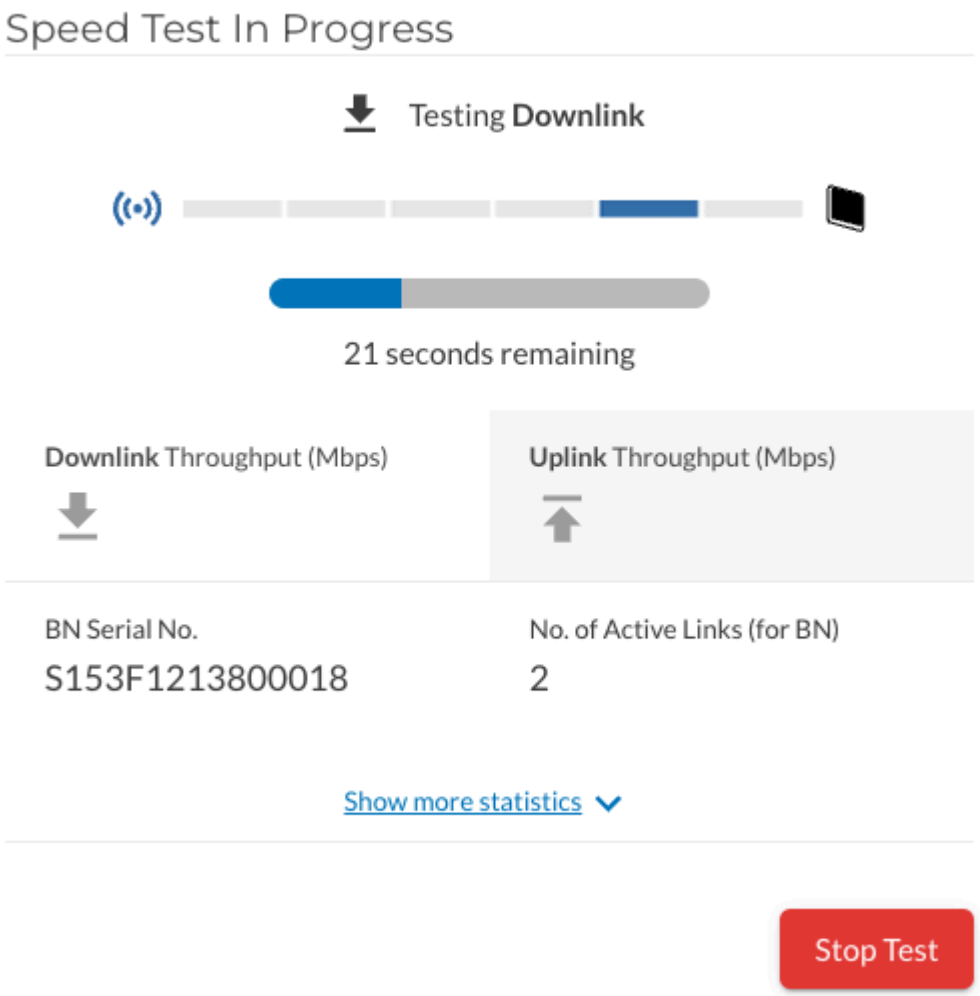
If you select Speed Test, you see a warning that the subscriber's traffic may be affected, and that the speed test can be run on only one link per base node simultaneously. You can run only 1 speed test to a base node at a time.

To start the test, Select **Cancel** or **Start Test**.

The test begins with a downlink test, which takes about 30 seconds. TCS suspends normal data transfer, then sends test data from the base node to the remote node to determine the downlink speed. During the downlink test, the remote node reports the signal-to-noise ratio (SNR) to TCS. As the test proceeds, TCS displays this information.

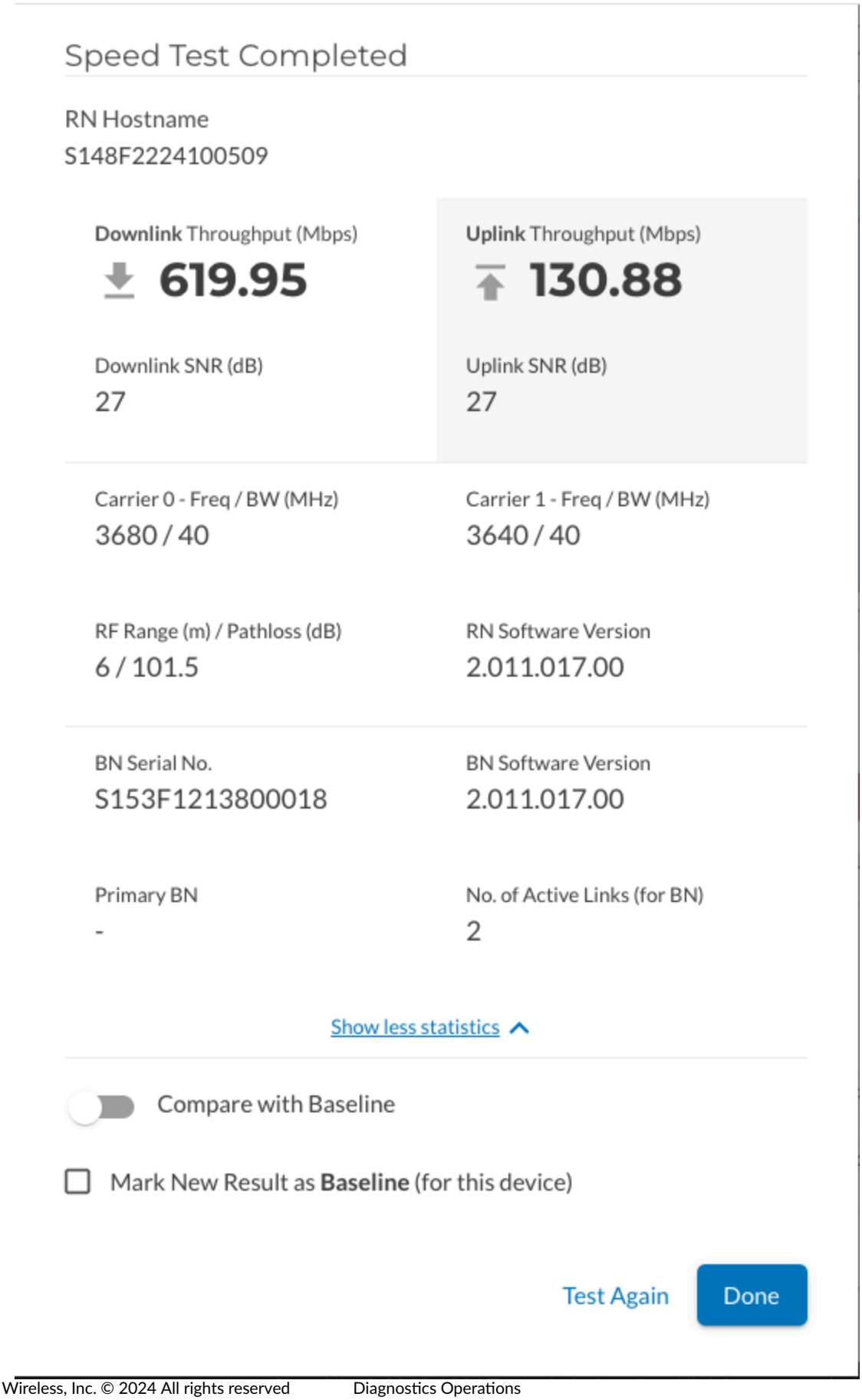
TCS then begins the uplink speed test, which takes about an additional 30 seconds. TCS continues to suspend normal data traffic, then sends test data from the remote node to the base node. During the uplink test, the base node reports the SNR of the incoming signal to TCS.

If you need to stop the test, select **Stop Test**.



Speed Test in Progress

When the uplink test is complete, TCS displays the speed test report. Select **Show More Statistics** to see the expanded report.


Speed Test Completed
RN Hostname
S148F2224100509
Downlink Throughput (Mbps)
619.95
Uplink Throughput (Mbps)
130.88
Downlink SNR (dB)
27
Uplink SNR (dB)
27
Carrier 0 - Freq / BW (MHz)
3680 / 40
Carrier 1 - Freq / BW (MHz)
3640 / 40
RF Range (m) / Pathloss (dB)
6 / 101.5
RN Software Version
2.011.017.00
BN Serial No.
S153F1213800018
BN Software Version
2.011.017.00
Primary BN
-
No. of Active Links (for BN)
2
Show less statistics
Compare with Baseline
Mark New Result as Baseline (for this device)
Test Again
Done

Speed Test Completed

- Downlink and Uplink throughput (Mbps)
- Downlink and Uplink SNR
- Carrier (Carrier 1 for the uplink)
- Carrier frequency (MHz)
- Carrier bandwidth (MHz)
- RF Range in meters (m)
- RN Software Version
- BN serial #
- BN Software Version
- Primary BN
- No. of Active Links (for BN)

You can conduct speed tests during installation as you make adjustments to the network. When you find an optimal configuration, you can establish the speed test of the configuration as the baseline speed test against which you can compare future speed tests. To establish a baseline, conduct a speed test. When the speed test completes, select **Mark New Result as Baseline (for this device)** and **Done**.

TCS stores the result with previous speed tests, but marks it as the baseline, so that you can compare future speed tests with it without having to search for it in the speed test history.

As you monitor, audit, or troubleshoot your network, you can compare periodic or ad hoc speed tests with the baseline. To compare your current speed test with the baseline, conduct a speed test. When the speed test completes select **Compare with Baseline** and **Done**.

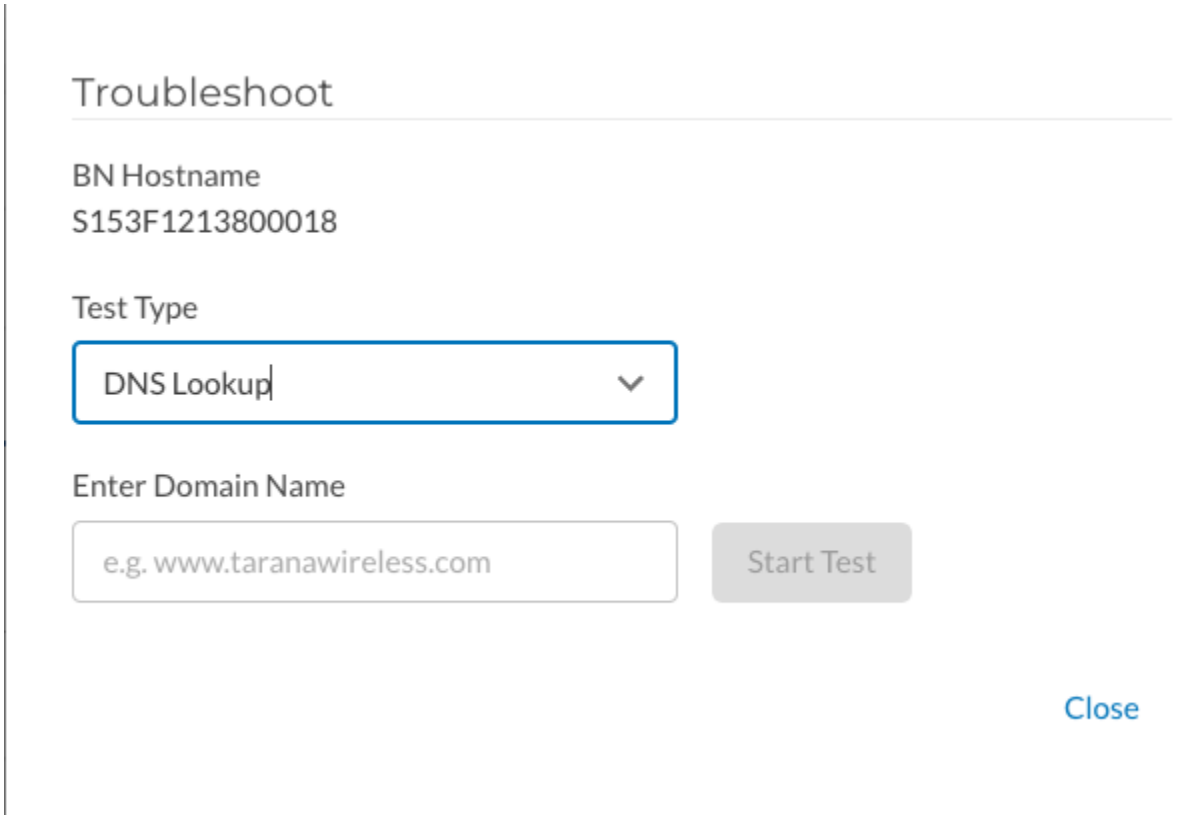
When you enable Compare with Baseline, the Speed Test report dialog displays the results from the current test in normal-color text followed by the baseline values in green text.

API Baseline Speed Test

There's an API for a baseline speed test. The API call is described in the Diagnostics section of the Swagger API documentation, and accessible at the URL `/v1/network/radios/{serialNumber}/speed-test/set-baseline`.

Troubleshoot

For a base node you can select **DNS Lookup**, **Ping**, or **Trace Route** from the dropdown. Enter the domain name and select Start Test.



Troubleshoot

For a remote node you can only perform a DNS Lookup.

Snapshot

Snapshot collects a set of logs intended for troubleshooting when working with Tarana Technical Support. To save a snapshot, select the **Snapshot** icon ( ) on the top right of the screen. Select **Capture Snapshot** to record a snapshot, or **View Operations** to see a list of snapshots that have been performed for this device. The text under the icon changes to "Snapshot Request sent successfully" when the snapshot is complete.

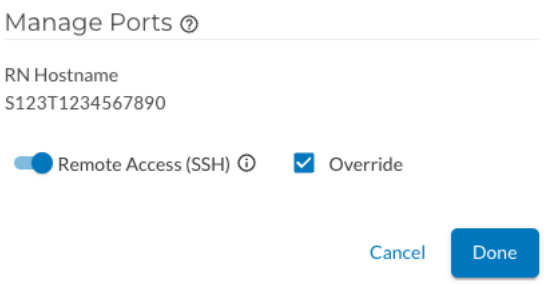
Snapshots can be retrieved from TCS by Tarana Support and engineers.

Manage Port

Select **Manage Ports** to activate or deactivate SSH access. Unless overridden, each port inherits the global configuration. The default is deactivated.

To activate SSH port 22 access on a particular device, do the following:

1. Log in to TCS.
2. Navigate to **Devices > List**.
3. Select the device serial number to view the single device page of the device you want to configure.
4. Select **Manage Port (** **) > Manage Ports** from the tool bar.
5. By default, the switch reflects the current global setting. To override the default setting, select **Override**, and then activate **Remote Access (SSH)** to allow SSH access on the device.

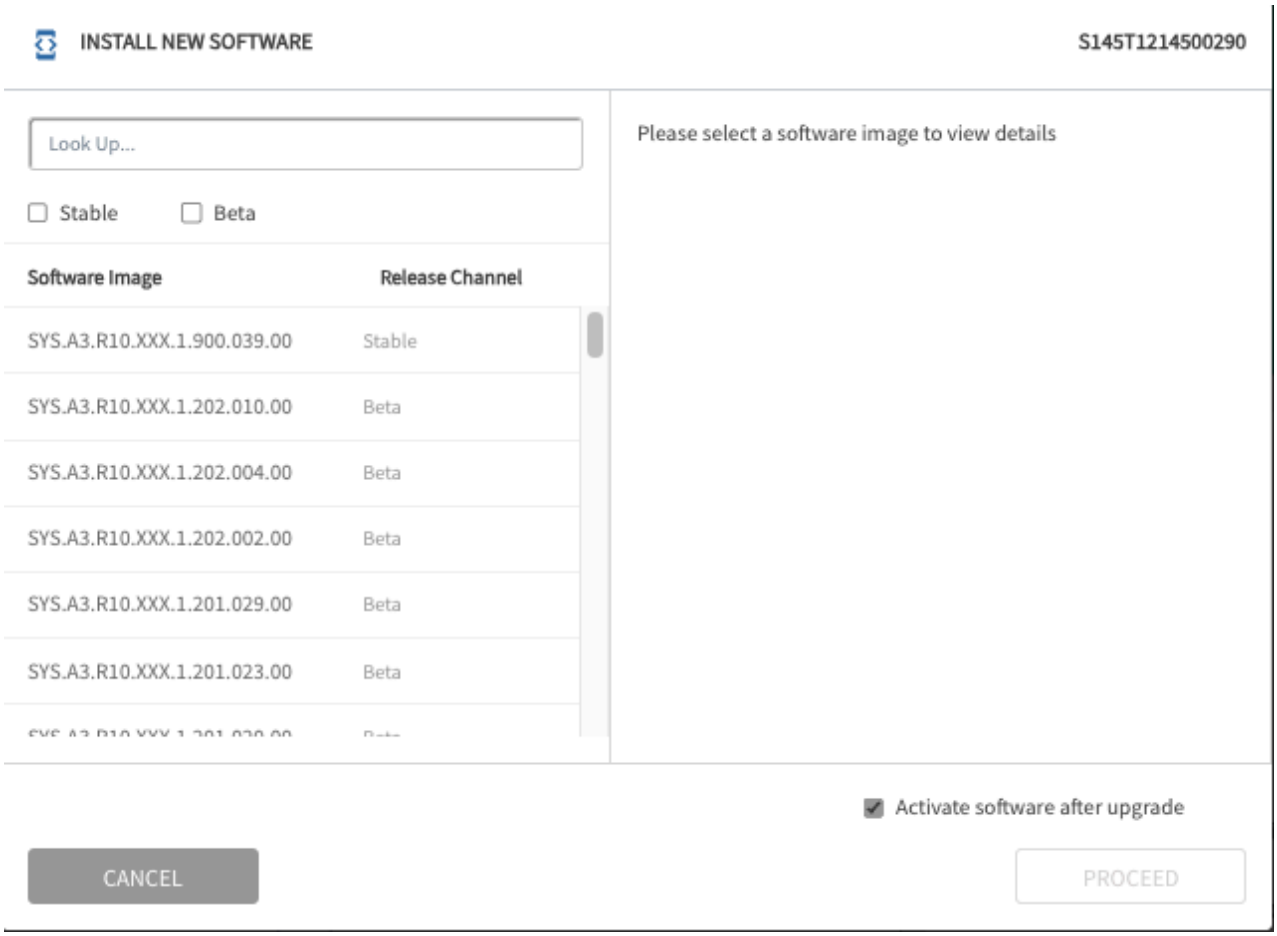


6. Select **Done**.

Software Install

To install new software in this device, select the **Software install** icon ( ). Select **Install New Software** to perform a software installation, **Switch Boot Bank** to switch between System 1 or 2 boot banks, or **View Operations** to see the history of operations on the device.

When you choose **Install New Software**, you see a list of available image files. You can check boxes to select **Stable** or **Beta**. When you select an image, you see the build date and file size. Check **Activate software after upgrade** if you want the device to immediately reboot after installation. Select **Proceed** to continue with the software upgrade, or **Cancel** to exit.



Upgrade Device Software

To switch the boot bank on a device using the TCS interface, do the following:

1. Log in to TCS with OP Admin privileges.
2. Navigate to **Devices > List** to display devices.
3. Select the serial number of the device to view the single device page.
4. Select **Install Software ( ) > Switch Boot Bank**.

NOTE
You can switch the boot bank on only one device at a time.

When you select **View Operations**, you see a list, by serial number and hostname, of operations on the device. You can choose columns to view with the Settings (⚙) icon. Under Action(s) you can select **Retry** to perform the operation again. Use the filter (to filter by Operation ID, Batch ID, or Operation Status.

You can limit the display to a time period: Last 1 hour, last 24 hours, last 1 week, last 2 weeks, or a custom time period.

Reboot Operations

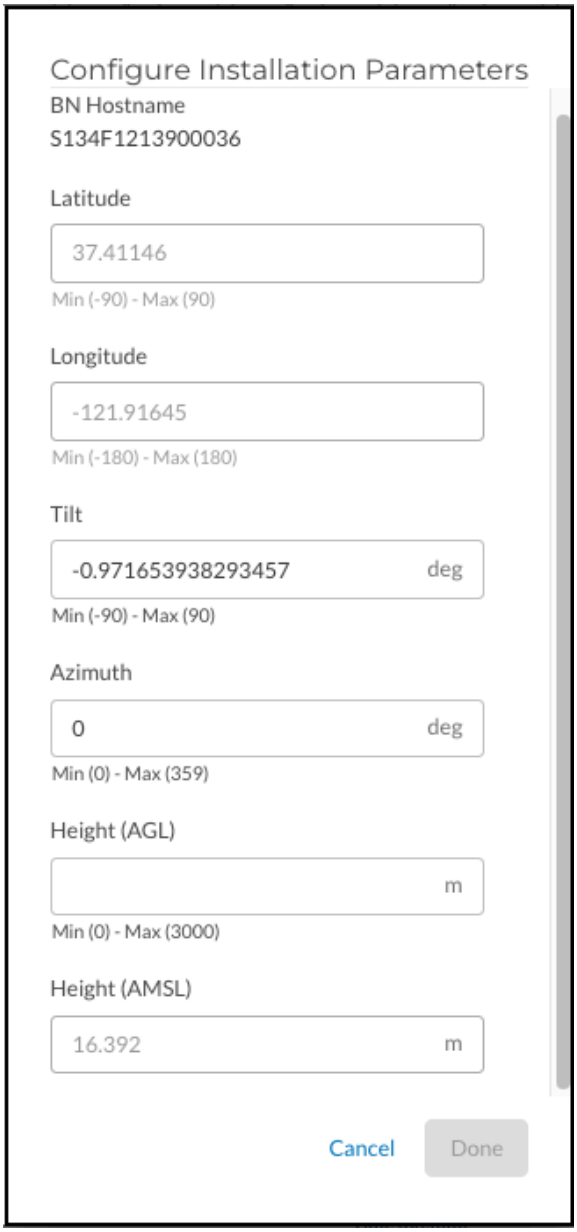
To perform reboot operations, select the **Reboot** icon (⏻). Select **Reboot** to perform a reboot, or **View Operations** to see the history of operations on the device.

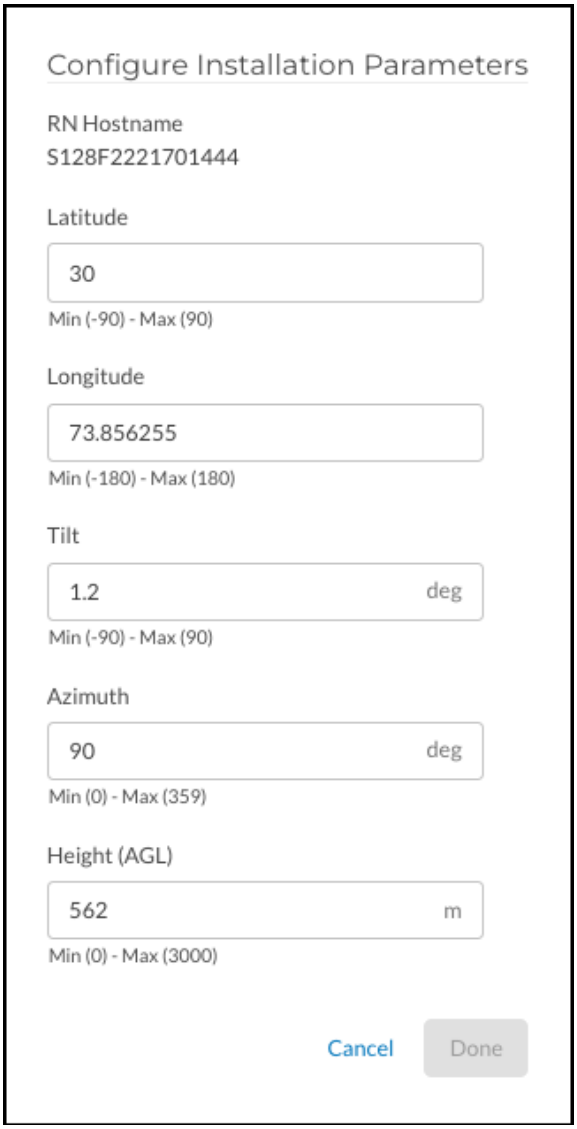
When you choose **Reboot**, the system asks you to confirm the action. Choose **No** to exit or **Yes** to continue.

Device Configuration

To perform various actions on a device, select the **Settings** icon (⚙) and choose an action from the drop down list:

Configure Installation Parameters



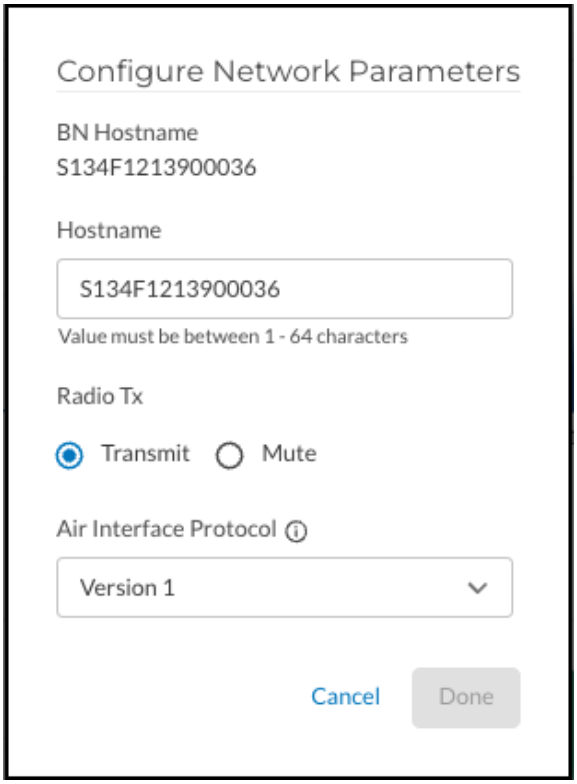


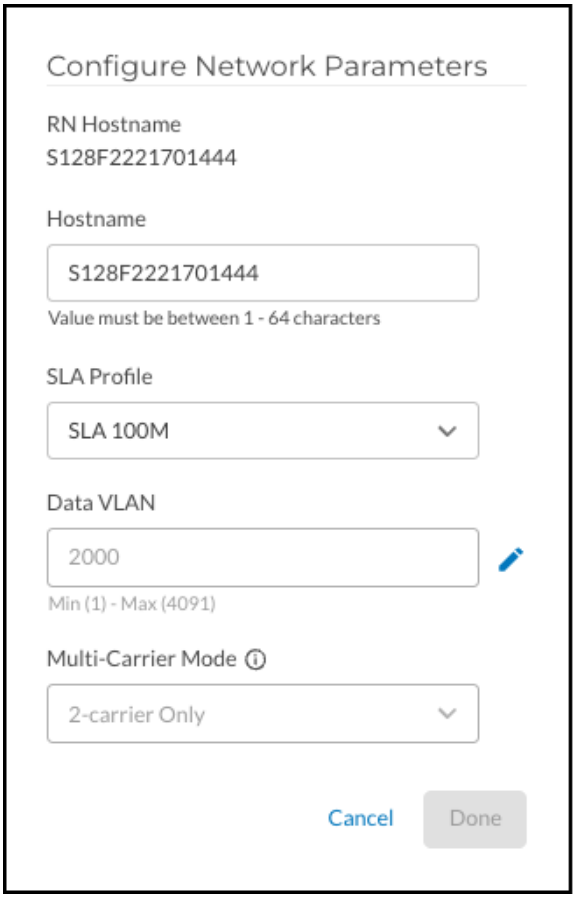
Base Node and Remote Note

- **Latitude**: Grayed out for base nodes and for 6GHz remote nodes because you can't change the value.
- **Longitude**: Grayed out for base nodes and for 6GHz remote nodes because you can't change the value.
- **Tilt**: Minimum (-90), maximum (90). The CBRS protocol requires an up tilt to be registered as negative and a down tilt as positive.

- **Azimuth**: Minimum (0), maximum (359)
- **Height (AGL)**: Minimum (0), maximum (3000)
- **Height: (AMSL)**: Only for base nodes.

Configure Network Parameters





Base Node and Remote Node

- **Hostname**:
  Hostname must be from 1 to 63 characters long. Valid characters are ASCII(7) letters from a to z, A to Z, digits 0 to 9, hyphen, and underscore. It may not start or end with a hyphen. Consecutive hyphens (2 or more) are not allowed. Hostname is case-sensitive. Not allowed: spaces, special characters, periods.
- **Radio Tx**: Transmit or Mute. Base node only.
- **Air Interface Protocol (AIP)**: (Base node only) 6-GHz (UNII-5 / UNII-7) and quad-carrier operations require minimum Air Interface Protocol Version 1. Air Interface Protocol Version 1 supports 6GHz devices and enhances signaling capabilities across 3GHz /

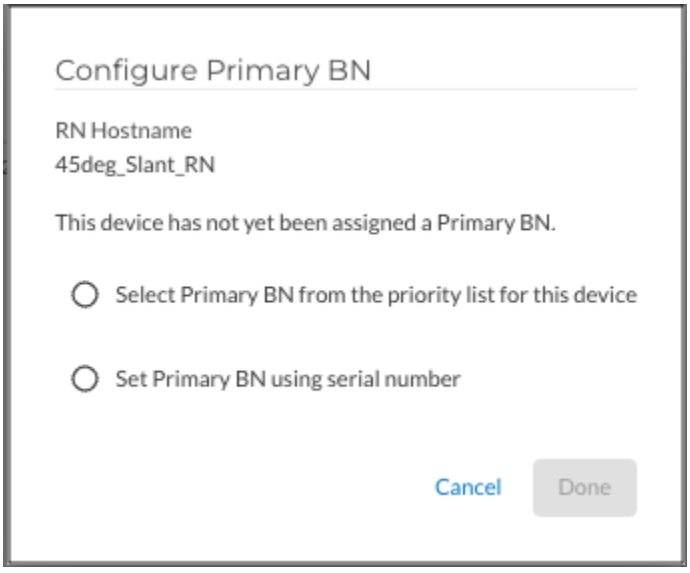
5GHz / 6GHz devices. For details about Air Interface Protocol, including versioning and migration, see Air Interface Protocol Version 1 (page 162).

- **SLA Profile**: The service level agreement (SLA) on each remote node, applied to both uplink and downlink traffic.
- **Data VLAN**: An optional VLAN setting that overrides the VLAN setting on the base node (the remote node doesn't tag or untag frames).
- **Multi-Carrier Mode**: V2.0+ Select 2-carrier or 4-carrier mode. Only 6-GHz RNs on software version 2.0 or higher support 4-carrier mode. 5-GHz and 3-GHz devices support only 2-carrier mode. 6-GHz devices use only two carriers (2x40 MHz) if configured in 2-carrier mode.

Configure Primary Base Node (Remote Node Only)

NOC L1 NOC OP OP ADMIN

This feature is disabled by default. A pop up shows the current assigned Primary Base Node for this device.



Configure Primary Base Node

If your role is OP Admin, you can select a radio button for one of these options:

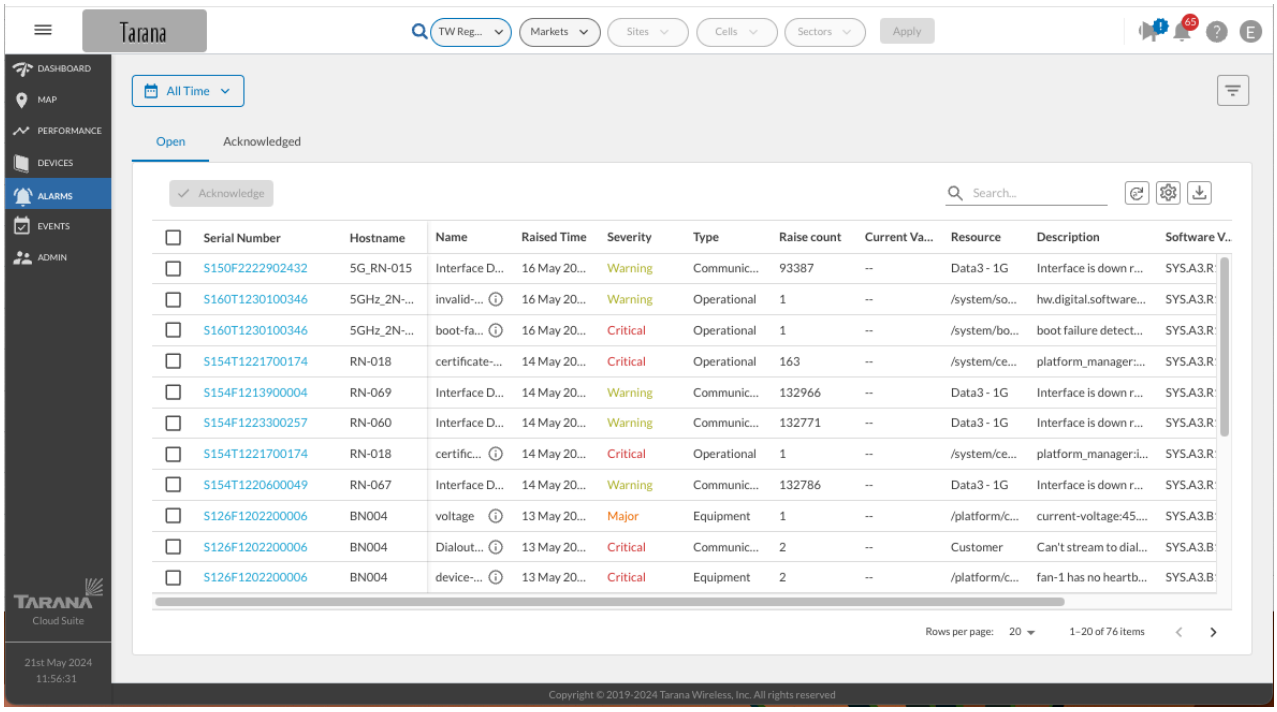
- Select Primary BN from the priority list for this device
- Set Primary BN using serial number
- Remove the Primary BN for this device.

Reset Telemetry Data

Reset Telemetry Data : A popup shows a message that DL Life Time Peak and UL Life Time Peak will be reset for the device, and can't be undone. Select **No** or **Yes** to cancel or proceed.

Alarms Dashboard

Select **Alarms** in the left side navigation pane to open the Alarms dashboard. TCS stores alarm information for up to three months.



Alarms Dashboard

The default view is of alarms for the last device you viewed.

Make sure that you've chosen the correct network entity from the drop-down menus at the top. This filters the network down to the granularity you need. Because the menus are hierarchical, start by selecting the Region, then Market, Site, Cell, and Sector, as needed.

To sort in ascending or descending order, select a column heading.

There are two tabs you can use to view alarms: Open and Acknowledged. When an alarm is raised, it appears in the Open tab. When you select an alarm, then select Acknowledge, it moves from the Open tab to the Acknowledged tab. When you un-acknowledge an alarm, it moves from the Acknowledged tab back to the Open tab.

You can acknowledge alarms that don't require action, such as minor alarms that arise because of known conditions. If you determine that an acknowledged alarm requires action, you can un-acknowledge the alarm.

You can limit the display to a time period: Last 1 hour, last 24 hours, last 1 week, last 2 weeks, or a custom time period.

Enter any value in the Search... box. If it appears in any of the fields, the rows are filtered to show only those rows.

Icons at the top of the table let you control refresh rate, change settings, or download data.

Select the Filter icon ( ) to filter the data by alarm source (BN, RN, or TCS), severity, alarm type, and hostname or serial number.

Alarm types include:

- **Communication:** Error in communication. Example: network interface down, unable to get DHCP address (if enabled), IP address conflict, unable to resolve hostname (DNS failure).
- **Environmental:** Issues with the operational environment. Example: the number of GPS satellites available for GPS is low.
- **Equipment:** Hardware error. Example: temperature isn't within thresholds.
- **Integrity:** Integrity errors.
- **Operational:** Error in system operations. Example: a remote node is unable to reach its base node, high CPU utilization, low disk space, no GPS update, timing error, firmware error.
- **Other:** Any alarms that aren't otherwise classified.
- **Physical:** Physical problems with a device.
- **Processing:** Error in system processing. Example: configuration update failure.
- **Qos:** Quality of service.
- **Security:** Security alarms.
- **Time domain:** Timing alarms.

The data displayed for each column doesn’t refresh automatically. To change this behavior, select the **Auto-Refresh icon** ( ). It remains on for your user account even after you log out. Select it again to turn off Auto-Refresh.

Use the **Settings** icon ( ) to choose which fields are displayed and control row density. Options include:

- **Current Value:** The current value from the last alarm as applicable. For example, if a CPU utilization alarm is raised and the associated value is 60%, the current value reflects the 60%.
- **Description:** A brief description of the alarm.
- **Hostname**: Identifier used to distinguish the device on a network. By default, hostname is the device serial number.
- **Name:** The name of the alarm.
- **Raise Count:** The number of times this alarm has been raised.
- **Raised Time:** The time the alarm was raised.
- **Recommended Action:** Recommended action to resolve the alarm.
- **Resource:** The source of the alarm within the system.
- **Serial Number**: A string that uniquely identifies a device or component. Displayed by default.
- **Severity:** The severity of the alarm (WARNING, MINOR, MAJOR, CRITICAL).
- **Software Version**: The software version the device is running.
- **Type:** The alarm type.

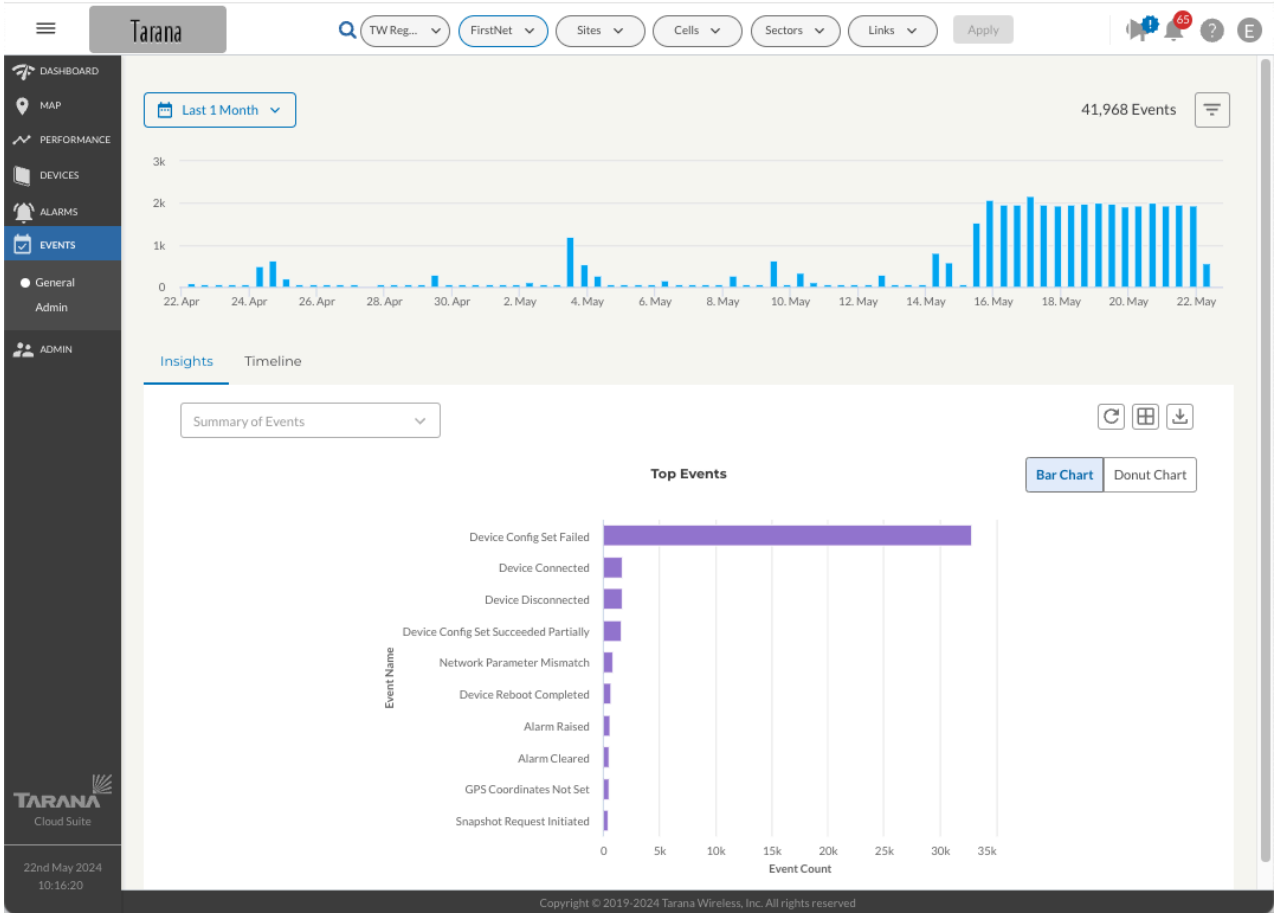
Select the fields you want to display, then **Apply**. These changes remain for your user account even after you log out. Use **Reset** to clear your selection.

Select the **Download** icon (⭳) to download a comma separated (CSV) list of all displayed alarms (meaning the saved file content is filter sensitive). Navigate to the folder on your local device where you want to save the file.

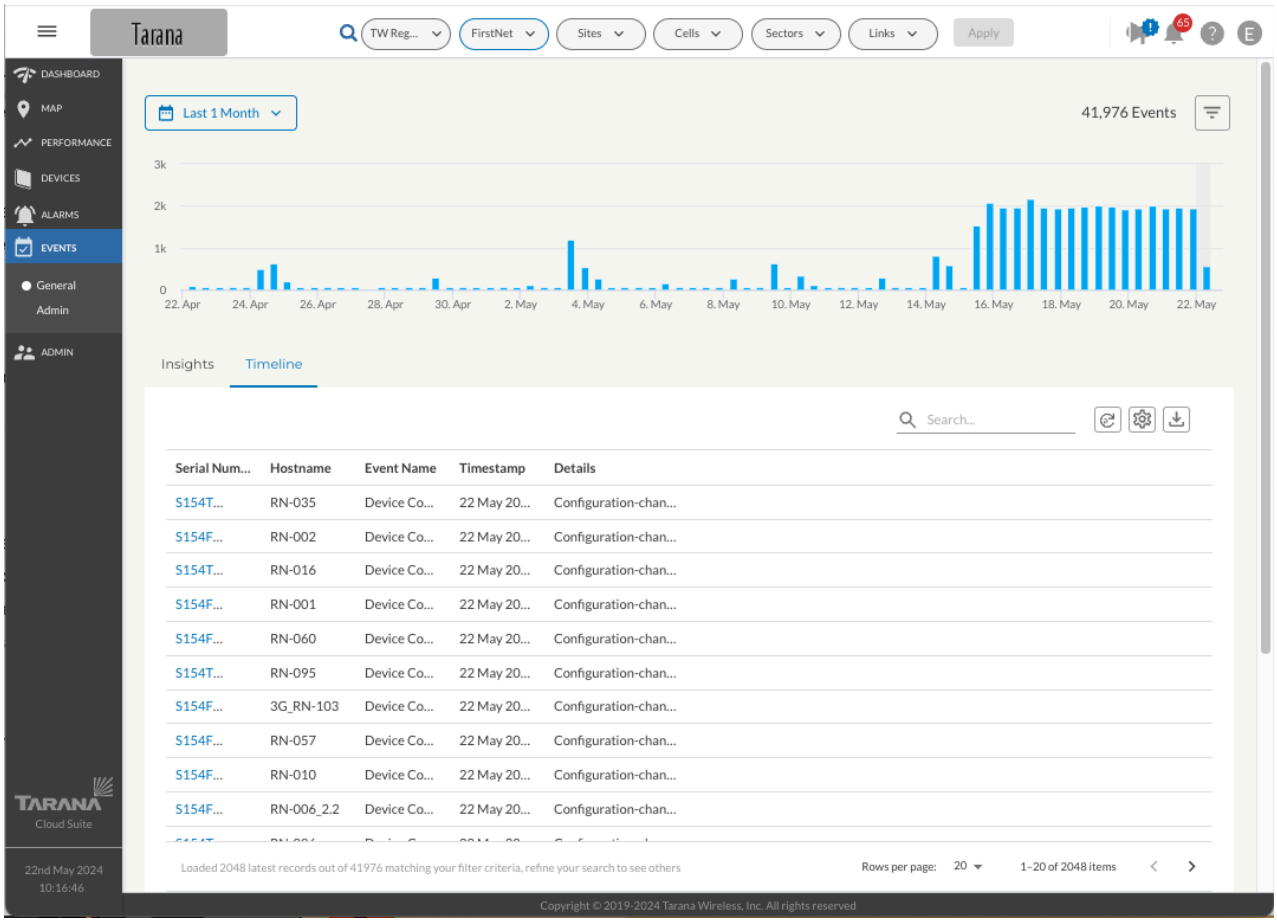
Events Dashboard

To open the Events dashboard, select **Events** in the left side navigation pane. TCS stores event information for up to three months.

At the top of the page there's a vertical bar chart that summarizes activity over time. Below is a pane with two tabs: Insights and Timeline. The Insights tab displays a horizontal bar chart with the top events by number. You can choose to view the events as a donut chart. The Timeline tab displays a table of events in time order with the most recent events at the top.



Events - Insight View



Events - Timeline View

Make sure that you've chosen the correct network entity from the drop-down menus at the top. This filters the network down to the granularity you need. Because the menus are hierarchical, start by selecting the Region, then Market, Site, Cell, and Sector, as needed.

Sector represents the selection of the Sector base node. The Events dashboard has an extra layer of filtering granularity, Links. The Links filter includes a drop-down showing all remote nodes connected to the selected base node under Sector. To see events for that remote node, select a specific remote node under Links.

You can limit the display to a time period: Last 1 hour, last 24 hours, last 1 week, last 2 weeks, or a custom time period.

Enter any value in the Search... box. If it appears in any of the fields, the rows are filtered to show only those rows.

Icons at the top of the table let you control refresh rate, change settings, or download data.

Select the Filter icon (⚌) to filter the events by event type, specific event, hostname or serial number, or email ID. Event types are:

- **All Events:** Lists all events regardless of type.
- **Network:** Network-related events, such as Device Connected / Disconnected.
- **Alarm:** Events that may require attention, such as Interface Down or TCS Unreachable.
- **Operations:** Events that describe manual interventions, such as Device Configuration Set Initiated.
- **Spectrum:** Events for the CBRS spectrum. When the Spectrum Access System (SAS) rejects a grant request, the unsuccessful grant appears in this tab. By collecting grant request rejection messages in a single location, administrators can use the information to troubleshoot network behavior.
- **Admin:** Administrative events (only visible to OP Admin).
- **Config**: Configuration events.

The data displayed for each column doesn't refresh automatically. To change this behavior, select the **Auto-Refresh icon** (⟳). It remains on for your user account even after you log out. Select it again to turn off Auto-Refresh.

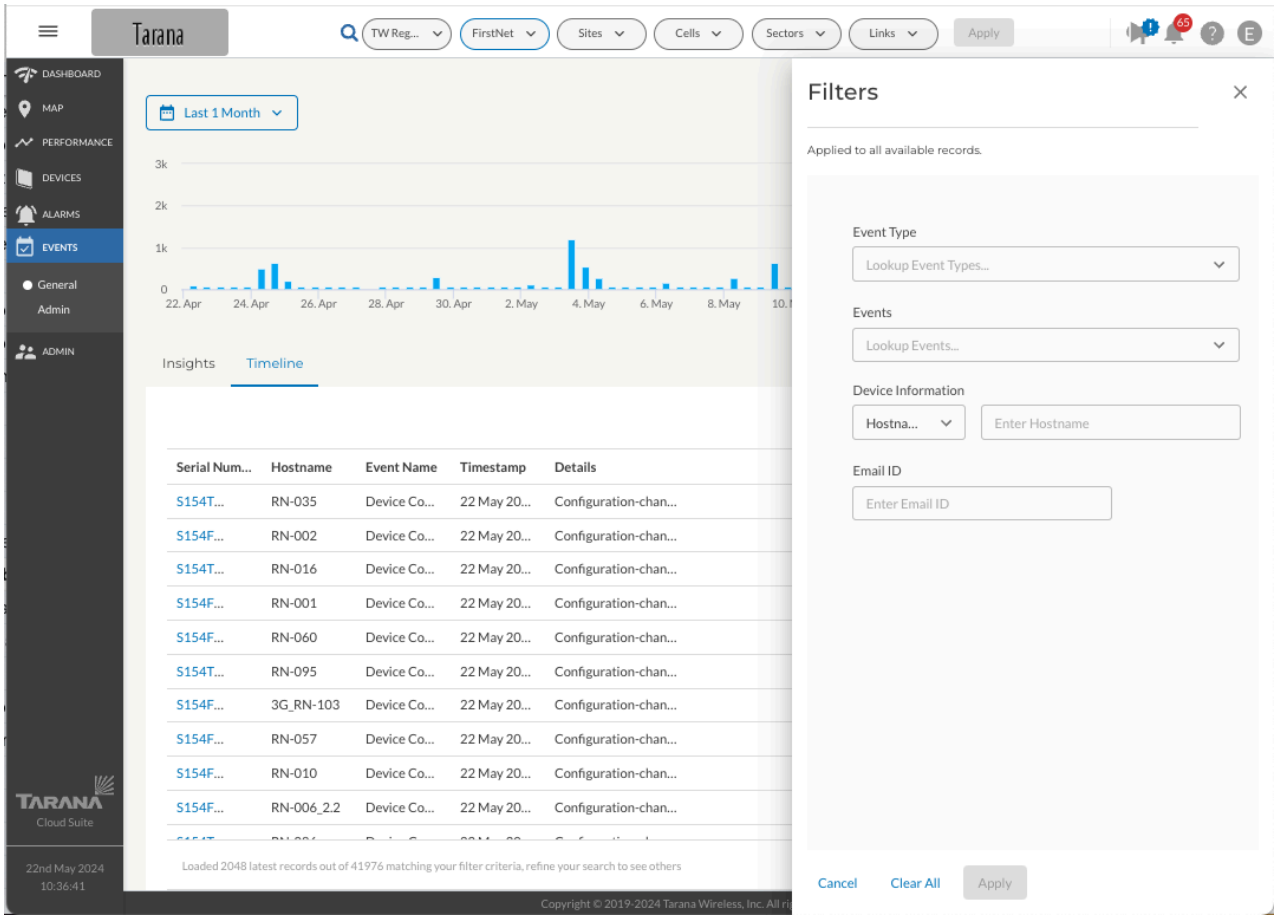
Use the Settings icon (⚙) to choose which fields are displayed and control row density. Options include:

- **Alarm Duration:** How long the alarm persisted before being cleared.
- **Alarm ID:** Brief description of the alarm.
- **Category:** Category of the alarm.
- **Details:** Detailed description.
- **Event Name:** Alarm Raised or Alarm Cleared.
- **Event Source:** Source of the event: TCS, remote node, base node.
- **Hostname**: Identifier used to distinguish the device on a network. By default, hostname is the device serial number.
- **Serial Number:** Serial number of the device. This is a link you can use to see the device's detail page.
- **Severity:** Warning, Major, or Critical.
- **Software Version:** Software version of the device.

- **Timestamp:** Timestamp when alarm was initiated.
- **User Email:** User email.

Select the fields you want to display, then **Apply**. These changes remain for your user account even after you log out. Use **Reset** to clear your selection.

Admin: If your role is OP Admin, you can select the Admin event type. Select it to see administrative events in the network. These include alarm, network, operations, spectrum, and other events. Within type, you can filter in different ways. You can also search by hostname or email ID.



Events Table Filter

TCS Admin Actions

All of these actions require you to have the OP Admin role. Use the Admin menu in the navigation pane to perform them:

- Network Configuration (page 103)
- Configure Alerts (page 123)
- Manage User Accounts (page 124)
- Software Inventory (page 129)
- Add and Test Webhooks (page 130)
- Manage APIs (page 135)

Network Configuration

A network entity is a group of base nodes and remote nodes, within a hierarchy. Before you can assign equipment, you must create the hierarchy. Hierarchy is defined from highest to lowest:

- **Region:** Typically a large geographic area like a small country, or part of a large country.
- **Market:** A geographical area within a Region, like a large city or metropolitan area.
- **Site:** An installation within a Market, like a tower.
- **Cell:** An array of base nodes at a Site, used to service remote nodes that are within proximity of the Site.
- **Sector:** An individual base node and its connected remote nodes.

A Region can contain multiple Markets, Markets can include multiple Sites, and Cells can include multiple Sectors, depending on specific deployment requirements. Each hierarchy entity assigns its attributes to all deployed devices beneath it.

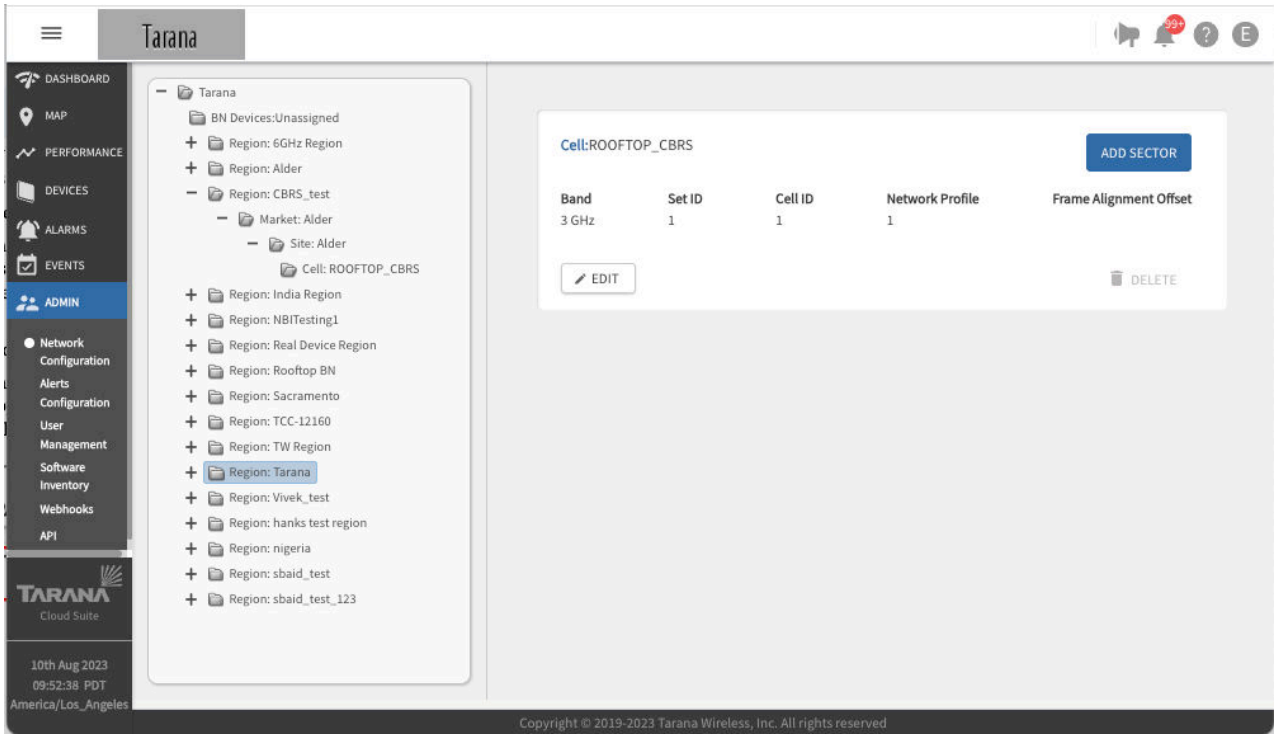
At the top of the configuration hierarchy is the Operator, which is typically the name of the company that owns the G1 devices. Beneath the operator folder is a folder for unassigned base nodes, BN Devices: Unassigned. All base nodes that have not yet been assigned to a network are placed in this location in the network list.

Base nodes are added to TCS by Tarana. When an operator orders a base node, that base node's serial number is reported by distribution to Tarana support, who add it to the

Operator's instance of TCS. It then appears in the BN Devices: Unassigned folder. You can configure an alert to inform you when base nodes have been added.

This level also includes customer-defined deployment regions.

Below that is a hierarchical view of the operator network as defined by the operator that shows configured regions. Select the plus (+) sign to expand each region and show the rest of the hierarchy.



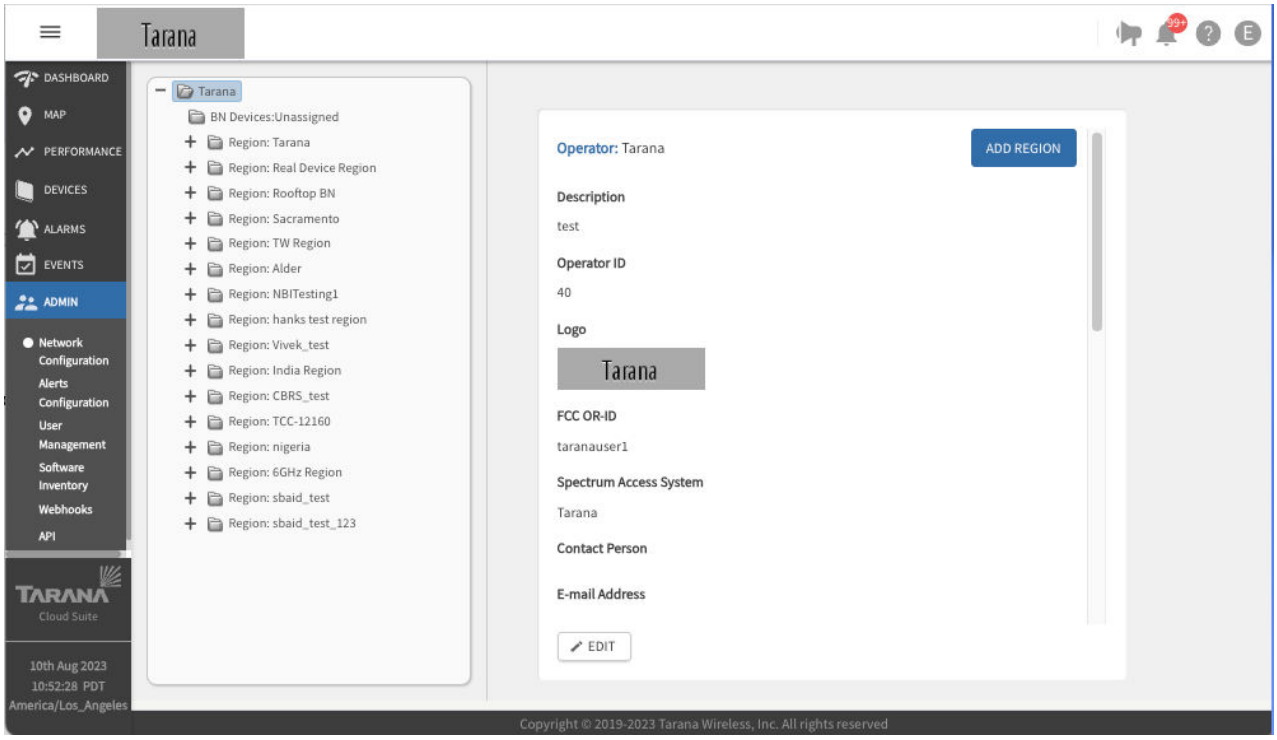
Network Configuration Hierarchy

To configure your network, select **Admin > Network Configuration** from the navigation pane.

Edit Operator

NOC L1 NOC OP OP ADMIN

An Operator in TCS typically refers to the company that owns the Tarana equipment. Operator Name is typically the purchasing company name. To edit operator information and policies, choose the operator name at the top of the hierarchy tree and select **Edit**. If you make any changes, select **Done** to save them or **Exit** to cancel.



Operator Configuration

Operator configuration information includes:

- **Operator Name:** The name of the operator.
- **Description**: An informative description (optional).
- **Operator Logo:** Allows an operator to upload a logo file for an image that's displayed on the TCS portal and appears in the upper left corner of every TCS window. File must be in PNG, JPG, or GIF format with a maximum size of 500KB. Select **See more guidelines** to see logo image requirements. The logo is displayed at 50px high and 145px wide. If you upload a larger or smaller image, it's resized.
- **Contact Person**: Name of a contact person (optional).
- **E-mail Address**: The contact person's email address (optional).
- **Time Zone:** The time zone for the maintenance window and timestamps within TCS.
  The time zone set here only affects the maintenance window used for the auto software upgrade policy. All other timestamps shown in TCS are based on the individual user's time zone setting under User Profile.
  For networks that cross time zones, admins should note that this one time zone is applied to all network devices for purposes of imposing the auto upgrade policy. Software upgrades are service affecting when the device finishes the download and then reboots.

- **Default SLA Profile:** The Service Level Agreement profile. You can't edit this value.
- **CBRS Configuration:**
  - **FCC OR-ID:** Only required for CBRS operation. The FCC OR-ID is assigned to customers by the Spectrum Access System (SAS) provider.
  - **SAS Provider:** Only required for CBRS operation (supported values are Google or Federated Wireless).
- **AFC Configuration:** Automatic Frequency Coordination Server. AFC is mandated by the FCC and is used to ensure that an unlicensed device doesn't interfere with a licensed incumbent device. You can configure the server you want to handle this.
- **Primary BN Settings:** This allows TCS to automatically set the currently connected base node as the primary and enables users to set Primary BN on the Devices table.
  If this feature is disabled, TCS won't set a primary base node for any remote nodes.
  If you toggle the feature on, use the drop down to choose a time delay to connect to an alternate base node. The recommended value is 15 minutes.
  Select whether to reconnect to the Primary BN manually or automatically.
- **Maintenance Window**: A daily or weekly period of time available for maintenance operations (upgrade devices to the minimum software version). Duration is 0 - 1440 minutes.
- **Software Upgrade Settings:**
  - **Software Auto-Upgrade**: Select Daily or Weekly. Indicates if an automatic software upgrade policy for new devices is in effect. If so, all new devices added to the network are automatically upgraded to the minimum software version specified. You can override this at the sector level to allow for sector-level testing of new software releases. New devices added to the network are automatically upgraded only during the maintenance window.

    NOTE
    When a software upgrade is triggered by this setting, TCS pushes both the base node and remote node images to the base node and instructs the base node to push the image to the remote node at the maintenance window time setting.

  - **Set Maintenance Time**: The time software upgrades are applied.
  - **Software Auto Upgrade**: Day of the week software upgrades are applied.
  - **Duration**: Duration allowed for software upgrades.
  - **BN Software (Minimum Version)**: The minimum software version required for base nodes. New devices are upgraded to this minimum.

  - **RN Software (Minimum Version)**: The minimum software version required for remote nodes. New devices are upgraded to this minimum.
  - **E-Mail IDs to be notified**: One or more email addresses (comma separated).
- **Telemetry**: Information for metrics collector end point configuration (optional). Enter the Access Key, the Destination Address, Port, streaming interval from the drop down, and use the toggle to turn streaming off or on. You can override primary base node, software upgrade policy, and telemetry settings at the sector level on a sector by sector basis.
- **Access Control**: Controls the level of access given to Tarana Support. When network administrators contact Support to work out an issue, Support needs complete access to the network to make changes. You can disable both levels of Support access to prevent any changes.
  - **Enable Support**: Standard Support access, which allows Support to change TCS configuration.
  - **Advanced Support**: Advanced Support, which access allows SSH access to the network. It's disabled by default. To enable advanced support access, you must first grant standard Support access, then activate Advanced Support.
- **Manage BN Ports, Manage RN Ports**: Use the toggle to activate or deactivate SSA. It's disabled by default. You can enable it for an individual device on that device's individual page.
- **Multicast Control**: *V2.0+* Toggle to control the type of multicast traffic that's forwarded by a base node to and from its connected remote nodes. This is supported only on devices with software version 2.0 or higher.

Add Regions

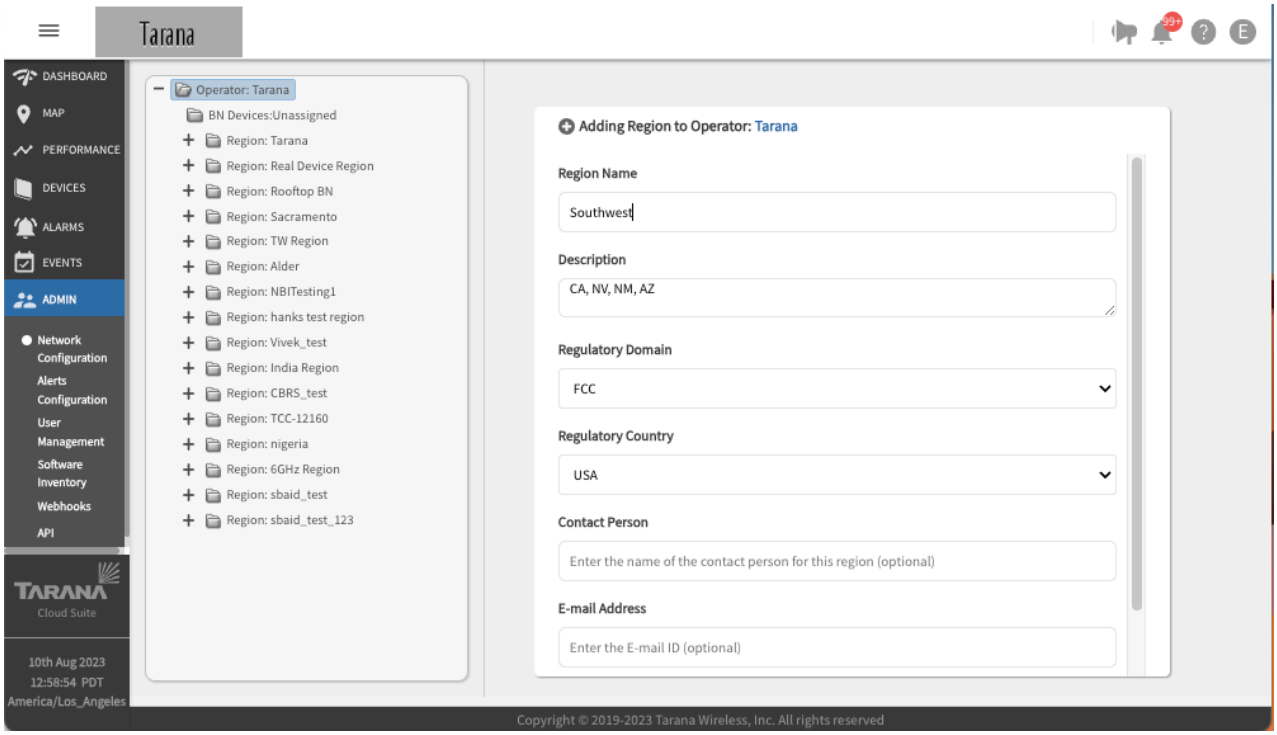
To add a region, open the Operator on the hierarchy tree, select **Add Region**, and enter this information:

- **Region Name:** Name of the region.
- **Description**: An informative description (optional).
- **Regulatory Domain:** The applicable regulatory domain where the network is deployed. Select a domain from the drop down.
- **Regulatory Country:** The country where the network is deployed. Select a country from the drop down.
- **Contact Person**: Name of a contact person (optional).

- **E-mail Address**: The contact person's email address (optional).

Select **Done**. The new region appears in the network list on the left.

To modify an existing region, select the region name from the network list and select **Edit**.



Add a New Region

Edit Regions

NOC L1 NOC OP OP ADMIN

To modify an existing region, select the region name from the network list and select **Edit**. You can edit any of the fields.

You can also control base node telemetry at the Region level.

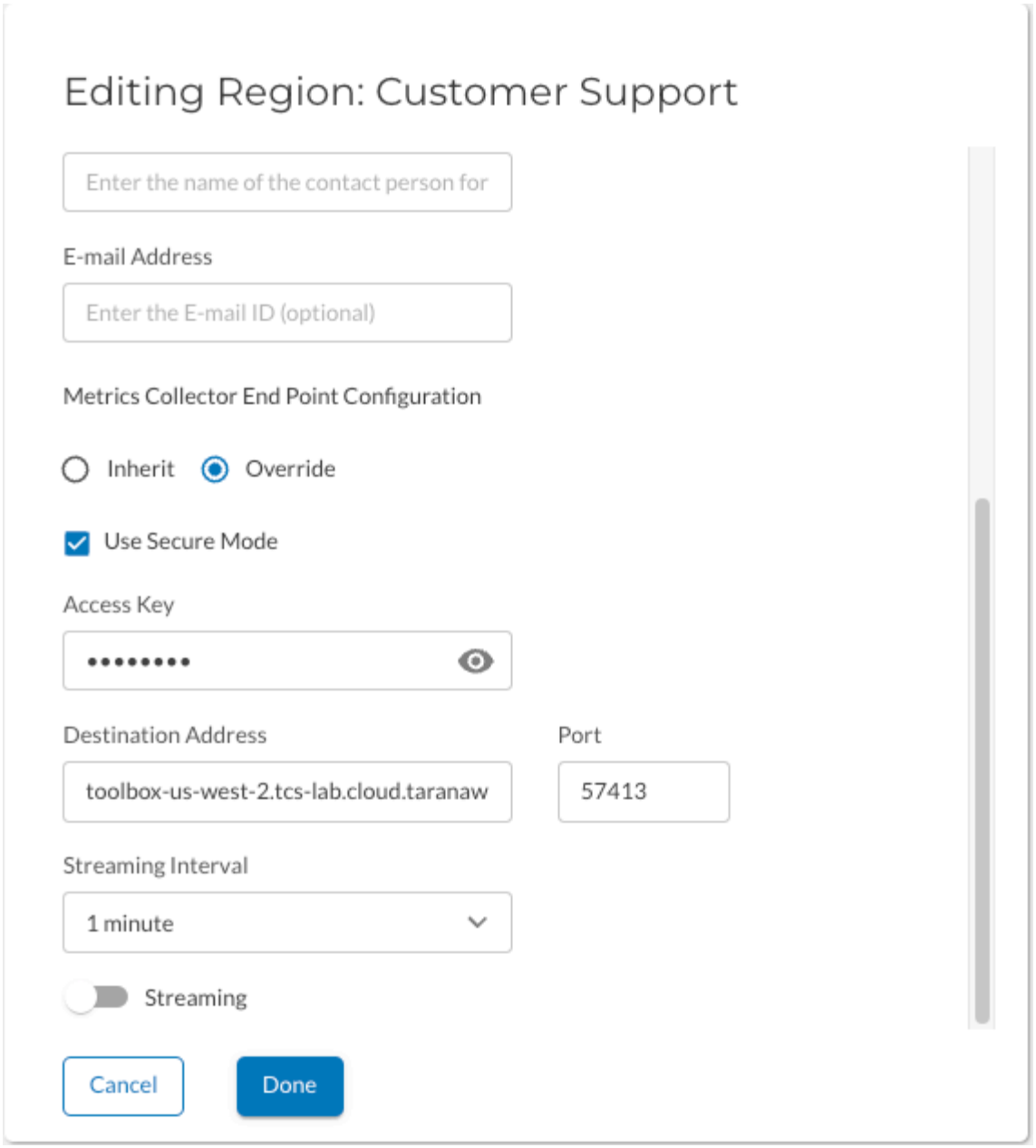
By default, the telemetry configuration at the region level inherits the configuration from the global operator level. If you select **Override**, these telemetry controls activate:

- **Secure Mode:** Select to enable encrypted TLS transport. Default is cleared.
- **Access Key:** The ASCI access key required to authenticate to the server. This key can be up to 64 characters long. Default is none.
- **Destination Address:** Destination URL or IP address of the host that receives the telemetry data from the base node. Default is telemetry.taranawireless.com.

- **Port:** Destination TCP port of the telemetry endpoint. Default is 80.
- **Streaming Interval:** Interval of time that the device streams information to the telemetry endpoint. Default is 1 minute.
- **Streaming Enabled:** When activated, allows the device to stream information to telemetry endpoints. Default is Deactivated.

NOTE

Sectors now inherit their telemetry from the parent region. If the region-level override is configured, the sector inherits its configuration from the modified region. Otherwise, the sector inherits from the global configuration at the operator level as before.



Edit Telemetry at the Region Level

Add Markets

NOC L1 NOC OP OP ADMIN

To add a market, open the Region on the hierarchy tree and select **Add Market**,, then enter this information:

- **Market Name:** Name of the market.

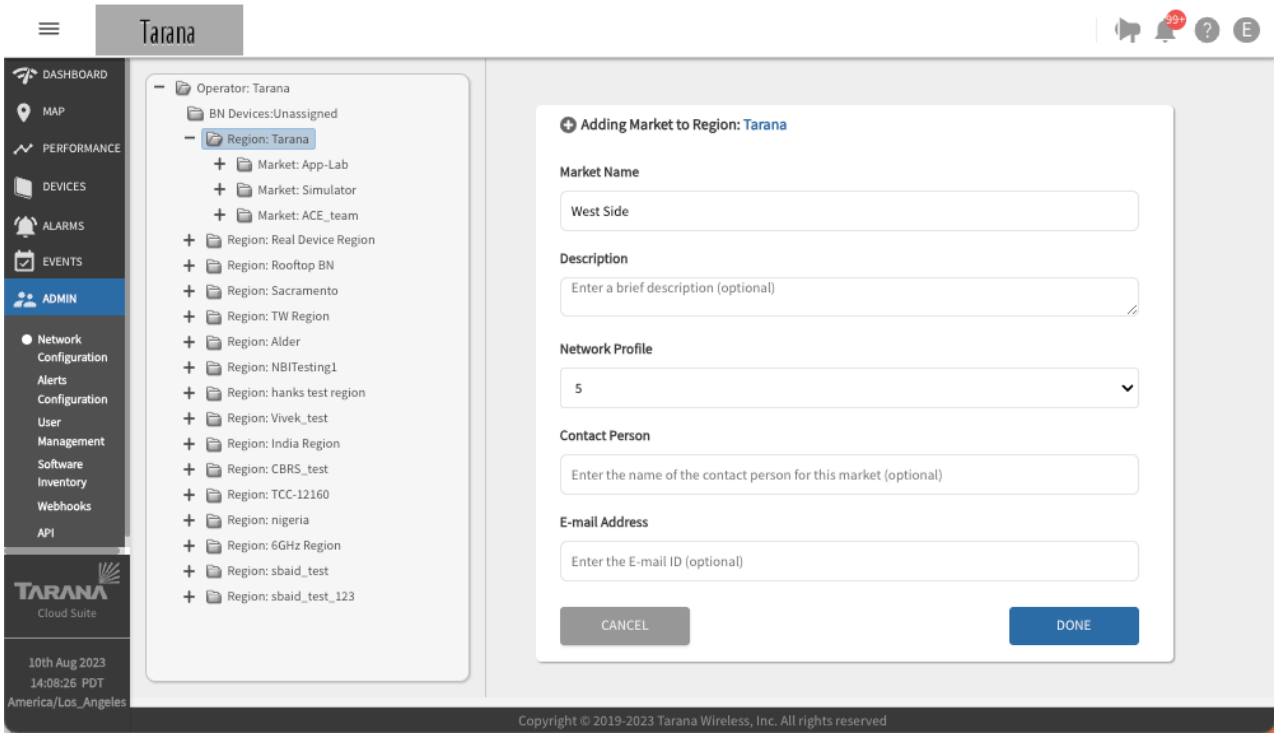
- **Description**: An informative description (optional).
- **Network Profile**: Defines the overall ratio of downlink throughput to uplink throughput and link distance. All cells with overlapping coverage and frequencies must use the same network profile to avoid unnecessary interference. The network profile is configured at the cell and market levels.

Network Profile	Maximum Cell Range	Downlink (DL) Symbols	Uplink (UL) Symbols	DL:UL Ratio
1	15 km	36	8	4.5:1
2	30 km	32	8	4:1
5	15 km	32	12	2.67:1
6	15 km	28	16	1.75:1

- **Contact Person**: Name of a contact person (optional).
- **E-mail Address**: The contact person's email address (optional).

Select **Done**. The new Market appears in the network list on the left underneath the corresponding region.

To modify an existing Market, select the market name from the hierarchy tree and select **Edit**



Add a Market

Add Sites

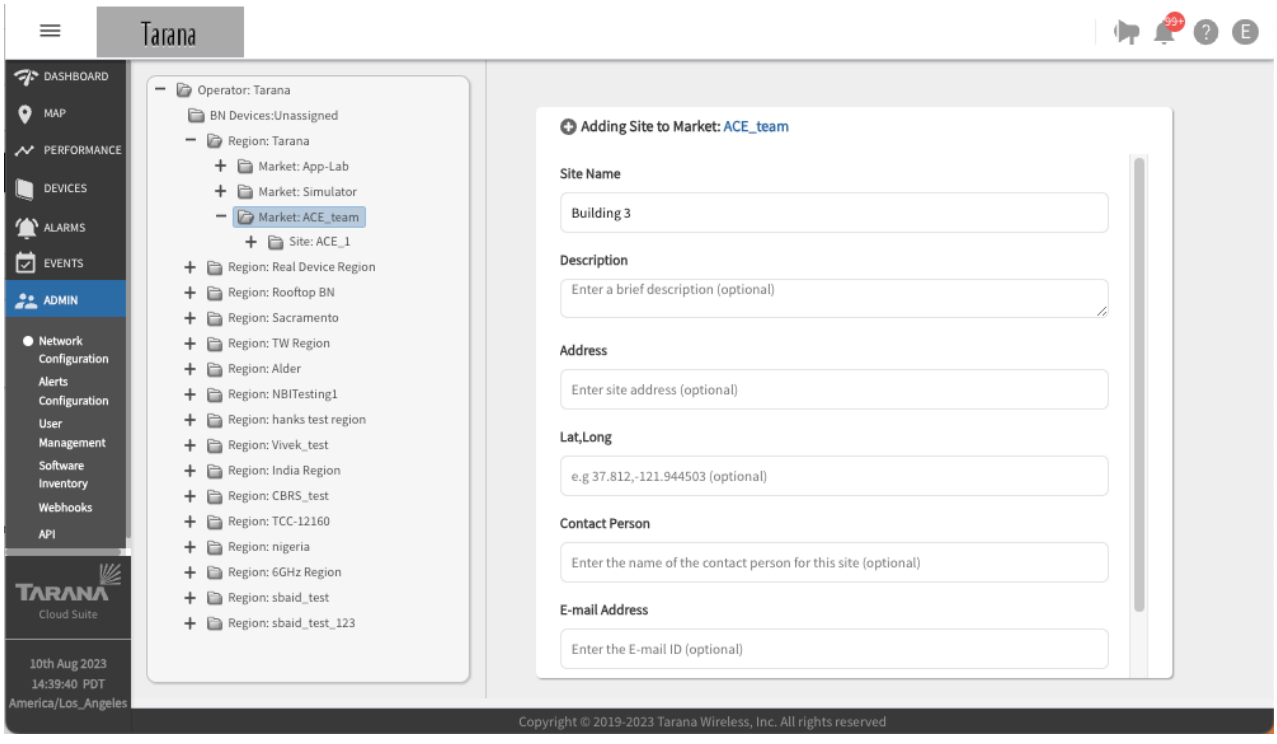
NOC L1 NOC OP OP ADMIN

To add a Site, open the Region and Market on the hierarchy tree and select **Add Site**, then enter this information:

- **Site Name:** Name of the site.
- **Description**: An informative description (optional).
- **Address:** Site address (optional).
- **Lat, Long:** Latitude and longitude coordinates of the site in decimal notation (optional).
- **Contact Person**: Name of a contact person (optional).
- **E-mail Address**: The contact person's email address (optional).

Select **Done**. The new Site appears in the network list on the left underneath the corresponding market.

To modify an existing Site, select the Site Name from the network list and select **Edit**.



Add a Site

Add Cells

To create a Cell, open the Region, Market, and Site on the hierarchy tree and select **Add**, and enter this information. Tarana Support can advise you on the optimal values.

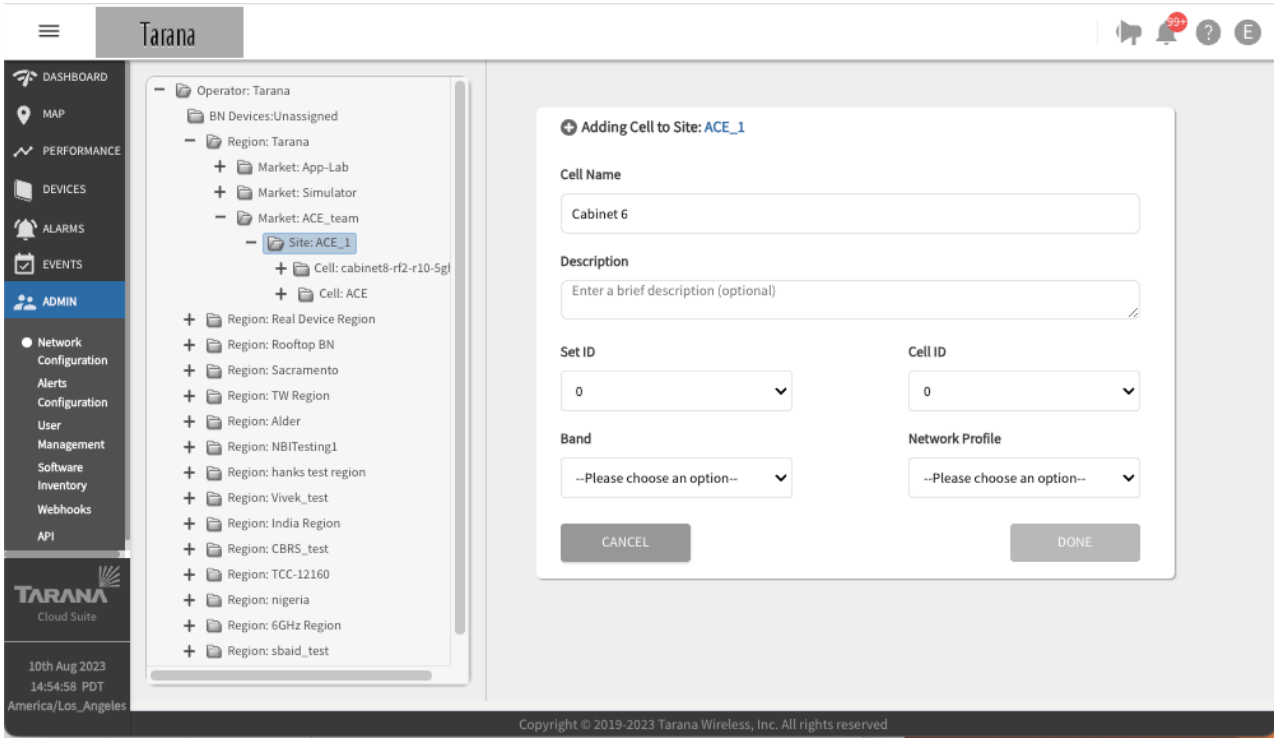
- **Cell Name:** Name of the cell.
- **Description**: An informative description (optional).
- **Set ID:** Identifier for a set. A set ID is part of the planning ID that uniquely identifies a sector base node. A group of 24 cells form a set. Use the drop down to select a value from 0 - 5. The planning ID uses the format <set ID><cell ID><sector ID>.
- **Cell ID :** Identifier for the cell, used to distinguish base nodes that belong to different cell sites. Use the drop down to select a value from 0 - 23.
- **Band:** The frequency band the cell uses. Use the drop down to select 3GHz, 5 GHz, or 6GHz.
  Once you've added a Cell to a Site, you can no longer edit the band, only the Set ID, Cell ID, and Network Profile. If you need to change the band, you must delete the cell and add it again at the Site level.
- **Network Profile**: Defines the overall ratio of downlink throughput to uplink throughput and link distance. All cells with overlapping coverage and frequencies must use the same network profile to avoid unnecessary interference. The network profile is configured at the cell and market levels.

Network Profile	Maximum Cell Range	Downlink (DL) Symbols	Uplink (UL) Symbols	DL:UL Ratio
1	15 km	36	8	4.5:1
2	30 km	32	8	4:1
5	15 km	32	12	2.67:1
6	15 km	28	16	1.75:1

NOTE
Network Profiles 5 and 6 require device software release 0.975 or higher.

Select **Done**. The new cell appears in the network list on the left beneath the corresponding site.

To modify an existing Cell, select the Cell Name from the hierarchy tree and select **Edit**.



Create a New Cell

For 3 GHz (CBRS) cells, TCS automatically sets the number of microseconds to a value of 2775.

Add Sectors

NOC L1 NOC OP OP ADMIN

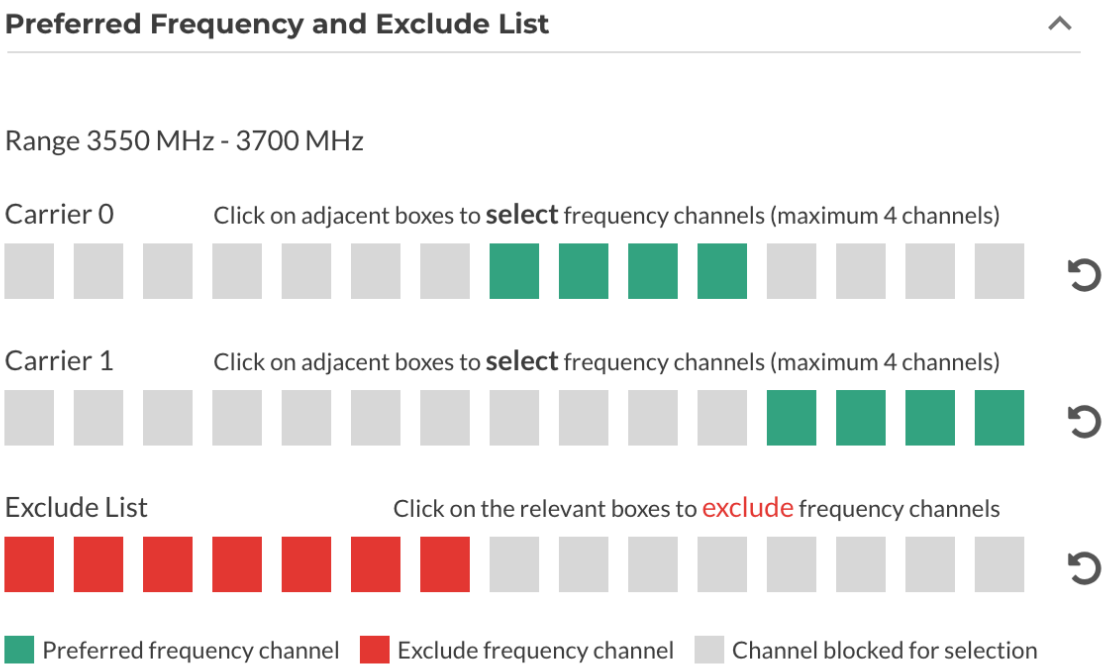
To add a Sector, open the Region, Market, Site, and Cell on the hierarchy tree and select **Add Sector**, then enter this information:

- **Sector Name**:
  Sector name can't be null or empty. It must be from 1 to 64 characters long with no spaces at beginning or end. Valid characters are ASCII(7) letters from a to z, A to Z, the digits from 0 to 9, hyphen, and underscore. It may not start or end with a hyphen. Consecutive hyphens (2 or more) are not allowed. Not allowed: spaces, special characters, periods
- **Description**: An informative description (optional).
- **Carrier Configuration**:
  - *V2.0+* Configure the sector base node to operate in dual-carrier (2x40 MHz) or quad-carrier (4x40 MHz) mode. Only 6-GHz base nodes running software 2.0 or higher can

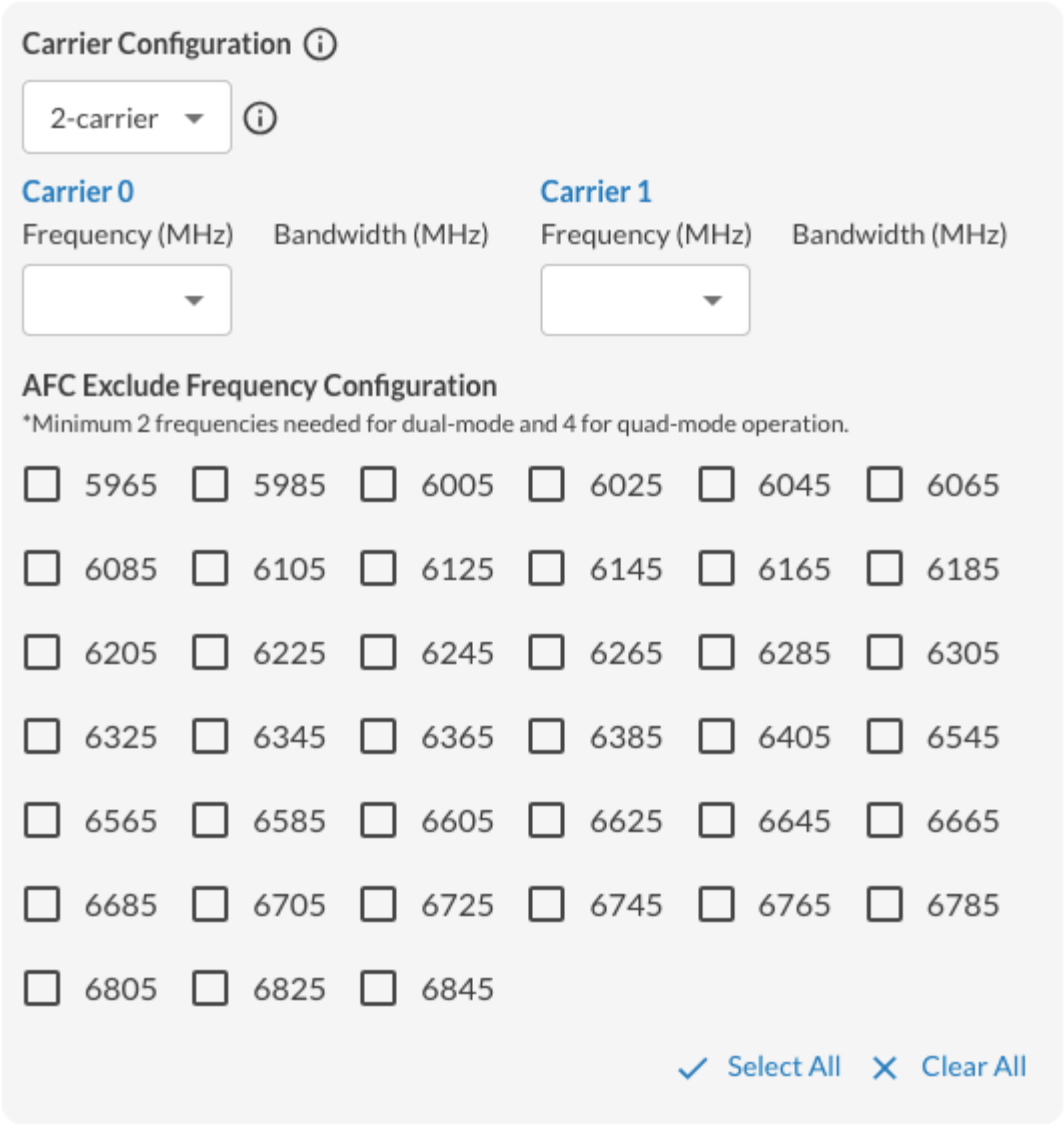
operate in quad-carrier mode. A change in mode will result in a radio reset of the base node, which will temporarily disconnect all connected remote nodes.

- **Carrier *n***: Frequency and bandwidth of the carrier, where *n* is the number of the carrier (0 – 3).

  For 3MHz sectors, you can specify carrier frequencies to prefer or exclude.



  For 6GHz sectors, you can specify a set of frequencies to exclude for UNII-5 and UNII-7.



When you add or edit a sector, TCS uses the regulatory domain and country that you set for the region to limit the supported frequencies and TX power level. Values that aren't supported in that region aren't listed in the drop downs. TCS then pushes those values to existing base nodes within that region, and any base nodes that you add to it. This makes it easier to add regions that are within new regulatory countries and domains.

- **Transmit Power Configuration**

> **NOTE**
> You should leave this at 30 dBm (default value) except in lab and testing environments.

  - **BN Tx Power (dBm)** : Value must be 0 - 30.

  - **RN Tx Power (dBm)** : Value must be 0 - 30.

- **Network Services**
  - **Classification Type** : Method used to examine internet-side traffic for quality of service (QoS) markings. The base node honors these markings to prioritize inbound traffic on the data ports. Select one of these values:
    - **VLAN 802.1p** : Use this mechanism to apply QoS markings at the media access control (MAC) level.
    - **DSCP** : Use differentiated services code point (DSCP) to determine QoS.
  - **Downstream ARP** : Toggle to enable or disable. When you enable downstream ARP, you can reach customer-premises equipment (CPE) to test for device reachability and connectivity.
    TCS makes this distinction between a base node being reachable and connected:
    Connected: Base nodes send registration messages through the uplink channel, and this continuous upstream communication notifies TCS that the base node is connected.
    Reachable: TCS communicates downstream to the base node through a dedicated VPN, sending configuration updates and other information. As long as there is traffic passing through the VPN to the base node, TCS determines that the base node is reachable.
  - **DHCP Relay Agent** : Toggle to enable or disable. For details about the DHCP Relay Agent, see DHCP Option 82 Support (page 141).
  - **Buffer Allocation Profile**: *V2.0+* Controls buffer allocation method of the data traffic for all remote nodes in the sector. Supported on devices with software version 2.0 or higher. Select one of these values:
    - **Default**: Use standard buffer sizes.
    - **Maximum Size**: Use maximum size buffers for maximizing data rates.
- **Primary BN Settings** : Select **Inherit** or **Override**.
  Use the toggle to set a primary base node.
- **Software Upgrade Settings** : Select **Inherit** or **Override**.
  Globally, you set this with Operator Configuration (page 104) but later you can change the minimum software release for a base node and remote node on a per sector basis. This allows an admin to test new software upgrades sector by sector before upgrading the entire network.

NOTE
When a software upgrade is triggered by this setting, TCS pushes both the base node and remote node images to the base node and instructs the base node to push the image to the remote node at the maintenance window time setting.

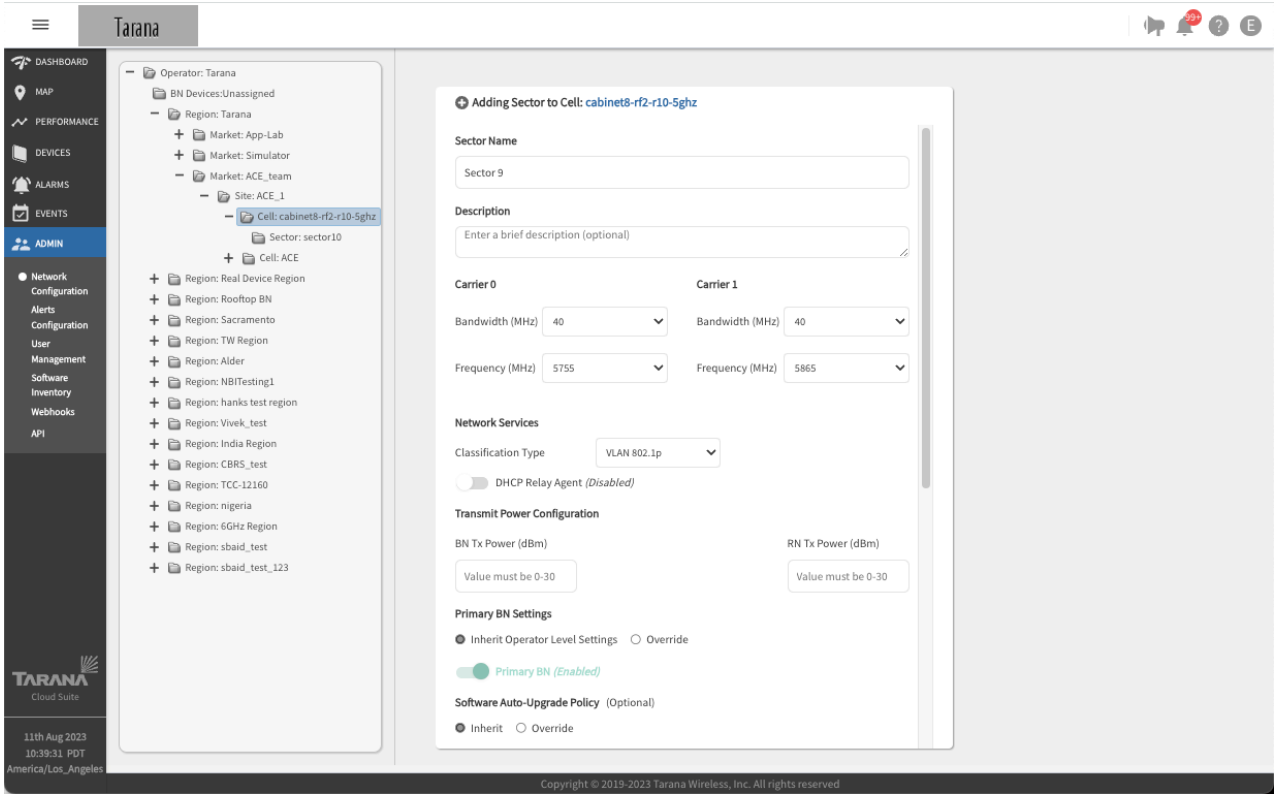
  - If you set the toggle to Software Auto-Upgrade to on, use the BN Software (Minimum Version and RN Software Minimum Version) drop downs to set the software version.
  - **E-Mail IDs to be notified** : Enter E-mail IDs to be notified, separated by commas.
- **Telemetry** : Set End Point Configuration details at the **Operator** level, but later you can set Metrics Collector End Point Configuration to **Inherit** or **Override** and toggle **Streaming** to on.

Select **Done**. The new Sector appears in the network list on the left beneath the corresponding Cell.

To modify an existing Sector, select the Sector Name from the network list and select **Edit**.

Once you've added a sector, you can add base nodes to it from the Devices unassigned folder by selecting **Add BN Device**. If you need to change them, select **Change BN Device**.

For details, see Add a Base Node to a Sector (page 121).



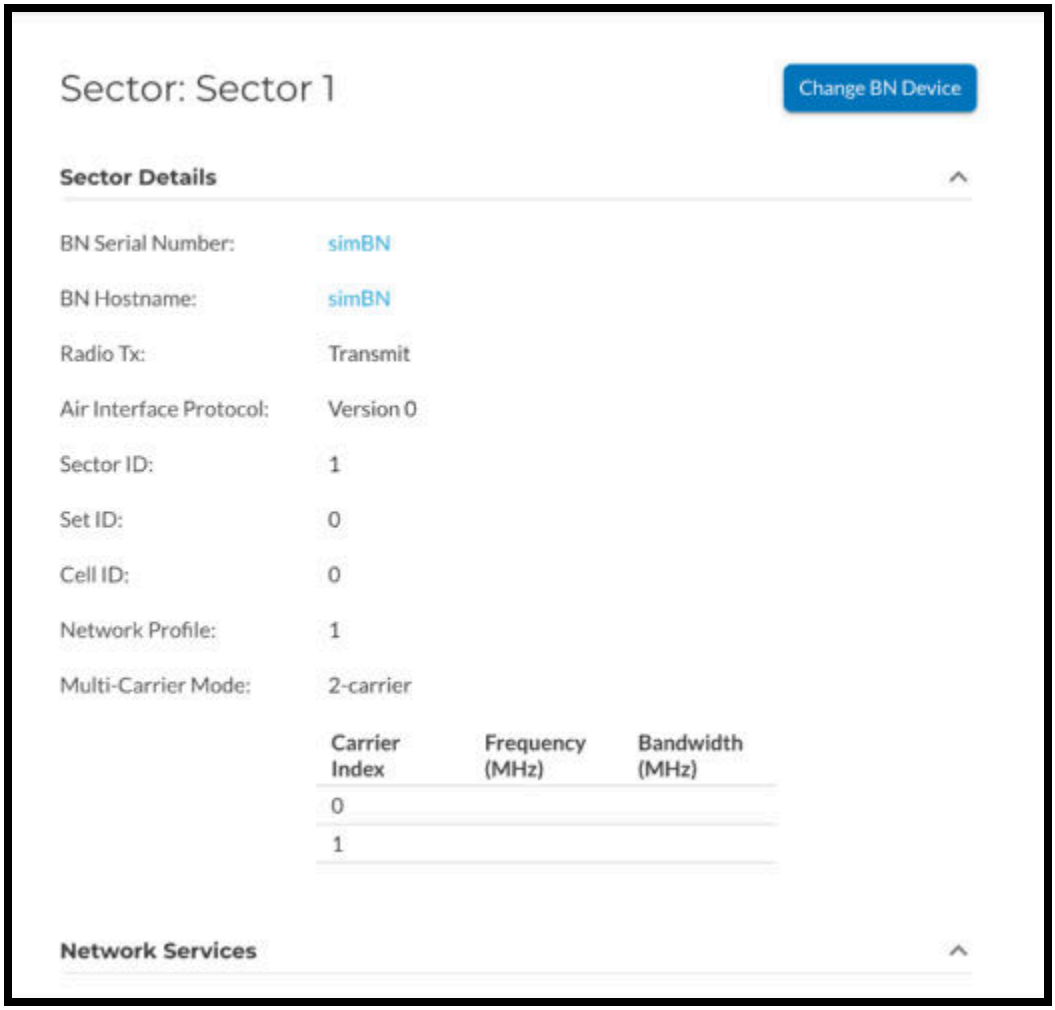
Add a Sector

Edit Sectors

NOC L1 NOC OP OP ADMIN

When replacement devices are delivered, users with Op Admin privileges can change the serial number and name of the base node device and preserve the configuration from the previous device.

Navigate to the sector that contains the base node to be replaced and select **Change BN Device**.

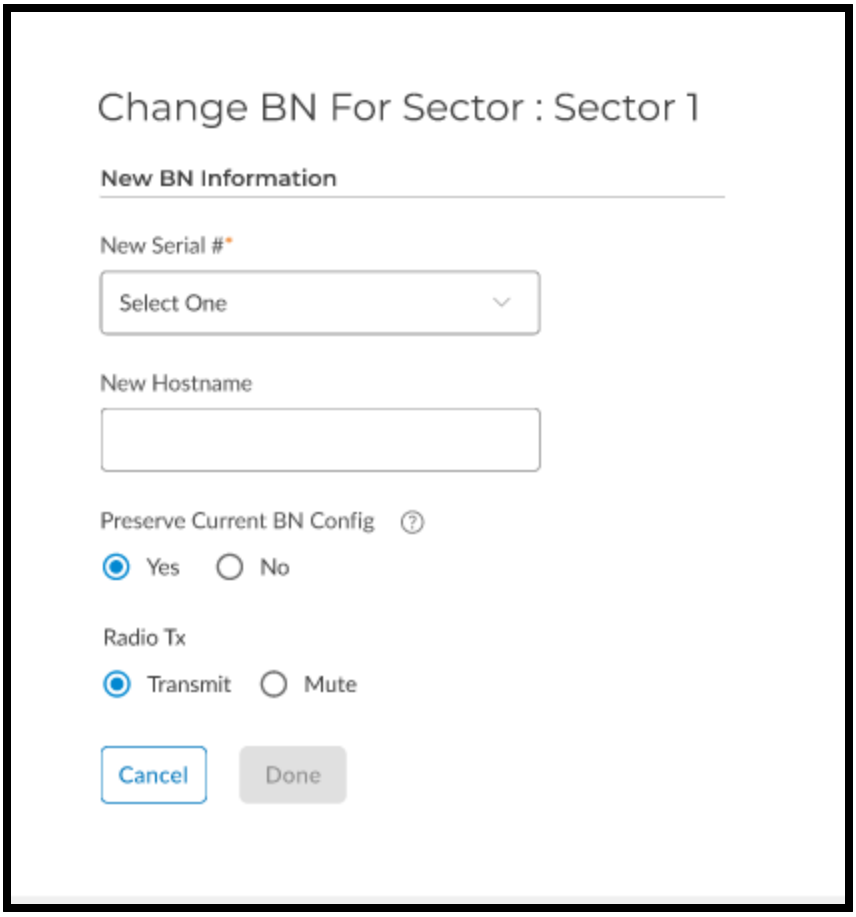


Enter the new base node serial number. The new base node hostname is optional.

When you replace a base node, you have the option to transfer the prior base node configuration to the replacement base node. Select **Yes** under Preserve Current BN Config. TCS preserves the base node configuration, and deploys the configuration to the new base node after it boots.

Under Radio Tx, select **Transmit** or **Mute**.

Select **Done**, or **Cancel** to exit.



Add a Base Node to a Sector

To add a base node to a Sector, open the Region, Market, Site, Cell, and Sector on the hierarchy tree and select **Add BN Device**, then enter this information:

- **Device ID:** Choose a device from the dropdown list of base nodes in the BN Devices Unassigned folder.
- **Hostname:** Configurable name of the device.
  Hostname must be from 1 to 63 characters long. Valid characters are ASCII(7) letters from a to z, A to Z, digits 0 to 9, hyphen, and underscore. It may not start or end with a hyphen. Consecutive hyphens (2 or more) are not allowed. Hostname is case-sensitive. Not allowed: spaces, special characters, periods.
- **Radio Tx:** Select Transmit or Mute.

Select **Done**.

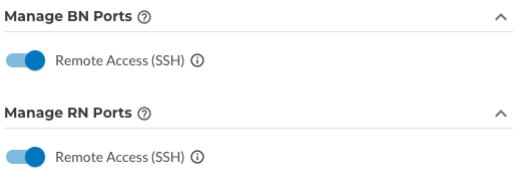
Manage Port Access

TCS administrators can control external access to some ports.

SSH port 22 is activated by default, but an administrator can deactivate it either globally in the network configuration or on individual devices on the single device page using the Manage Port ( ) tool.

To activate SSH port 22 globally, do the following:

1. Log in to TCS.
2. Navigate to **Admin > Network Configuration**.
3. Select **Edit**.
4. In the Manage BN Ports section, activate **Remote Access (SSH)** to allow SSH access on port 22 globally on base nodes.
5. In the Manage RN Ports section, activate **Remote Assess (SSH)** to allow SSH access on port 22 globally on remote nodes.



6. Select **Done**.

To activate port access locally, see Manage Port (page 87).

Edit Sector to Use Deep Buffer Mode

 *v2.0+*

You can activate deep buffer mode on devices running software version 2.0 to minimize packet loss in certain testing environments.

Currently, shallow buffers are used in the remote node switch to reduce latency. However, in some circumstances, a shallow buffer can contribute to dropped frames. In circumstances in which latency is more tolerable than frame drops, deep buffer mode is the preferred option.

When you use small packets for testing, deep buffer mode helps to handle the burst of small packets and reduce packet loss.

Tarana recommends that you use the Default value for real world traffic scenarios.

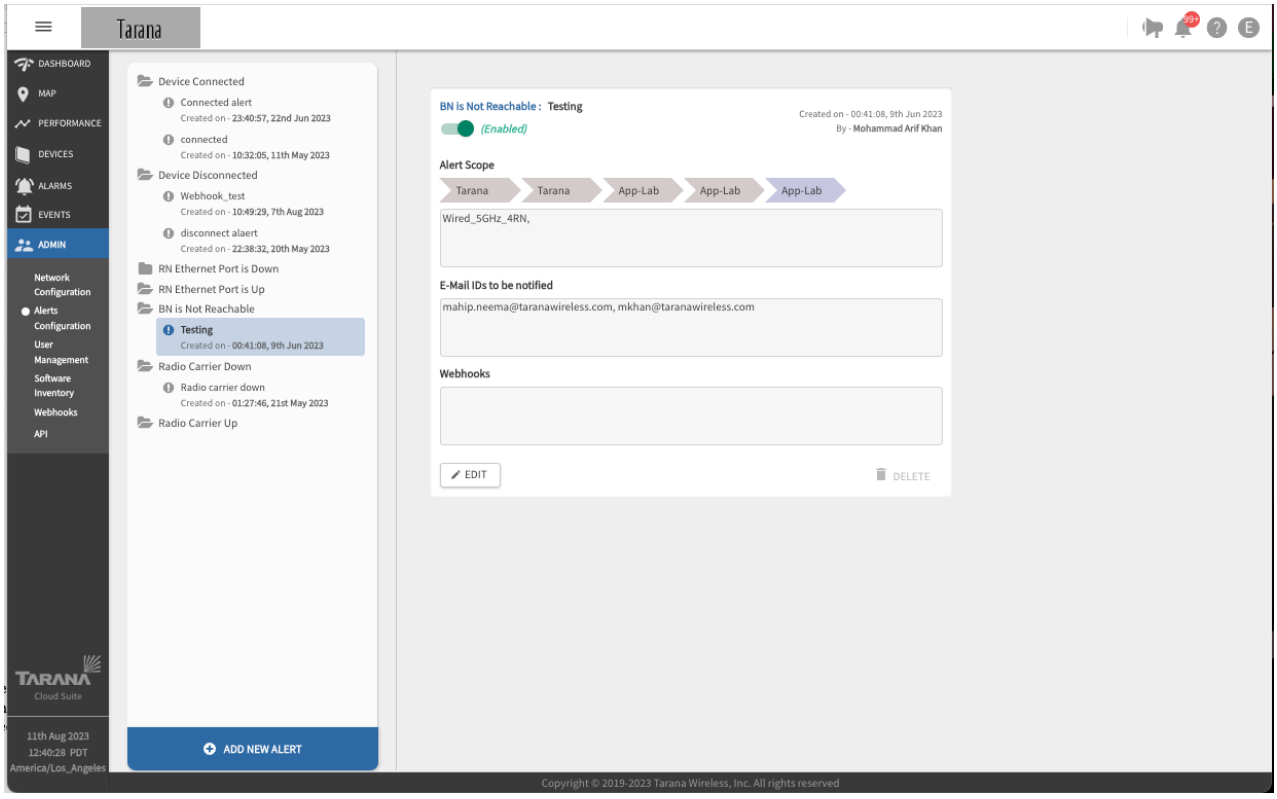
To activate deep buffer mode, do the following:

1. Log in to TCS.
2. Navigate to **Admin > Network Configuration**.
3. In the network hierarchy, navigate to the sector you want to configure.
4. Select **Edit** to edit the sector.
5. In the Network Services section, select **Maximum Size** from the the Buffer Allocation Profile drop-down list, and then select **Done**.

Configure Alerts

To configure email alerts by cause and by network scope, select **Admin > Alerts Configuration** from the navigation pane.

You see a list of folders for the types of alarms you can add, with any alerts already added for that type. Select an alert to see its details.



Alerts Configuration

NOC L1 NOC OP OP ADMIN

NOTE
Some alerts do not require all the fields mentioned below. You can safely ignore fields that are mentioned in the following steps but do not appear in the workflow.

To add a new alert, first log in to TCS, navigate to **Admin > Alerts Configuration**., and then select **Add New Alert**.

Step 1: Configure the alert parameters.

1. If prompted to choose between creating a webhook and creating an alert, select **Create Alert**.
2. Select the alert type from the **Alert Type** drop-down list.
3. If prompted to select the device type, select it from the radio buttons.
4. If prompted to select the alert scope, select **Click To Set Alert Scope**, and then select the appropriate network scope within which the alert is active.
5. Select **Proceed**.

Step 2: Configure the alert reporting.

1. If prompted, select the subscope. This step requires you to select the network scope within the main scope you selected in Step 1-4. For example, if you select a region in Step 1-4, then Step 2 prompts you to select one or more markets to monitor for events. Likewise, if you select a market in Step 1-4, then Step 2 prompts for one or more sites.
2. Select the notification modes.
    a. **Email**: Select, and then enter one or more email addresses separated by commas.
    b. **Webhooks**: Select, and then select one or more of the available webhooks.
3. Select **Done**.

Manage User Accounts

To add new users or edit their permissions, select **Admin > User Management** from the main TCS page.

Display User Accounts

To display user accounts, select **Admin > User Management** from the navigation pane. You see a list of all users currently configured on the system, with these fields:

Firstname: First name.

Lastname: Last name.

Role: Administrative role.

Email: Email address.

Mobile: Mobile phone number.

Last Sign In: Last time this account signed into TCS.

Creation Time: When the account was created.

CPI Certified: Whether the user is a certified professional installer.

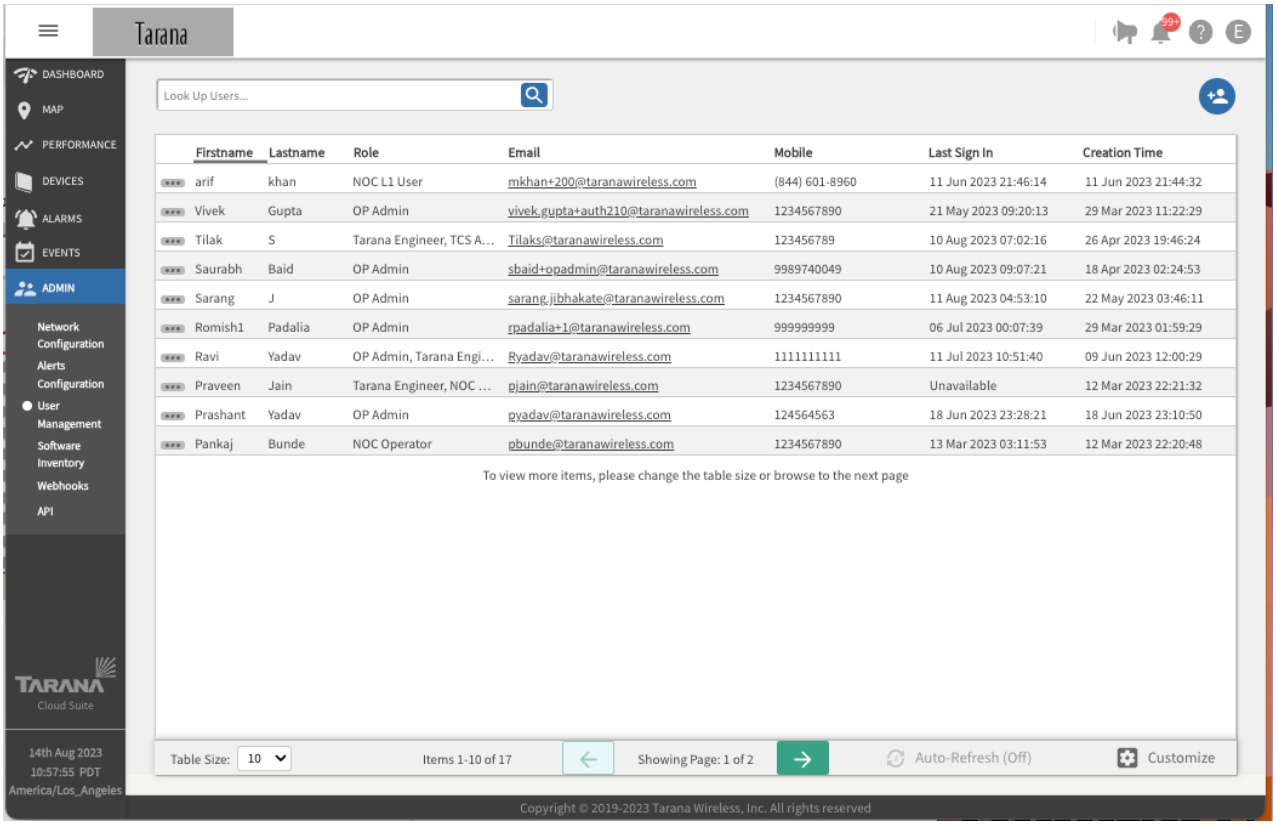
Action(s): Use this to edit the user's personal information.

Use the three dot menu (⋮) to delete accounts or reset an account's password.

Enter any value in the Search... box. If it appears in any of the fields, the rows are filtered to show only those rows.

Icons at the top of the table let you control refresh rate, change settings, or download data.

To sort in ascending or descending order, select the column heading. You can adjust the width of each column by dragging.



Display Users

The data displayed for each column doesn't refresh automatically. To change this behavior, select the **Auto-Refresh icon** (). It remains on for your user account even after you log out. Select it again to turn off Auto-Refresh.

Choose columns to display by selecting the **Settings icon** (). Select the fields you want to display, then **Apply**. These changes remain for your user account even after you log out. Use **Reset** to clear your selection.

Add User Accounts

NOC L1 NOC OP OP ADMIN

To add a new user account, select **Add User** at the top of the page, then enter this personal information:

- **First Name:** User's first name.
- **Last Name:** User's last name.
- **Email Address:** User's email address.

- **Mobile Number:** User's mobile number.
- Hover over each checkbox to see a description of the role.

Check the box for the **Role** you want to assign to this user. Roles assign permissions to the new user. For detailed descriptions, see User Roles (page 12). Roles from lowest to highest are:

- **NOC L1 User**
- **NOC Operator**
- **OP Admin**

There are three user roles that support multi-tenancy for retailers. Roles and permissions are similar to existing TCS User Profiles and Roles. User roles for multi-tenancy are:

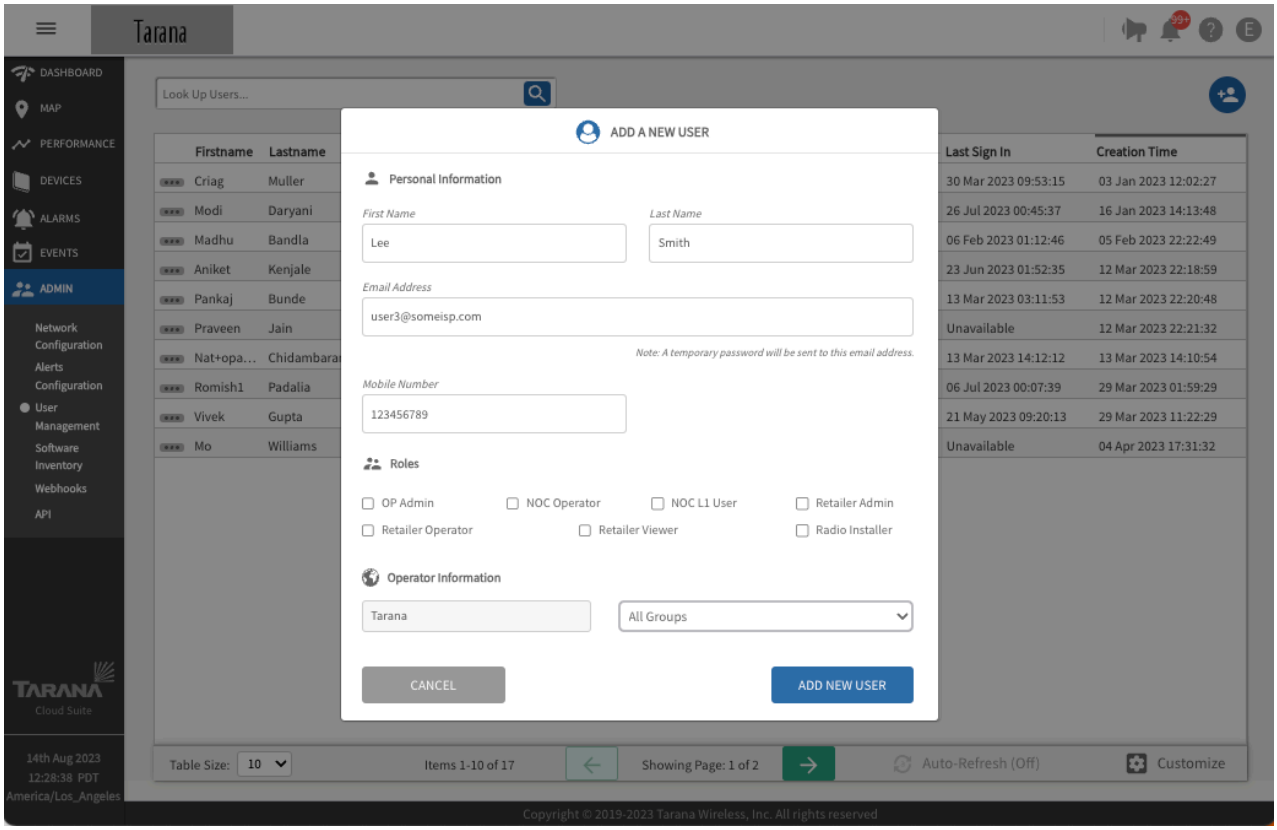
- **Retailer Admin**
- **Retailer Operator**
- **Retail Viewer**

The **Radio Installer** role is for users who install remote nodes with Tarana's mobile app.

Operator Information: Select **All** if the user should be included in all groups, or **Single** if you want to specify one group.

Use the **Operator Name** drop down list to select the operator, and **Group Name** to select groups that should include this user.

Select **Add New User** to add the user account or **Cancel** to exit without saving changes.



Add User Account

Edit, Delete, or Reset Password for User Accounts

NOC L1 NOC OP OP ADMIN

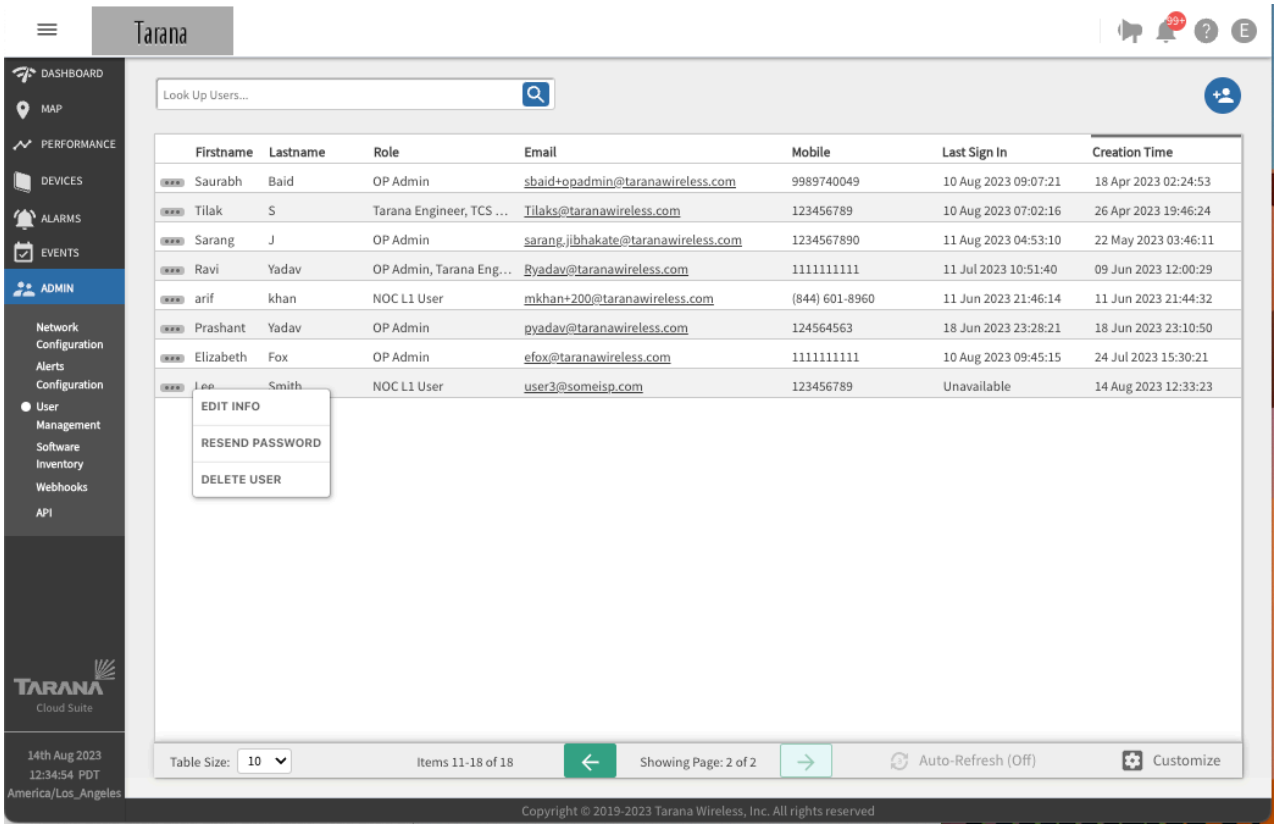
You must have OP Admin privileges to see the Admin menu and select User Management to edit, reset password, or delete an existing account.

To edit a user account, select **Edit** in the user's row. Enter the information and select **Close** to cancel or **Update** to make the changes. You can't edit the email address. If the address changes you must delete the account and add a new one.

To delete a user account or send an email for the user to reset their password, select the three dot menu in the right column (⋮) and select one of these options:

Delete User: Confirm that you want to delete the user by selecting **Delete User**, or select **Cancel**.

Resend Password: Enter an email address and select **Confirm**.



Manage User Accounts

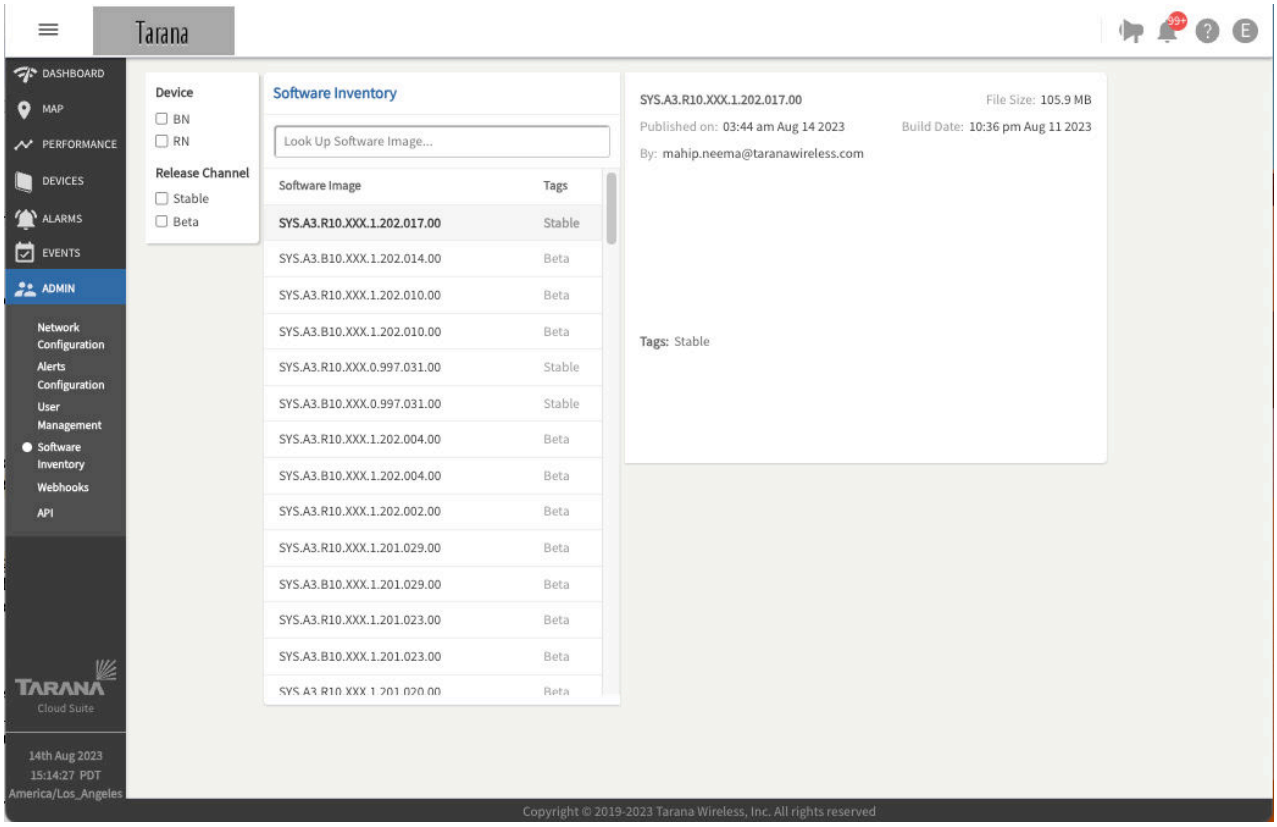
Software Inventory

NOC L1 NOC OP OP ADMIN

To view software inventory, select **Admin > Software Inventory** from the navigation pane.

Select the Device (**BN** or **RN**) and Release Channel (**Stable** or **Beta**) to filter. Use the search box to find a particular release.

The blue hyperlink for Release Notes directs you to Tarana support. To see the release note, you must log in to your Tarana Support account.



Software Inventory

Add and Test Webhooks

Webhooks are an event-based notification process that allows an application to notify another application, process, or person when a monitored event that generates an alarm occurs. An alarm-raising system event generates an alarm that invokes the webhook, which then sends a message to an application. Webhooks are one-way communications, unlike API calls, which are two-way and require an application or process to request information and wait for service to respond.

TCS can send alert email messages when events occur. You can configure these alerts to generate email notifications:

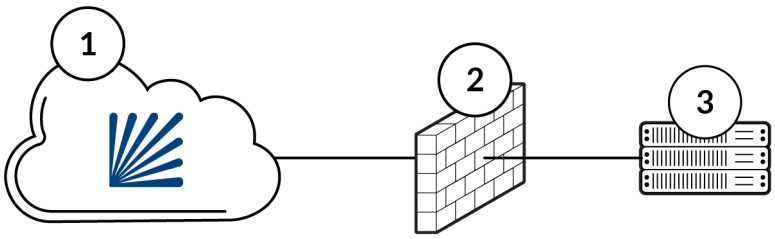
- Device disconnected
- Device reconnected
- Remote node Ethernet port down
- Remote node Ethernet port up
- Base node unreachable
- Radio carrier down

- Radio carrier up

Radio carrier status alerts indicate the status of the SAS grant for CBRS devices, rather than general transmit status of the radio. For example, an alert indicating that the radio carrier is down occurs, when the grant is suspended or terminated. Similarly, an alert indicating that the radio carrier is up occurs when the grant is authorized or when a suspension is lifted.

NOTE
On devices running 0.989 or earlier versions, both carriers must have active grants at both the base node and remote node in order to pass data traffic. Devices running 0.990 or later can pass data traffic on any carrier with an active grant at the base node and remote node.

Webhooks respond to the events and automatically send push messages directly to webhook receivers, as illustrated here. A TCS instance running in the cloud creates a webhook message and sends it through the Tarana cloud to the local router. You must configure its ACL to allow webhook messages from TCS so it can reach the local message server.



Reference	Description
1	TCS Instance running in the cloud. This is the source of the webhook message.
2	Local router firewall or access control list (ACL). The ACL must allow incoming webhook messages from TCS.
3	Local message server or application

You can configure and test webhooks directly in TCS. If you don't have any webhook receivers configured on your network, you can use public webhook receivers, such as https://webhook.site, to configure and test your webhooks.

TCS supports any HTTPS endpoint as a webhook receiver.

Add or Edit a Webhook

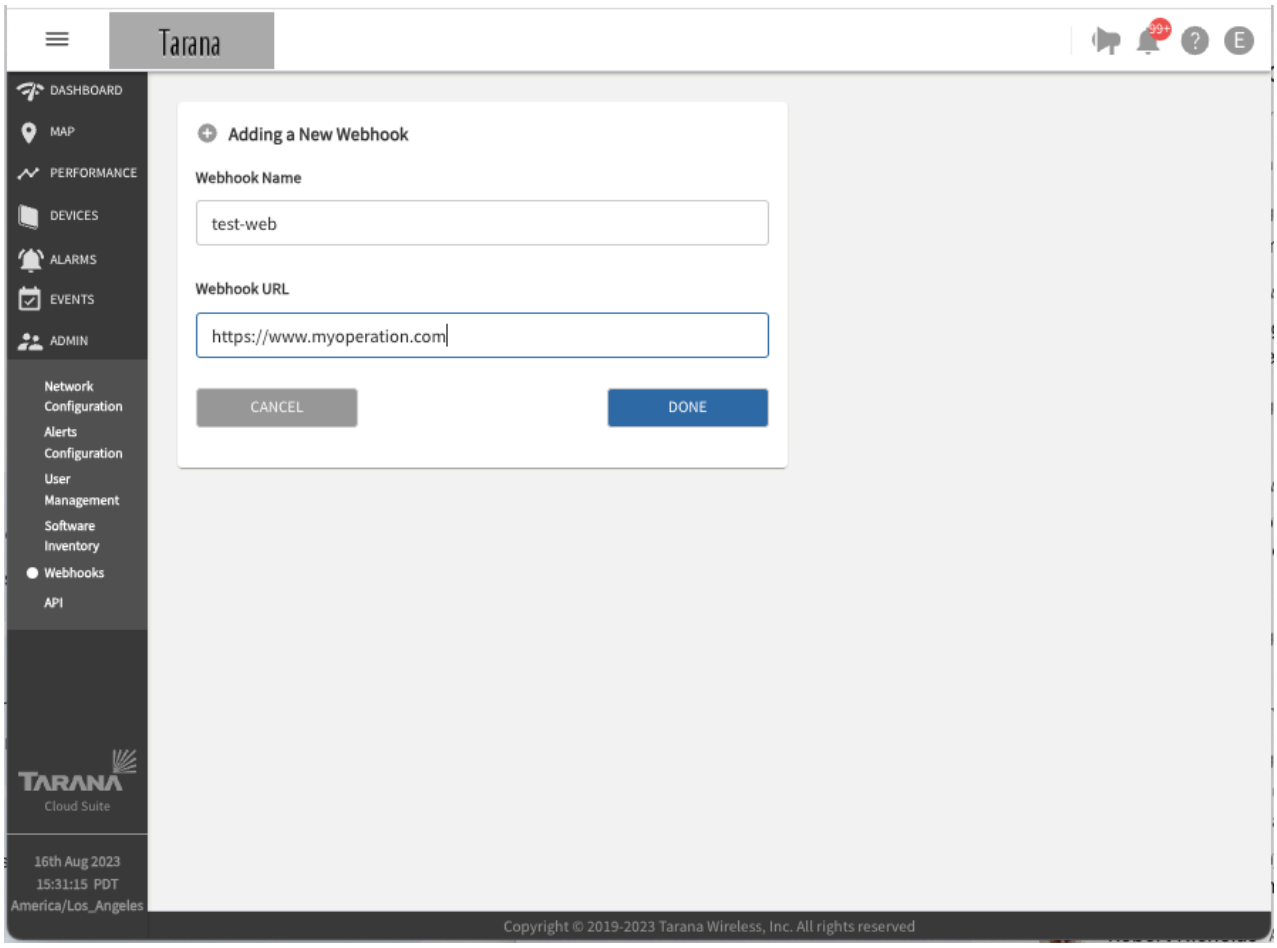
NOC L1 NOC OP OP ADMIN

Tarana supports a maximum of 5 webhooks destinations. To create a new webhook, follow these steps:

1. Select **Admin** > **Webhooks** from the navigation pane.
2. Select **Add New Webhook**.
3. Enter these values:

- Webhook Name: A unique and descriptive name for your webhook. This name appears in the list of webhooks that you add to TCS.
- Webhook URL: URL of the receiving interface.

Select **Done**.



Add a Webhook

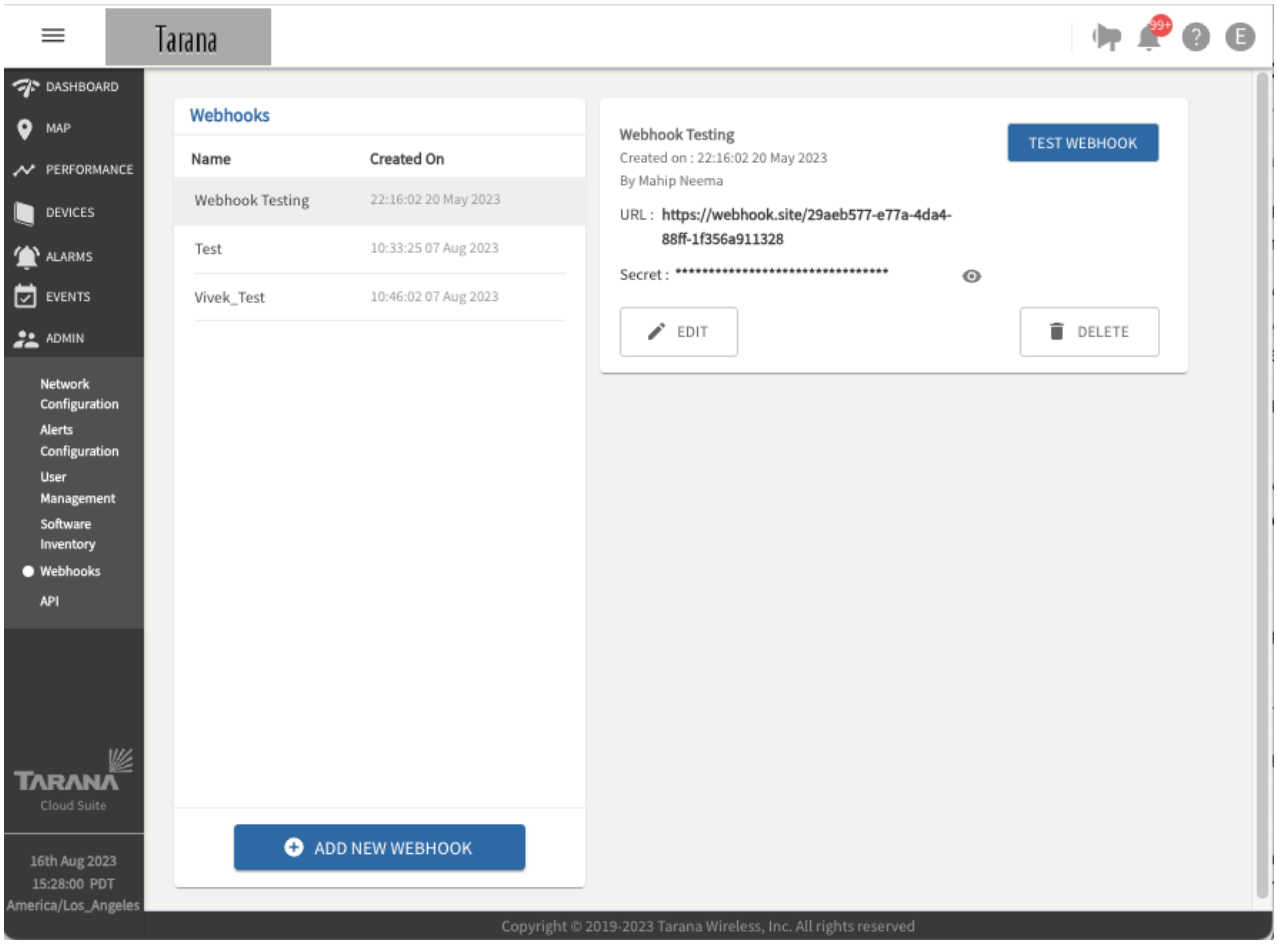
NOTE
When you add a webhook, TCS automatically generates a secure secret, which you can view when you test the webhook.

Test a Webhook

NOC L1 NOC OP OP ADMIN

To test a webhook, follow these steps:

1. Select **Admin** > **Webhooks** from the navigation page.
2. Choose the webhook that you want to test from the list of available webhooks.
3. Select **Test Webhook**.
4. TCS displays a status message. Make sure that the expected result is correct. If it isn't, verify that the webhook URL and secret are correct in the webhook.



Test a Webhook

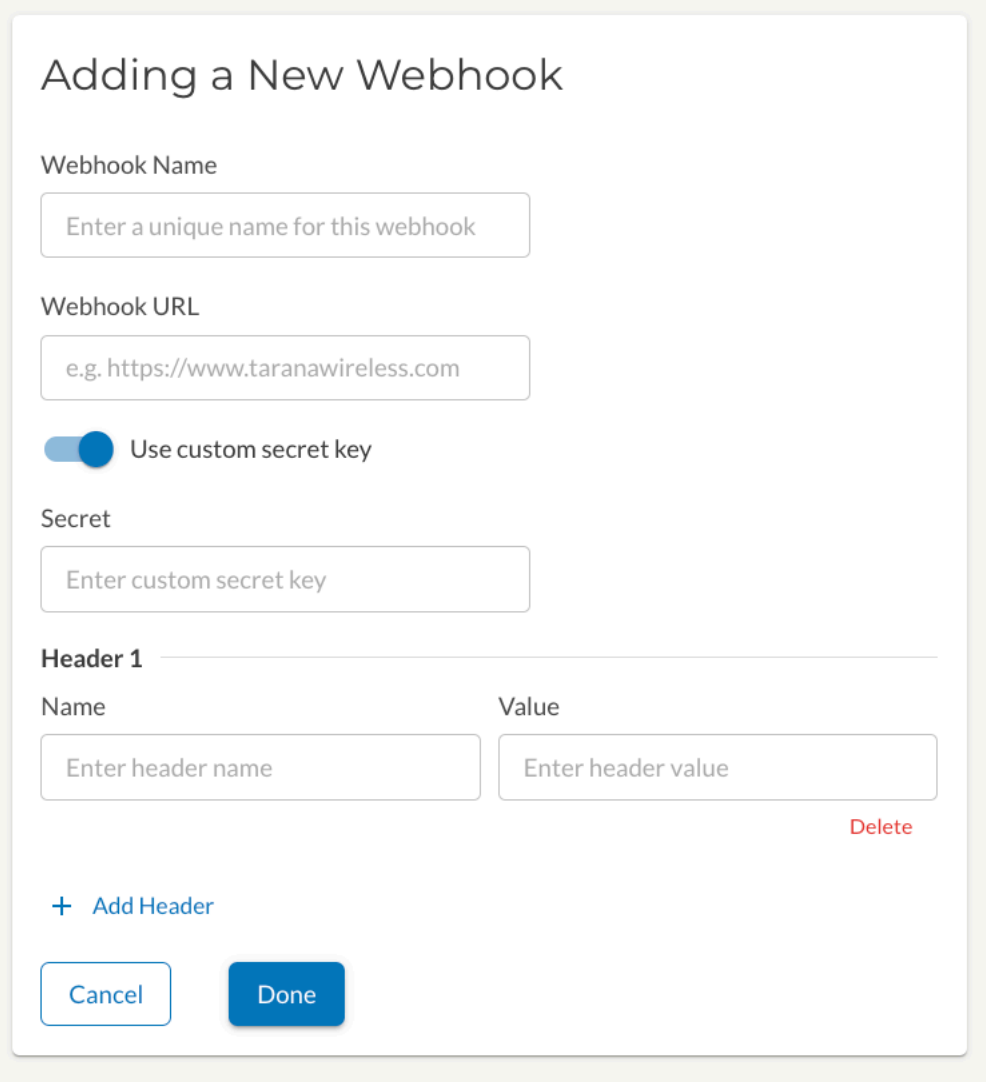
For details about configuring alerts, see Configure Alerts (page 123).

Custom Webhook Authentication Keys

When you add a webhook, TCS automatically creates a secure secret, which you can view when you test the webhook.

You can also create your own secret and header in TCS.

When you create a webhook, toggle **Use Custom Secret Key** to on, and then enter your custom secret key. Select **Add Header (+)**, and then enter a header name and value. You can add additional headers.



You can configure a maximum of 5 webhooks. Each webhook can have a maximum of 3 custom headers:

- **Secret**: Secret must be from 8 to 255 characters long. Valid characters are ASCII(7) letters from a to z, A to Z, digits 0 to 9, hyphen, and underscore.

- **Name**: Name must be from 1 to 64 characters long. Valid characters are ASCII(7) letters from a to z, A to Z, digits 0 to 9, hyphen, and underscore.
- **Value**: Value must be from 1 to 512 characters long. Valid characters are ASCII(7) letters from a to z, A to Z, digits 0 to 9, hyphen, and underscore.

Manage APIs

APIs provide a way for network administrators to automate tasks. To view or authorize APIs, select **Admin > API** from the navigation pane. You see the web address for the server or servers and a list of APIs for your operator listed by entity. Use the drop down to view APIs for that entity.

Select **Get** or **Post** to run each API.

NOTE
Each operator has a quota of 10k API calls per calendar month.

Swagger API Documentation

Swagger is a framework for creating interactive API documentation. TCS now links directly to the TCS NorthBound API documentation using the Swagger framework.

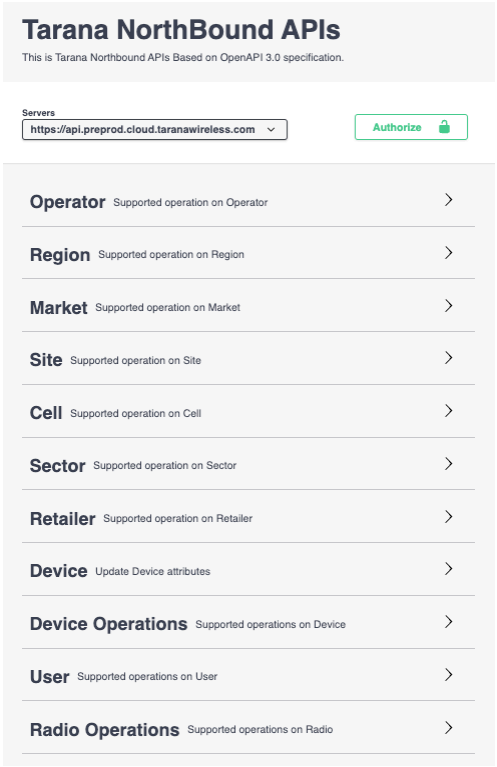
Customer Application

You can use the Swagger API documentation to view the URL, structure, and syntax of an API call without the need to refer to a separate PDF document. Whereas PDF and other external documentation can become stale as improvements are made to the API, Swagger documentation is always current because it takes its content from the API.

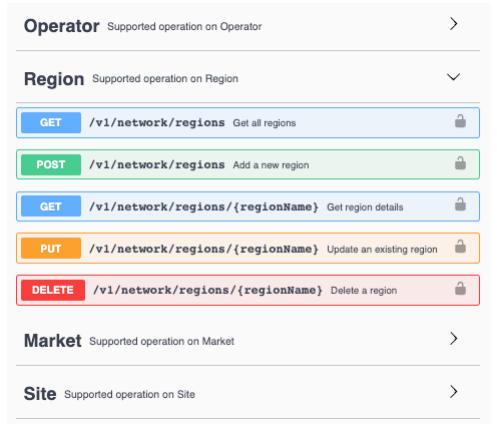
In addition to using Swagger as a reference, you can also use it to make API calls directly to TCS. Sending API calls in this way simplifies testing and troubleshooting new or existing APIs. You can also use Swagger as a convenient way to issue calls to production networks without needing additional third-party apps or browser extensions.

Feature Description

Swagger documentation appears as a collapsed accordion list with only the top-level items visible. For example, currently the following are the top-level Swagger items:



When you select an item the section expands to review the API calls that are available.



API calls are color-coded by their function with blue and green indicating non-destructive methods that view or add data, and orange and red indicating destructive methods that change or remove data.

Call Method	Color in Swagger	Description
Get	Blue	Retrieve information without changing databased content
Post	Green	Add information to the database
Put	Orange	Update or change existing information in the database
Delete	Red	Remove information from the database

You can select an API call in the accordion list to reveal details about the specific call. Each API call can have the following information:

- Parameters
- Request Body
- Responses

To view Swagger documentation, do the following:

1. Log in to TCS with Op Admin privileges.
2. Navigate to **Admin > API** to open the Tarana NorthBound APIs page in a new browser tab.
3. Select the category to reveal the individual API calls available.
4. Select the call to expand the section and view the API calls details including the endpoint URL, parameters, body, responses, and so on.

In addition, each API call has a Try It Out button that you can select to activate the parameter fields and the Execute button, which you can use to send an API call to TCS.

Currently all responses are in application/json media type.

When you execute a live API call, Swagger displays the following in the Responses section:

- **Curl**: The command line curl string that the API generates and sends to TCS. The curl command defines the method and media type.
- **Request URL:** The TCS NorthBound API is a RESTful API that operates over HTTP and defines the endpoint using a URL.
- **Server Response Body**: The JSON-formatted response includes information regarding the success of the call along with supporting information, such as what information was retrieved or changed.

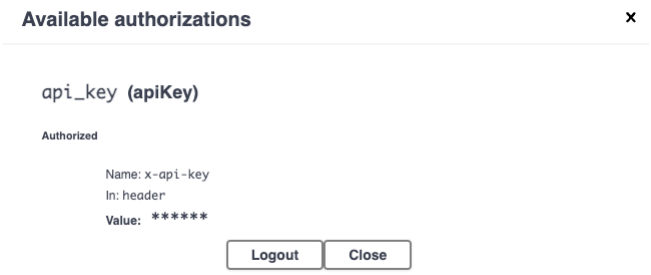
NOTE
You can select the Download button to download the response body in JSON format. The response headers are not included.

- **Server Response Header**: Indicates the content length and media type.

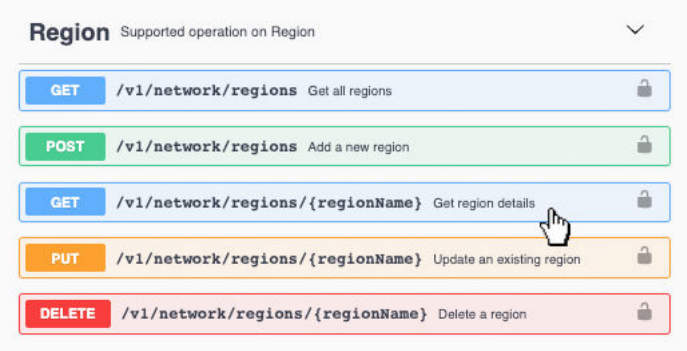
The following procedure sends the Get Region Details API call to TCS and returns. To send an API call you must obtain an API key from Tarana.

To send a Get Region Details API call to a device using Swagger, do the following:

1. Log in to TCS with Op Admin privileges.
2. Navigate to **Admin > API** to open Tarana NorthBound API page in a new browser tab.
3. Select **Authorize** to open the authentication dialog.
4. Enter your API key in Value field, and then select **Authorize** If you are already authorized to issues API calls, then the dialog indicates that you are authorized and does not have a field to enter a key.
5. When the dialog authenticates the key and confirms that you are authorized to issue API calls, select **Close** to close the dialog.



6. Select **Region** to expand the list of available API calls.
7. Select **Get region details** to expand the section and reveal the details.



8. Select **Try it out** to make the fields interactive and reveal the Execute button.
9. Enter the name of the target region in the Region Name field, and then select **Execute**. TCS produces the following example response body, except with details matching your queried region:

```
{
  "data": {
    "id": 12345,
    "name": "NameOfTheRegionQueried",
    "operatorId": 1234,
    "operatorName": "UsuallyTheProviderName",
    "networkProfile": 1,
    "notes": "RegionDescription",
    "contactPerson": "John Doe",
    "email": "johndoe@example.com",
    "regulatoryDomain": "FCC",
    "regulatoryCountry": "USA"
  },
  "error": null
}
```


Base Node Telemetry Streaming

TCS provides a way for companies to configure Tarana base nodes to send telemetry data directly to third-party network management systems using Google Remote Procedure Calls (gRPC) Network Management Interface (gNMI).

By default, TCS collects all telemetry data through the base node. If you have a network management system (NMS) that collects and aggregates telemetry data from multiple sources, you can configure your Tarana network to stream telemetry data directly to your aggregating NMS.

You can configure base node telemetry streaming globally, at the region level, or at the sector level. When you configure streaming globally, all base nodes in the network stream telemetry data to the Network Management Interface (NMI). When you configure streaming at the region or sector level, you configure it as an exception to the global configuration, meaning that if you activate telemetry streaming globally, all regions or sectors stream telemetry except those you specifically exclude at the region or sector level. If you deactivate telemetry streaming globally, no sectors stream telemetry data except those you specifically activate at the region or sector level.

To activate telemetry streaming, first configure TCS with the telemetry collection endpoint server information.

To configure TCS to use a telemetry streaming collection endpoint, follow these steps:

1. Navigate to Admin > Network Configuration.

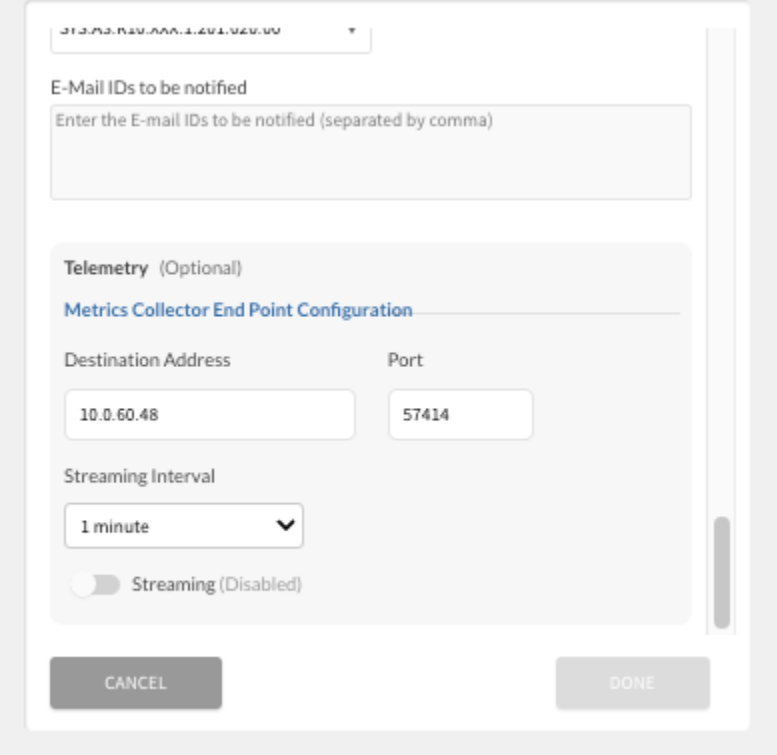
2. To display global settings, select the **Operator** name in the network entity tree.

3. Select **Edit** at the bottom of the settings pane.

4. Enter the metrics collector end point information:

- **Destination Address:** Destination URL or IP address of the host that receives the telemetry data from the base node. (Default: telemetry.taranawireless.com).
- **Port:** UDP port on which the host receives telemetry data.
- **Streaming Interval:** Select an interval for the base node to send telemetry data. Allowable values are from 1 minute to 60 minutes.

5. Select **Done** to commit the configuration changes and exit.



Admin Network Configuration - Telemetry

To configure base node telemetry streaming globally, follow these steps:

1. Ensure that the telemetry collection endpoint is configured, then activate the feature by toggling the **Streaming** switch to on.

2. Select **Done** to commit the configuration changes.

If telemetry streaming is configured but disabled at the Operator level, you can enable it at the Region or Sector level. Follow these steps:

1. Navigate to Admin > Network Configuration.

2. Navigate to the Region or Sector in the network entity tree, then select the entity name to display the settings.
3. Select **Edit** at the bottom of the settings page.
4. In the Metrics Collector End Point Configuration section, select **Override**.
5. Enter **Destination Address**, **Port**, and **Streaming Interval**, and toggle the Streaming switch to activate the feature.
6. Select **Done** to commit the configuration changes and exit.

DHCP Option 82 Support

DHCP Option 82 is the DHCP Relay Agent Information Option. When a DHCP client requests an IP address in a network using a DHCP relay agent, the relay agent uses the Option 82 contents to ensure that the client receives the IP address when the DHCP server responds and to ensure the identities of the communicating devices.

In a Tarana network using DHCP Option 82, the base node acts as a DHCP relay. When you enable DHCP Option 82 on a base node, it receives client DHCP requests, and then relays the DHCP request to the DHCP server with the DHCP Option 82 information included. DHCP servers that are Option 82-enabled respond to the base node, and the base node removes the Option 82 information, and forwards the DHCP response to the client. The client device doesn't play a role in the DHCP Option 82 exchange and can't detect when DHCP Option 82 is used or that the DHCP relay exists on the network. Because of this transparent operation, you don't need to do any additional configuration on the remote node for DHCP Option 82 to function.

Option 82 information includes one or more sub-options that contain information shared by the base node. The sub-options are defined for a relay agent that's co-located in a public circuit access unit. Common sub-options include the Agent Circuit ID for the incoming circuit, and an Agent Remote ID that provides a trusted identifier for the remote high-speed modem.

An Option 82-enabled DHCP server can use a relay agent identity and client source-port information to administer IP addressing policies based on client and relay agent location within the network.

A device operating as an Option 82 relay agent for DHCP clients can enhance network access protection in these ways:

- The relay agent can block attempts to use an invalid Option 82 field to imitate an authorized client.
- The relay agent can block attempts to use response packets with missing or invalid Option 82 sub-options to imitate valid response packets from an authorized DHCP server.

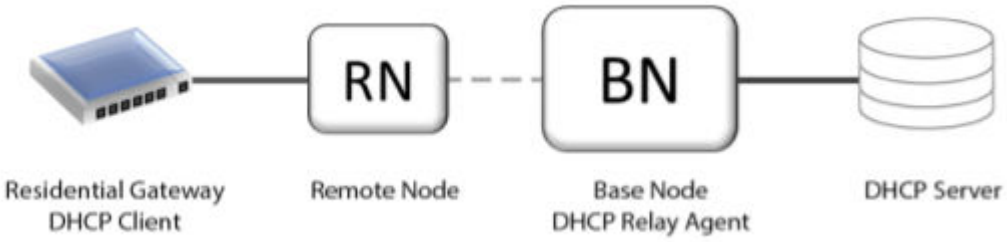
This describes how the DHCP Option 82 protocol functions and how you can configure your base node to act as a DHCP relay using Option 82.

For the DHCP with Option 82 to function properly the following must be true you must:

• Configure the client device to request an IP address via DHCP.

• Configure the base node to act as a DHCP relay and it must have the required sub-options, such as the Agent Circuit ID or Agent Remote ID configured. In a Tarana network, the AgentCircuit ID identifies the remote node, and the Agent Remote ID identifies the base node. In TCS the Agent Circuit ID and Agent Remote ID are combined in a single control labeled Remote / Circuit Identifier Type, which can use either the MAC address or the serial number of the devices.

• Configure the DHCP server to accept and respond to DHCP Option 82. The base node defines the Option 82 values using lower case, so configure the DHCP server accordingly.



General DHCP Option 82 Network Topology

In this image, the residential gateway is an end-user device that's connected to the remote node. When it requests an address from the DHCP server, the request moves through the remote node and the base node to the DHCP server. The DHCP server response returns through the base node and the remote node to the residential gateway. This is the detailed process:

1. The residential gateway initiates the DHCP exchange by requesting an IP address using the DHCP protocol without DHCP Option 82 information.

2. The remote node receives the DHCP Request packet and retransmits it to the base node unaltered.

3. The base node, acting as the DHCP relay, receives the DHCP request packet, inserts the DHCP Option 82 fields, and sends the new DHCP Request packet to the DHCP server.

4. The DHCP server receives the DHCP Request packet and decodes the DHCP Option 82 fields, which it uses to uniquely identify the base node and remote node pair.

5. The DHCP server responds by sending the DHCP Response packet that includes the DHCP Option 82 fields back to the base node.

6. The base node receives the DHCP Response, removes the DHCP Option 82 fields, and forwards the DHCP Response packet to the residential gateway.

7. The residential gateway uses the DHCP Response to configure its IP address information.

To configure the base node to act as a DHCP Relay Agent and include DHCP Option 82 information, follow these steps:

1. Log in to TCS with Op Admin privileges.

2. Navigate to Admin > Network Configuration, then navigate to the sector containing the base node you want to configure.

3. Select the sector to view the sector configuration, and select **Edit**.

4. Use the toggle to enable **DHCP Relay Agent**.

5. Choose either **Serial Number** or **MAC Address** from the Remote / Circuit Identifier drop-down list.

6. Select **Done** to save the changes.

Alternatively, you can use the base node Web UI to configure the base node by selecting its serial number link from the Devices list, then selecting the Web UI action and making the same configuration changes.

Device Web UI

Devices have a web UI that you can access from TCS, or directly by entering the IP address into a browser. The default IP address is 192.168.10.2. Chrome is the supported browser. Once a remote node is deployed, you can't access the remote node web UI except by proxying from TCS.

You can log directly into a device from the individual device view window. Select the **Web UI** icon ( ) to open a new browser window and log in to the device's Web UI. This is a similar interface to the one you see if you directly connect through the management port on the device.

To access the Web UI from TCS you must have the NOC Operator or OP Admin role in TCS. Web UI login and password information for this device is required.

Once you've completed the initial deployment, don't use the web UI for configuration changes. Configuration settings in TCS overwrite web UI settings. To avoid misconfiguration, always use TCS once the device is registered and connected to TCS. TCS flags configuration mismatches with an alarm.

Web UI Navigation Pane Actions

Once you've logged into the Web UI you can select actions from the navigation pane on the left. Actions differ for Base Nodes and Remote Nodes.

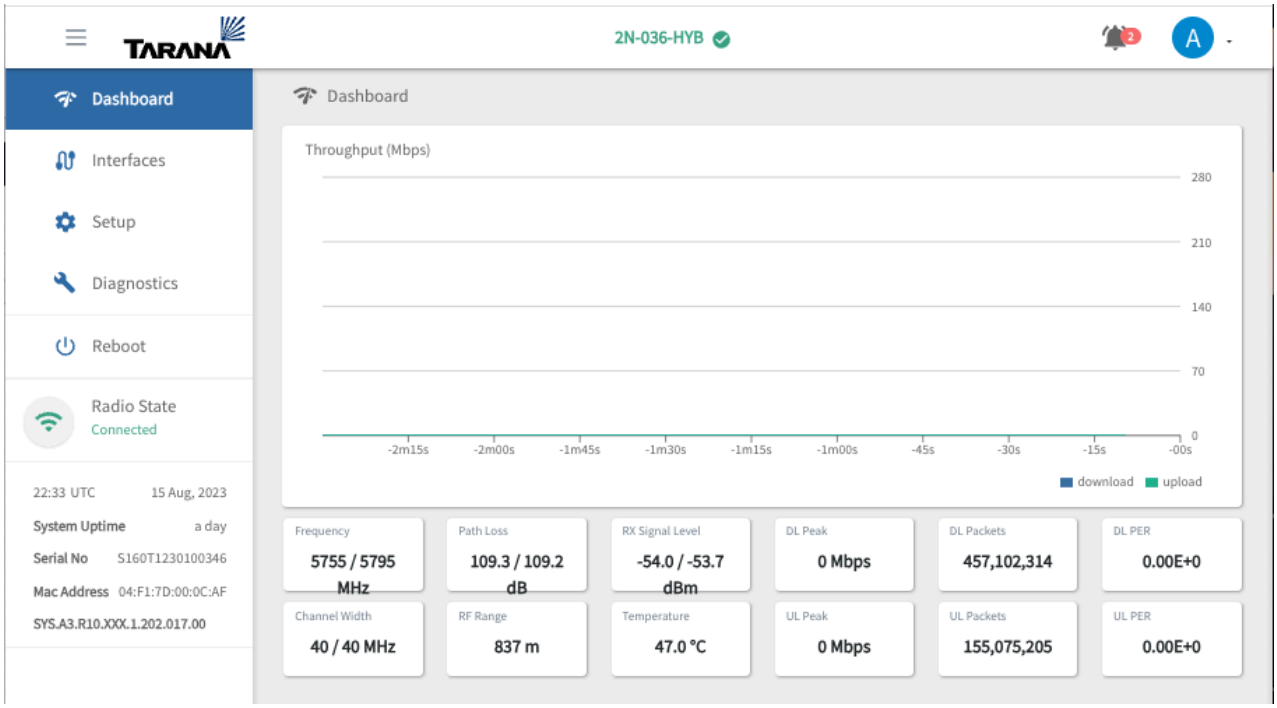
Device Dashboard (Remote Node Only)

When you log in to a remote node's web UI, the device dashboard displays information about that node. The Hostname of the device is listed at the top. If the Hostname is in green text the device is connected to TCS. An alarm icon in the top right corner displays in red to indicate active alarms that may require attention.

The screen shows a graphical display of current upload and download traffic in Mbps. This information is displayed under the graph:

- **Frequency:** Operating frequency of the radio in GHz.
- **Channel Width:** Channel width in MHz.
- **Path Loss:** Measured path loss in dB.

- **RF Range:** Length of the path taken by the signal between communicating devices, which includes reflections and diffractions (in meters).
- **Rx Signal Level:** Received signal in dBm.
- **Temperature:** Internal temperature of the remote node at the board.
- **DL Peak:** Highest measured download throughput, in Mbps, since the link was brought up.
- **UL Peak:** Highest measured download throughput, in Mbps, since the link was brought up.
- **DL Packets**: Number of packets transmitted in the downlink direction.
- **UL Packets**: The number of packets transmitted in the uplink direction.
- **DL PER:** Downlink packet error rate.
- **UL PER:** Uplink packet error rate.



Web UI Remote Node Dashboard

NOTE
In a G1 network, Path Loss is an important metric for determining the link quality. Path Loss dictates the achievable MCS level.

Base Node Interfaces

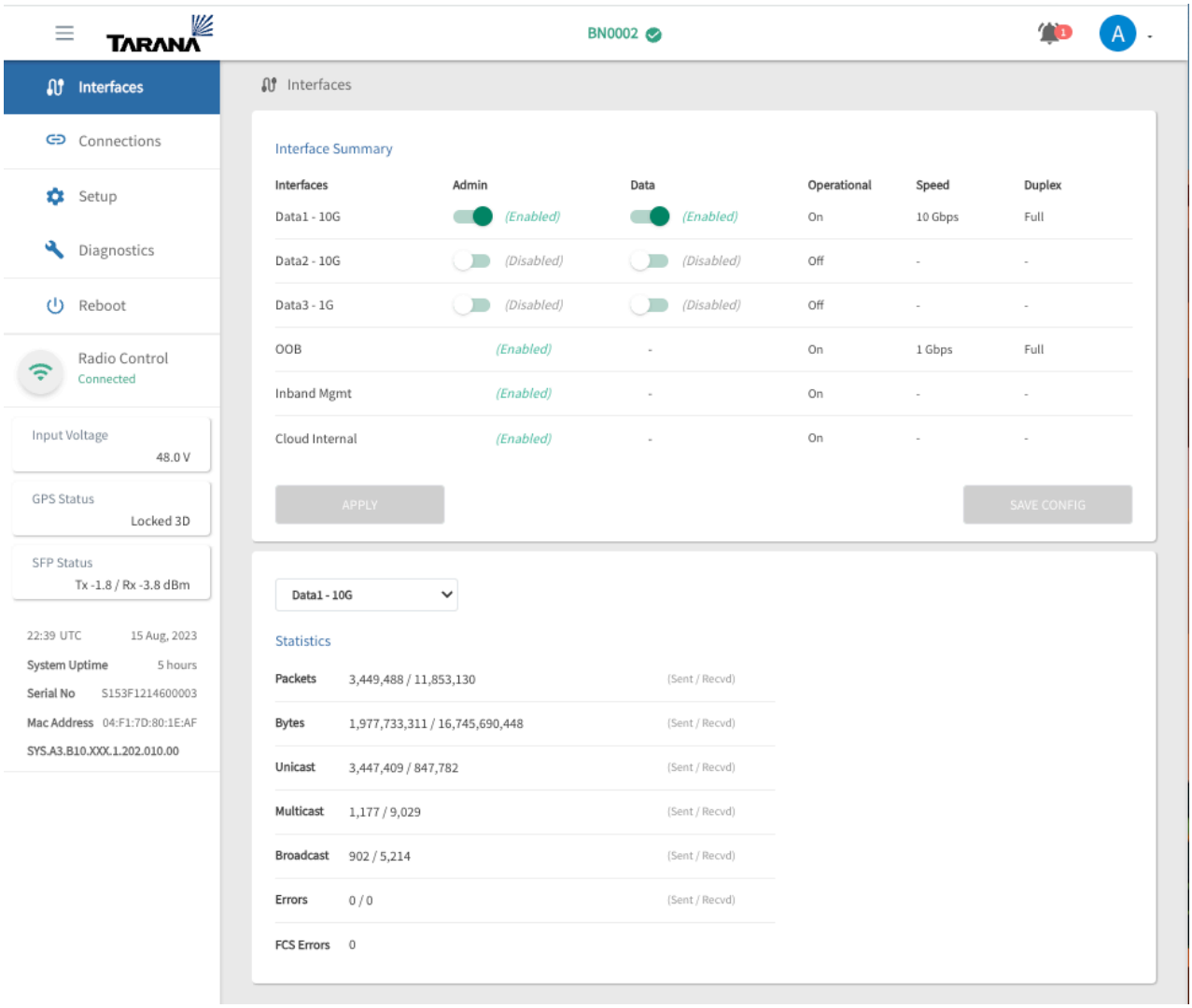
To view or edit network interface configurations, select **Interfaces** from the navigation pane.

Use the toggles in the top box to switch between different modes on each network interface.

NOTE
You can’t disable In-Band management, Out-of-Band (OOB) management, or the Cloud Internal interface (TCS).

If you made changes, select **Save Config**. New configuration settings aren't used until you select **Apply** or the system is rebooted.

The lower box shows network statistics for each interface. Use the drop down to switch between network interfaces.



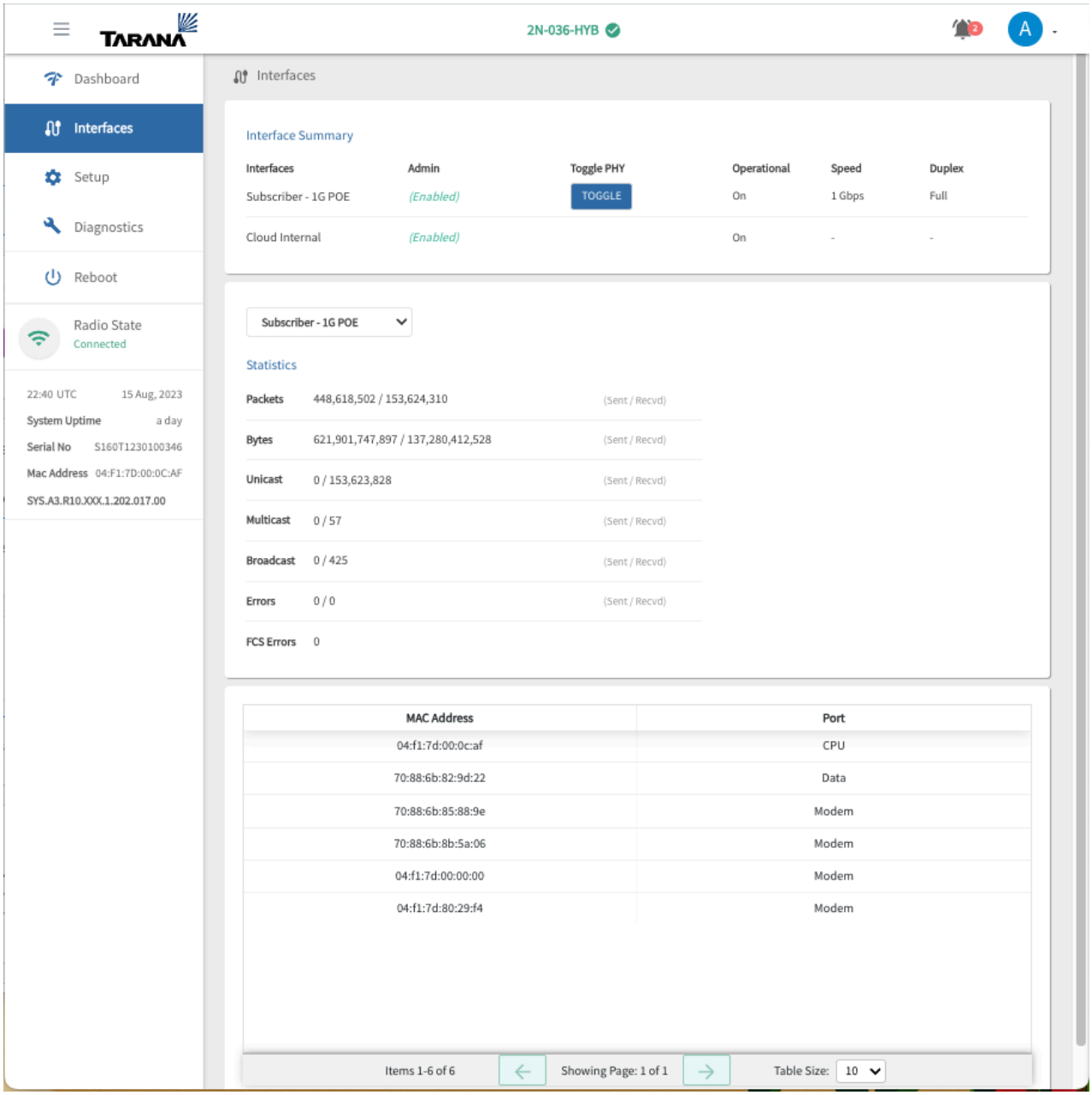
Web UI Network Interface Summary and Statistics (Base Node)

Remote Node Interfaces

To view or edit network interfaces, select **Interfaces** on the navigation pane. A summary view at the top displays operation information: whether the interface is administratively enabled, operational status, interface speed, and duplex capability. Select **Toggle** to toggle PHY.

The middle box displays statistics. Use the drop down to display detailed information about a specific network interface.

The lower box displays MAC addresses and ports.



Web UI Network Interface Summary and Statistics (Remote Node)

Device Connections (Base Node Only)

To view information about connected remote nodes, select **Connections** from the navigation pane . A summary of sector statistics is shown at the top:

- **Utilization:** Percentage of sector capacity in use.
- **Active Connections:** Number of remote nodes currently connected to the base node.
- **Connection Requests:** Number of remote nodes that have attempted to connect to the base node, including the number of failed attempts, if any.

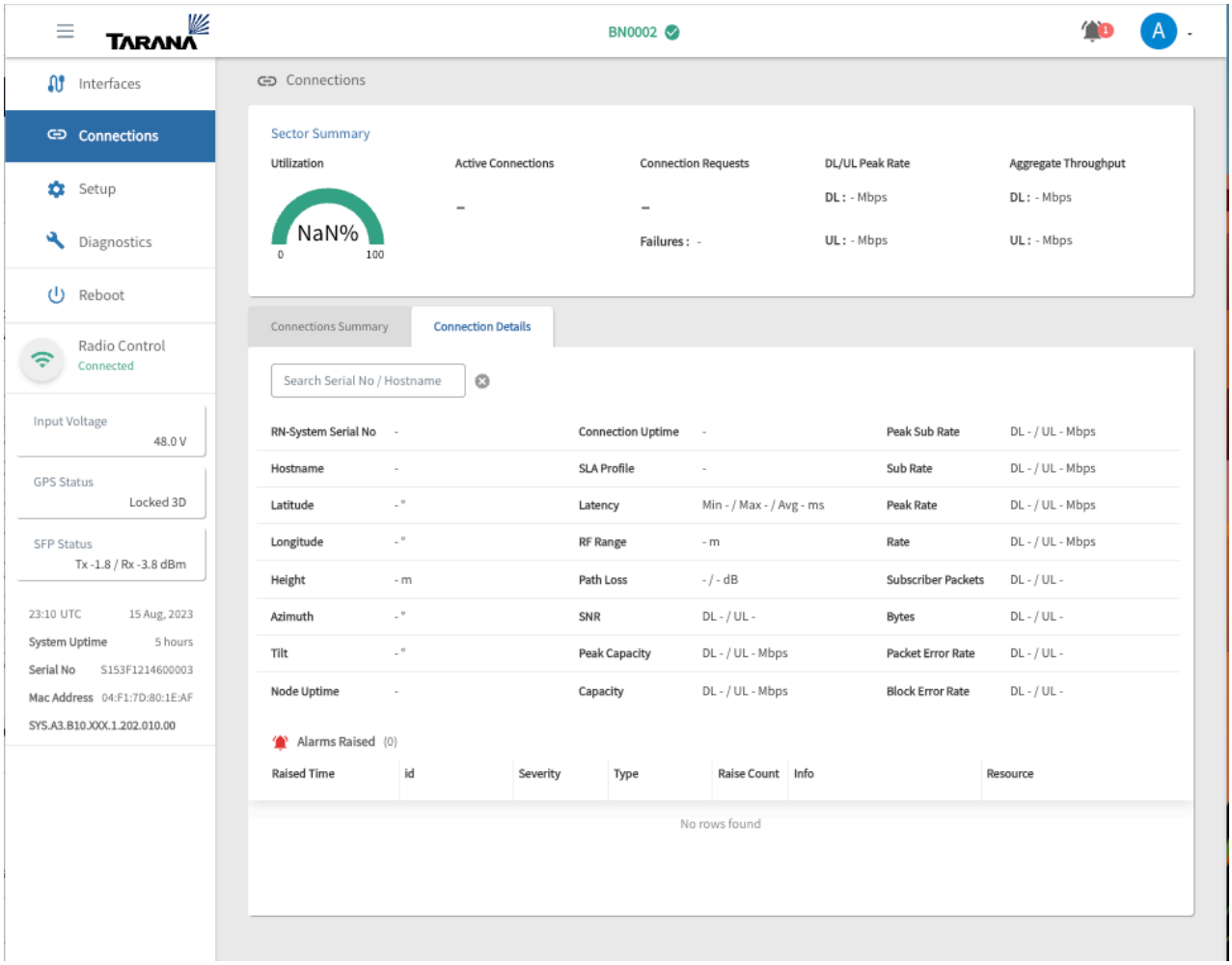
- **DL / UL Peak Rate:** Current capacity in use by the connected devices, by connection direction (download and upload).
- **Aggregate Throughput:** Amount of data throughput being passed through the base node, by connection direction (download and upload).
- **Failures:** The number of failures.

Information for connected devices is shown below the sector summary. There are two tabs, Connections Summary and Connections Details.

Connection Summary shows:

- Serial number. To see that device's page, select its serial number.
- Hostname
- Link Uptime
- RF Range in meters
- Downlink Block Error Rate expressed in scientific (e) notation
- Uplink Block Error Rate expressed in scientific (e) notation
- Downlink capacity in Mbps
- Uplink capacity in Mbps
- Mac Table list - select **Show** to view it.

Connection Details shows more detail about the device. You can also see this information by entering the device serial number or hostname in the search bar.

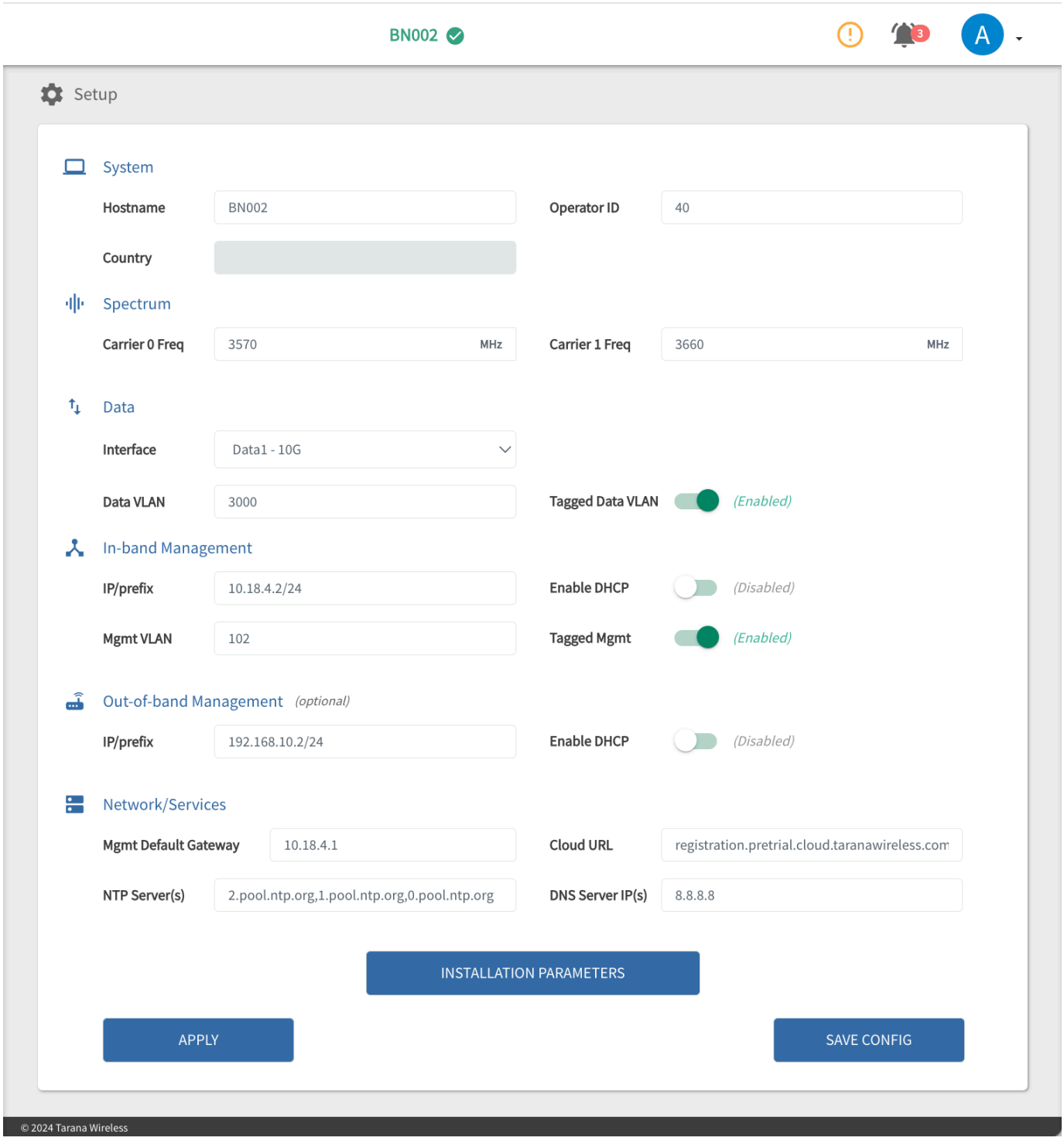


Web UI Device Connections

Base Node Setup

When you log in to a base node's web UI, you see the device setup screen. This is a summary of the current configuration where you can make changes.

The Hostname of the device is shown at the top. If it’s displayed in green, the device is connected to TCS. An alarm icon in the top right corner changes to red to indicate active alarms that require attention.



Base Node Configuration Setup

You can change these configuration options:

- **System**: Required device information.

- **Hostname**: Configurable name of the device.
- **Operator ID**: Base nodes and remote nodes must share the same Operator ID to connect.
- **Country**: The regulatory domain in which the radios operate. This determines available channels and transmit power.
- **Carrier 0 Frequency**: Frequency for the carrier 0 radio, in MHz.
- **Carrier 1 Frequency**: Frequency for the carrier 1 radio, in MHz.

- **Data**: Specifies the data port.
  - **Interface**: Physical port (Data1, Data2, Data3) used for data transmission.
  - **Data VLAN**: All data on the data interface is tagged with the specified VLAN. The default Data VLAN is 2000. Allowed values are 2 - 4091. For more about VLANs, see VLANs and Quality of Service (page 164).
  - **Tagged Data VLAN**: Use the toggle to disable or enable. To travel in both directions, traffic coming into any data port must be tagged with the Data VLAN number.
  - **Enable DHCP Relay Agent**: Enable DHCP Option 82, which includes base node and remote node identification information during the DHCP process.
  - **Remote / Circuit Identifier Type**: Identifier to use in DHCP Option 82 identification. The Agent Remote ID identifies the base node and the Agent Circuit ID identifies the remote node. Choose **Serial Number** or **MAC Address** from the drop-down.

NOTE
This control is only visible when **Enable DHCP Relay Agent** is enabled.

- **In-Band Management**: Configuration for the in-band management port.
  - **IP / Prefix**: IP address and subnet mask. Subnet mask must be in CIDR notation. Example: /24. You can enter an IP address manually only if **Enable DHCP** is set to **Disabled**.
  - **Enable DHCP**: Enable or disable DHCP. For details about the DHCP Relay Agent, see DHCP Option 82 Support (page 141).
  - **Mgmt VLAN**: If you enter a value, all traffic on the in-band management port is tagged with the specified VLAN. You can enter a management VLAN manually only if **Tagged Management** is set to **Enabled**.

> **NOTE**
> The in-band management VLAN must be different from the Data VLAN.

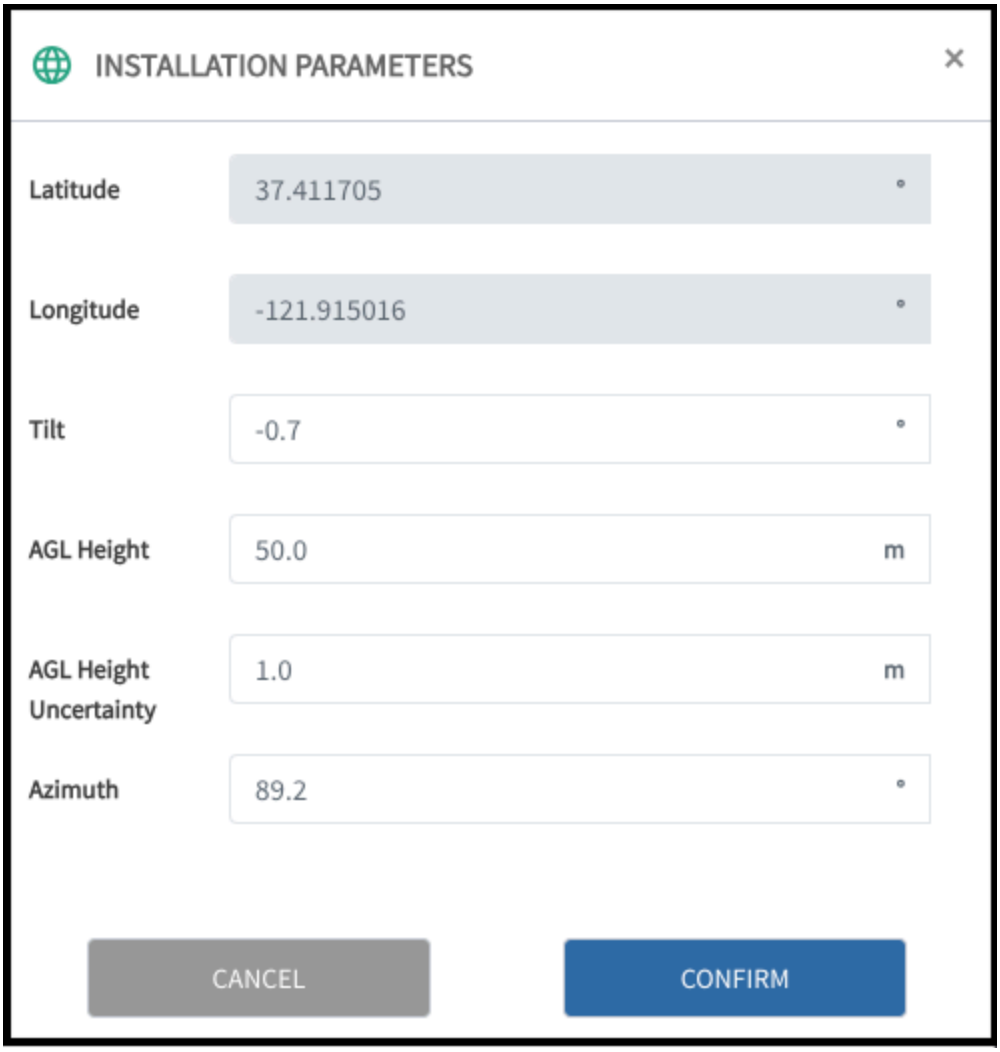
  - **Tagged Mgmt**: Enable manual assignment of a management VLAN.

- **Out-of-Band Management**: Out-of-band management port. Value is optional.
  - **IP / Prefix**: IP address and subnet mask. The subnet mask must be in CIDR notation. Example: /24. You can enter an IP address manually only if **Enable DHCP** is set to **Disabled**.
  - **Enable DHCP**: Enable or disable DHCP.

> **NOTE**
> Don’t enable DHCP for both in-band and out-of-band management. VLAN tagging isn't available for out-of-band management.

- **Network / Services**: Other network services.
  - **Mgmt Default Gateway**: Default gateway for the device.
  - **Cloud URL**: URL for the TCS system associated with this operator.
  - **NTP Server(s)**: By default, the NTP Server is set to **2.pool.ntp.org,1.pool.ntp.org,0.pool.ntp.org**. You can configure this parameter using an IP address or FQDN. This parameter can't be blank, but by default, the NTP is not used because the base node uses GPS for synchronization.
    If you need this value for lab testing (when the base node doesn't have a view of the sky for GPS synchronization), contact Tarana Support for assistance.
  - **DNS Server IP(s)**: Domain Name Servers (DNS) used to resolve the TCS URL. Enter servers as IP addresses.

Select **Installation Parameters** to verify the values, You can edit **Tilt**, **AGL Height**, **Height Uncertainty**, and **Azimuth**, .



Base Node Installation Parameters

IMPORTANT
Height and uncertainty must be entered by the professional installer or operator. Installers are obligated to verify the accuracy of the height during the configuration of the device.

- **Tilt**: Vertical angle, measured in degrees, from the horizon (0 degrees).
- **AGL Height**: Installed height above ground level (AGL).
- **AGL Height Uncertainty**: The potential margin of error in determining the antenna height in relation to the ground level.
- **Azimuth**: Horizontal angle of device installation as measured clockwise from north.

If you made any changes, select **Save Config**. If you want the changes to take effect immediately, select **Apply**. New configuration settings aren't applied until you select **Apply** or the system is rebooted.

Notes

- If you're configuring the base node pre-deployment in a lab, it helps to keep it close to a window so it can get a GPS sync with satellites.
- These values are reserved and you can't use them as any part of a G1 network:
  - Reserved VLANs: 4092, 4093, and 4094
  - Reserved IP subnets: 172.27.0.0/18 and 10.240.0.0/12
- The Data VLAN (optional but strongly recommended in a production network) and the Management VLAN (optional) are on the data port. They must be separate VLANs.
- On the switch north of the base node, the IP subnet associated to the Data VLAN entering the base node data port must be different from the In-band Management IP subnet.
- Out-of-band management is optional. If you use it, you must configure it to use a different IP subnet as In-band management.
- For DHCP with Option 82 to function properly the following must be true:
  - You must configure the client device to request an IP address via DHCP.
  - You must configure the base node to act as a DHCP relay and it must have the required sub-options, such as the Agent Circuit ID or Agent Remote ID configured. In a Tarana network, the AgentCircuit ID identifies the remote node, and the Agent Remote ID identifies the base node. In TaranaCloud Suite (TCS), the Agent Circuit ID and Agent Remote ID are combined in a single control labeled **Remote / Circuit Identifier Type**, which can use either the MAC address or the serial number of the devices.
  - You must configure the DHCP server to accept and respond to DHCP Option 82. Because the base node defines the Option 82 values using lower case, configure the DHCP server accordingly.
- These IP ports must be open to allow the base node to reach TCS:
  - 443 (TCP for HTTPS)
  - 53 (UDP for DNS)
  - 123 (UDP for network time)

  Also, the TCS URL(s) used by the G1 devices should be in a permit / allow list so all Tarana devices can connect to TCS.

- Once you've completed the initial deployment, don't use the web UI for configuration changes. Configuration settings in TCS overwrite web UI settings. To avoid misconfiguration, always use TCS once the device is registered and connected to TCS. TCS flags configuration mismatches with an alarm.

NOTE
For CBRS installations, change the Cloud URL to: registration.trial.cloud.taranawireless.com:443

For CBRS installations, enter your CPI ID. The base node won't be able to access the spectrum until you do this.

Remote Node Setup

The Hostname of the device is shown at the top. If it’s displayed in green, the device is connected to TCS. An alarm icon in the top right corner shows in amber when the device is disconnected, or red when the device is rebooting.

To set up or edit the device configuration, select **Setup** from the navigation pane and enter values for these fields:

- **Operator ID:** Base nodes and remote nodes must share the same Operator ID to connect.
- **Primary BN:** Activate to assign a primary base node, then enter the Planning ID of the base node. You can find it in the Planning ID column on the Devices page.
- **Search for BNs:** When you select **Search for BNs** the remote node starts or restarts the search operation. It searches for base nodes with the same operator ID, primary base node, and priority list, unless you reset configurations.

NOTE
This action interrupts subscriber service.

- **Radio State:** Indicates if the radio is searching, initializing, calibrating, or connected. Before a remote node connects to a base node, it searches for a viable base node signal. The list of detected base node signals is represented by the Search Metric as the remote node scans through the supported frequencies. After the remote node completes the scanning process, it enters the Initialization stage with the base node that has the highest Search Metric. The remote node then goes through the Calibration stage before it establishes the connection to the base node.
  You can repeat this process by selecting **Search for BNs**.

> **NOTE**
> Don't move the remote node while it's in the Calibration stage.

- **Alignment Metric:** Once the remote node is connected to a base node, the Alignment Metric appears, a unitless dial whose values range from 0 - 30, with 30 being the best alignment for a remote node. It's based on multiple factors, not any one metric. Once the remote node is aimed, the dial responds in real time and may be used as part of antenna aiming during installation.

> **NOTE**
> The recommended minimum value for a usable link is 10.

- **Hostname:** Remote node hostname.
- **Data VLAN:** Enter the remote node Data VLAN here. The Data VLAN always exists between the base node and the upstream router. Defining a Data VLAN on the remote node overrides only what the base node uses for that remote node's traffic. For more about VLANs, see VLANs and Quality of Service (page 164).
- **Latitude:** Geographical latitude of the remote node in decimal notation.
- **Longitude:** Geographical longitude of the remote node in decimal notation.
- **Tilt:** Vertical (elevation) angle of device installation as measured from the horizon (0 degrees).
- **Height (AGL):** Installed height above ground level.
- **Azimuth:** Horizontal angle of device installation as measured clockwise from north.

> **NOTE**
> You can enter all values manually on this page, or from the Remote Node Location Metrics (page 61) page.

For 5 GHz remote nodes, Latitude and Longitude are necessary only for an accurate Map View in TCS. Height, Tilt, and Azimuth are optional.

For CBRS remote nodes, all five of these parameters are required to acquire a grant, otherwise the remote node will be stuck trying to acquire spectrum.

If you made any changes, select **Submit Changes**. For a 5GHz remote node, configuration changes are applied immediately.

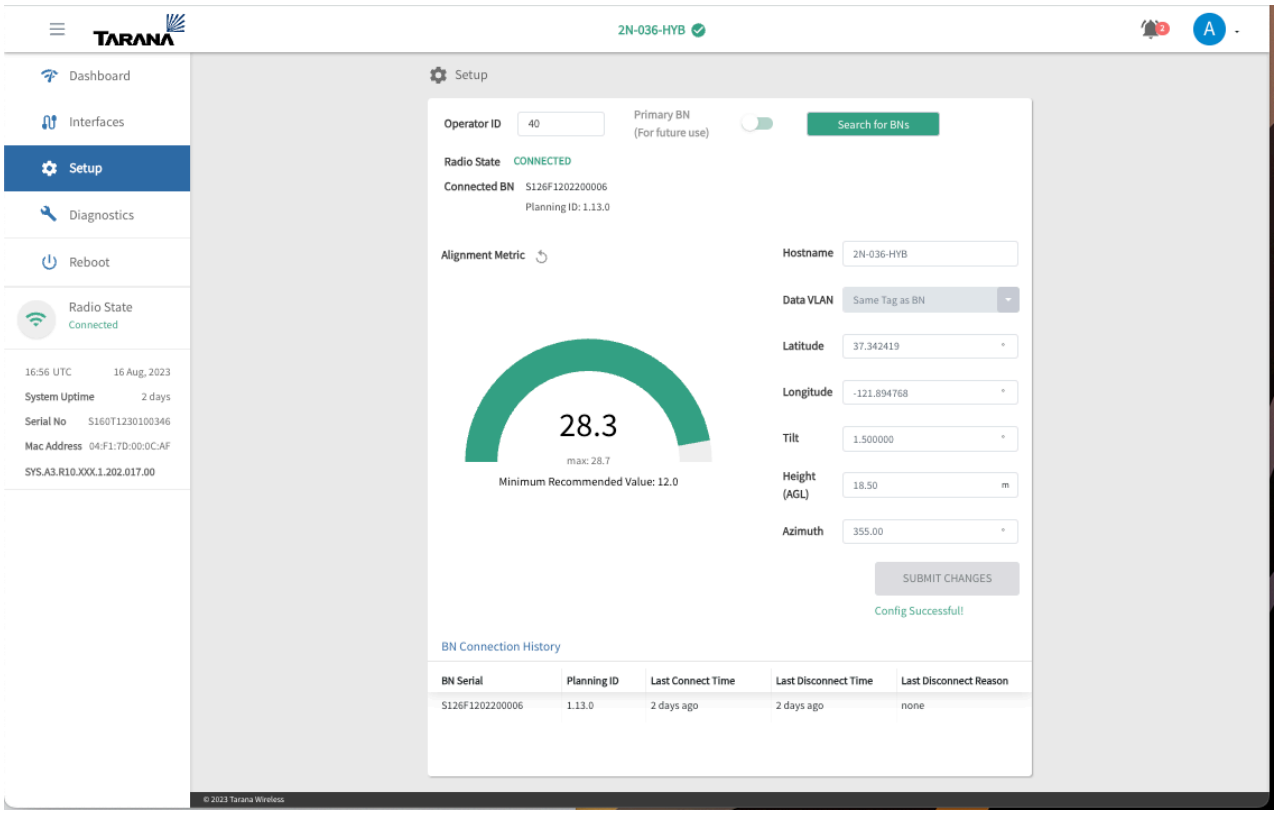
If this is a CBRS remote node, you see a pop up where you must verify the location metrics and enter the CPI ID.

Field personnel can enter the string "USE_FROM_TCS" (not case sensitive) instead of a CPI ID. TCS holds the device information but doesn't add the remote node until a user with NOC OP or OP Admin permissions enters the CPI ID along with installation parameters. See the Remote Node Install Guide for details.

BN Connection History

These values are displayed for reference:

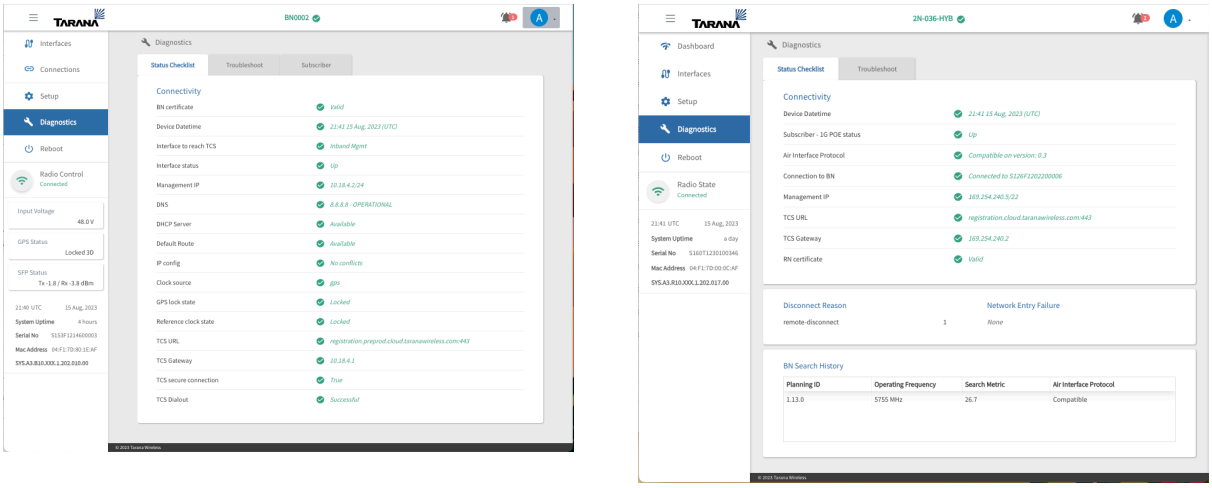
- **BN Serial:** The serial number of the base node to which the remote node is connected.
- **Planning ID:** The planning ID of the device.
- **Last Connect Time:** Last time the device was connected.
- **Last Disconnect Time:** Last time the device was disconnected.
- **Last Disconnect Reason:** Reason for the last disconnect.



Remote Node Configuration Setup

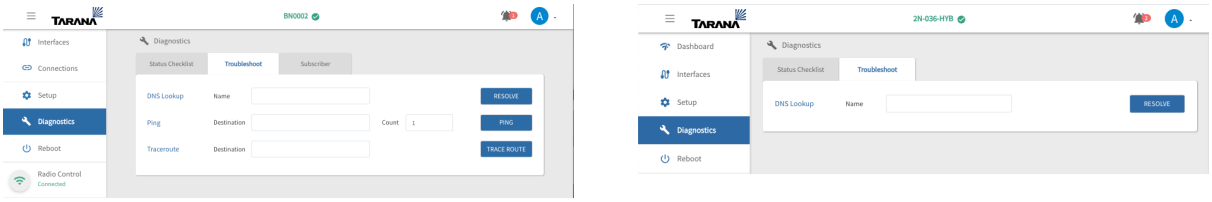
Diagnostics

To view a checklist of key system status indicators, select **Diagnostics** from the navigation pane. The base node interface shows three tabs: Status Checklist, Troubleshoot, and Subscriber. The remote node interface shows Status Checklist and Troubleshoot.



Base Node and Remote Node Diagnostics (Status Checklist Tab)

DNS lookup, Ping, and Trace Route tools are available for a base node. DNS Lookup is available for a remote node.

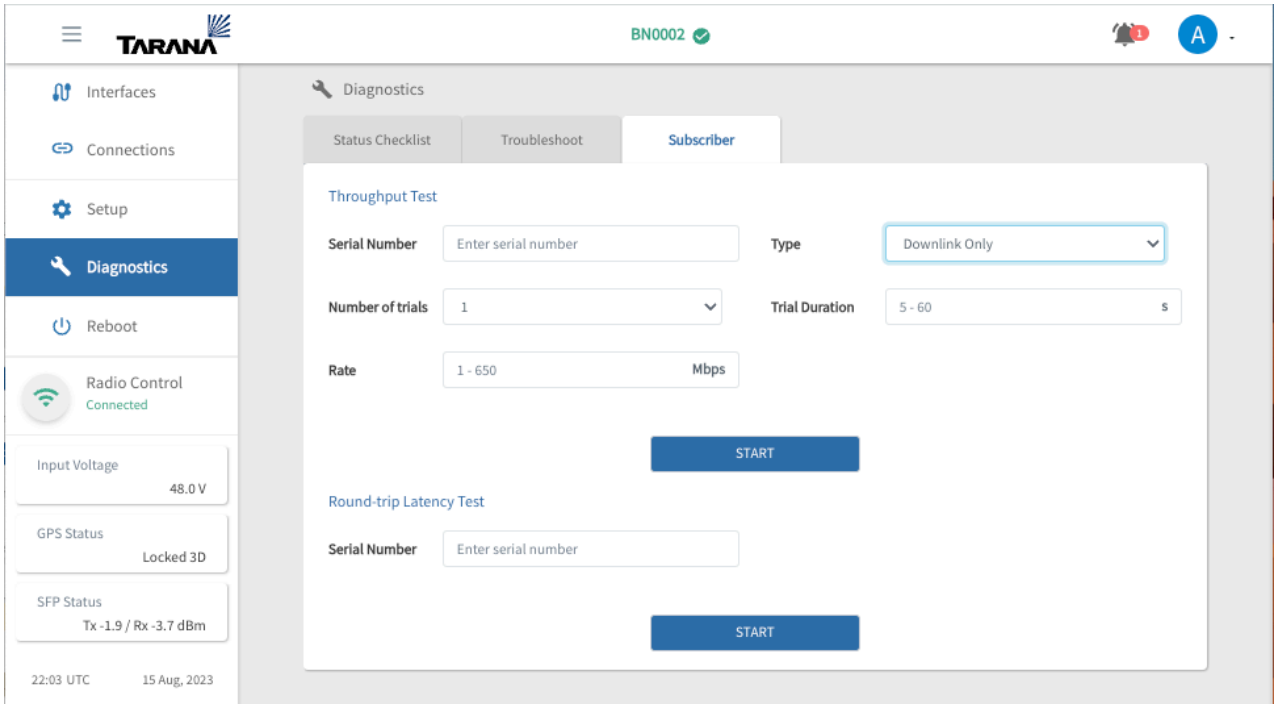


Base Node and Remote Node Diagnostics (Troubleshoot Tab)

In the base node interface, use the Subscriber tab to test throughput of the base node to the remote node link. You can run only one test from or against a base node at a time.

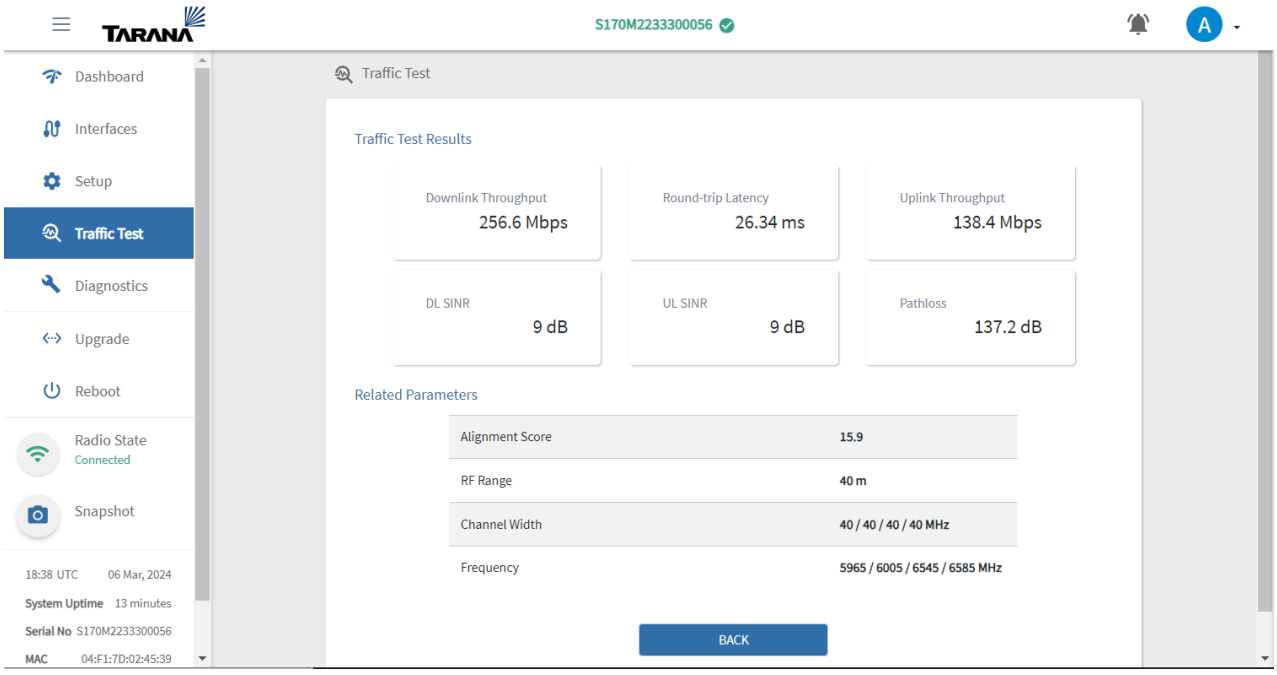
For a Throughput Test, enter the serial number of the base node, then select **Downlink Only** or **Roundtrip** under type. Enter the number of trials, the trial duration, and rate, then select **Start**.

For a Round-trip Latency Test, enter the serial number of the base node, then select **Start**.



Base Node Throughput Tests (Subscriber)

You can run a traffic test by logging in to a node directly. Enter the IP address into a browser. The default IP address is 192.168.10.2.

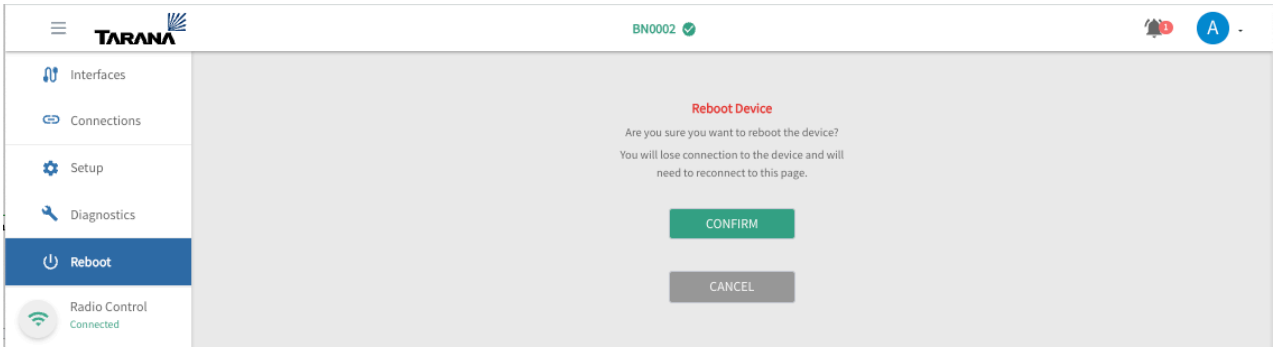


Traffic Test

Device Reboot

To reboot the device, select **Reboot** from the navigation pane. Select **Confirm** to reboot immediately or **Cancel** to cancel the reboot.

NOTE
Rebooting a base node affects service for all associated remote nodes.



Reboot Device

Radio Control

The device's radio state appears in the navigation pane.

To mute or unmute the radio on a base node, select the **Settings** icon (⚙) in the upper right corner of the window. Select **Transmit**, then **Done**.

NOTE
Muting a base node turns off the radios. The base node stops transmitting / receiving and all connected remote nodes are immediately disconnected.

Air Interface Protocol Version 1

The Tarana Air Interface Protocol (AIP) controls the signaling between a base node and its remote nodes.

Devices running software 0.9x use AIP version 0 and support the 3 GHz and 5 GHz bands. Devices running software version 1.2 or later support AIP version 0, but can also support AIP version 1, which improves signaling and adds support for the 6 GHz band.

AIP version 1 is not backward compatible with AIP version 0, so plan carefully when selecting AIP version 1 or deploying a 6 GHz environment.

The AIP protocol version also appears in the device status card on the single device page.

Migrate devices to software version 1.2

To migrate base nodes and remote nodes successfully to software version 1.2, you must upgrade the remote nodes in a sector first before upgrading the base node. By upgrading the remote nodes first, you ensure that the base node can communicate with the remote nodes after the upgrade.

Upgrade Remote Node Software

To upgrade remote node software, do the following:

1. Log in to TCS with Op Admin or NOC Operator privileges.
2. Navigate to **Devices > List**, and then select **RN** to view the list of remote nodes.
3. Select the remote node serial number to open the single device page.
4. Select **Install Software** ( ) then **Install New Software** from the tool bar drop-down list.
5. Select **Activate Software After Download**.
6. Select the software image you want to install from the Install New Software dialog, then select **Proceed**.

Repeat this procedure for each remote node in the sector.

Upgrade Base Node Software

To upgrade the base node software, do the following:

1. Log in to TCS with Op Admin or NOC Operator privileges.
2. Navigate to **Devices > List**, and then select **BN** to view the list of base nodes.
3. Select the base node serial number to open the single device page.
4. Select **Install Software** ( ) then **Install New Software** from the tool bar drop-down list.
5. Select **Activate Software After Download**.
6. Select the software image you want to install from the Install New Software dialog, and then select **Proceed**.

After the base node and all remote nodes of a sector are running software version 1.2 or later, you can migrate the base node to AIP version 1 to take advantage of the enhanced signaling.

Migrate Base Node to AIP Version 1

To migrate a remote node from AIP version 0 to version 1, do the following:

1. Log in to TCS with Op Admin or NOC Operator privileges.
2. Navigate to **Devices > List**, and then select **BN** to view the list of base nodes.
3. Select the base node serial number to open the single device page.
4. Select **Configuration** ( ) then select **Configure Network Parameters** from the tool bar drop-down list.
5. Select **Version 1** from the Air Interface Protocol drop-down list, and then select **Done**.

VLANs and Quality of Service

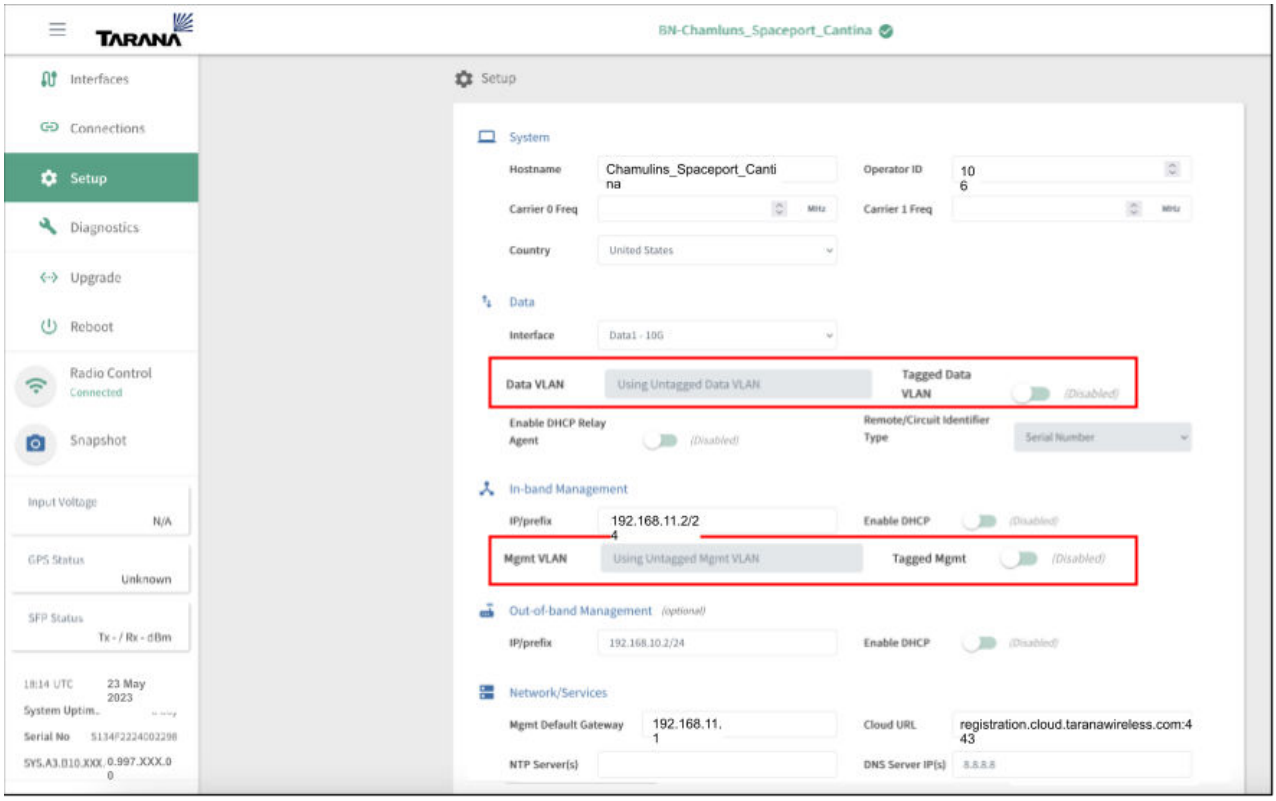
VLANs on G1 Devices

Appropriate VLAN configuration is crucial for the proper functionality of the Tarana devices. You must complete this so the devices will pass data traffic. Although devices may show up on TCS without any VLAN configuration, it's important to understand that this is the result of management traffic sent from the devices to TCS and not data traffic.

Tagged and untagged management traffic is supported. By default, management traffic is untagged. You configure this optional feature through the base node's web UI.

Base Node VLANs

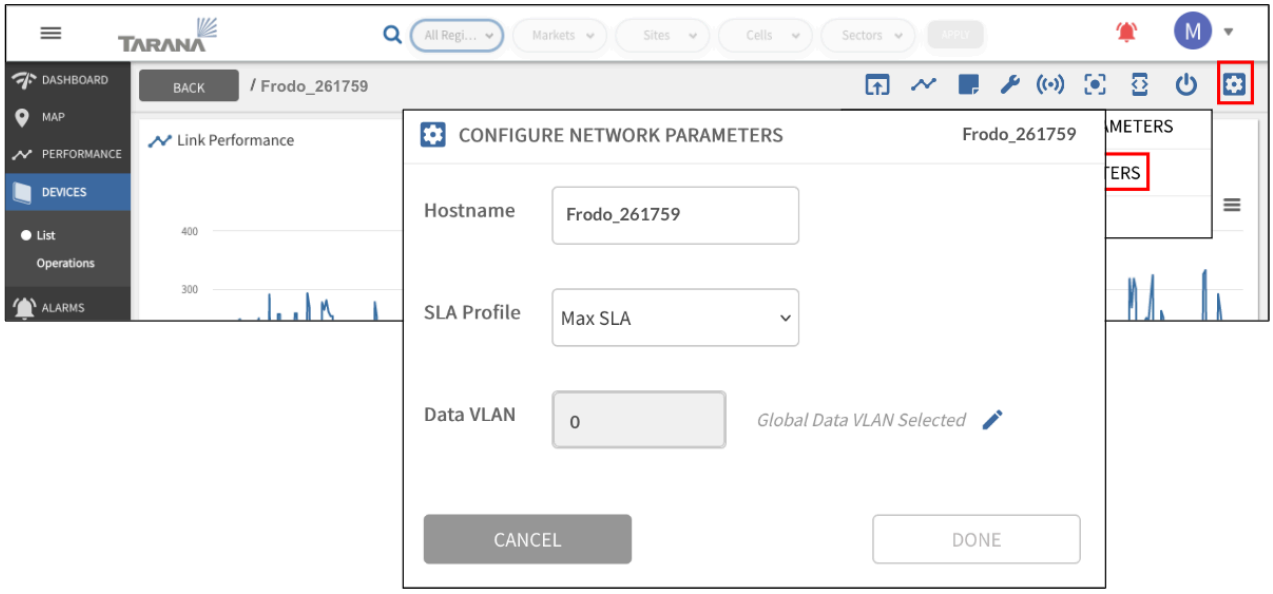
The base node's data ports (DATA1, DATA2, DATA3) support tagged and untagged data frames (untagged with software version 0.99x or higher) between itself and the router. By default, the base node tags egressing data frames toward the router with VLAN 2000. Arriving frames sent from the network router to the base node's data port must therefore also be tagged with this VLAN number. You can change the default Data VLAN by using the base node's web UI, as seen here, or configure it so there's no Data VLAN and traffic is untagged.



Configure VLANs on the base node Web UI

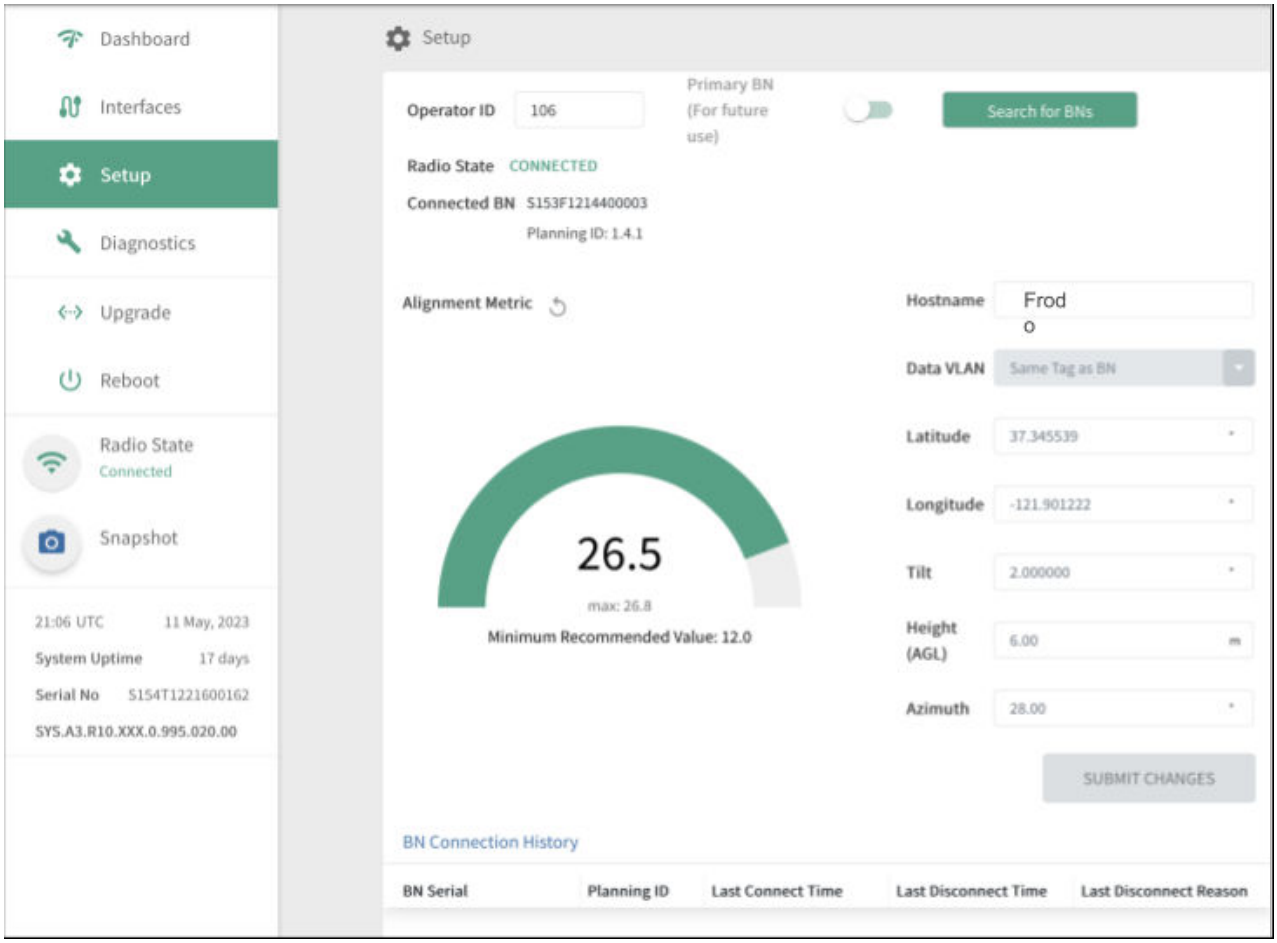
Remote Node VLANs

The optional VLAN setting on the remote node overrides the VLAN setting on the base node. The remote node doesn't tag or untag frames. In this case, arriving frames sent from the network router to the base node’s data port must be tagged with the VLAN number of the remote node’s setting. In the image below, this would be VLAN 50.



Configure the Data VLAN on the Remote Node in TCS

This image shows the remote node's default VLAN setting in the Web UI.



Configure the Data VLAN on the remote node Web UI

Tarana VLAN Logic

These images detail the VLAN logic for Tarana devices. Note this logic allows for multiple VLANs to pass through the remote node's data port. If you require tagged frames downstream of the remote node, you must configure the VLAN at the network switch / router.

There are two points to consider regarding VLAN settings of Tarana devices:

- The Data VLAN between the base node and connected router (or switch) is optional, but enabled by default. Untagged data frames can be sent and received.
- The optional Data VLAN setting on the remote node doesn't cause the remote to tag frames. Rather, it overrides the Data VLAN setting on the base node.

Scenario	RN Data VLAN Setting	BN Data VLAN Setting	Frame Structure Between BN Data Port and Router
Untagged frame at RN's data port	No setting	Tagging disabled	DA | SA | Etype | DATA | FCS

No Data VLAN at End Device Port, Remote Node, or Base Node

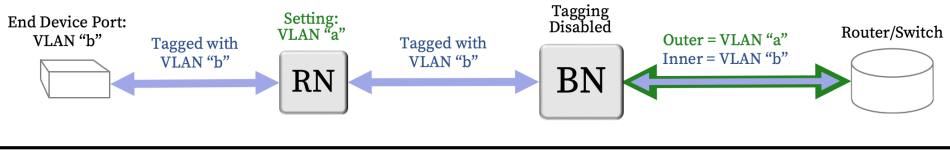
The remote node's Data VLAN setting (VLAN “a” in this example) overrides the base node's Data VLAN setting. The remote node doesn't tag or untag frames. You set the remote node's VLAN by using TCS on the remote node's Device page, or its web UI. Note that if the base node has multiple remote nodes connected, each with a different VLAN setting, the base node / router connection must be a VLAN trunk.

Scenario	RN Data VLAN Setting	BN Data VLAN Setting	Frame Structure Between BN Data Port and Router
Untagged frame at RN's data port	VLAN “a”	Tagging disabled	DA | SA | 802.1Q Header (TPID=8100, VLAN “a”) | Etype | DATA | FCS

Remote Node VLAN "a", No Data VLAN at End Device Port or Base Node

If the remote node has a Data VLAN setting, tagged frames between the end device and the router are encapsulated between the base node and the router by the remote node setting's VLAN number (VLAN “a”). For this segment, the frames have an outer tag (VLAN “a”), and an inner tag (VLAN “b”). The router or managed switch must be configured appropriately to account for the encapsulation of VLANs. Multiple VLANs are allowed to ingress the remote node's data port. Note that if the base node has multiple remote nodes connected, each with a different VLAN setting, the base node / router connection must be a VLAN trunk.

Scenario	RN Web UI Data VLAN Setting	BN Web UI Data VLAN Setting	Frame Structure Between BN Data Port and Router
Tagged frame at RN's data port (VLAN “b”)	VLAN “a”	Tagging Disabled	DA | SA | 802.1Q Header (TPID=8100, VLAN “a”) | 802.1Q Header (TPID=8100, VLAN “b”) | Etype | DATA | FCS (Outer Tag) (Inner Tag)



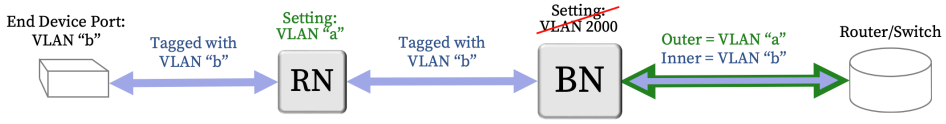
VLAN Set at End Device Port and Remote Node, Base Node Data VLAN Untagged

Scenario	RN Data VLAN Setting	BN Data VLAN Setting	Frame Structure Between BN Data Port and Router
Untagged frame at RN's data port	No setting	VLAN 2000 (default)	DA | SA | 802.1Q Header (TPID=8100, VLAN 2000) | Etype | DATA | FCS

Default Data VLAN Set at Base Node, No Data VLAN on End Device Port or Remote Node

Tagged frames between the end device and the router are encapsulated between the base node and the router by the remote node-setting's VLAN number (VLAN "a"). For this segment, the frames have an outer tag (VLAN "a"), and an inner tag (VLAN "b"). The router or managed switch must be configured appropriately to account for the encapsulation of VLANs. Multiple VLANs are allowed to ingress the remote node's data port. Note that if the base node has multiple remote nodes connected, each with a different VLAN setting, the base node / router connection must be a VLAN trunk.

Scenario	RN Web UI Data VLAN Setting	BN Web UI Data VLAN Setting	Frame Structure Between BN Data Port and Router
Tagged frame at RN's data port (VLAN "b")	VLAN "a"	VLAN 2000 (default)	DA | SA | 802.1Q Header (TPID=8100, VLAN "a") (Outer Tag) | 802.1Q Header (TPID=8100, VLAN "b") (Inner Tag) | Etype | DATA | FCS



VLAN Set at End Device Port, Remote Node, and Base Node

With no Data VLAN settings on the remote node, and "Tagged Data VLAN" disabled on the base node, tagged frames originating from end devices will be forwarded by the base node to the router with no Data VLAN setting on the remote node, and "Tagged Data VLAN" disabled on the base node. The minimum software release for End Device tagged traffic when the base node is set for untagged data is 1.202.009.00.

Scenario	RN Data VLAN Setting	BN Data VLAN Setting	Frame Structure Between BN Data Port and Router
Tagged frame at RN's data port (VLAN "b")	No setting	Tagging disabled	DA | SA | 802.1Q Header (TPID=8100, VLAN "b") | Etype | DATA | FCS

End Device tagged traffic when Base Node is set for Untagged Data

Multiple VLAN Scenarios

The diagram below illustrates these considerations:

- Different remote nodes connected to the same base node can have different VLAN settings.
- Multiple VLANs can pass through a single remote node.
- Untagged frames can pass through the same remote node that passes multiple VLANs.

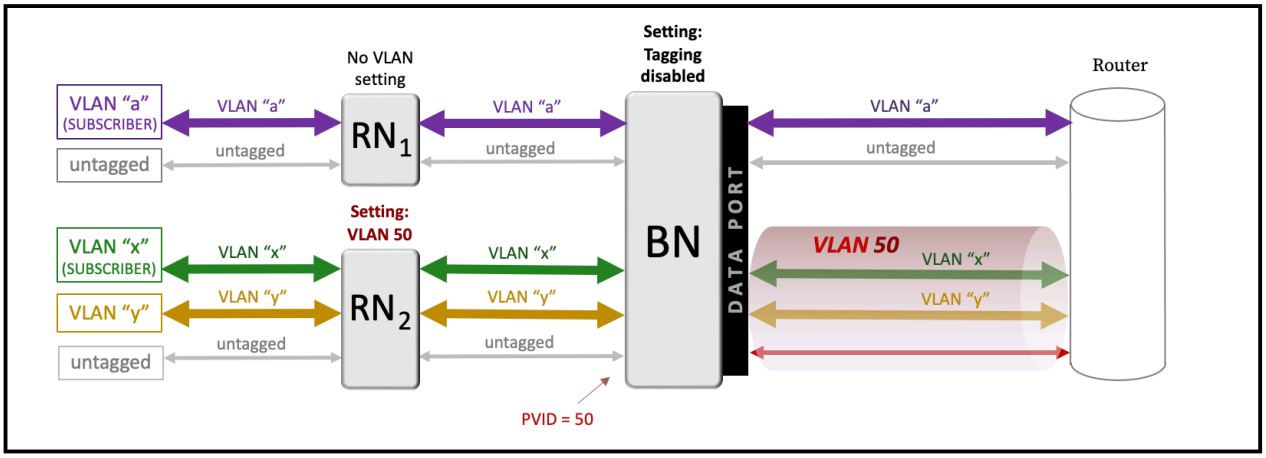
Depending on the desired tag for a frame egressing out of the remote node's data port, you must configure the appropriate tagging at the router.

In the scenario below, one of the remote nodes has a Data VLAN setting (VLAN 50, in this case), and the other does not. This setting instructs the base node to tag untagged frames coming from this remote node with Data VLAN 50 between the base node and the router. Tagged frames coming from this remote node will be encapsulated with VLAN 50 as an outer tag between the base node and the router. For “Subscriber” VLANs (VLAN “x”), note that an appropriate DHCP pool would be needed to distribute IPs among the subscribers in this VLAN.

Scenario	RN Data VLAN Setting	BN Data VLAN Setting	Frame Structure Between BN Data Port and Router
Multiple VLANs required outside of multiple RNs. Untagged traffic will also be required to pass through the RNs and BN	RN_1: No setting RN_2: VLAN 50	Tagging disabled	DA SA Etype DATA FCS DA SA VLAN "a" Etype DATA FCS (OUTER TAG) (INNER TAG) DA SA VLAN 50 VLAN "x" Etype DATA FCS DA SA VLAN 50 VLAN "y" Etype DATA FCS DA SA VLAN 50 Etype DATA FCS

Multiple VLAN Scenario

Multiple VLAN Scenario



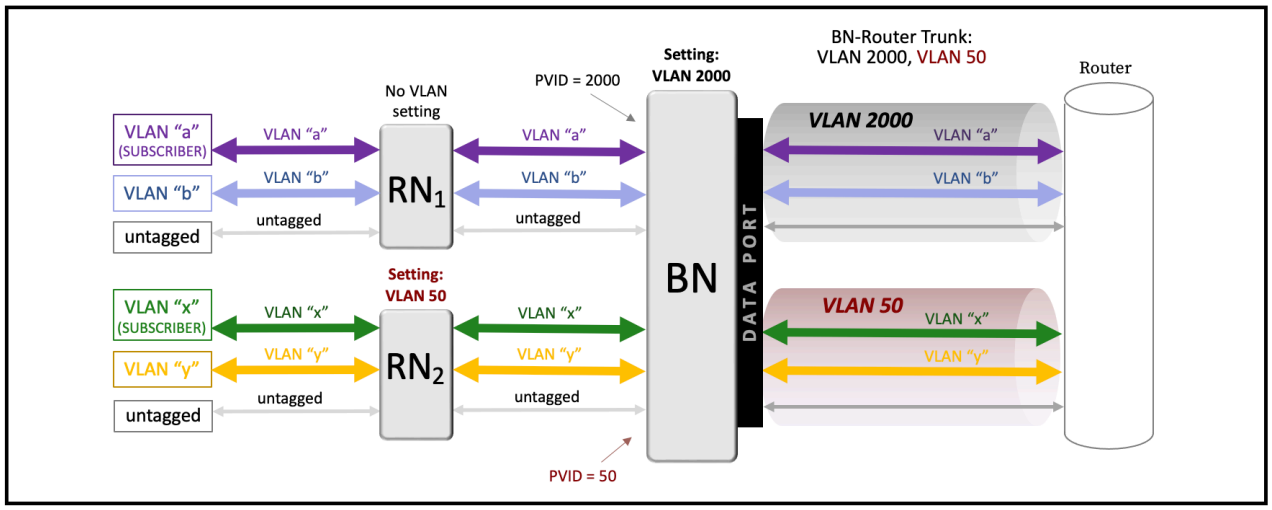
Multiple VLAN Scenario, Base Node Untagged

The following diagram shows frame-structure scenarios where the base node does implement a tagged data VLAN setting.

In the scenario below, one of the remote nodes has a VLAN setting (VLAN 50, in this case) and the other does not. This setting overrides the VLAN setting on the base node, therefore, the VLANs passing through this remote node are encapsulated between the base node and router in VLAN 50 instead of the default VLAN 2000. For "SUBSCRIBER" VLANs (VLANs "a" and "x"), note appropriate DHCP pools would need to be allotted in order to distribute IP addresses among the subscribers on these VLANs.

Scenario	RN Data VLAN Setting	BN Data VLAN Setting	Frame Structure Between BN Data Port and Router
Multiple VLANs required outside of multiple RNs. Untagged traffic will also be required to pass through the RNs.	RN1: No setting RN2: VLAN 50	VLAN 2000 (default)	(OUTER TAG) (INNER TAG) DA SA VLAN 2000 VLAN "a" Etype DATA FCS DA SA VLAN 2000 VLAN "b" Etype DATA FCS DA SA VLAN 2000 Etype DATA FCS DA SA VLAN 50 VLAN "x" Etype DATA FCS DA SA VLAN 50 VLAN "y" Etype DATA FCS DA SA VLAN 50 Etype DATA FCS

Multiple VLAN Scenario



Multiple VLAN Scenario, Base Node Tagged

Quality of Service

Traffic classification can be based on 802.1p Quality of Service (QoS) or Differentiated services (DSCP) and mapped to 8 hardware queues in the base node and 4 hardware queues in the remote node. Tarana only transports QoS-marked frames and doesn't implement QoS.

When queues are full, the drop policy is tail drop.

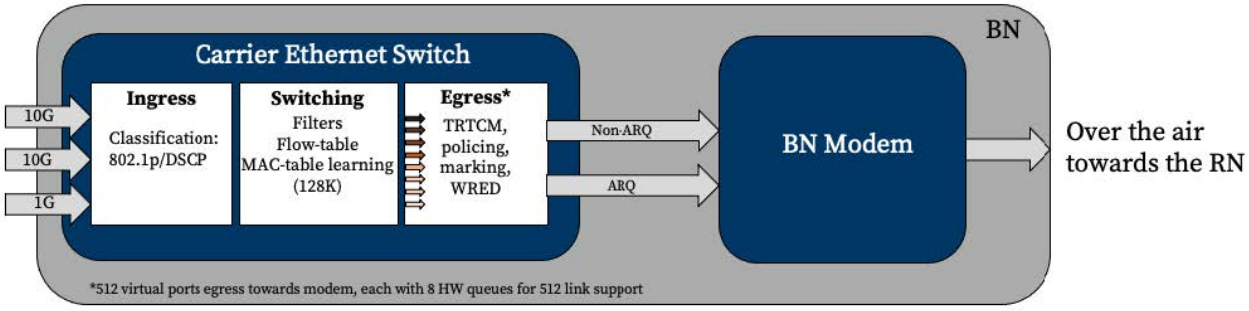
Set the Classification Type parameter on a per-base node basis in Network Configuration > Region > Market > Site > Cell > Sector. The color coding in the charts below shows how traffic is queued in the base node compared to the remote node.

Class of Service	Traffic	BN Queues	RN Queues
7	Network Control		
6	Internetwork Control		
5	Voice (Non-ARQ)		
4	Video		
3	Critical Apps		
2	Excellent Effort		
1	Background		
0	Best Effort		

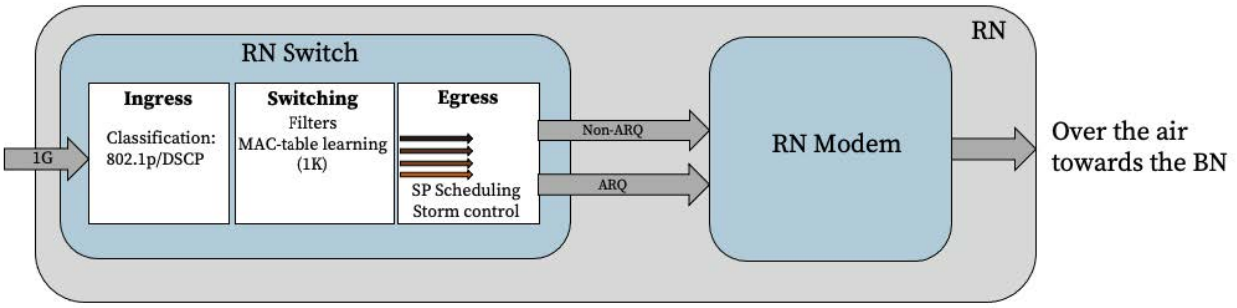
802.1p QoS Queues

IP Precedence Value	Traffic	DSCP Value (Decimal)	Traffic	BN Queues	RN Queues
111	Network	111 000 (56)	CS7		
110	Internet	110 000 (48)	CS6		
		101 110 (46)	EF Non-ARQ		
101	Critical	101 000 (40)	CS5		
		100 110 (38)	AF43 (High drop probability)		
		100 100 (36)	AF42 (Medium drop probability)		
		100 010 (34)	AF41 (Low drop probability)		
100	Flash Override	100 000 (32)	CS4		
		011 110 (30)	AF33 (High drop probability)		
		011 100 (28)	AF32 (Medium drop probability)		
		011 010 (26)	AF31 (Low drop probability)		
011	Flash (Voice Signaling or Video)	011 000 (24)	CS3		
		010 110 (22)	AF23 (High drop probability)		
		010 100 (20)	AF22 (Medium drop probability)		
		010 010 (18)	AF21 (Low drop probability)		
010	Immediate	010 000 (16)	CS2		
		001 110 (14)	AF13 (High drop probability)		
		001 100 (12)	AF12 (Medium drop probability)		
		001 010 (10)	AF11 (Low drop probability)		
001	Priority	001 000 (8)	CS1		
000	Routine or Best Effort	000 000 (0)	CS0		

DSCP Queues



Queuing on the base node



Queuing on the remote node

Troubleshooting

These are common scenarios and suggested troubleshooting steps. For more help, contact Tarana support.

TCS Troubleshooting

The following are common scenarios and suggested troubleshooting steps. For more help, contact Tarana support.

TCS Loads Slowly or Doesn't Work as Expected

If the TCS web UI doesn’t work as expected it may be a browser issue. Always use a browser that's up to date. If this doesn’t address the issue, try clearing cache and reload.

Remote Node Troubleshooting

The following are common scenarios and suggested troubleshooting steps. For more help, contact Tarana support.

Can't Connect to Remote Node Web UI

There are two ways to connect to the web UI of the remote node:

- Using TCS
- Through a laptop directly connected to the PoE injector powering the remote node

TCS Can't Connect to Remote Node, or Remote Node Doesn't Appear

To appear in TCS, a remote node must be connected to a base node that has an internet connection. Without a connection to a base node, the only way to access the remote node web UI is by using a laptop connected to the remote node PoE injector.

Once the remote node connects to the base node, it sends heartbeats over the link every 30 seconds. The remote node isn’t visible in TCS until the base node receives at least one of these heartbeats.

If you access the remote node web UI with TCS and it appears to be slow or unresponsive, this may be due to excessive retries or dropped packets between the remote node and the base node. Confirm the link signal strength and antenna alignment to ensure a strong signal.

Laptop Can't Connect to Remote Node

Access the web UI by connecting a laptop to the Ethernet port of the remote node PoE injector. To confirm connectivity, perform these checks:

- The laptop must be connected using a gigabit Ethernet full-duplex link. Half-duplex or fast ethernet (100 Mbps) connections aren't supported by the remote node.
- The laptop must be configured with the appropriate IP address and subnet. By default, the IP address of a remote node is 192.168.10.2.
- Check the hardware between the laptop and the remote node. It's possible that a remote node can power up but can’t be accessed using the web UI. Common issues include:
  - Faulty or improperly terminated Ethernet cables
  - Dirty cable terminators
  - Excessively long Ethernet cable run. The entire length from laptop to remote node can't exceed 100 m.

Remote Node Isn't Connecting to Base Node

If the remote node is powered up but not connecting to the base node, there are several issues that can cause this.

Verify that the primary base node configuration is correct. If it's incorrect or different from intended base node, it will cause a 15 minute holdoff timer to activate, resulting in high search time.

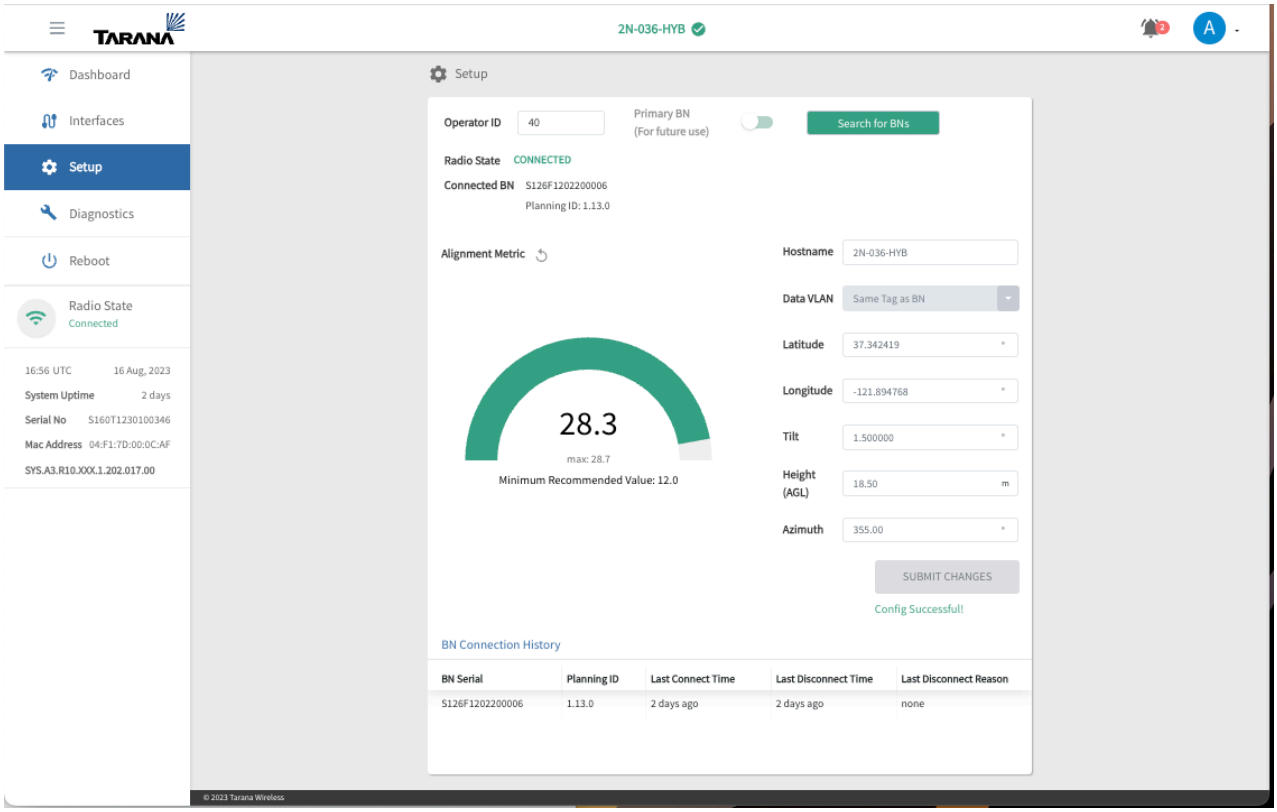
Remote Node Doesn't Boot

If the remote node isn’t fully booted, it can’t connect to the base node. Check the STATUS LED on the bottom edge of the remote node to determine its boot status. If it’s fully booted and operational, the LED is shown in green. For more information about remote node LED status lights, see Device LED Lights (page 187).

Remote Node Calibration Incomplete

After initial power up, the remote node searches for nearby base nodes. Once it selects a base node, it goes through a calibration process before the link is fully established and ready for use. A remote node can take 5 - 7 minutes to fully boot and connect to a base node.

To determine the remote node radio state, log in to the remote node web UI. Select **Setup** and confirm the value of the Radio State field.



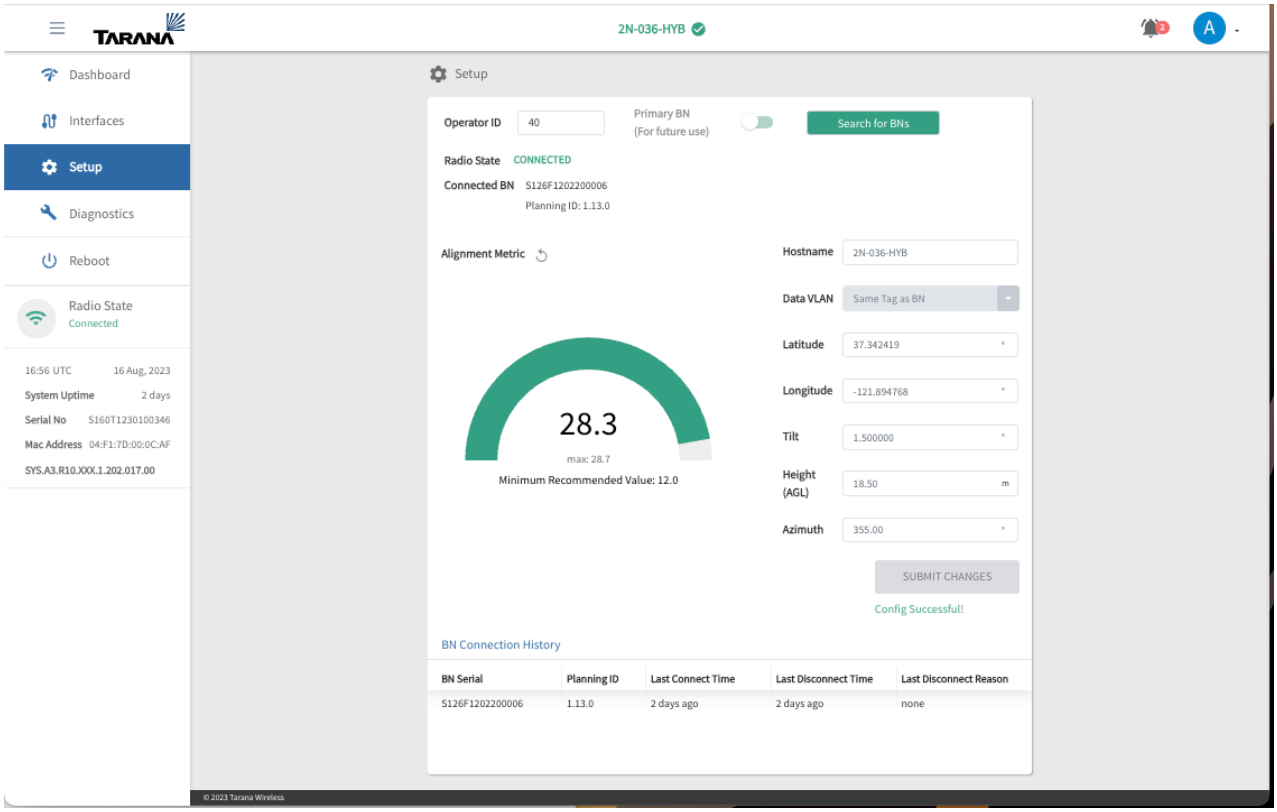
Confirm Remote Node Radio State

Incorrect Operator ID

The remote node uses the Operator ID to determine which base nodes are suitable candidates for a link. The remote node must have the same Operator ID as its intended base node.

To verify and configure the remote node operator ID, follow these steps:

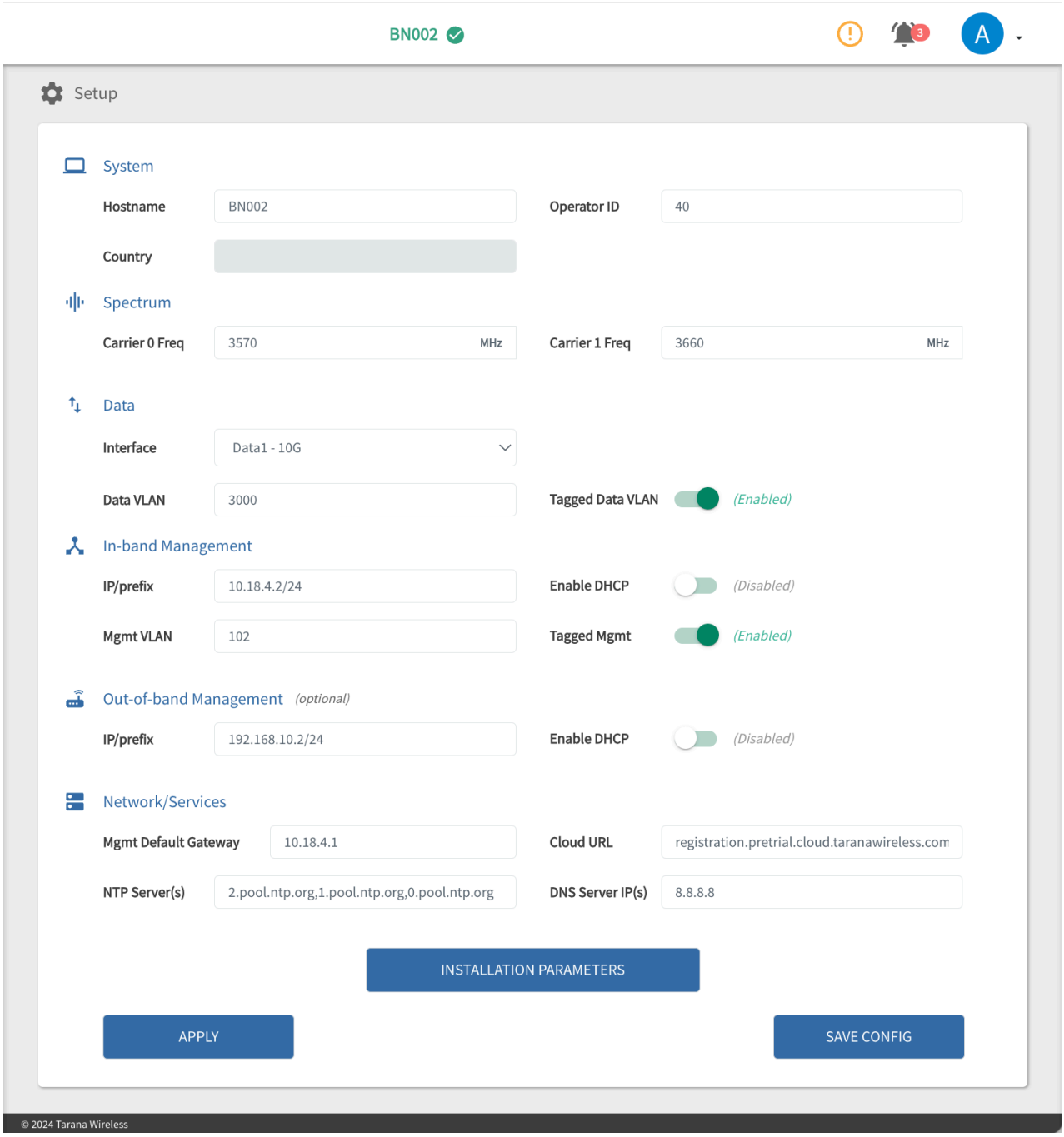
1. Verify the Operator ID of the base node by logging in to the base node and using the Setup menu to check the Operator ID field.
2. Log into the remote node Web UI.
3. Select **Setup** from the navigation pane.
4. Check the value displayed in the Operator ID field and modify it if it's not correct.



Check Operator ID in Remote Node Web UI

Base Node Radio is Muted

If the base node isn't transmitting, the remote node won't be able to see the base node and connect. To verify that the base node is transmitting, log into the base node web UI and check the Radio Control icon () in the navigation pane. It should be marked as Connected, in green. If it isn’t, select the icon to unmute the radio. If the radio is muted, the LINK LED on the base node is red.



Unmute Base Node Radio

Remote Node Performance / Low Throughput

If the remote node is connected but not performing at expected levels, there are several issues that may apply.

Remote Node is Connected to the Wrong Base Node

If the remote node isn't connected to the optimal base node, it may have a weaker link, which delivers a lower than expected throughput.

To verify, follow these steps:

1. Log into TCS.
2. Select **Devices** from the navigation pane.
3. Make sure the toggle is set to show remote nodes, not base nodes.
4. Find the row that corresponds to the remote node in question.
5. Verify the remote node is connected to its intended base node by checking the Connected BN column. This shows the hostname of the base node to which the remote node is connected.

Service Level Agreement is Incorrect

The service level agreement (SLA) of the remote node directly affects its throughput.

To verify, follow these steps:

1. Log into TCS.
2. Select **Devices** from the navigation pane.
3. Make sure the toggle is set to show remote nodes, not base nodes.
4. Find the row that corresponds to the remote node in question.
5. Select the serial number of the remote node to open the remote node individual device page.
6. Check the SLA Profile on the Information card. You can modify the SLA by selecting the **Settings** icon, then **Configure Network Parameters**.

For more information on viewing the SLA for the remote node, see Remote Node SLA (page 73).

Residential Equipment Isn’t Connecting

If the remote node is connected but customer (residential) equipment isn't connecting (router, Wi-Fi access point, etc.), the device connected directly to the Ethernet port of the remote node PoE injector may not support gigabit Ethernet. The Ethernet port of the remote node is full-duplex gigabit-only and doesn't support negotiating to a slower link speed (100BaseTX, etc.).

To verify, follow these steps:

1. Log into TCS.
2. Select **Devices** from the navigation pane.
3. Make sure the toggle is set to show remote nodes, not base nodes.
4. Find the row that corresponds to the remote node in question.
5. Select the serial number of the remote node to open the individual device page.
6. Check the Errors row in the Interface Statistics card.

Remote Node is Rebooting

A remote node can reboot for a number of reasons.

To verify, follow these steps:

1. Log into TCS.
2. Select **Devices** from the navigation pane.
3. Make sure the toggle is set to show remote nodes, not base nodes.
4. Find the row that corresponds to the remote node in question.
5. Check the message in the Boot Reason column for more information.

Base Node Troubleshooting

The following are common scenarios and suggested troubleshooting steps. For more help, contact Tarana support.

Base Node Doesn't Show in TCS

If the base can’t resolve the TCS address, it won't appear in TCS. To verify it, follow these steps:

1. Log into the base node web UI by connecting to the management or out-of-band management port.
2. Select **Setup** from the navigation pane.
3. Check the DNS Servers listed under Network Services. Verify the IP address is correct.
4. Select **Save Config**.

If the DNS Server information is correct:

1. Use ping to check that the configured servers are responding.

2. Verify that other websites load properly. If they do, contact Tarana Technical Support for further help.
3. If the base node has connectivity to the internet and can reach TCS, check if it's been assigned to a sector in TCS. If it hasn't been assigned it won't show up in the Devices view but is listed in the network configuration under BN Devices: Unassigned. To verify this, go to Admin > Network Configuration.

Base Node Doesn't Boot

To boot properly, the base node requires a minimum of 40 VDC. If the voltage supplied to the base node is too low the base node might not fully boot or might go into a continuous reboot cycle. The status LEDs on the base node may illuminate even if it hasn't fully booted.

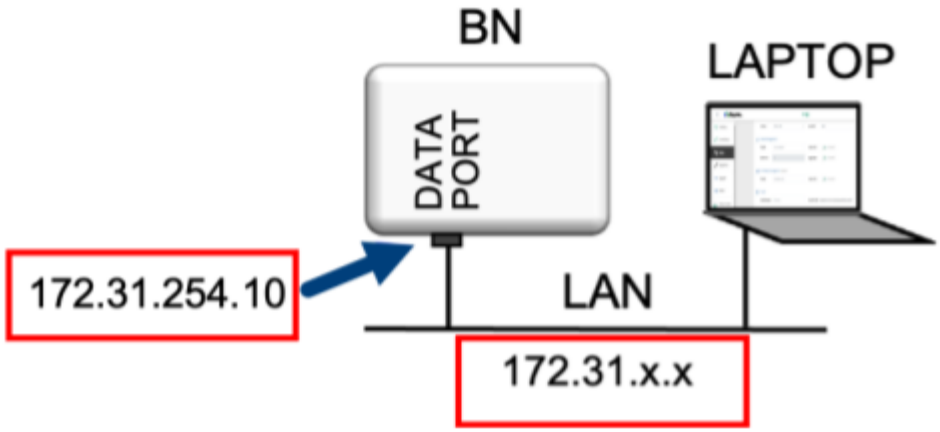
Verify that the input voltage from the base node power supply can compensate for the voltage drop across the cable run to the base node. Proper installation requires calculation of the voltage drop across the entire power cable.

Laptop Can't Connect to Base Node Web UI

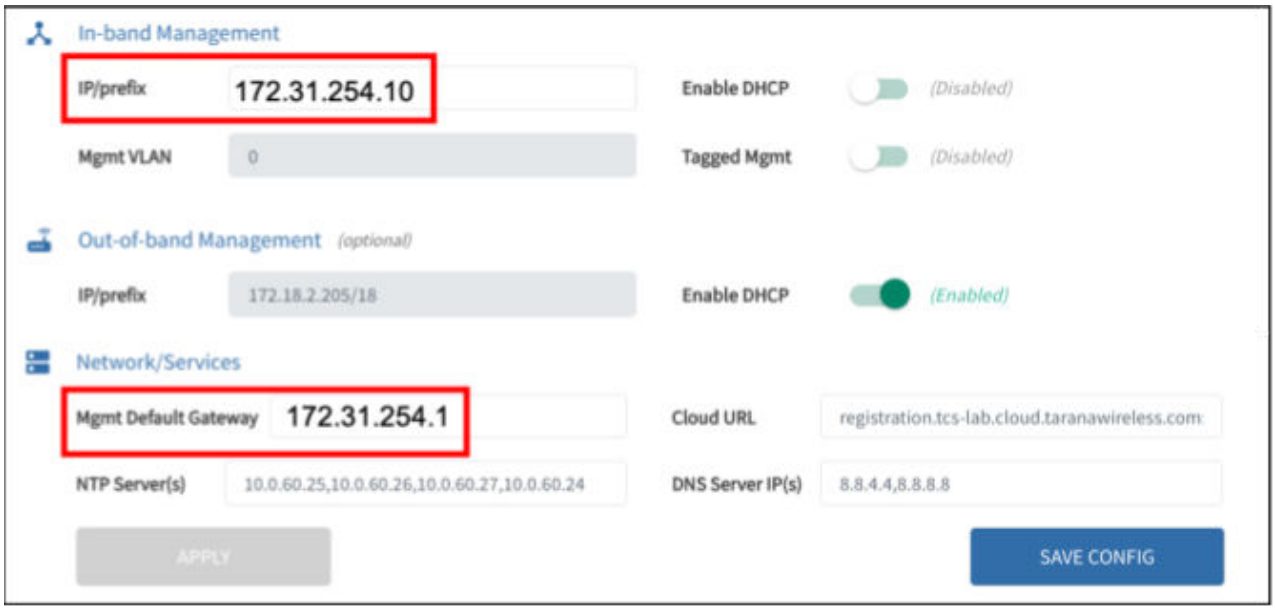
If the laptop can't connect to the base node, there are several issues that can cause this.

In-Band Management IP Address is Incorrect

If the In-band Management IP address is configured to be outside the LAN subnet, the Web UI won't be accessible from a laptop connected to that LAN. Confirm that the In-band Management IP is on the same subnet as the LAN default gateway. Open the Web UI for the base node and compare the IP address for In-Band Management to the IP address for the Mgmt Default Gateway.



Laptop and Base Node on the Same LAN

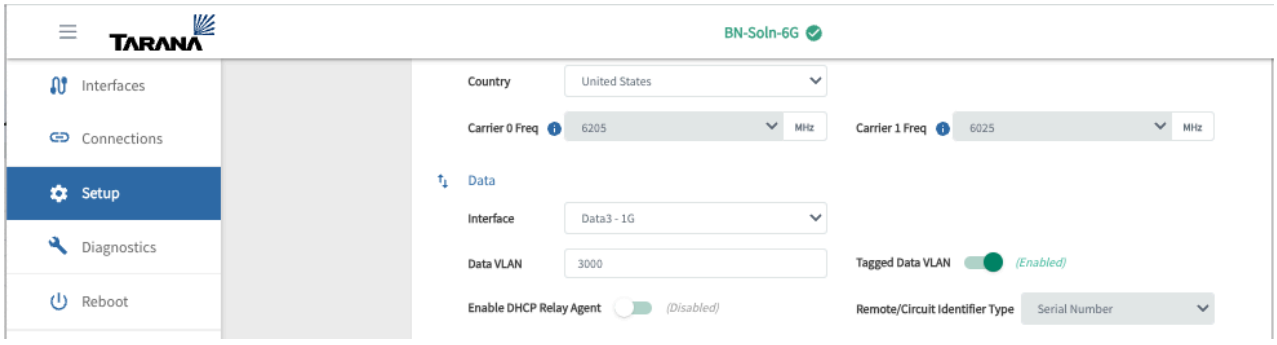


In-band Management IP for Base Node

Data Flows in Only One Direction

If data traffic is flowing in only one direction across a Tarana RF link (between the base node and remote node), this could be because data traffic coming into the base node is untagged when it should be tagged. Traffic coming into any of the data ports (Data1, Data2, Data3) must be tagged with the Data VLAN, if it has been left enabled. By default, the data VLAN on the base node is 2000. The VLAN tag must agree with whatever the base node is configured for, if it's configured to tag traffic. If a Data VLAN isn't configured, traffic must be untagged. This includes traffic coming from the server side (southbound traffic).

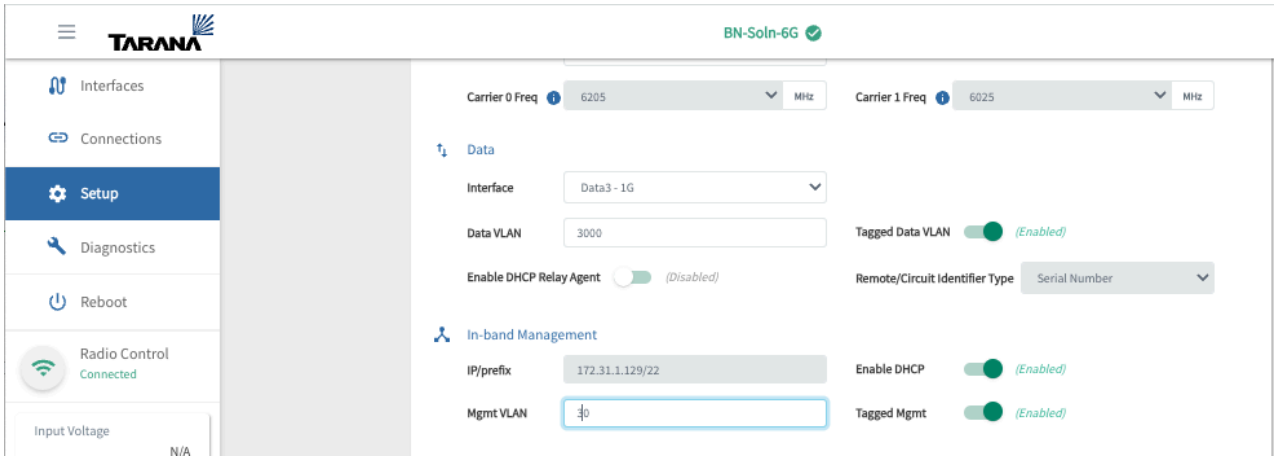
Use the Web UI Setup page to verify that the Data VLAN is set.



Data VLAN on the Base Node

VLAN Management Number is Incorrect

If you've enabled Tagged Mgmt, all management traffic for the base node is tagged. Use the Web UI Setup page to make sure you're using the correct VLAN number. If management traffic shouldn't be tagged, toggle the Tagged Mgmt switch to **Disabled**.



Management VLAN Configuration

Base Node Can't Connect to TCS

If the base node can't connect to TCS, you may be using an incorrect transceiver.

If you use an SFP transceiver in either of the DATA1 or DATA2 ports, the connection may not function. Each of these ports requires a SFP+ transceiver. Each SFP+ transceiver used on a fiber optic cable must support the same wavelength. The DATA1 and DATA2 ports require a full-duplex 10 Gbps connection.

Base Node is Disconnected from TCS

If the base node is disconnected from TCS, there are several issues that can cause this.

Base Node Alarm

If a base node becomes disconnected from TCS, TCS displays an alarm.

To verify that the base node is disconnected, follow these steps:

Log into TCS.

Select **Alarms** from the navigation pane.

Check for any open alarms by searching for the base node in question.

You can find more information about the base node status on the Performance menu:

1. Select **Device** from the navigation pane.

2. Find the row that corresponds to the base node in question.
3. To open the device specific page, select the base node hostname.
4. Check the Information card to confirm what network entities it belongs to (Market, Site, Cell).
5. Select Performance in the navigation pane.
6. Set the toggle in the upper left-hand corner of the screen to Compare KPIs.
7. Select Customize and select KPIs that may indicate a reason for the disconnect. These can include CPU Utilization, Input Voltage, etc.

NOTE
The base node may reboot if the voltage drops below 40V.

8. Choose the time period to graph the data. Click and drag the mouse to zoom in on the graph.

Base Node Can’t Resolve TCS Address

If the base node can't resolve the TCS address, it won't show in TCS.

To verify the TCS address, follow these steps:

1. Log in to the base node web UI by using the OOB management port if that port was cabled at installation. Connect a laptop to the OOB management port or to the switch that port is connected to. Put the laptop on the same IP subnet as the OOB management IP address, and open a browser window with this address: https://192.168.10.2
   This example uses the default OOB management IP address. If this IP was changed at installation, use the appropriate address.
   If the OOB management port hasn't been cabled, connect the laptop to a switch connected to the base node's data port. Put the laptop on the same IP subnet as the in-band management IP address, and open a browser window with this address: https://192.168.10.2
   This example uses the default in-band management IP address. If this IP was changed at installation, use the appropriate address.
2. After logging into the web UI, select **Setup** from the navigation pane.
3. Check the DNS Servers listed under Network Services. Verify the IP address is correct.
4. Select **Save Config**.

If the DNS Server information is correct:

1. Use ping to check the configured servers are responding.
2. Verify that other websites load properly. If they do, contact Tarana Technical Support for help.

Sector Goes Down (Base Node Becomes Muted)

If the base node loses its GPS lock, it mutes itself. This disconnects all connected remote nodes and effectively brings down the sector.

To verify GPS lock status, follow these steps:

1. Log into TCS.
2. Select **Devices** on the navigation pane.
3. Find the row that corresponds to the base node in question.
4. Select the serial number of the base node to open the individual device page.
5. Check the Information card to verify network entities for the base node (Market, Site, Cell, etc.).
6. Select **Performance** on the navigation pane.
7. Use the network selector tool at the top of the screen, using the network entities for the base node (Market, Site, Cell, etc.). Select **Apply**.
8. Set the toggle in the upper left-hand corner of the screen to **Compare KPIs**.
9. Select **Customize** then select **GPS Lock Status** from the list of available KPIs.
10. Choose the time period to graph the data. Click and drag the mouse to zoom in on the graph.

Device LED Lights

You can use the LED lights on the base node and remote node to determine the current state of the device. The devices have slightly different behavior.

Base Node Normal Operation

These states indicate normal operations.

State	Power	Link	Status
Power off	Off	Off	Off
Startup[a.]	Red (blinking)	Off	Off
Initial boot loader	Amber (solid)	Amber (solid)	Amber (solid)
Linux booting	Green (blinking)	Off	Off
Linux booted	Green (solid)	Any color or state	Off
Radio not initialized	Green (solid)	Off	Off
Radio initializing	Green (solid)	Amber (blinking)	Green (solid)
Waiting for GPS lock / spectrum allocation	Green (solid)	Red (blinking)	Green (solid)
Radio calibration	Green (solid)	Amber (solid)	Green (solid)
Operational (no remote nodes connected)	Green (solid)	Green (blinking)	Green (solid)
Operational (remote nodes connected)	Green (solid)	Green (solid)	Green (solid)
Radio muted (no link)	Green (solid)	Red (solid)	Any color or state
Factory reset	Amber (blinking)	Amber (blinking)	Amber (blinking)

[a.]May indicate a hardware failure if the base node stays in this state for more than approximately 1 minute.

NOTE
Do not use the base node's reset button.

Base Node Faults

These states indicate possible faults.

State	Power	LInk	Status
Hardware fault	Red (blinking or solid)	Off	Off
Boot failure	Amber (solid)	Off	Off
Runtime error (warning)[a.]	Green (solid)	Any color / state	Amber (blinking)
Runtime error (critical)[b.]	Green (solid)	Any color / state	Red (blinking)

[a.]Indicates one or more of the following:

- Alarm raised

- Lower modulation
- Packet errors above threshold
- GPS lock loss
- Upgrade failed

[b.]Indicates one or more of the following:

- Link down
- Watchdog error
- Hardware failure

Base Node Data Links

These states indicate ethernet status on the data ports:

State	Data 1	Data 2	Data 3
100 Mbps Link Up	Yellow (solid)	Yellow (solid)	Yellow (solid)
100 Mbps Link Activity	Yellow + green (blinking)	Yellow + green (blinking)	Yellow + Green (blinking
1 Gbps Link Up	Green (solid)	Green (solid)	Green (solid)
1 Gbps Activity	Green (blinking)	Green (blinking)	Green (blinking)

Remote Node Normal Operation

These states indicate normal operations.

State	Ethernet	RF	Status
Power off	Off	Off	Off
Startup[a.]	Any	Off	Off
Initial boot loader	Any	Amber (solid)	Amber (solid)
Linux booting	Any	Off	Green (blinking)
Linux booted	Any	Any color or state	Green (solid)
Radio not initialized	Any	Off	Green (solid)
Radio initializing	Any	Amber (blinking)	Green (solid)
Searching for base node	Any	Red (blinking)	Green (solid)
Radio calibration	Any	Amber (solid)	Green (solid)
Syncing / connecting	Any	Green (blinking)	Green (solid)
Link up	Any	Green (solid)	Green (solid)
Radio muted (no link)	Any	Red (solid)	Any color or state
Factory reset	Any	Red (solid)	Blue (solid)

[a.]May indicate a hardware failure if the base node stays in this state for more than approximately 1 minute.

NOTE
Do not use the base node's reset button.

Remote Node Faults

These states indicate possible faults.

State	Ethernet	RF	Status
Hardware fault	Any	Off	Red (solid)
Boot failure	Any	Off	Amber (solid)
Runtime error (warning)[a.]	Any	Green (solid)	Amber (blinking)
Runtime error (critical)[b.]	Any	Any color / state	Red (blinking)

[a.]Indicates one or more of the following:

- Alarm raised
- Lower modulation
- Packet errors above threshold
- Upgrade failed

[b.]Indicates one or more of the following:

- Link down
- Watchdog error
- Hardware failure

Remote Node Data Links

State	ETH / MGMT
1 Gbps Link Up	Green (solid)
1 Gbps Activity	Green (blinking)

Alarm Descriptions

This section covers alarms as reported by TCS, including type, severity, and descriptions of each alarm.

Communication Alarms

This section covers communication type alarms.

ID	Description	Severity	Thresholds	Current Value
DHCP-server-unavailable	DHCP server unavailable, no IP address received Raise Condition=no IP address	CRITICAL	Pass/Fail	N/A
DNS-resolution-failure	Host name resolution failure Raise Condition=DNS lookup failed	CRITICAL	Pass/Fail	N/A
DNS-server-failure	DNS server failure Raise Condition=DNS server unreachable	CRITICAL	Pass/Fail	N/A
IP-conflict	IPv4 conflict from DHCP server Raise Condition=duplicate IP address	CRITICAL	Pass/Fail	N/A
Modem-packet-drops	Modem packet drops exceed threshold in interval	MINOR		
Route-unavailable	Default route unavailable Raise Condition=default gateway unreachable	CRITICAL	Pass/Fail	N/A
TCS-unreachable	Default dial-out registration with TCS failure Raise Condition=registration failed	CRITICAL	Pass/Fail	N/A

Environmental Alarms

This section covers environmental type alarms.

ID	Description	Severity	Thresholds	Current Value
GPS-satellites-low	Number of available GPS satellites for sync is low	MAJOR		N/A
GPS-unlocked	GPS lock lost Raise Condition=lock lost	MINOR	Pass/Fail	N/A
Reference-unlocked	Reference clock is not locked Raise Condition=clock not locked	MAJOR	Pass/Fail	N/A

Equipment Alarms

This section covers equipment type alarms.

ID	Description	Severity	Thresholds	Current Value
Bus-probe-failure	Hardware bus(i2c, spi, pci etc) probe failures Raise Condition=probe failed	CRITICAL	Pass/Fail	N/A
Device-failure	Hardware device failure, failed to read FPGA Raise Condition=read failed	CRITICAL	Pass/Fail	N/A
Over-temperature	Temperature of the device outside thresholds	CRITICAL	10, 95, 10	Degrees Celsius
Voltage	Input voltage is not within thresholds	CRITICAL	38.34, 68.91, 5	Voltage

Operational Alarms

This section covers operational alarms.

ID	Description	Severity	Thresholds	Current Value
Boot-bank-switchover	System did not boot from desired partition Raise Condition=boot failed	MAJOR	Pass/Fail	N/A
Boot-failure	CAP initialization script failed Raise Condition=script failed	CRITICAL	Pass/Fail	N/A
Certificate-load-failure	Load failed due to key mismatch or key not present Raise Condition=key mismatch/not present	CRITICAL	Pass/Fail	N/A
Connection-down	RN has not been able to reach the required BN Raise Condition=unreachable	CRITICAL	Pass/Fail	N/A
Corrupt-software	Software image is corrupted Raise Condition=software corrupt	CRITICAL	Pass/Fail	N/A
CPU-usage-high	Relative CPU usage is high	CRITICAL	10, 90, 10	CPU usage (%)
Disk-EMMC-MLC-lifetime	Disk EMMC hardware completed lifetime (MLC), reported as percentage	MINOR	10, 70, 0	MLC (%)
Disk-inodes-low	Number of inodes available is low Raise Condition= Clear Condition=	MAJOR	5, 10, 5	Inodes available (%)
Disk-space-low	Amount of disk space available is low Raise Condition=signal issue	MAJOR	5, 10, 5	Space available (%)
Emergency-reboot	Unrecoverable device failure Raise Condition=device failure	CRITICAL	Pass/Fail	N/A
Firmware-mismatch	Firmware version mismatch Raise Condition=version mismatch	CRITICAL	Pass/Fail	N/A
Invalid-configuration	Configuration is not valid or invalid digboard slot Raise Condition=config invalid Clear Condition=??	CRITICAL	Pass/Fail	N/A

ID	Description	Severity	Thresholds	Current Value
MAC-RACH-attempt-exceeded	MAC RACH attempts exceeded	MAJOR		N/A
Memory-low	Amount of available RAM is low	MAJOR	10, 10, 10	Percentage of RAM
Missing-configuration	Mandatory configuration node-mode not available, could not read from parameter service. Raise Condition=read failed	CRITICAL	Pass/Fail	N/A
Modem-eth-FIFO-alarm	Ethernet FIFO error Raise Condition=FIFO error	MAJOR	Pass/Fail	N/A
OS-out-of-memory	Out of memory Raise Condition=out of memory	CRITICAL	Pass/Fail	N/A
OS-runtime	OS runtime errors Raise Condition=Runtime error	CRITICAL	Pass/Fail	N/A
Radio-init-failure	Radio initialization failed Raise Condition=init failed	CRITICAL	Pass/Fail	N/A
Software-upgrade-failure	Software upgrade failed Raise Condition=upgrade failed	WARNING	Pass/Fail	N/A
Storage-failure	Mount partition failure Raise Condition=mount failed	CRITICAL	Pass/Fail	N/A
Unknown	Unknown failure observed Raise Condition=unknown error	WARNING	N/A	N/A
Version-mismatch	Component version mismatch Raise Condition=version mismatch	CRITICAL	Pass/Fail	N/A
Watchdog-reboot	System reboot due to SMC watchdog expiration Raise Condition=watchdog timer expired	CRITICAL	Pass/Fail	N/A

Processing Alarms

This section covers processing type alarms.

ID	Description	Severity	Thresholds	Current Value
Bootup-config-failure	Configuration application failed Raise Condition=config failed	MINOR	Pass/Fail	N/A

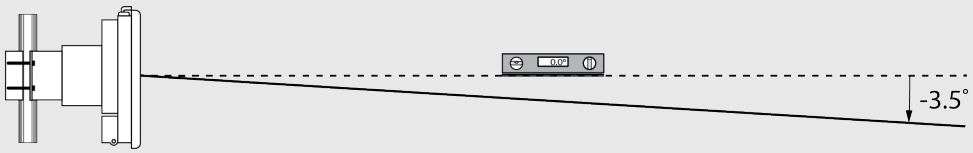
Beamwidth Reference

Refer to the following table of horizontal and vertical beamwidths for base nodes.

	3 GHz CBRS	5 GHz	6 GHz
3 dB Horizontal Beamwidth	68˚	64˚	60˚
6 dB Horizontal Beamwidth	98˚	98˚	95˚
3 dB Vertical Beamwidth	12.5˚	8.5˚	6.8˚
6 dB Vertical Beamwidth	17˚	11.8˚	9.7˚

ELECTRICAL TILT

3 GHz base nodes have an electrical tilt of -3.5°. This means that when the 3 GHz base node is aimed parallel to the ground, the actual beam center is angled toward the ground by 3.5°.



Refer to the following table of horizontal and vertical beamwidths for remote nodes

	3 GHz CBRS	5 GHz	6 GHz
3 dB Horizontal Beamwidth	63˚	58˚	66˚
6 dB Horizontal Beamwidth	95˚	83˚	97˚
3 dB Vertical Beamwidth	17.6˚	14˚	12.1˚
6 dB Vertical Beamwidth	24.3˚	19.5˚	16.4˚