



G1 Administration Guide

18-0025-001

November 27, 2023

Table of Contents

Supported Releases	5
Intended Audience	6
Related Documents	7
G1 Network Architecture	8
Tarana Cloud Suite (TCS) Overview	9
Log In To TCS	9
User Profiles and Roles	9
TCS Layout	10
User Profile	12
Multi-Tenant Support for Retailers	15
Network Entities	17
Region	17
Market	17
Site	17
Cell	17
Sector	18
Filter Network Entities	18
Search Network Entities	18
Dashboard	20
Map View	22
Map View Device Details	23
Map View Search Bar	26
Map Overlay	26
Display Device Hostnames	27
Filter Map by Metrics	28
View an Individual Device Dashboard	30
Performance	31
Metrics (Analytics)	31
Compare KPIs	32
Compare Entities	36
Devices View	38
Device List View	38
Customize Device List Table	40
Individual Device Dashboard	45
Device Operations View	62
TCS Alarms	65
TCS Events	67
Admin Events	68
TCS Admin Actions	71
Network Configuration	71
Manage Networks	71
Manage Operator	72
Alerts Configuration	80
Base Node Telemetry Streaming	84
DHCP Option 82 Support	86
User Management	88
Display User Accounts	88
Create User Accounts	89
Edit, Delete, or Reset Password for User Accounts	90

Software Inventory	91
Manage Webhooks and Configure Alerts	92
Add a Webhook	93
Test a Webhook	94
API	95
Swagger API Documentation	96
Device Web UI	98
Web UI Navigation Pane Options	98
Web UI Dashboard (Remote Node Only)	98
Web UI Base Node Interfaces	99
Web UI Remote Node Interfaces	100
Web UI Device Connections (Base Node Only)	101
Web UI Base Node Setup	103
Web UI Remote Node Setup	107
Web UI Diagnostics	109
Web UI Device Reboot	111
Web UI Radio Control	111
Troubleshooting	113
TCS Troubleshooting	113
TCS Loads Slowly or Doesn't Work as Expected	113
Remote Node Troubleshooting	113
Can't Connect to Remote Node Web UI	113
Remote Node Isn't Connecting to Base Node	114
Remote Node Performance / Low Throughput	116
Base Node Troubleshooting	117
Base Node Doesn't Show in TCS	117
Base Node Doesn't Boot	118
Laptop Can't Connect to Base Node Web UI	118
Base Node Can't Connect to TCS	120
Base Node is Disconnected from TCS	120
Sector Goes Down (Base Node Becomes Muted)	121
Air Interface Protocol Version 1	122
Device LED Lights	124
Base Node Normal Operation	124
Base Node Faults	124
Base Node Data Links	125
Remote Node Normal Operation	125
Remote Node Faults	125
Remote Node Data Links	126
TCS Alarm Descriptions	127
Communication Alarms	127
Environmental Alarms	127
Equipment Alarms	127
Operational Alarms	127
Processing Alarms	128
VLANs and Quality of Service	129
VLANs on G1 Devices	129
Base Node VLANs	129
Remote Node VLANs	129
Tarana VLAN Logic	131
Multiple VLAN Scenarios	133

Quality of Service 135

Supported Releases

This guide supports these current G1 and G6 models:

Model	Supported releases
RN 5GHz	G1 RN5AS1002, G1 RN5AS1012, G1 RN5AS1012
RN CBRS (Cat B)	G1 RN3AS1001, G1 RN3AS1011
BN 5GHz	G1 BN5AS1002
BN CBRS (Cat B)	G1 BN3AS1001
RN 6GHz	G1 RN6AHB012
BN 6GHz	G1 BN6AS1002

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.

Related Documents

For more information on base node installation, see the Base Node Installation Guide: https://www.taranawireless.com/bn_manual

For more information on remote node installation, refer to the Remote Node Installation Guide: https://www.taranawireless.com/rn_manual

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 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 at a single location (referred to as a cell), arranged in sectors. A collection of base nodes at a single location is 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 250 concurrent remote node connections. When you deploy a cell of four base nodes, the cell can support up to 1000 remote nodes distributed evenly at 250 per base node.

For more information and planning and deployment, see the G1 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.

- From a laptop with internet connectivity, open a tab in Chrome:
For 5GHz and 6GHz, navigate to <https://cloud.taranawireless.com>.
For 3GHz devices, navigate to <https://portal.trial.cloud.taranawireless.com>.
- 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://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.

User Profiles and 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.

These roles are defined as follows:

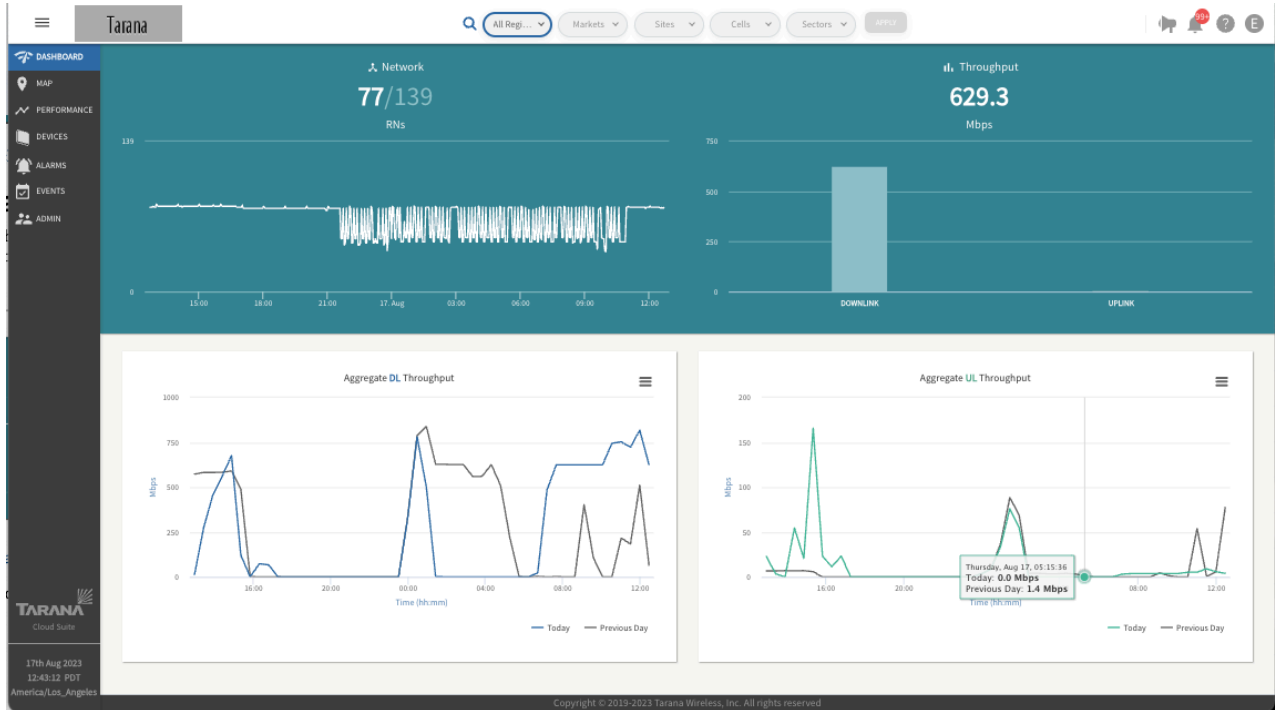
Action	NOC L1 User	NOC Operator	OP Admin
View Dashboard Page	Yes	Yes	Yes
View Map Page	Yes	Yes	Yes
View Performance Page	Yes	Yes	Yes
View Devices Page	Yes	Yes	Yes

Action	NOC L1 User	NOC Operator	OP Admin
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
Create Snapshots	No	Yes	Yes
Reboot Device	No	Yes	Yes
Create and Configure Networks	No	No	Yes
Create and Configure Network Policies	No	No	Yes
Create 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
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
Create or Modify Device Notes	No	Yes	Yes
View Device Notes	Yes	Yes	Yes
Reconnect Device to Network	No	Yes	Yes

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

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 Layout

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 create 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:

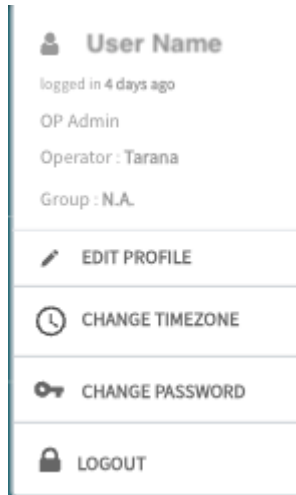


Notification, Alarm, Support, User Profile icons

- 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 your first initial.

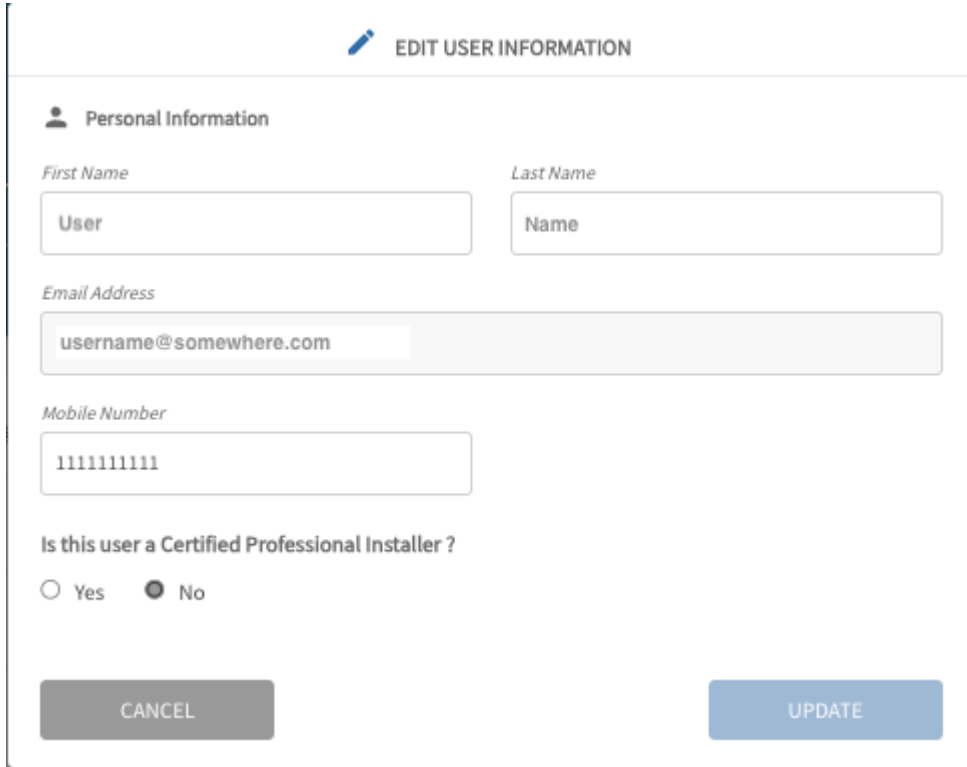
User Profile

To see your user profile information, select the **user profile icon**. You can change user profile information, time zone, or password here.



User Profile Information

To edit your profile, select **Edit Profile** and enter your first name, last name, and mobile number. Select **Submit**. You cannot change your email address. If you need to change your email, an Admin must create a new account and delete this one.



EDIT USER INFORMATION

Personal Information

First Name: User

Last Name: Name

Email Address: username@somewhere.com

Mobile Number: 1111111111

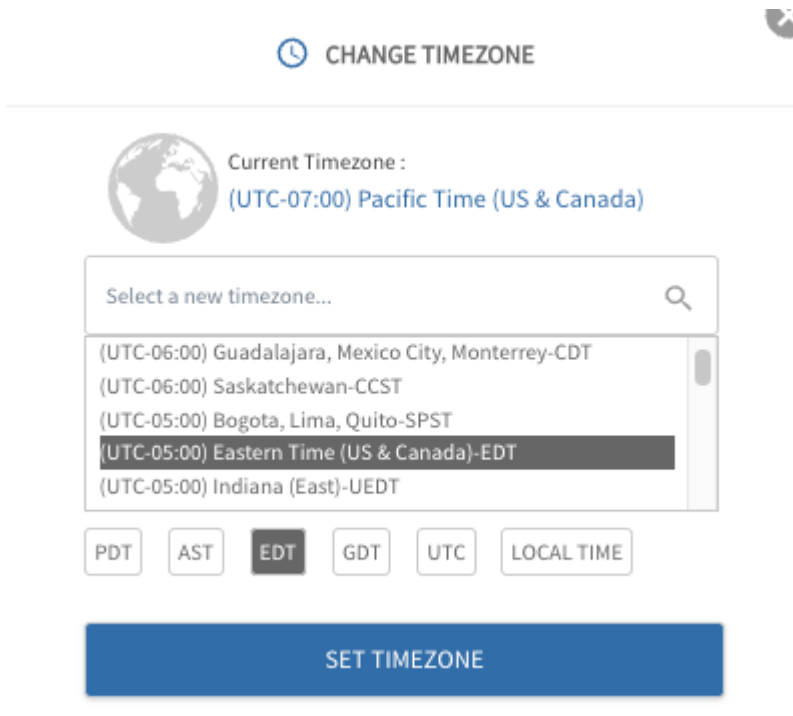
Is this user a Certified Professional Installer?

Yes No

CANCEL **UPDATE**

Edit User Information

To change the timezone, select **Change Timezone** and choose a new timezone from the dropdown, then select **Set Timezone**. This is pulled from the time on your computer.



CHANGE TIMEZONE

Current Timezone : (UTC-07:00) Pacific Time (US & Canada)

Select a new timezone...

- (UTC-06:00) Guadalajara, Mexico City, Monterrey-CDT
- (UTC-06:00) Saskatchewan-CCST
- (UTC-05:00) Bogota, Lima, Quito-SPST
- (UTC-05:00) Eastern Time (US & Canada)-EDT
- (UTC-05:00) Indiana (East)-UEDT

PDT **AST** **EDT** **GDT** **UTC** **LOCAL TIME**

SET TIMEZONE

Edit User Profile Time Zone

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

To enter your CPI credentials, do the following:

1. Log in to TCS.
2. Navigate to **User Profile > Edit Profile**.
3. Enter your 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 you are a certified professional installer.
5. Enter your CPI ID.
6. Upload your CPI certificate in .p12 format.
7. Enter your CPI certificate password.
8. Select **Update**.

The screenshot shows a web form titled "EDIT USER INFORMATION" with a pencil icon. The form is divided into sections. The "Personal Information" section includes fields for "First Name" (containing "Elizabeth") and "Last Name" (containing "Fox"). Below this is the "Email Address" field (containing "efox@taranawireless.com") and the "Mobile Number" field (containing "1111111111"). A question "Is this user a Certified Professional Installer?" has the "Yes" radio button selected. The "CPI ID" field contains the placeholder text "*Enter CPI ID". The "CPI Certificate" section features a dashed border and a central upload icon with the text "Upload file in .p12 format". The "CPI Certificate Password" field contains the placeholder text "*Enter CPI Password". At the bottom, there are two buttons: a grey "CANCEL" button and a blue "UPDATE" button.

Enter CPI ID and Certificate

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**.

OT SET YOUR NEW PASSWORD

OT ENTER CURRENT PASSWORD

OT ENTER NEW PASSWORD

Min. 8 characters, use at least one number, one uppercase letter, one lowercase letter and one special symbol eg. Alpha14@5

OT CONFIRM NEW PASSWORD

UPDATE PASSWORD

User Profile Password Change

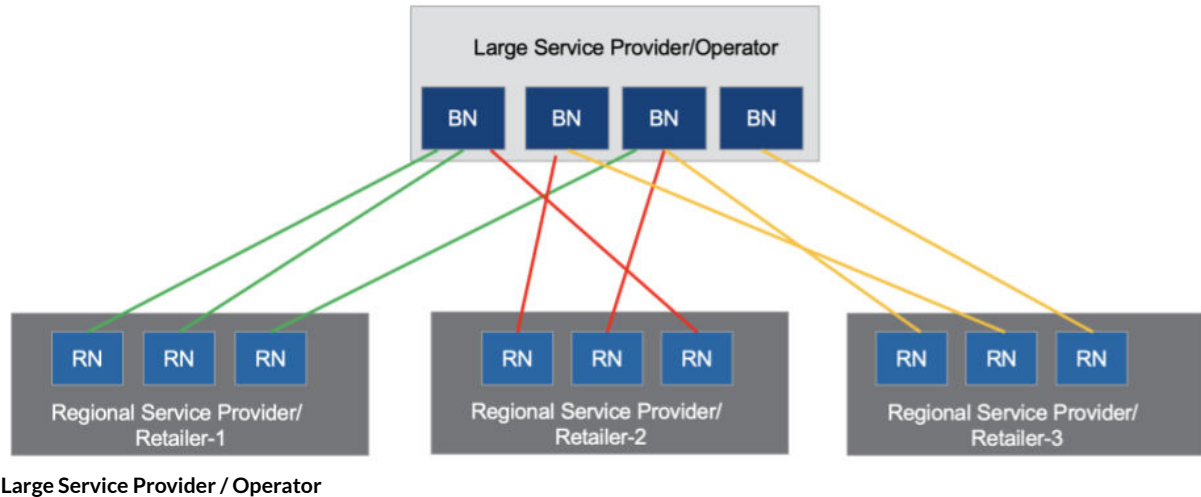
Reset Password

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.

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.



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 create and manage the TCS hierarchy and manage 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 cannot 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.

Retailer Name is a parameter in the remote node's Planning Metrics in the Device view.

Three user roles support multi-tenancy for retailers. A user with OP Admin rights can create 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 \[9\]](#). 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 create 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 creates 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 for details.

Network Entities

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:

- Region
- Market
- Site
- Cell
- Sector

You create and name entities in the Admin > Network Configuration section of the TCS. After you create and name each entity, you assign or edit related attributes, as needed.

See the [Network Configuration \[71\]](#) section for information about configuring these entities. OP Admin rights are required 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.

A Cell is composed of up to 4 base nodes. 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 \[44\]](#) for more information.

Sector

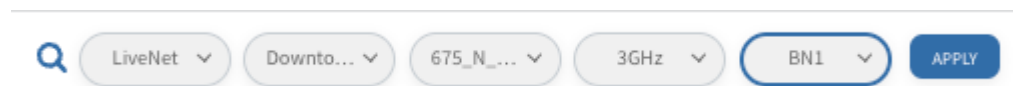
A Sector is an individual base node and all of its connected remote nodes, though a base node doesn't define a Sector. Use TCS to define a Sector as an abstract. This allows a base node and remote nodes to be swapped out of a Sector while the Sector name and attributes stay the same, though the actual 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 create the most granular filter for network devices, select individual entities from Region through Sector and select **Apply**.



Granular Filter of Network Entities

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



All Network Entities

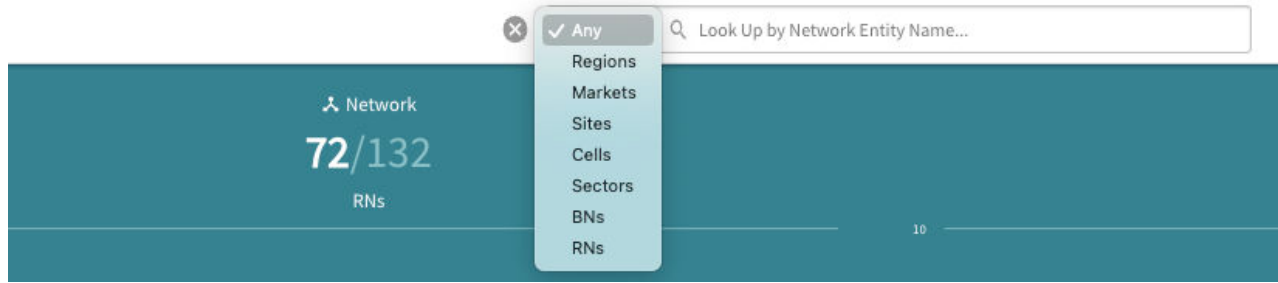


NOTE

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.

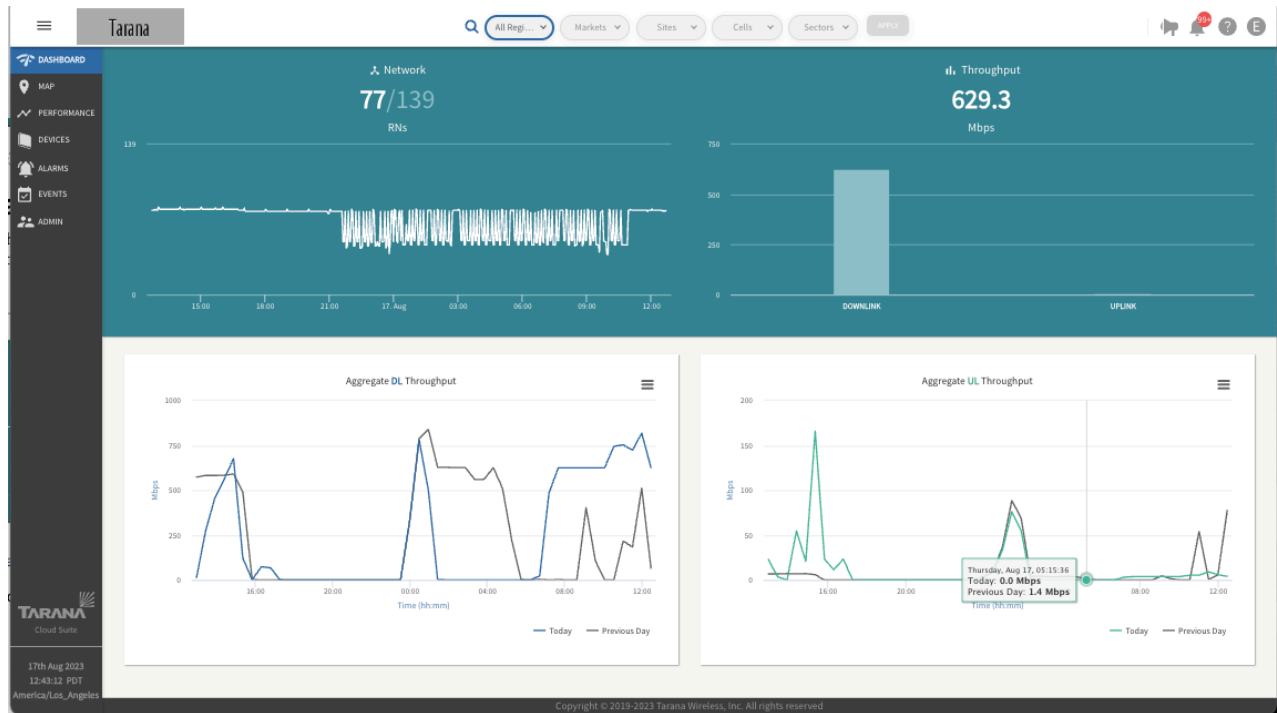


Global Search Bar

Dashboard

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

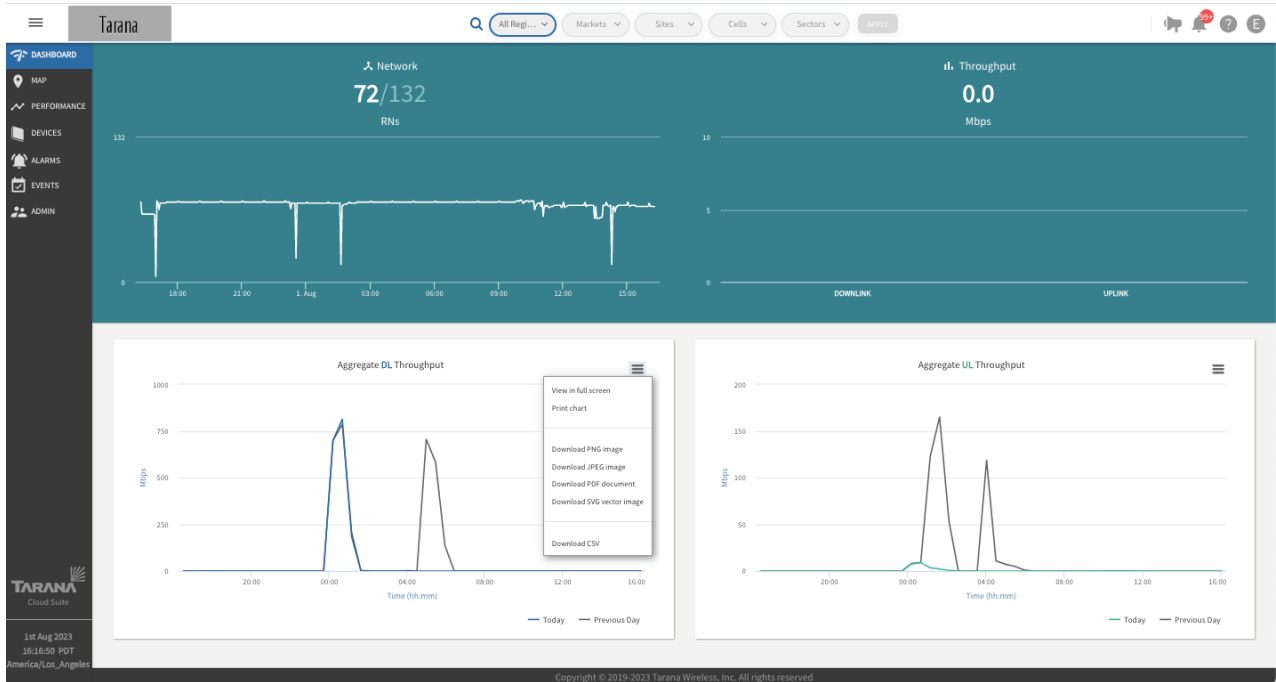
Hover the mouse over each tile to display information about that specific data point.



TCS Dashboard

To view the data displayed on the individual throughput information 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.

G1 Administration Guide



Download Dashboard Data

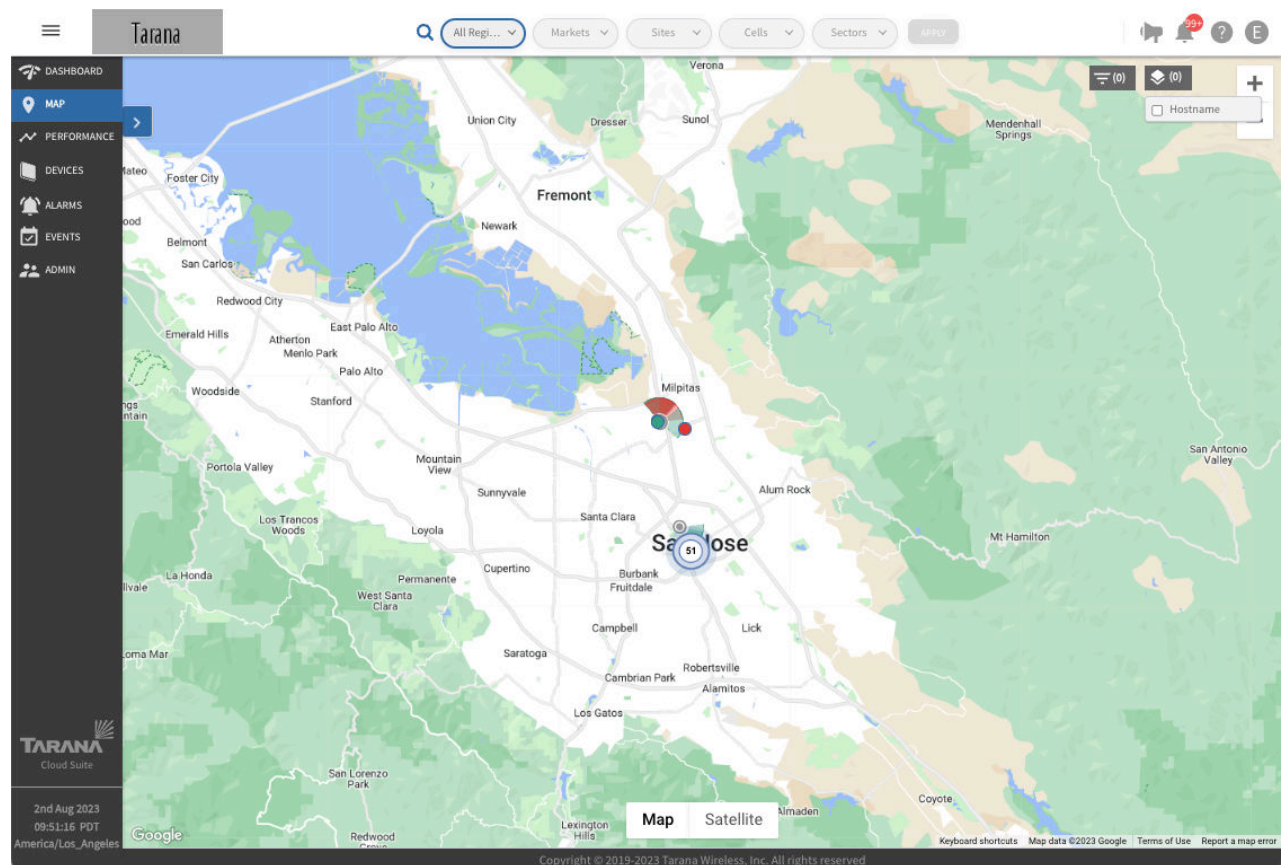
The DL Peak Throughput Distribution shown in the example above reflects actual throughput and not capacity.

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 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.

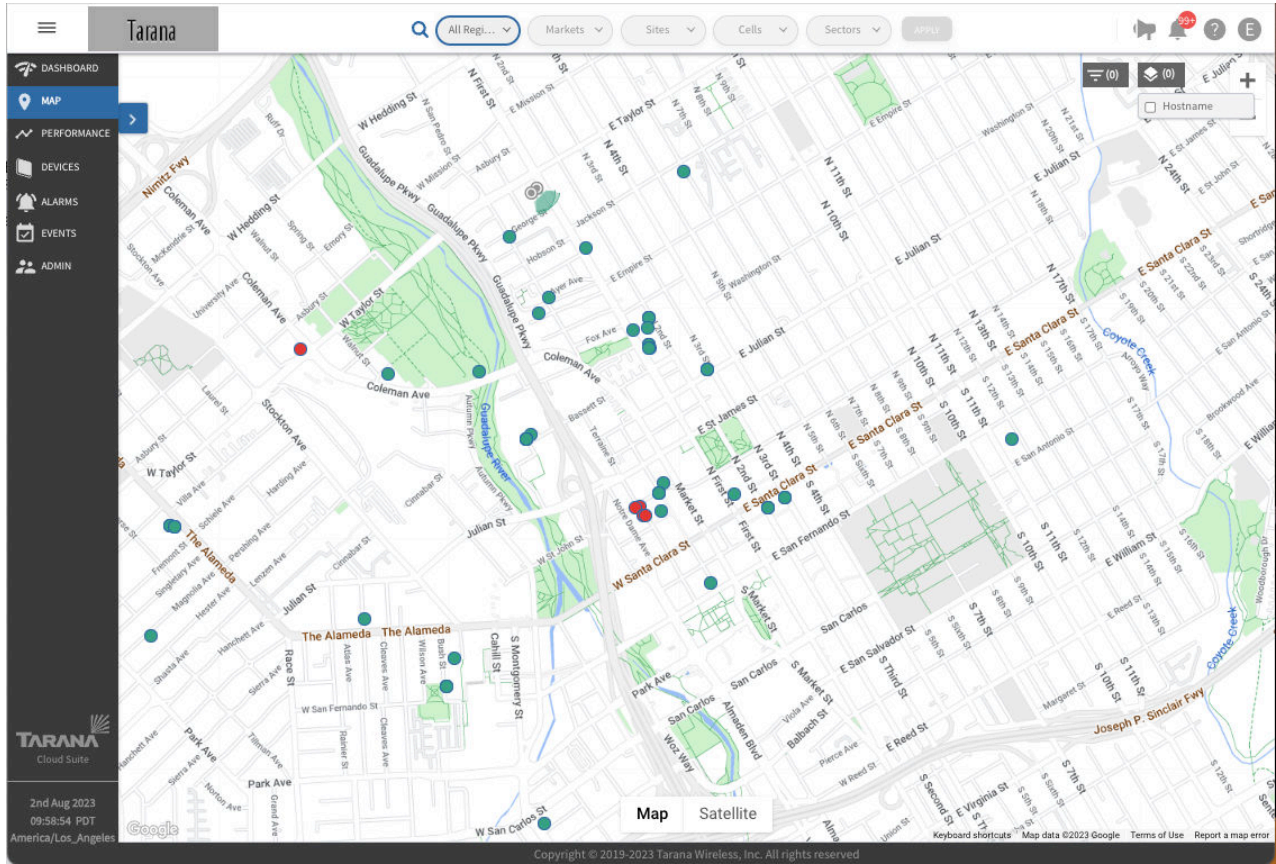
By default, any devices associated to this network are displayed on a street map. You can add terrain to the street view or switch to satellite view.



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.



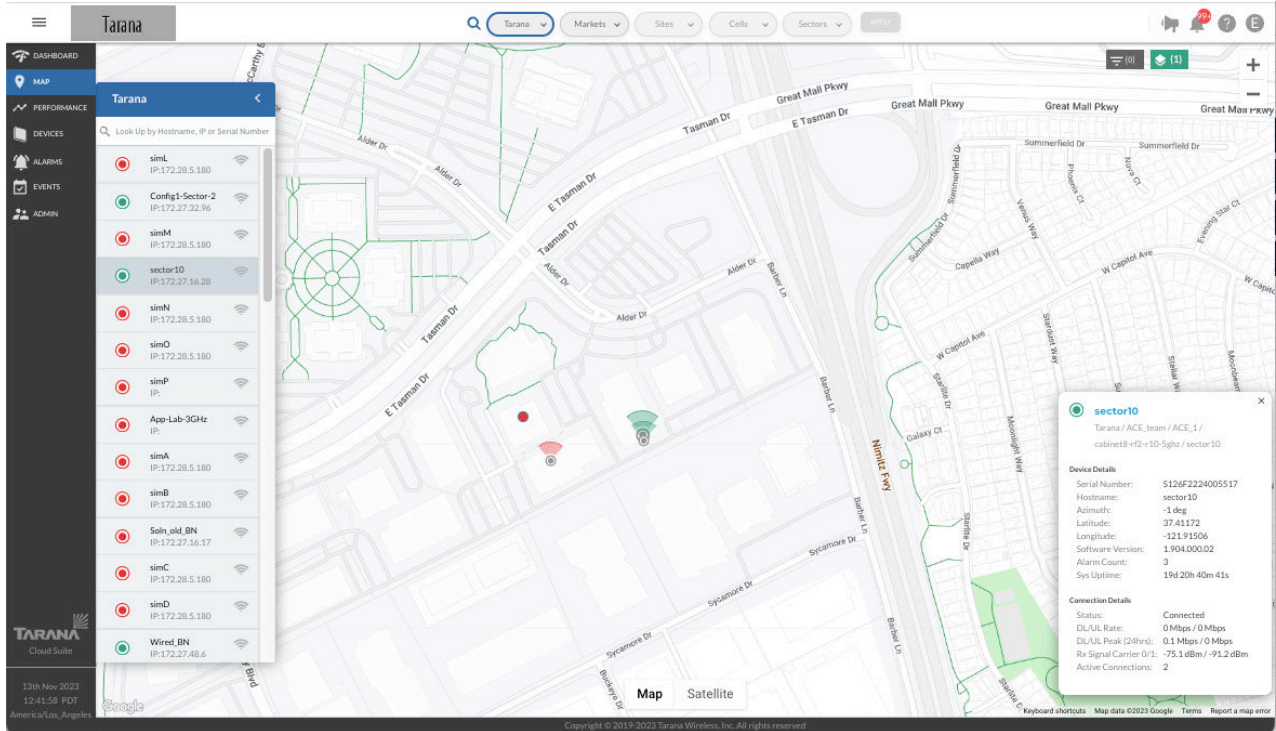
Map View of Base Nodes and Remote Nodes

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

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:

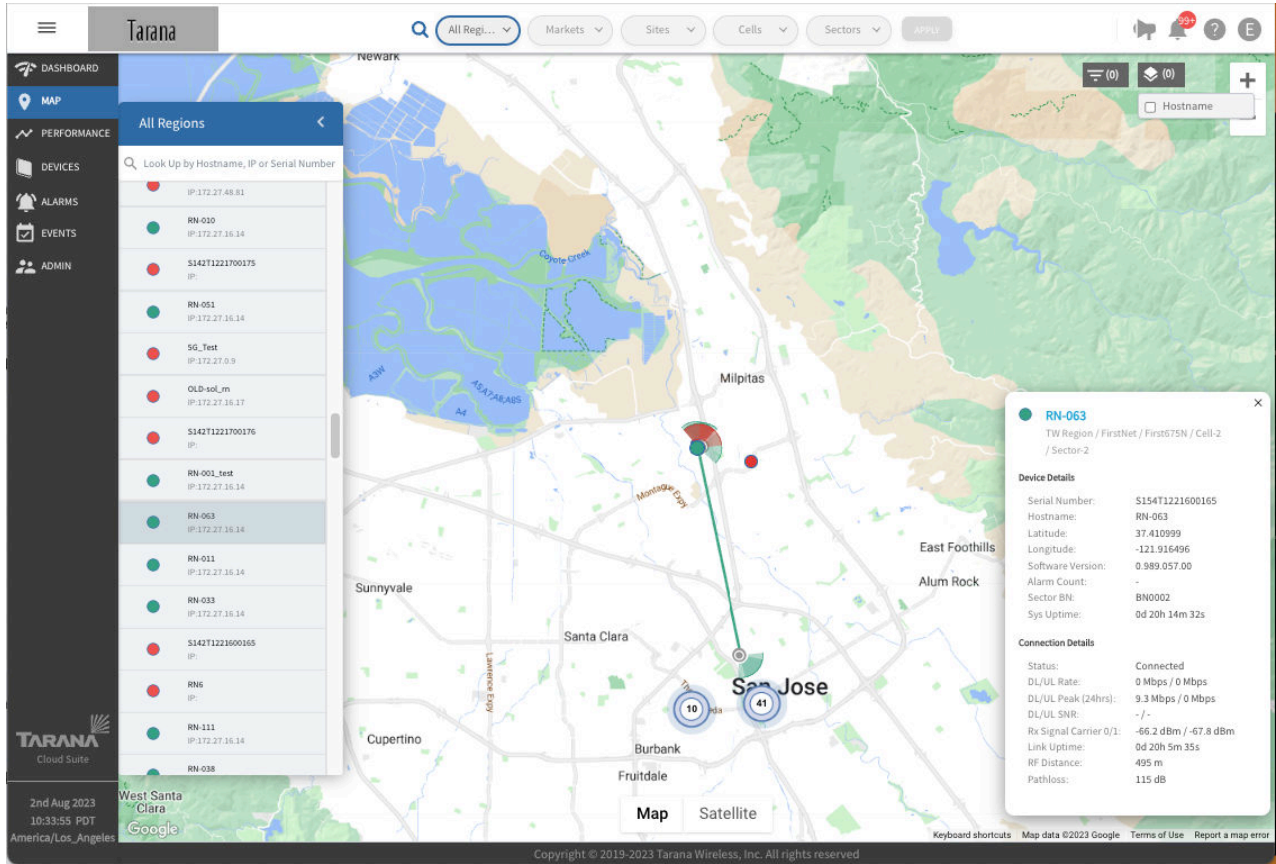
Device Details

- 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

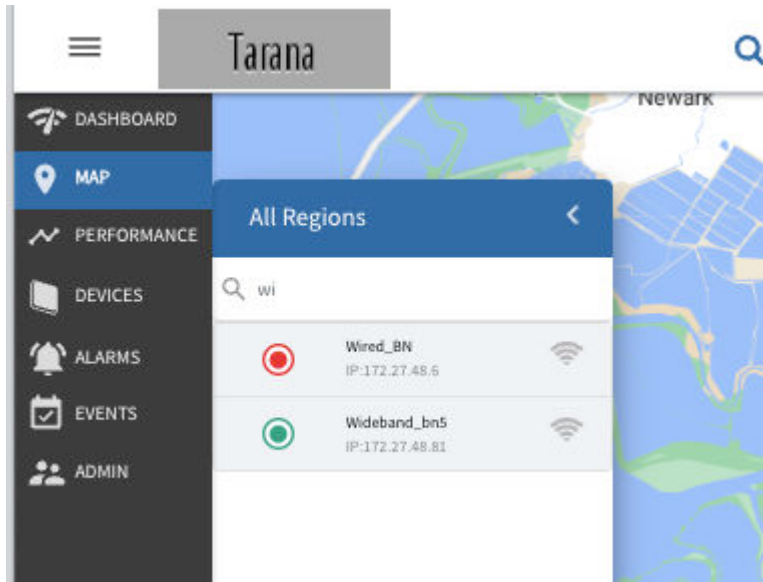
Connection Details

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

- Pathloss

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. In a well-planned environment, you see a 360° view with some overlapping coverage areas.

To see 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 antenna signals on the map next to the base node are colored:

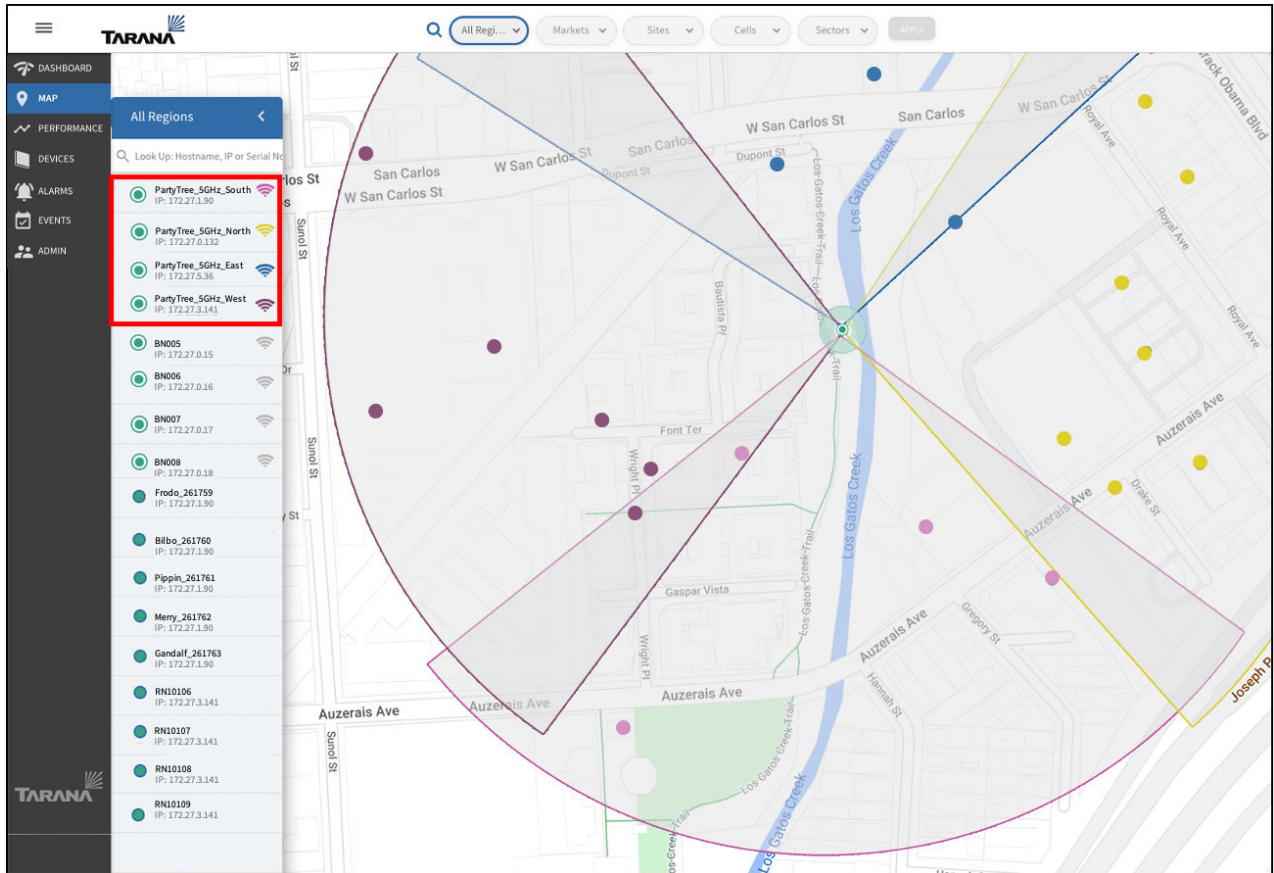
- Pink
- Yellow
- Blue
- Purple

Each base node has a colored arc on the map that corresponds to these colors, showing its coverage area. 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 area. 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 area. All remote nodes associated to that base node are shaded yellow. The third and fourth base nodes are similarly colored.

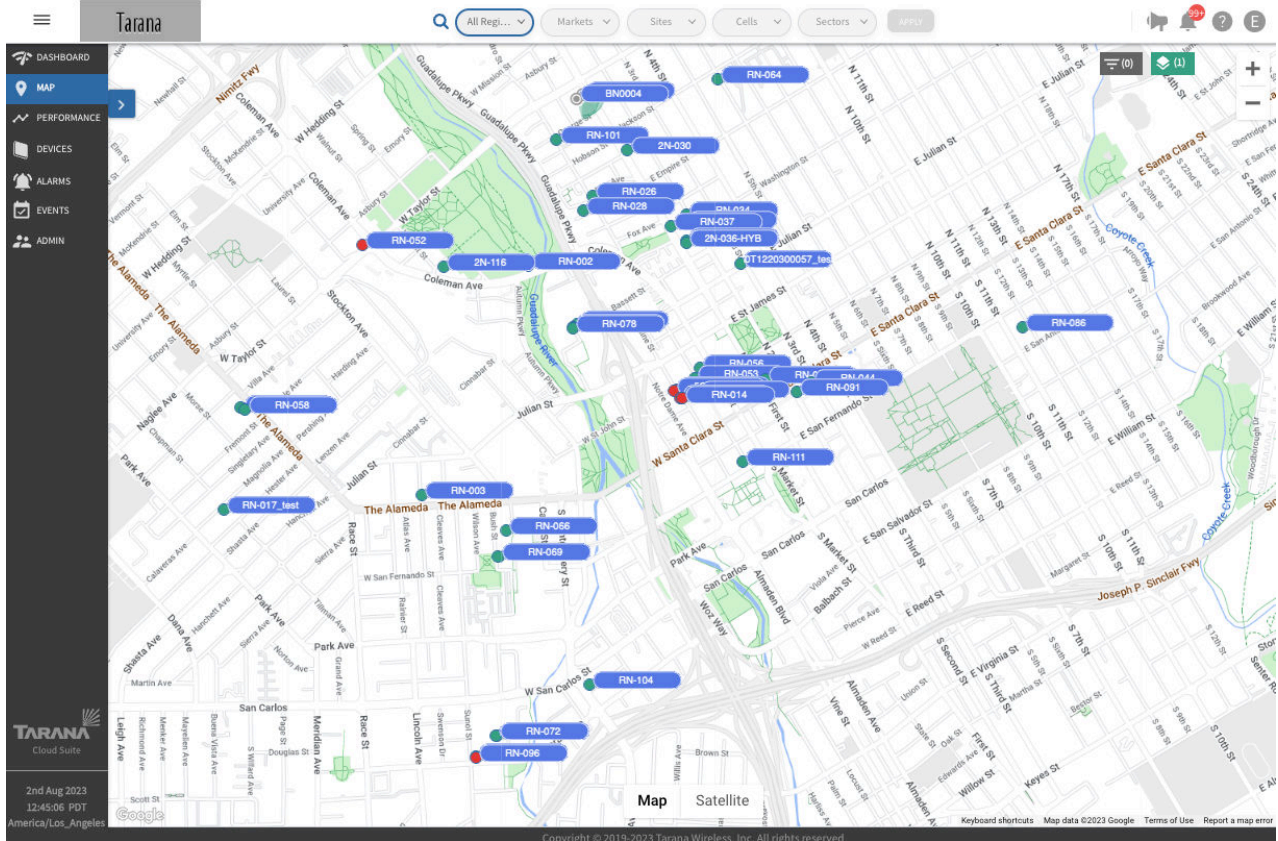
Even when one base node coverage area overlaps another base node area, it's easy to see which remote nodes are associated to a particular base node.



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**.

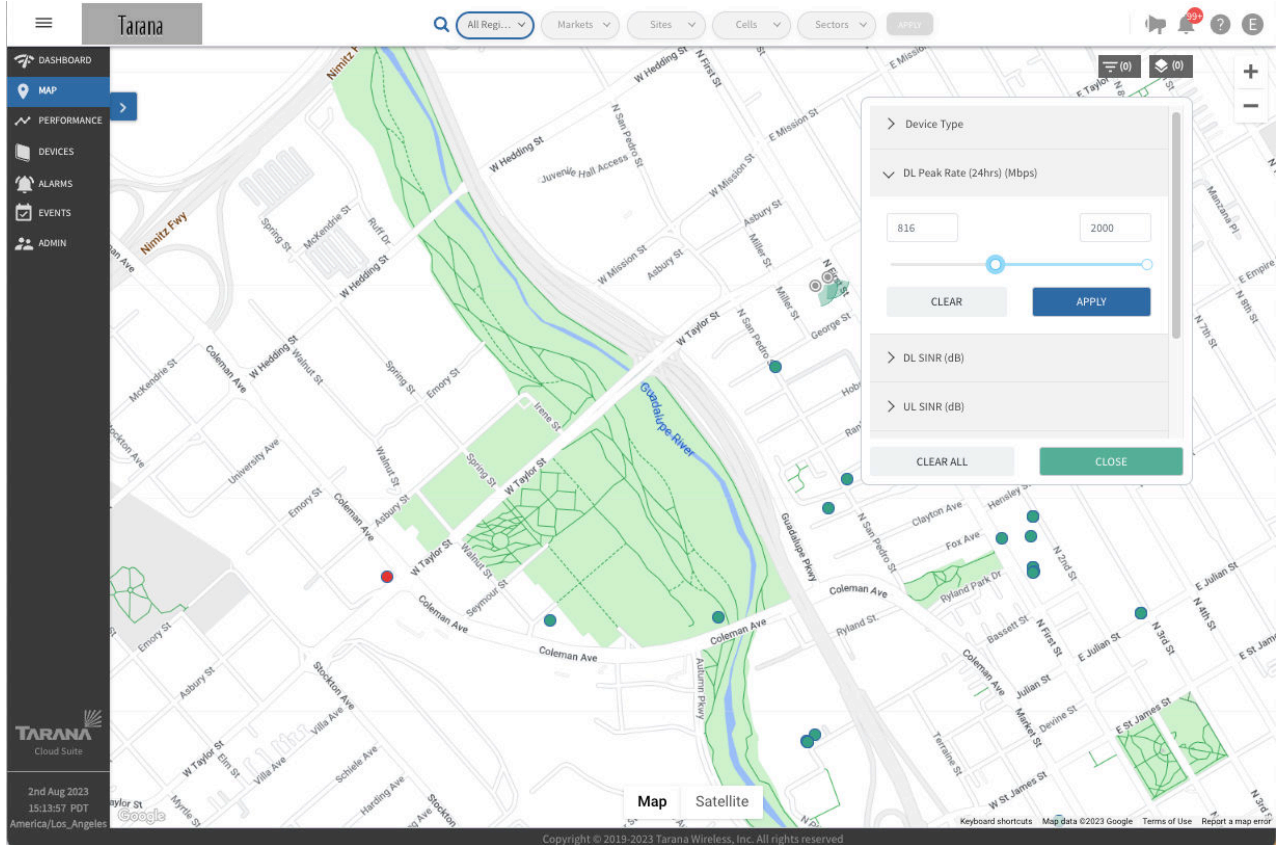


Display Device Hostnames

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 (24hrs) (Mbps):** Peak download from the previous 24 hours. Adjust the slider to select a value between 1 and 2000.
- **DL SINR (dB):** Signal to Interference Noise Ratio (SINR) for downlink connections, in dB. Adjust the slider to select a value between -99 and 35.
- **UL SINR (dB):** SINR for uplink connections, in dB. Adjust the slider to select a value between -99 and 35.
- **Pathloss (dB):** Measured path loss, in dB. Adjust the slider to select a value between 75 and 165.
- **DL Tonnage (24hrs):** Amount of data sent in the downlink direction over the previous 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 over the previous 24 hours, in gigabytes.

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

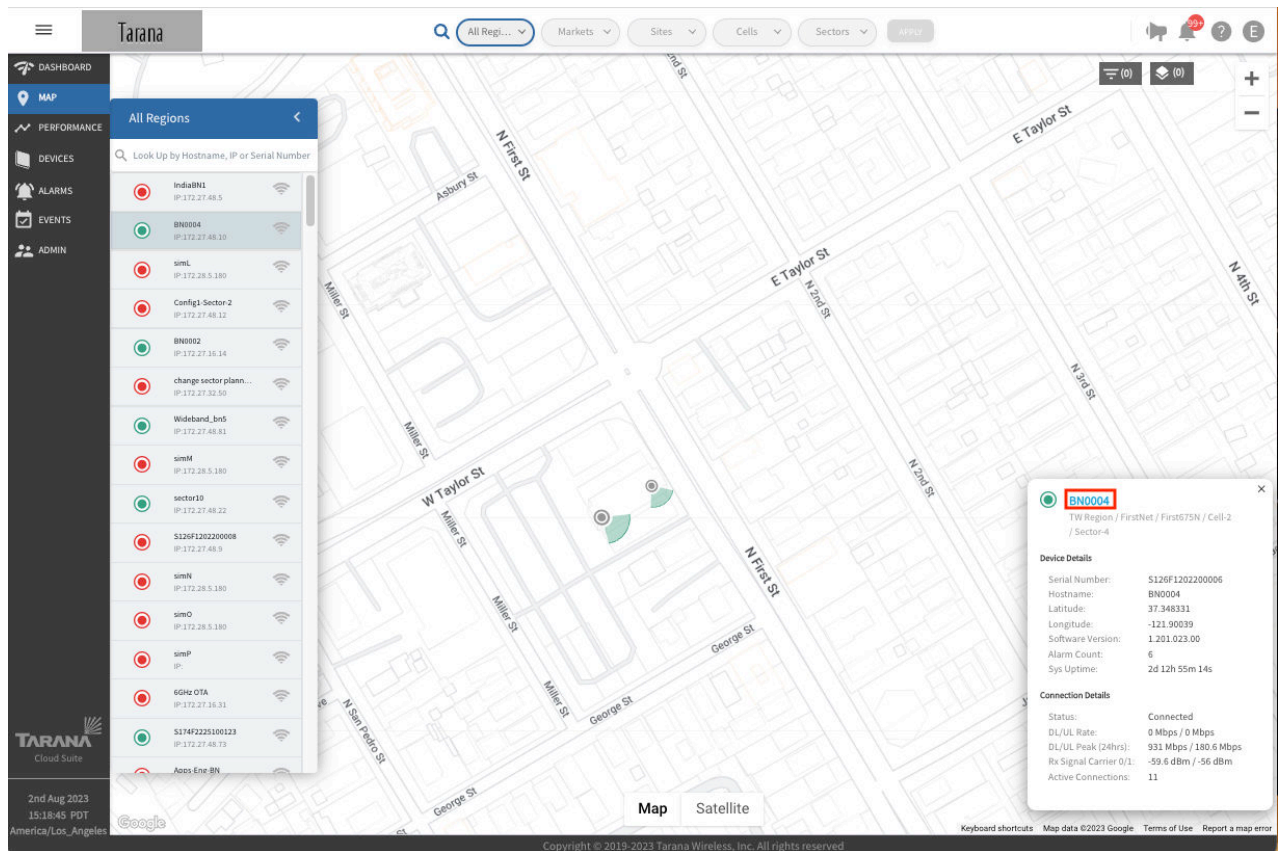
Select **Apply** to save the filter and apply it to the map view. Select **Clear** to reset the filter to its default values.

Select **Clear All** to clear the filters from the display and **Close** to close the filter dialogue 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 \[45\]](#) for details.



View Individual Device Dashboard from Map

Performance

Performance metrics are a valuable troubleshooting tool for individual devices or to compare multiple devices. To see performance metrics for G1 network devices, select **Performance** in the left side navigation pane. Use the toggle to set metrics to **Compare KPIs** or **Compare Entities**.

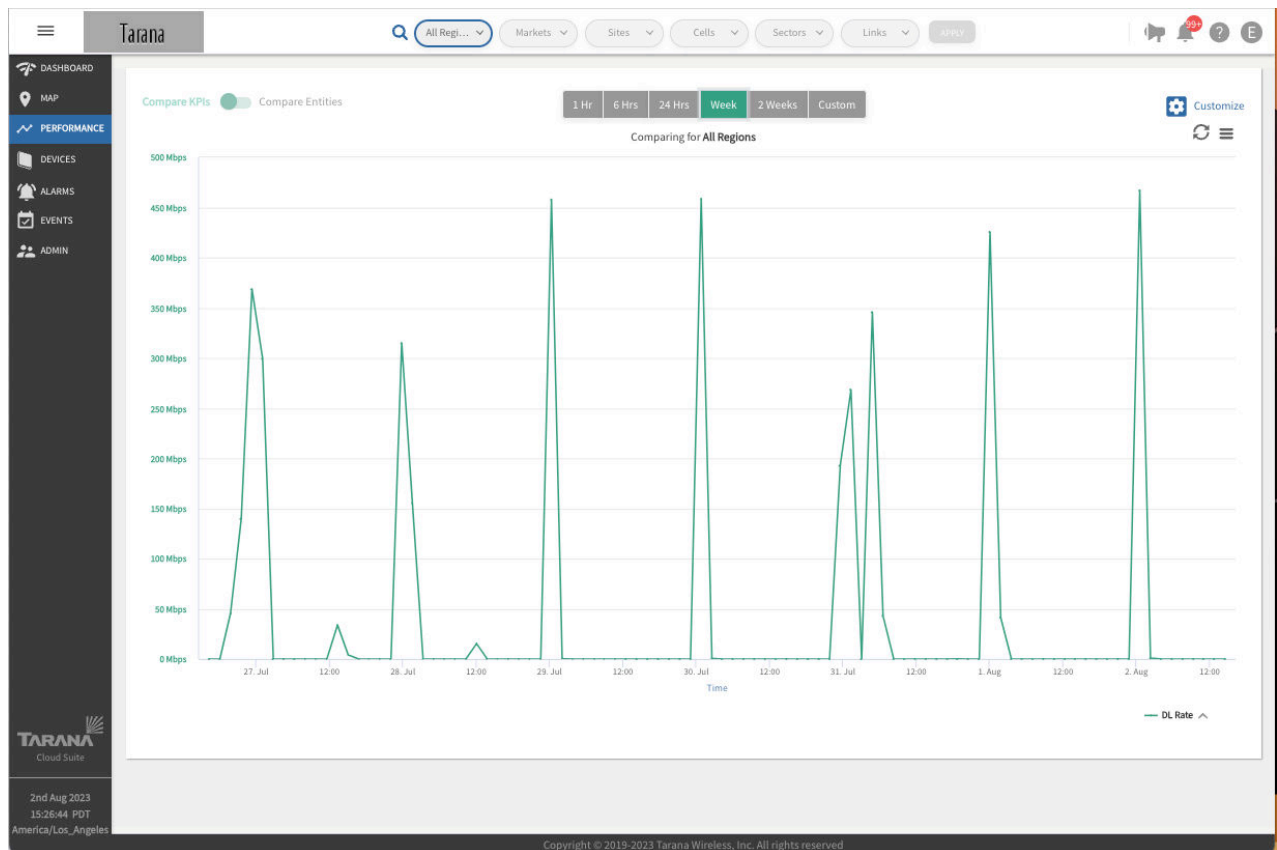
Metrics (Analytics)

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

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

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

Use the options on the display to select the time period for the data display. You can select 1 hour, 6 hours, 24 hours, 1 week, 1 month, or a custom time period that you define. If you select 1 hour, the

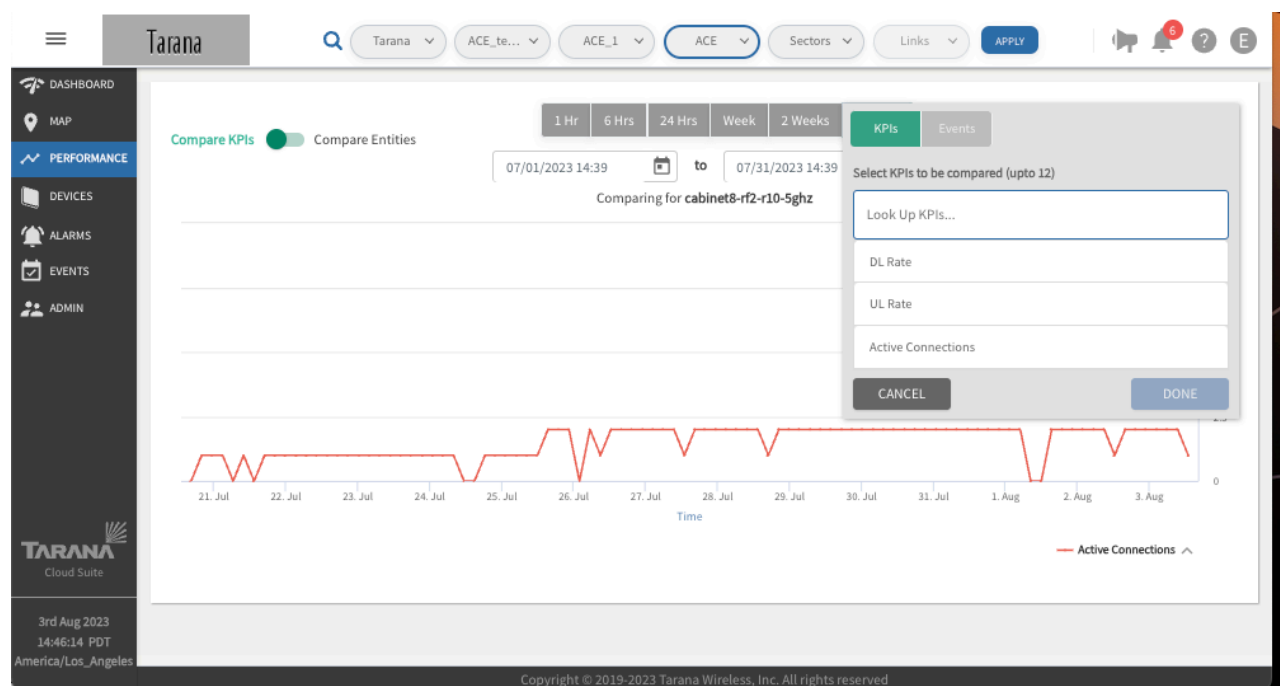
graph updates automatically every 30 seconds. If you select any other time period, you must select the refresh icon in the upper right corner to update the graph. TCS stores KPI data for three months.

Compare KPIs

Set the Compare KPIs 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 (🔧) from the top right to open a selection box of available KPIs for the network entity that's selected.

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.

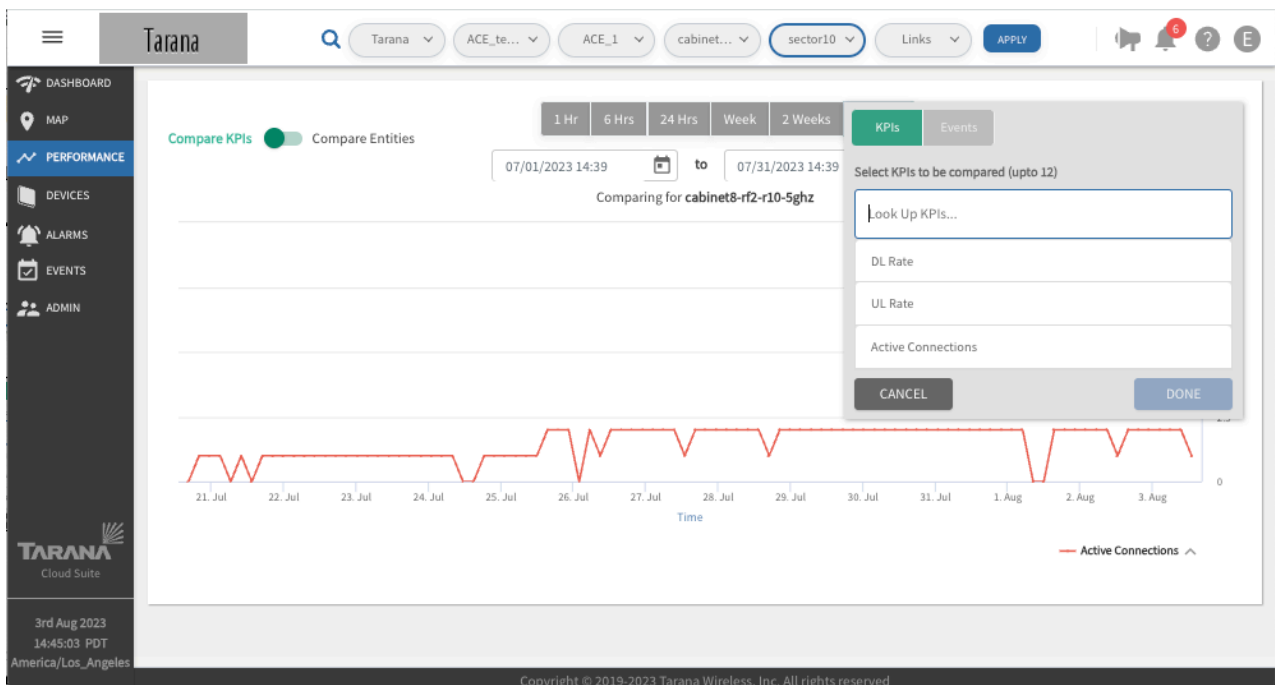


Customize KPIs for a Region, Market, Site, or Cell

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

- **Temperature:** Internal board temperature of the device.
- **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.
- **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.
- **Reference Lock Status:** Status of reference lock.
- **Frequency, Carriers 0 and 1:** Center frequency of first and second carrier band.

- **Bandwidth, Carriers 0 and 1:** Bandwidth of first and second carriers, in MHz.
- **Active Connections:** Number of remote nodes that are currently connected to a base node.
- **DL / UL Rate:** Download and upload rate.
- **DL / UL Peak:** Highest DL / UL rate detected in the last 150 seconds.
- **Interference Noise Ratio Max Carriers 0 and 1:** Maximum interference noise ratio of first and second carriers.
- **Sensitivity Loss Max Carriers 0 and 1:** Loss in sensitivity (system gain) due to operating at lower than max receiver gain. This is typically caused by strong receive signals or an increased noise figure, which results in a gain backoff. This also effectively reduces the incoming signal of interest. A lower value is better for this metric.
- **Rx Signal Carriers 0 and 1:** Received signal of first and second carriers in dBm.
- **DL / UL Peak Capacity:** Capacity of DL / UP peak use.
- **Input Voltage:** Input DC voltage to the base node.

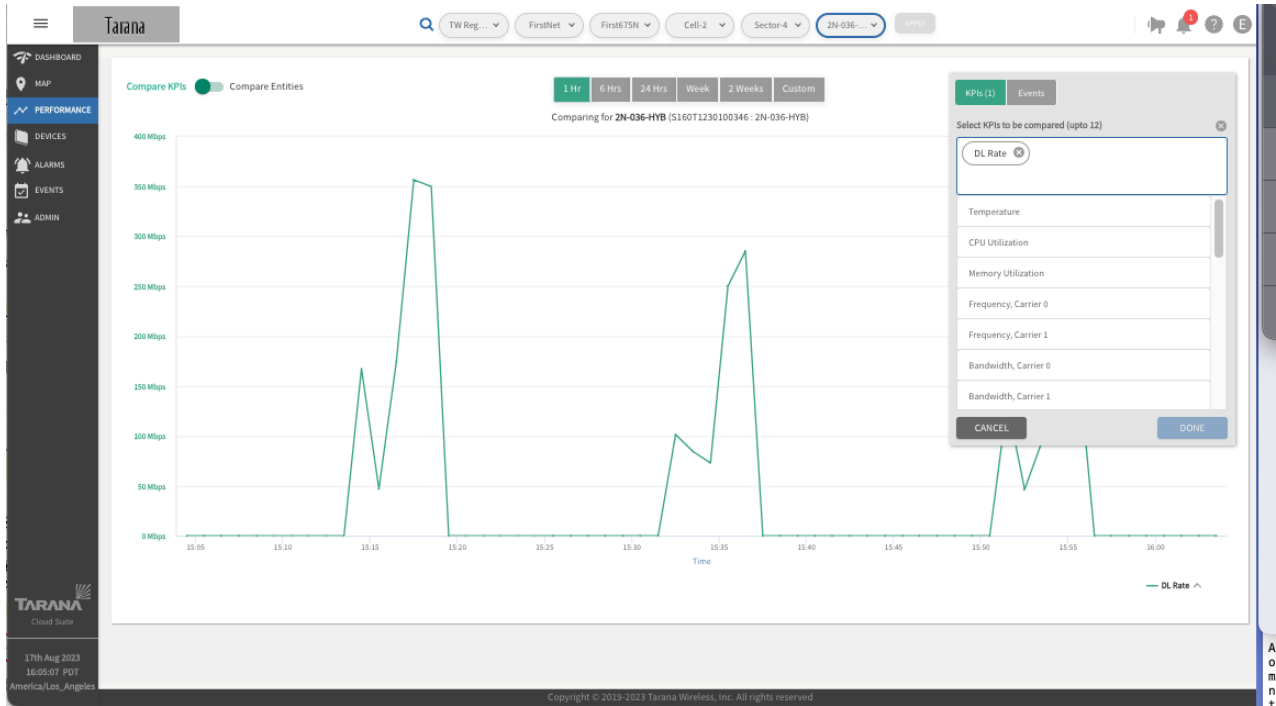


Customize KPIs for a Sector

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

- **Temperature:** Internal board temperature of the device.
- **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.
- **Frequency, Carriers 0 and 1:** Center frequency of first and second carrier band.
- **Bandwidth, Carriers 0 and 1:** Bandwidth of first and second carriers, in MHz.
- **Pathloss:** Measured path loss, in dB.
- **DL / UL SINR:** Signal to Interference Noise Ratio for downlink and upload connections, in dB.
- **DL / UL Rate:** Download and Upload rate.
- **DL / UL Peak:** Highest DL and UL rate detected in the last 150 seconds.
- **DL / UL PER:** Downlink / Uplink packet error rate.

- **DL / UL SNR:** Downlink / Uplink signal-to-noise ratio.
- **RF Distance:** Radio frequency distance, calculated to take into account reflection, refraction, etc..
- **Interference Noise Ratio Max Carriers 0 and 1:** Interference noise ratio maximum of first and second carriers.
- **Sensitivity Loss Max Carriers 0 and 1:** Sensitivity loss of first and second carriers.
- **Rx Signal Carriers 0 and 1:** Received signal of first and second carriers in dBm.

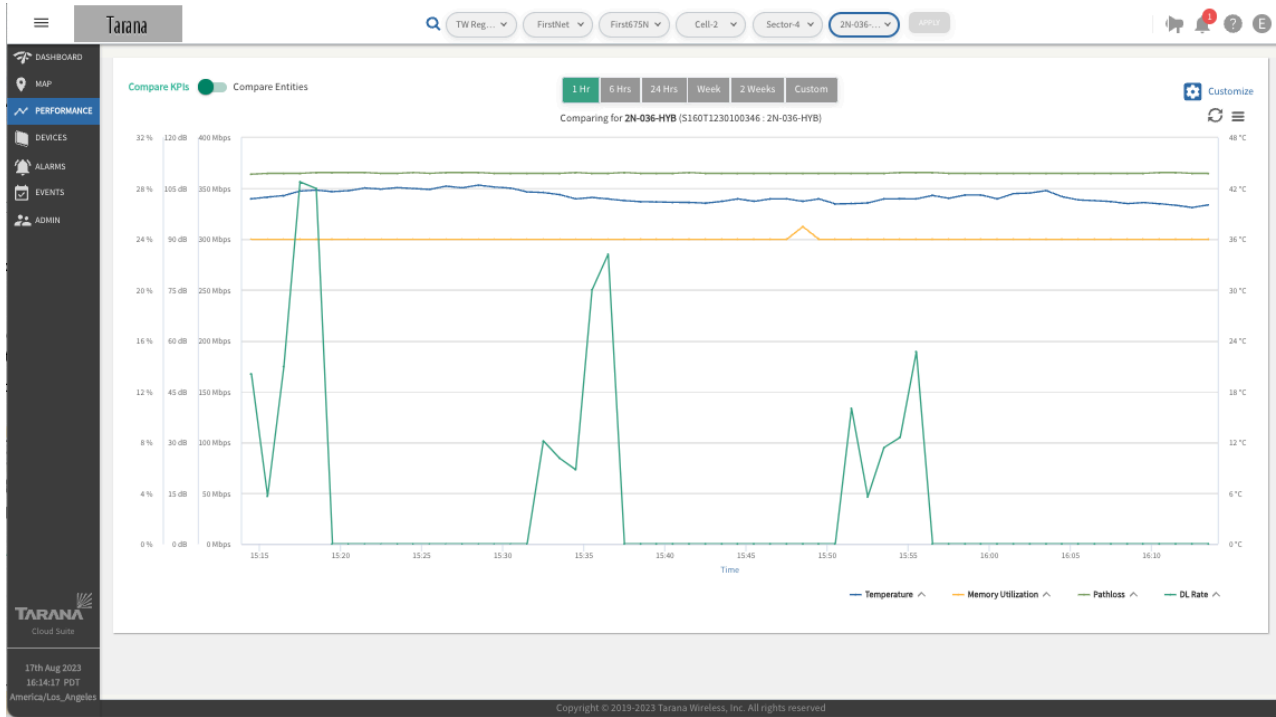


Customize KPIs for a Link

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. Make sure the toggle bar for Show Events Overlay is enabled.
3. Select the operations of interest and select **Done**.

This example shows KPIs for an individual Link with temperature, memory utilization, pathloss, and DL rates compared.



Overlay Events on a KPI Metric

Events are displayed in the green band at the top of the graph. Gray on the bar indicates the device was disconnected. Hover the mouse to see a listing of the values for a specific point in time.

In this example the base node from the previous example has a Reboot event (gray and green bar at the top) overlaid on the Input Voltage (selected from the KPI list) and data is displayed for the past month.

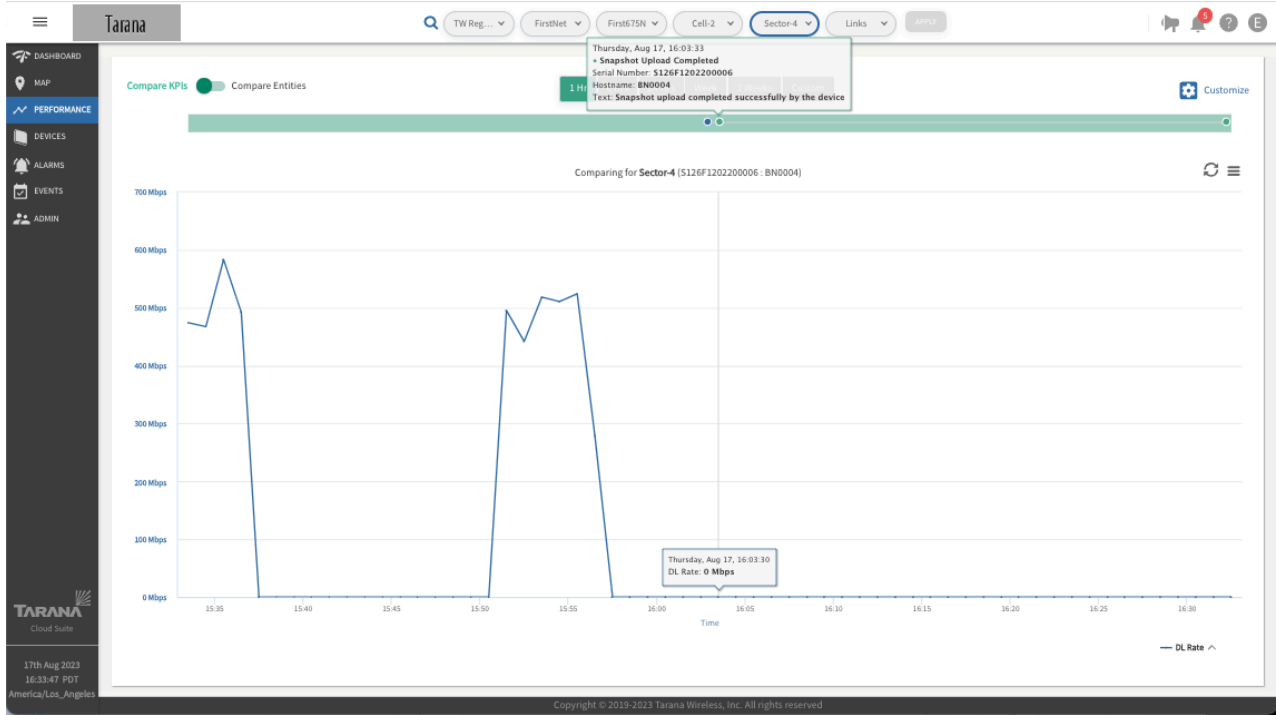
From this data, you see that the base node was powered but not yet connected to TCS for the first half of the month, the input voltage has remained stable above 45V, and no reboot event has been recorded.

In this example, an individual link (remote node) has Alarm events overlaid on two previously selected KPIs (Temperature and CPU Utilization) for the past month. The green and gray bar at the top with colored circles represents instances over the past month when Alarms were raised for this remote node.

This chart maps the remote nodes CPU Utilization and temperature over the same time period. The key at the bottom shows that temperature is tracked on the green graph and the right-side label for the y-axis shows the temperature units in Celsius.

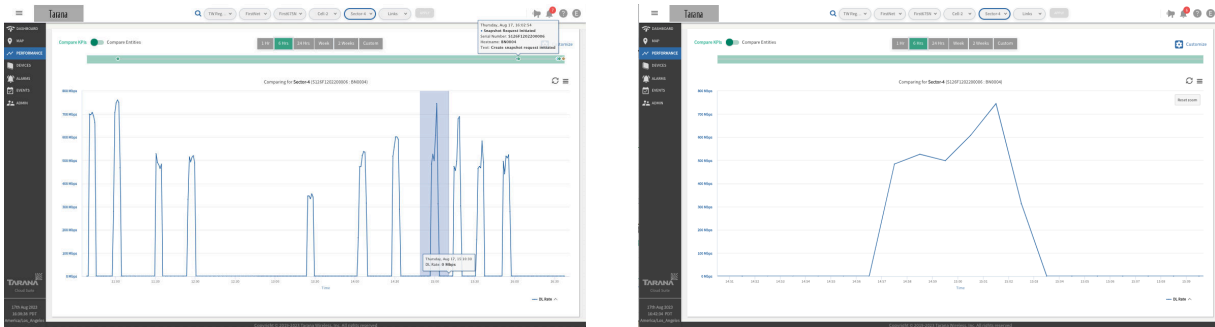
CPU Utilization is tracked with the blue graph and the left-side y-axis shows that the percentage of CPU Utilization held steady between 15 and 23%.

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.



Select zoom area and zoom area displayed

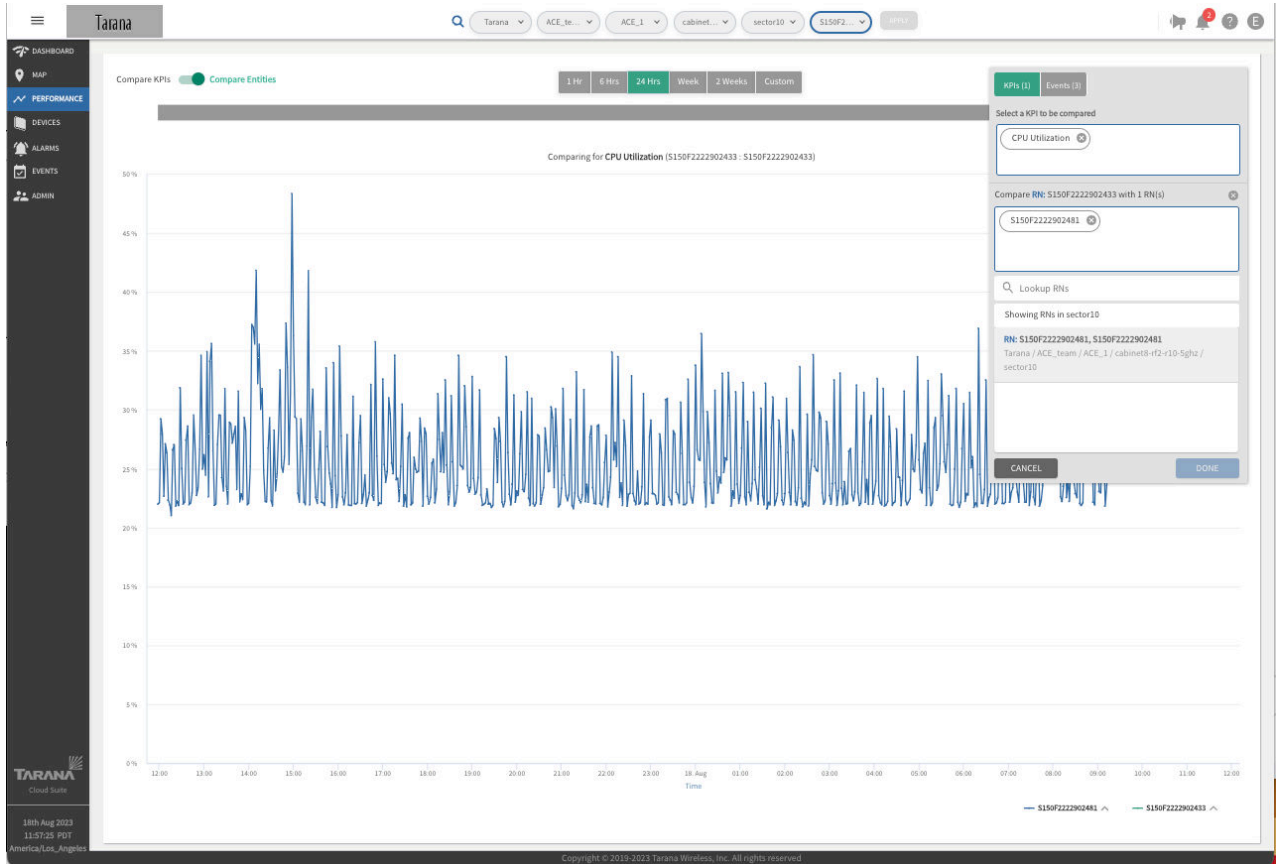
To reset the graph to the selected time frame, select **Reset Zoom**. Use the menu icon in the upper right to view the graph in full screen, print the chart, or download the chart as an image (PNG, JPEG, PDF, or SVG) or CSV file.

Compare Entities

Comparing entities or KPIs is a valuable troubleshooting tool.

Set the Compare KPIs toggle at the upper left corner of the Performance window to **Compare Entities**. Select the **Customize** icon.

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

Make sure you've selected KPIs in green. To select specific KPIs to compare between selected entities, scroll through the list of KPIs or select **Look Up KPI**. The first entity is the one filtered to in the upper middle network entity drop down boxes. In this example, a specific Link is selected. In the Compare Entities window, that remote node is compared to another remote node that's connected to the same base node. The KPI being compared is CPU Utilization. The time period is set to the last 24 hours.

Select **Done** to return to the graph and see the comparison.

By filtering down to a specific link (remote node), only remote nodes connected to the same base node are available to compare. By filtering to a specific sector (base node), you can compare any base nodes in the same cell.

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 left select either remote nodes or base nodes and use the filters to select a specific network.

To go to an individual device dashboard, select the serial number hyperlink. See [Individual Device Dashboard \[45\]](#) for details.

	Serial Number	Hostname	Primary BN (Hostname)	Connected... (Hostname)	Alarms Count	RF Range (m)	Path Loss (dB)	System Up... (d h m s)	Link Uptime (d h m s)	DL SINR (dB)	UL SINR (dB)
<input type="checkbox"/>	S154F1213800001	RN-012	BN0002	BN0002	1	676	129	2d 1h 35m 36s	1d 1h 6m 52s		
<input type="checkbox"/>	S154F1223300268	RN-014	BN1	BN0002	1			-	Last seen a m...		
<input type="checkbox"/>	S154T1223500275	RN-016	BN1	BN0002	1	1011	125	2d 1h 35m 24s	1d 0h 52m 5s		
<input type="checkbox"/>	S154F1214000012	RN-031	BN0002	BN0002	2	763	106	2d 1h 35m 35s	1d 1h 7m 5s		
<input type="checkbox"/>	S154F1214000005	RN-033	BN0002	BN0002	2	723	107	2d 1h 35m 19s	1d 1h 7m 5s	27.5	18.5
<input type="checkbox"/>	S154F1213300004	RN-034	BN0002	BN0002	1	723	107	2d 1h 35m 31s	1d 1h 8m 3s		
<input type="checkbox"/>	S154F1223300248	RN-037	BN0002	BN0002	1	723	109	2d 1h 35m 27s	1d 1h 8m 4s		
<input type="checkbox"/>	S154T1222500215	RN-044	BN0002	BN0002	1	1681	117	2d 1h 35m 23s	1d 1h 7m 6s		
<input type="checkbox"/>	S154T1220900074	RN-077	BN0002	BN0002	1	1065	110	2d 1h 35m 29s	1d 1h 8m 2s		
<input type="checkbox"/>	S154F1223300260	RN-078	BN0002	BN0002	1	1065	108	2d 1h 35m 46s	1d 1h 8m 3s		
<input type="checkbox"/>	S154F1223300267	RN-080	BN0002	BN0002	1	1051	108	2d 1h 35m 35s	1d 1h 6m 51s	27.5	18.5

Device List View

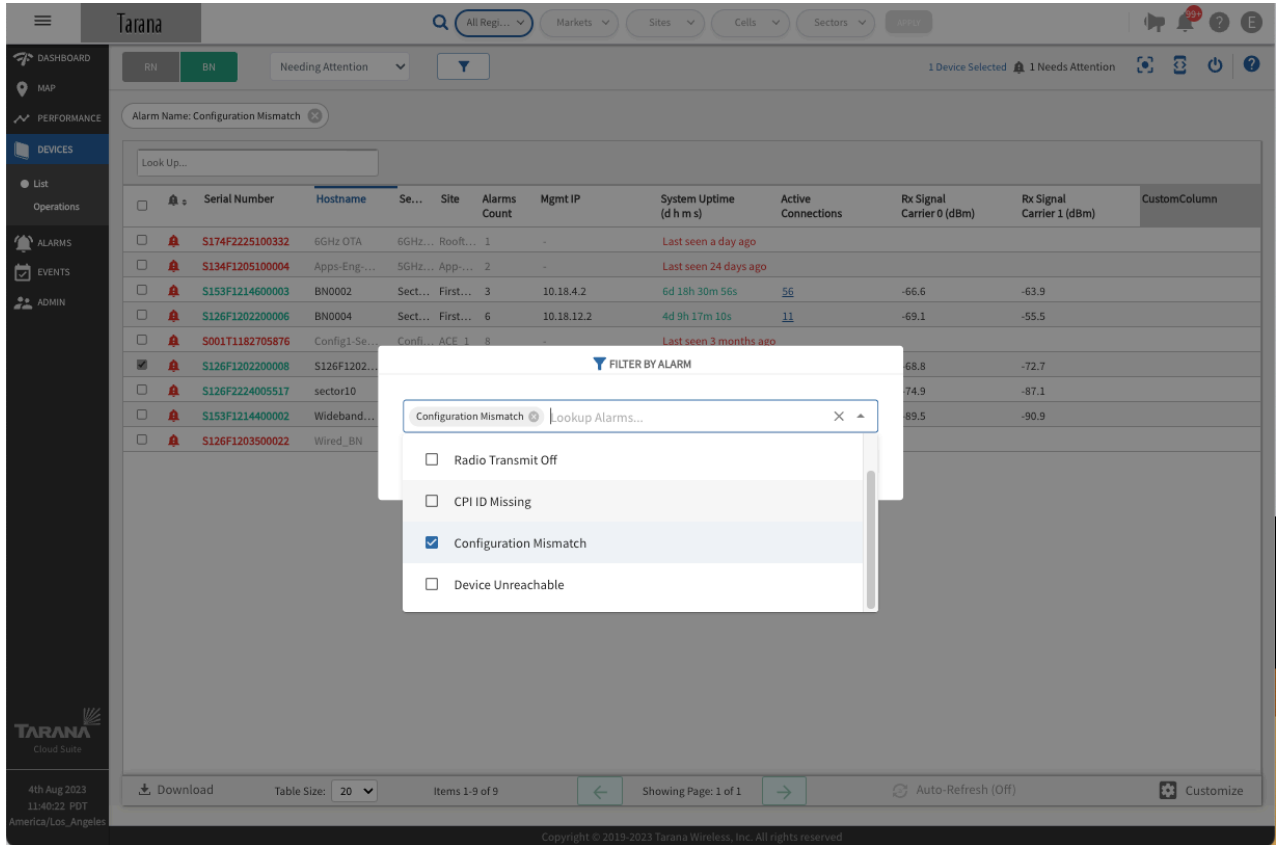
Serial numbers for devices that are up and connected are shown in green. Disconnected devices are shown in red. Devices that need attention are marked with a red bell.

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 these conditions:

- Primary BN Mismatch
- Radio Transmit Off
- CPI ID Missing
- Configuration Mismatch
- Device Unreachable

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



Filter by Alarm

If your role is NOC Operator, 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 \[58\]](#).

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

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

To sort in ascending or descending order, select the column heading. Column categories are dependent on the device type and you can customize them with the Customize icon at the bottom. For details, see [Customize Device Table \[40\]](#).

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

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.

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**.

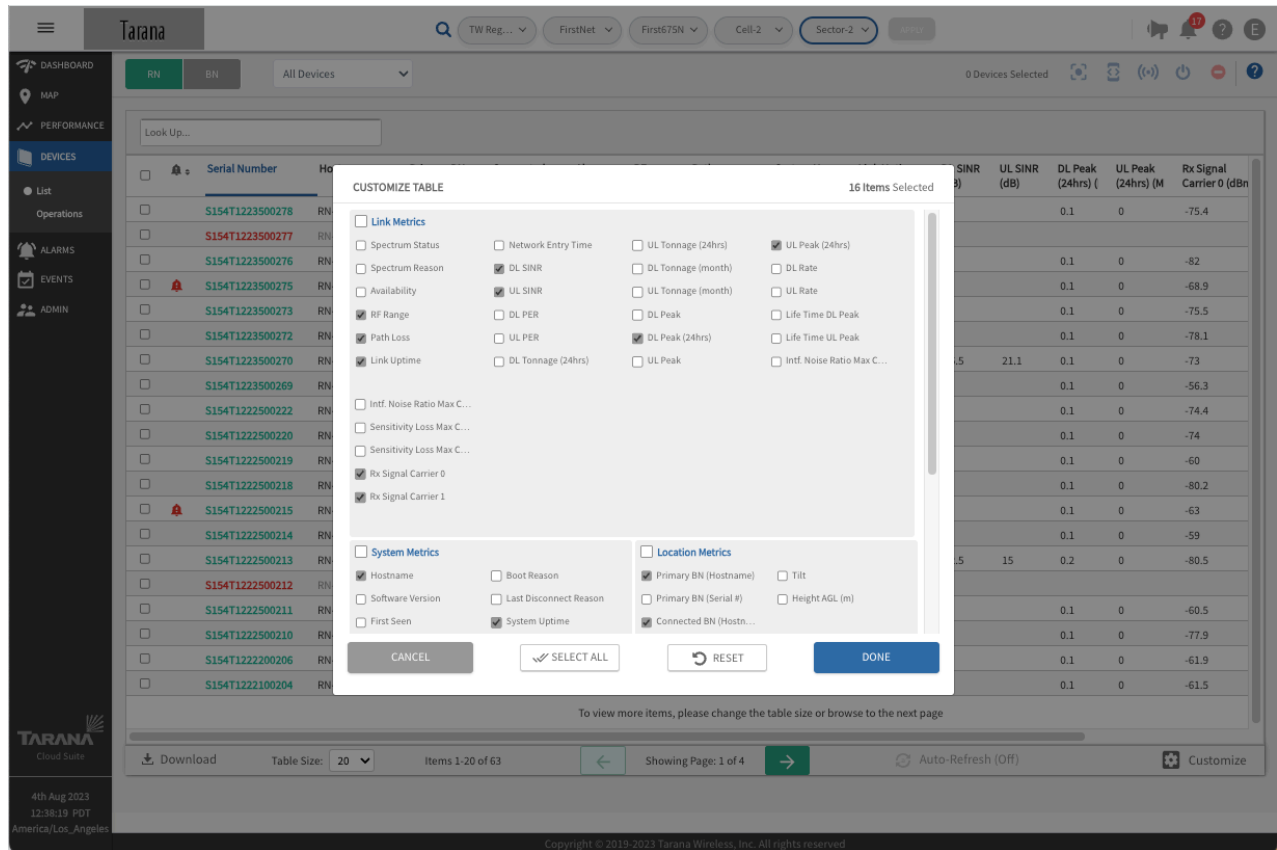
The data displayed for each column doesn't refresh automatically. To change this behavior, select **Auto-Refresh (On)** on the lower side of the screen. It remains on for your user account even after you log out.

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 and select **Download** in the bottom left corner. The file is saved to your local device.

Use the drop down at the bottom to control the table size, and use the arrows to move between pages.

Customize Device List Table

To customize the data table, select **Customize** in the bottom right corner and select the fields you want to see. Select **DONE** to update the display. These changes remain for your user account even after you log out.



Customize Device List View

Link Metrics

Link metrics provide measured operational information about the device link between the base node and remote node.

Base Node Link Metrics

- **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.
- **Spectrum Reason:** Reason for the spectrum status.
- **Active Connections:** Number of remote nodes that are currently connected to a base node.
- **Availability (month):** Time that the link was up regardless of which base node the remote node is connected to. Down time calculation includes unintentional reboots (watchdog timeout or crash) and time required to connect to an alternate base node. It doesn't include cold boots (powered off or a power outage), intentional reboots (such as user initiated or software upgrades), when an associated base node is powered off and no other base node is available, or when the base node data interface is down. This value is calculated as a percent to two decimal places. This parameter resets at the first of every month.
- **Intf. Noise Ratio Max Carrier 0:** Interference-to-noise ratio for carrier 0.
- **Intf. Noise Ratio Max Carrier 1:** Interference-to-noise ratio for carrier 1.
- **Sensitivity Loss Max Carrier 0:** Carrier 0 sensitivity loss, in dB, due to operating at lower than max received gain.
- **Sensitivity Loss Max Carrier 1:** Carrier 1 sensitivity loss, in dB, due to operating at lower than max received gain.
- **Rx Signal Carrier 0:** Received signal strength (including interference) on carrier 0 radio.
- **Rx Signal Carrier 1:** Received signal strength (including interference) on carrier 1 radio.
- **DL Peak:** Highest downlink rate, in Mbps, recorded within the last 150 seconds.
- **Life Time DL Peak:** Peak downlink speed, in Mbps, since the remote node associated to a base node (survives device reboot).
- **Life Time UL Peak:** Peak uplink speed, in Mbps, since the remote node associated to a base node (survives device reboot).
- **RF Utilization:** The amount of available bandwidth that's consumed by traffic, including management, control, and data traffic. The utilization value is displayed as a percentage of total airtime. If the utilization is too low to render accurately, a hyphen appears in the table.

Remote Node Link Metrics

- **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.
- **Spectrum Reason:** Reason for the spectrum status.
- **Availability (month):** Time that the link was up regardless of which base node the remote node is connected to. Down time calculation includes unintentional reboots (watchdog timeout or crash) and time required to connect to an alternate base node. It doesn't include cold boots (powered off or a power outage), intentional reboots (such as user initiated or software upgrades), when an associated base node is powered off and no other base node is available, or when the base node data interface is down. This value is calculated as a percent to two decimal places. This parameter resets at the first of every month.
- **RF Range:** Estimated distance traveled by the RF signal, taking into consideration signal reflection and refraction, in meters.

- **Path Loss:** Measured attenuation of the signal by air and obstructions of the link, in dB.
- **Link Uptime:** Length of time the link has been established.
- **Network Entry Time:** The amount of time the remote node took to establish a link to the base node the last time the remote node established an RF link.
- **DL SINR:** Downlink signal-to-interference-noise ratio, in dB.
- **UL SINR:** Uplink signal-to-interference-noise ratio, in dB.
- **LoS Distance:** Calculated distance between the base node and remote node. This is only available if you've configured the remote node with latitude and longitude information.
- **DL PER:** Downlink packet error rate.
- **UL PER:** Uplink packet error rate.
- **DL Tonnage (24hrs):** Amount of data sent in the downlink direction over the previous 24 hours, in gigabytes.
- **UL Tonnage (24hrs):** Amount of data sent in the uplink direction over the previous 24 hours, in gigabytes.
- **DL Tonnage (month):** Amount of data sent in the downlink direction in the last month, in gigabytes.
- **UL Tonnage (month):** Amount of data sent in the uplink direction in the last month, in gigabytes.
- **DL Peak:** Peak downlink speed, in Mbps, since the link was brought up (resets at device reboot).
- **DL Peak (24hrs):** Highest downlink rate, in Mbps, recorded within the last 24 hours.
- **UL Peak:** Peak uplink speed, in Mbps, since the link was brought up (resets at device reboot).
- **UL Peak (24hrs):** The highest uplink rate, in Mbps, recorded within the last 24 hours.
- **DL Rate:** Downlink layer 2 rate of data transfer, in Mbps, as assigned by the scheduler.
- **UL Rate:** Uplink layer 2 rate of data transfer, in Mbps, as assigned by the scheduler.
- **Life Time DL Peak:** Peak downlink speed, in Mbps, since the remote node associated to a base node (survives device reboot).
- **Life Time UL Peak:** Peak uplink speed, in Mbps, since the remote node associated to a base node (survives device reboot).
- **Rx Signal Carrier 0:** Received signal power on Carrier 0, in dBm.
- **Rx Signal Carrier 1:** Received signal power on Carrier 1, in dBm.
- **Intf. Noise Ratio Max Carrier 0:** The strength of the interfering signal over the noise floor at the signal's maximum point on Carrier 0.
- **Intf. Noise Ratio Max Carrier 1:** The strength of the interfering signal over the noise floor at the signal's maximum point on Carrier 1.
- **Sensitivity Loss Max Carrier 0:** Carrier 0 sensitivity loss, in dB, due to operating at lower than max received gain.
- **Sensitivity Loss Max Carrier 1:** Carrier 1 sensitivity loss, in dB, due to operating at lower than max received gain.

System Metrics

System metrics provide non-hardware-specific information about the device.

Base Node System Metrics

System metrics provide non-hardware-specific information about the device.

- **Hostname:** Hostname, if set, otherwise the system serial number.
- **Boot Reason:** The reason for the most recent boot.
- **Sector:** Administratively-assigned sector name.
- **Cell:** Administratively-assigned cell name.

- **Site:** Administratively-assigned site name.
- **Market:** Administratively-assigned market name.
- **Region:** Administratively-assigned region name.
- **Software Version:** Software version currently installed and in use on the device.
- **First Seen:** Timestamp of when this device was first seen by TCS. Used to establish warranty. If you remove a device from TCS, this date isn't reset. It will never change.
- **Notes:** Any notes added by an administrator or NOC Operator.
- **Active Bank:** The internal bank in which the active software resides.
- **Alarms Count:** Number of currently raised alarms on the device.
- **Mgmt IP:** The IP address set in the Web UI for the base node's in-band management address. This runs on the selected data port.
- **System Uptime:** Duration since the device was last rebooted.
- **CPU:** CPU utilization.
- **Memory:** Memory use.

Remote Node System Metrics

System metrics provide non-hardware-specific information about the device.

- **Hostname:** Hostname, if set, otherwise the system serial number.
- **Software Version:** Software version currently installed and in use on the device.
- **First Seen:** Timestamp of when this device was first seen by TCS. Used to establish warranty. If you remove a device from TCS, this date isn't reset. It will never change.
- **Notes:** Any notes added by an administrator or NOC Operator.
- **Active Bank:** The internal bank in which the active software resides.
- **Alarms Count:** Number of currently raised alarms on the device.
- **Boot Reason:** Reason for the last reboot.
- **Last Disconnect Reason:** Reason for the last disconnect.
- **System Uptime:** Duration since the device was last rebooted.
- **CPU:** CPU utilization.
- **Memory:** Memory use.

Hardware Metrics

Hardware metrics include information relevant to device identification or environment.

- **Serial Number:** Unique system identifier. You can't deselect this parameter.
- **Part No.:** System part number based on the hardware SKU.
- **MAC Address:** MAC (hardware) address of this device.
- **Temperature:** Internal board temperature of the device.
- **Voltage:** Input DC voltage (base node only).



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.

Base Node Location Metrics

Location Metrics provide device installation information.

- **Location:** Comma delimited latitude and longitude of the device in decimal notation.
- **Azimuth:** Horizontal angle of device installation as measured clockwise from true north.
- **Tilt:** Vertical (elevation) angle of device installation as measured from the horizon (0 degrees).
- **Height AGL (m):** Installed height above ground level (AGL).
- **Height AMSL (m):** Installed height above mean sea level.

Remote Node Location Metrics

Location Metrics provide device installation information.

- **Primary BN (Hostname):** Hostname of the base node set as this remote node's primary base node. This parameter is optional and not enabled by default. An admin with a role of OP Admin must enable this parameter before setting it.
- **Primary BN (Serial #):** Serial number of the base node set as this remote node's primary base node. This parameter is optional and not enabled by default. An admin with a role of OP Admin must enable this parameter before setting it.
- **Connected BN (Serial #):** Serial number of the connected base node with which the remote node is associated and maintains a link .
- **Location:** Comma delimited latitude and longitude of the device in decimal notation.
- **Azimuth:** Horizontal angle of device installation as measured clockwise from true north.
- **Tilt:** Vertical (elevation) angle of device installation as measured from the horizon (0 degrees).
- **Height AGL (m):** Installed height above ground level (AGL).
- **Connected BN (Hostname):** Hostname of the connected base node with which the remote node is associated and maintains a link.

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 \[22\]](#). Height, Tilt, and Azimuth are optional, but recommended.

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

Planning Metrics

Planning metrics describe device radio configuration information.

Base Node Planning Metrics

Planning metrics describe device radio configuration information.

- **Frequency Carrier 0:** Center frequency of first carrier band.
- **Frequency Carrier 1:** Center frequency of second carrier band.
- **Operational Bandwidth:** Channel width, in MHz.
- **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.

- **Mgmt VLAN:** An optional parameter that, if used, tags all management traffic on the in-band management port (data port selected) with the specified VLAN. Set it in the base node web UI.
- **Network Profile:** Establishes the DL / UL ratio of the TDD frame and maximum distance between a base node and remote node.

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

Remote Node Planning Metrics

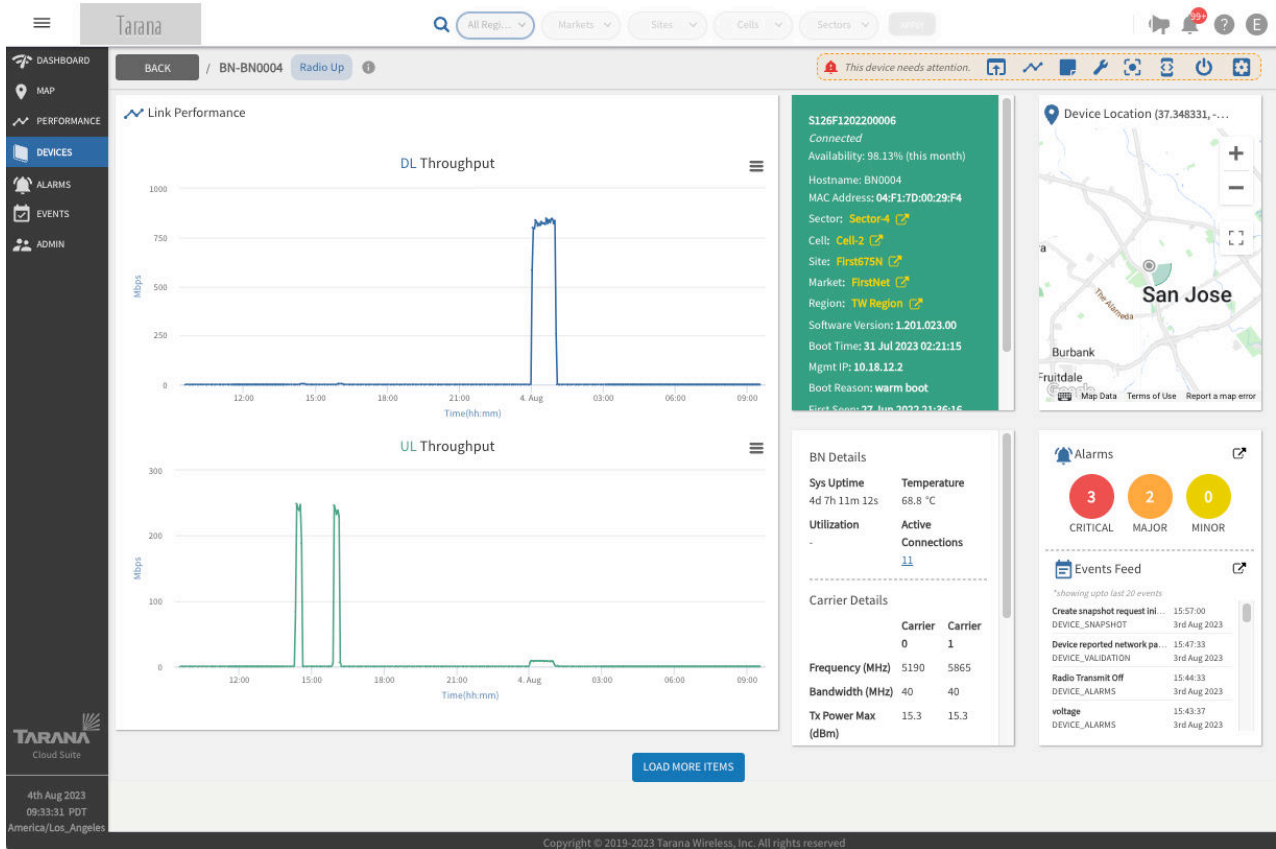
Planning metrics describe device radio configuration information.

- **Frequency Carrier 0:** Center frequency of first carrier band.
- **Frequency Carrier 1:** Center frequency of second carrier band.
- **Retailer Name:** Retailer for the remote node (for installations where large service providers allow different retailers to acquire subscribers).
- **Operational Bandwidth:** Channel width, in MHz.
- **Data VLAN:** An optional VLAN setting that overrides the VLAN setting on the base node (the remote node doesn't tag or untag frames).
- **SLA Profile:** The service level agreement (SLA) on each remote node, applied to both uplink and downlink traffic.

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).

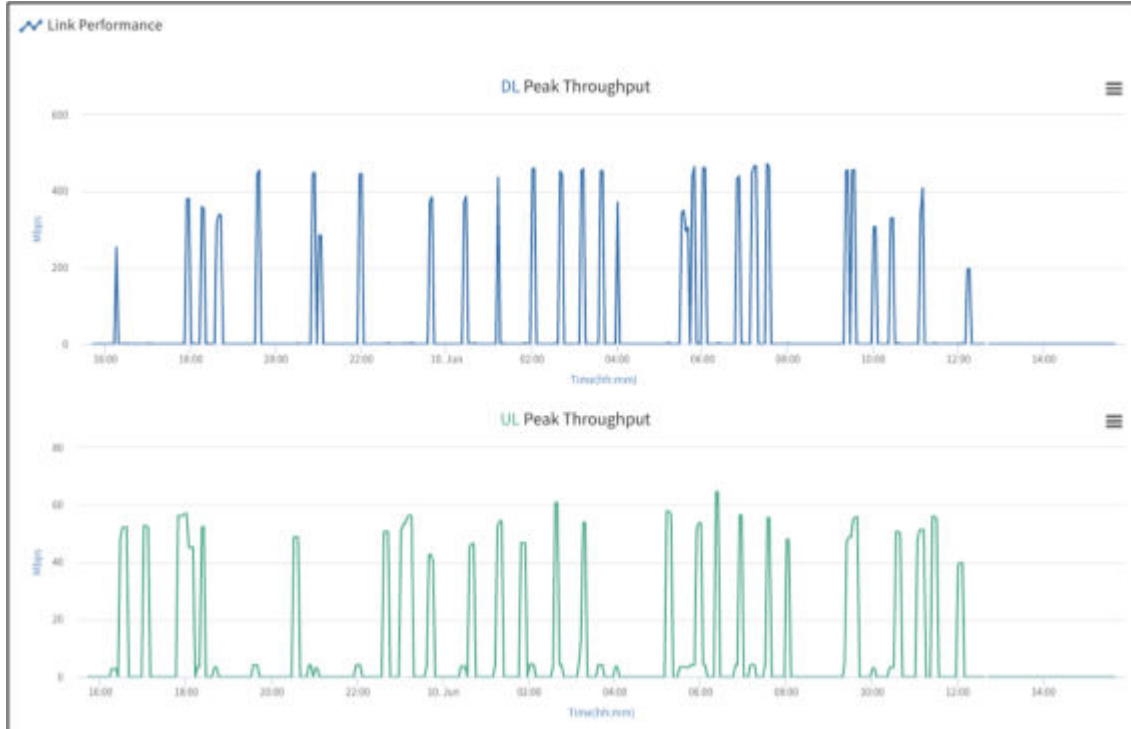
If your user role is NOC Operator or OP Admin, you can use the action icons at the top of the page to perform device management functions. For details, see [Device Dashboard - Action Icons \[58\]](#).



Individual Device List Dashboard

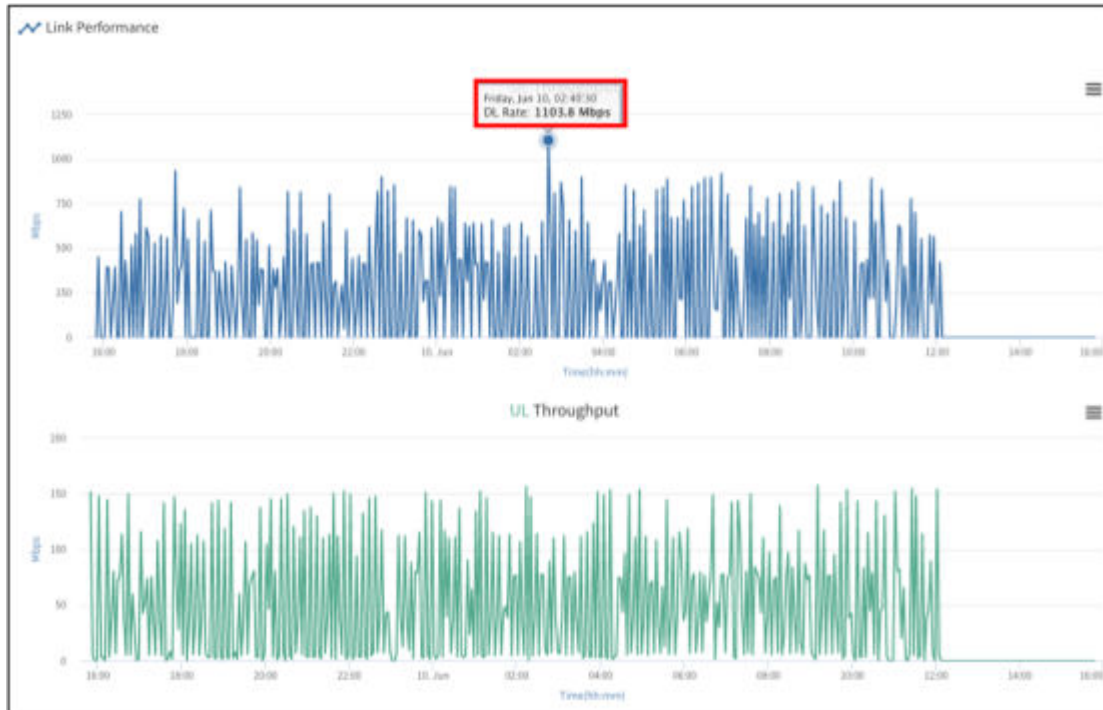
Link Performance

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 in yellow 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

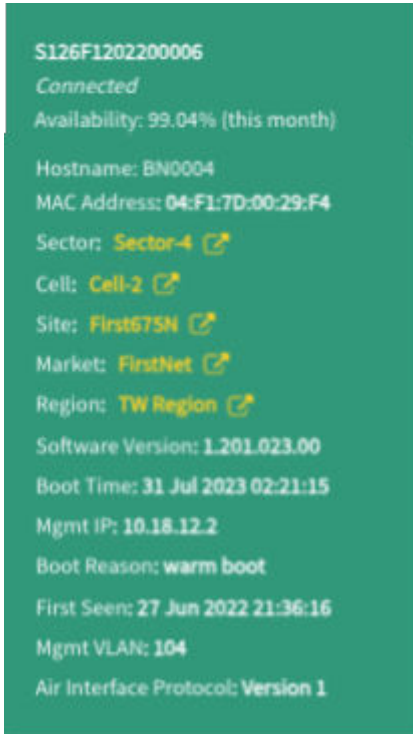
By default, the base node is configured with a Data VLAN of 2000. Both the management and Data VLANs are optional. If you use a management VLAN, it must be on a separate VLAN from the Data VLAN. For both VLANs, 4092, 4093, and 4094 are reserved.

The remote node device summary includes the SLA profile and Data VLAN. If your role is NOC Operator or OP Admin, you can use the Configuration action icon under Configure Network Parameters to 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)

You can find additional information about CBRS installations by selecting **CBRS** in the top left corner of the green Device Summary card in the device’s individual device page. If there are any error conditions such as registration or grant failures, the button turns red to alert you.

The base and remote node summary windows display Spectrum Availability, which includes the maximum EIRP for each grant and labels each as PAL or GAA. The summary window also shows the Last Failure Event and Last Heartbeat listed with corresponding timestamps for both the base node and remote node. There is an option to reacquire spectrum, but be aware that this affects service.



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.

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 under Configure Network Parameters to edit this.



NOTE

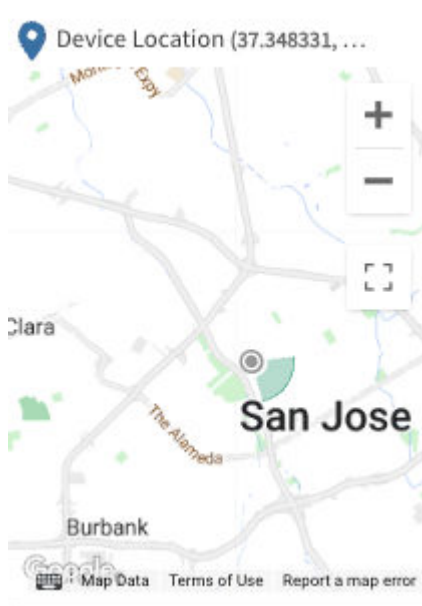
The SLA is applied to downlink and uplink traffic.

- 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

Users with NOC Operator or OP Admin roles can use the Configuration action icon under Configure Network Parameters to 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.

BN Details		
Sys Uptime	Temperature	
8d 9h 35m 10s	72.8 °C	
Utilization	Active Connections	
-	11	

Carrier Details		
	Carrier 0	Carrier 1
Frequency (MHz)	5190	5865
Bandwidth (MHz)	40	40
Tx Power Max (dBm)	15.3	15.3
Remote Tx Power Max (dBm)	27	27

BN Performance		
	DL	UL
Current Rate (Mbps)	0	0
Life Time Peak (Mbps)	897.108	279.321

Link Details		
Sys Uptime	Link Uptime	
0d 0h 29m 17s	0d 0h 25m 29s	
Pathloss	Temperature	
116 dB	44.5 °C	
LoS Distance	RF Distance	
0 m	1031 m	

Carrier Details		
	Carrier 0	Carrier 1
Frequency (MHz)	5660	5700
Bandwidth (MHz)	40	40
Tx Power Max (dBm)	23.8	23.8

Link Performance		
	DL	UL
SINR (dB)	-	-
24 hrs Peak (Mbps)	145.9	2.3
Life Time Peak (Mbps)	623.56	111.623
Current Rate (Mbps)	0	0
PER	0	0
24 hrs Tonnage (GB)	62.2	0.8

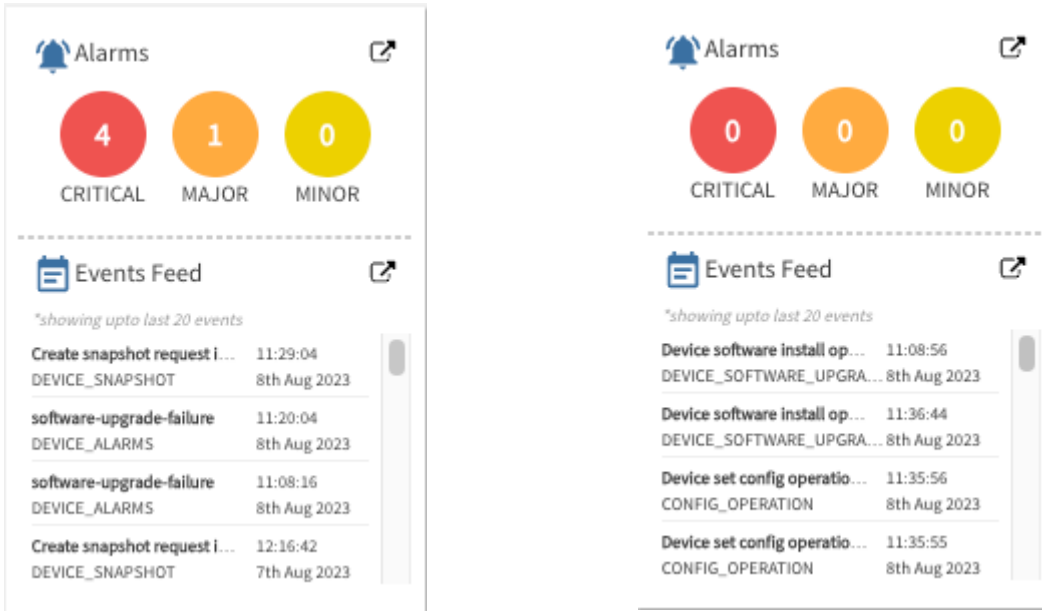
Network Entry		
	Time	Count
Search	0m 19s	2
Radio Calibration	1m 27s	-
RACH	0m 1s	-
Link Setup	0m 40s	-
Link Authentication	0m 0s	-

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.

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

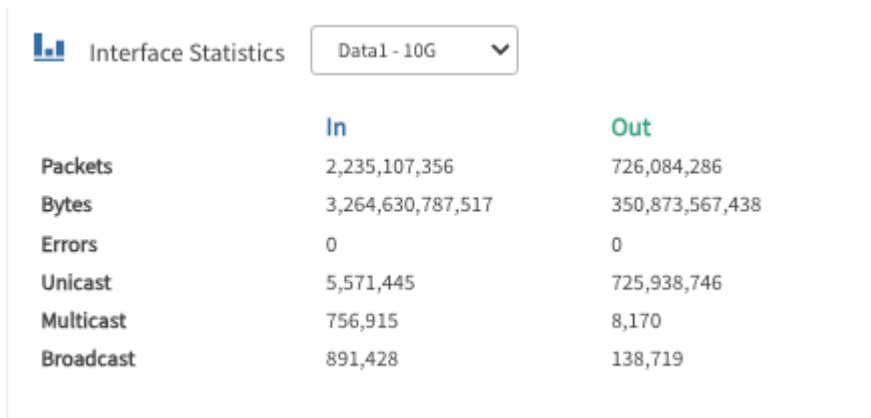
 Interface Summary

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

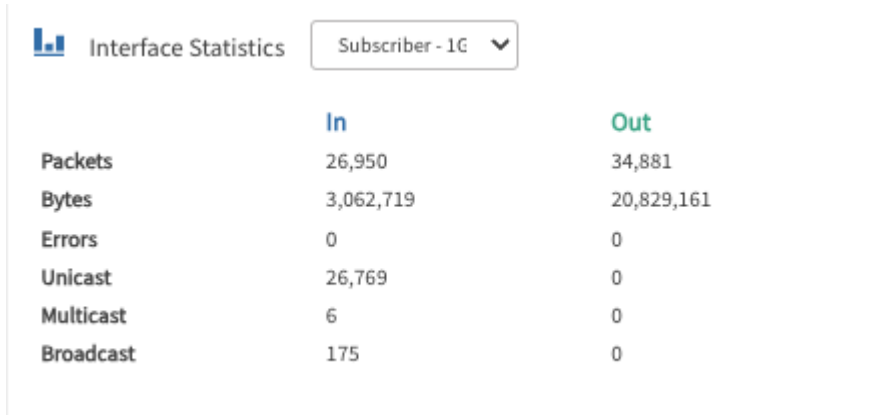
Interface Summary - Remote Node

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:

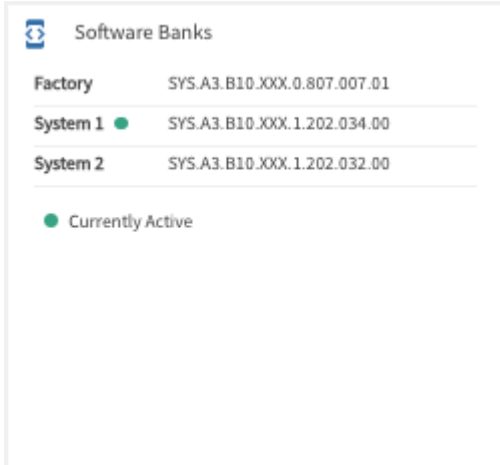
Factory: Software version loaded to factory defaults

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.

The screenshot shows a table titled "BN Disconnects (5)". The table has four columns: "Time Disconnected", "Time Connected", "Duration of Disconnect (hh:mm:ss)", and "Software Version".

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

At the bottom of the table, there is a footer that says "5 Records Available" and a scroll bar on the right side.

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 LP you see only icons for performance, notes, and diagnostics. The actions are:


- Log into the web UI
- View performance page
- Add or view notes
- Diagnostics
- Network operations (remote node only)
- Snapshot
- Software install
- Reboot the device
- Configuration



Action Icons

Hover over each icon to see what it does.

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 \[98\]](#) for details.

**NOTE**

You should 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.

View Performance

Select the Performance icon (⌘) to view Performance for this device. For details, see [TCS Performance \[31\]](#).

Add Notes

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**.

Figure 1.

Add Device Notes

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

Select the **Diagnostics** icon (🔧) to perform diagnostics operations. For a remote node you can select **Speed Test** or **Troubleshoot**. 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. For a base node, you can select **Troubleshoot**.

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.

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

When you run the speed test, TCS 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. When the downlink test is complete, TCS displays the following information in a report dialog:

- Downlink throughput in megabits per second (Mbps)
- Downlink SNR
- Carrier (Carrier 0 for the downlink)
- Carrier frequency in megahertz (MHz)
- Carrier bandwidth (MHz)
- RF Range in meters (m)
- Pathloss in decibels (dB)

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. When the uplink test is complete, TCS displays the speed test report dialog with the following information:

- Uplink throughput (Mbps)
- Uplink SNR
- Carrier (Carrier 1 for the uplink)
- Carrier frequency (MHz)
- Carrier bandwidth (MHz)

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

When a speed test is complete, you can set a particular speed test result as a baseline. 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 result, conduct a speed test as described above. When the speed test completes:

1. Select Mark New Result as Baseline (for this device).
2. Select 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 speed test. To compare your current speed test with the baseline, conduct a speed test as described above. When the speed test completes:

1. Enable Compare with Baseline.
2. Select 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.

If you select **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**. For a remote node you can only do 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.

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.

📦 INSTALL NEW SOFTWARE
S145T1214500290

Look Up...

Stable
 Beta

Software Image	Release Channel
SYS.A3.R10.XXX.1.900.039.00	Stable
SYS.A3.R10.XXX.1.202.010.00	Beta
SYS.A3.R10.XXX.1.202.004.00	Beta
SYS.A3.R10.XXX.1.202.002.00	Beta
SYS.A3.R10.XXX.1.201.029.00	Beta
SYS.A3.R10.XXX.1.201.023.00	Beta
SYS.A3.R10.XXX.1.201.020.00	Beta

Please select a software image to view details

CANCEL

Activate software after upgrade

PROCEED

Upgrade Device Software

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 **Configuration** icon (⚙️). Select an action from the drop down list:

- **Configure Installation Parameters:** Pop up shows these fields:
 - **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):** Grayed out for base nodes because you can't change the value.
- **Configure Network Parameters:** Pop up shows these fields:
 - **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.
 - **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 \[122\]](#).
 - **Toggle for Radio Tx:** Transmit or Mute. Base node only.
- **Configure Primary Base node (remote node only):** This feature is disabled by default. A pop up shows the current assigned Primary Base Node for this device. If your role is OP Admin, you can select a radio button for one of these options:
 - 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:** Popup shows a message that DL Lifetime Peak and UL Lifetime Peak will be reset for the device, and cannot be undone. Select **No** or **Yes** to cancel or proceed.

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.

G1 Administration Guide

Hostname	Timestamp	Device ID	Software Version	Device Upgrade Status	Operation Status	Download Progress	Device Message	Manage
Vivek_627	09 Aug 2023 02:51:00	S065T1203780627	0.997.029.00	SOFTWARE INSTALL COMP...	SUCCESS	100%	Upgrade success	⋮
S126F1202200008_BM_test	09 Aug 2023 02:50:00	S126F1202200008	0.997.029.00	DOWNLOAD COMPLETE	SUCCESS	100%	Download complete	⋮
BN0004	08 Aug 2023 21:53:41	S126F1202200006	0.997.031.00	DOWNLOAD COMPLETE	SUCCESS	100%	Download complete	⋮
2N-030	08 Aug 2023 21:53:41	S128F1210600195	0.997.031.00	SOFTWARE INSTALL COMP...	SUCCESS	100%	Upgrade success	⋮
2N-HY-015	08 Aug 2023 21:53:41	S160M2230400056	0.997.031.00	SOFTWARE INSTALL COMP...	SUCCESS	100%	Upgrade success	⋮
S150F2224100799	08 Aug 2023 21:53:41	S150F2224100799	0.997.031.00	SOFTWARE INSTALL COMP...	SUCCESS	100%	Upgrade success	⋮
2N-Hy-087	08 Aug 2023 21:53:41	S160M2230400049	0.997.031.00	SOFTWARE INSTALL COMP...	SUCCESS	100%	Upgrade success	⋮
2N-117	08 Aug 2023 21:53:41	S145T1214600291	0.997.031.00	SOFTWARE INSTALL COMP...	SUCCESS	100%	Upgrade success	⋮
2N-116	08 Aug 2023 21:53:41	S150F2222902432	0.997.031.00	SOFTWARE INSTALL COMP...	SUCCESS	100%	Upgrade success	⋮
2N-118	08 Aug 2023 21:53:41	S128F1210600291	0.997.031.00	SOFTWARE INSTALL COMP...	SUCCESS	100%	Upgrade success	⋮

To view more items, please change the table size or browse to the next page

Download Table Size: 10 Items 1-10 of 5425 Showing Page: 1 of 543 Auto-Refresh (Off) Customize

Device Operations View

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

Use the Customize icon (⚙️) on the bottom right to select information displayed.

To rerun a failed operation (for example, a software upgrade), use the three-dot icon in the Manage column for the operation to select **Retry**.

Use the search field to look up operations manually. Select the **Advanced** drop-down menu next to the search bar to further filter the results:

Operation Status: Select from **All**, **Queued**, **Running**, **Aborted**, **Success**, or **Failed**.

Period: Select from **All**, **Last 24 hours**, **Last 1 Week**, **Last 2 Weeks**, or **Last 1 Month**.

G1 Administration Guide

The screenshot displays the Tarana G1 Administration interface. The top navigation bar includes the Tarana logo, a search bar, and filters for All Regs., Markets, Sites, Cells, and Sectors. A sidebar on the left contains navigation options: DASHBOARD, MAP, PERFORMANCE, DEVICES (List, Operations), ALARMS, EVENTS, and ADMIN. The main content area shows a table of device upgrade operations with columns for Hostname, Timestamp, Device Upgrade Status, Operation Status, Download Progress, Device Message, and Manage. An advanced search panel is open, allowing filtering by Operation Status and Period. The table lists several successful upgrade operations for various devices.

Hostname	Timestamp	Device Upgrade Status	Operation Status	Download Progress	Device Message	Manage		
Vivek_627	09 Aug 2023 02:51	SOFTWARE INSTALL COMP...	SUCCESS	100%	Upgrade success	⋮		
S126F1202200008_BN_test	09 Aug 2023 02:50	DOWNLOAD COMPLETE	SUCCESS	100%	Download complete	⋮		
BN0004	08 Aug 2023 21:53	DOWNLOAD COMPLETE	SUCCESS	100%	Download complete	⋮		
2N-030	08 Aug 2023 21:53	SOFTWARE INSTALL COMP...	SUCCESS	100%	Upgrade success	⋮		
2N-HY-015	08 Aug 2023 21:53	SOFTWARE INSTALL COMP...	SUCCESS	100%	Upgrade success	⋮		
S150F2224100799	08 Aug 2023 21:53:41	S150F2224100799	0.997.031.00	SOFTWARE INSTALL COMP...	SUCCESS	100%	Upgrade success	⋮
2N-Hy-087	08 Aug 2023 21:53:41	S160M1230400049	0.997.031.00	SOFTWARE INSTALL COMP...	SUCCESS	100%	Upgrade success	⋮
2N-117	08 Aug 2023 21:53:41	S145T1214600291	0.997.031.00	SOFTWARE INSTALL COMP...	SUCCESS	100%	Upgrade success	⋮
2N-116	08 Aug 2023 21:53:41	S150F2222902432	0.997.031.00	SOFTWARE INSTALL COMP...	SUCCESS	100%	Upgrade success	⋮
2N-118	08 Aug 2023 21:53:41	S128F1210600291	0.997.031.00	SOFTWARE INSTALL COMP...	SUCCESS	100%	Upgrade success	⋮

To view more items, please change the table size or browse to the next page

9th Aug 2023 12:52:56 PDT America/Los_Angeles

Download Table Size: 10 Items 1-10 of 5425 Showing Page: 1 of 543 Auto-Refresh (Off) Customize

Copyright © 2019-2023 Tarana Wireless, Inc. All rights reserved

Advanced Lookup Options

TCS Alarms

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

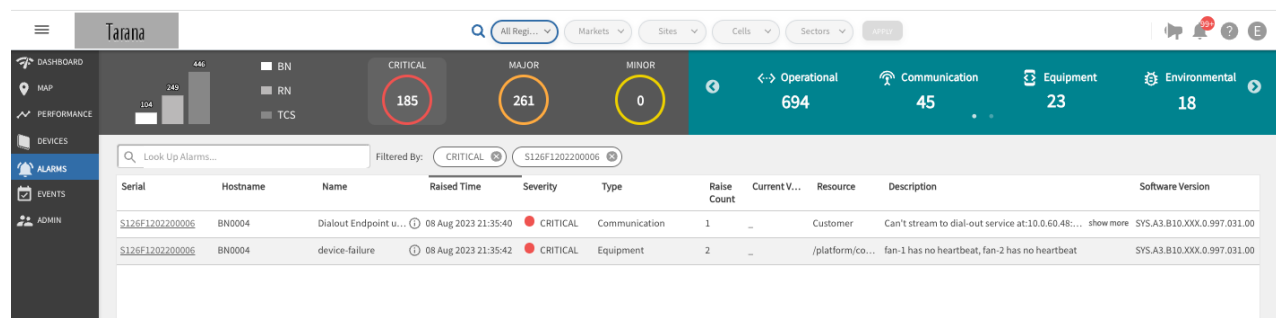
The default view is of alarms for the last device you viewed. Make sure that you've chosen the correct network entity from the drop-down menus at the top. This filters the network down to the granularity you need. Because the menus are hierarchical, start by selecting the Region, then Market, Site, Cell, and Sector.

Use the search bar on the top left to search or filter the list results based on attributes such as serial number or hostname.



NOTE

In this example, only alarms for the device named S126F1202200006 are shown.



Alarm Dashboard

The top of the alarm dashboard shows high-level information and filters for specific data. The left side (gray) displays a summary of alarms. The bar graph shows the number of alarms raised for base nodes, remote nodes and TCS. Select **BN**, **RN**, or **TCS** to filter the list to show alarms only on those devices.

The colored circles indicate the level of those alarms:


- Critical (red)
- Major (orange)
- Minor (yellow)

The number in each circle indicates the number of alarms that meet this criterion. Selecting a circle filters the list to show only alarms that meet the specified level.

The right side (green) breaks down alarms by type. Select each type to filter the displayed list. Alarm types include:

- **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.
- **Communication:** Error in communication. Example: network interface down, unable to get DHCP address (if enabled), IP address conflict, unable to resolve hostname (DNS failure).

- **Equipment:** Hardware error. Example: temperature isn't within thresholds.
- **Environmental:** Issues with the operational environment. Example: the number of GPS satellites available for GPS is low.
- **Qos:** Quality of service.
- **Physical:**
- **Other:** Any alarms that aren't otherwise classified.
- **Processing:** Error in system processing. Example: configuration update failure.

Use the **Customize** icon () on the lower right to modify which fields are displayed. Options include:

Serial Number: The device serial number.

Hostname: The device hostname.

Name: The name of the alarm.

Raised Time: The time the alarm was created.

Severity: The severity of the alarm (WARNING, MINOR, MAJOR, CRITICAL).

Type: The alarm type.

Raise Count: The number of times this alarm has been raised.

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%.

Resource: The source of the alarm within the system.

Description: A brief description of the alarm.

Software Version: The software version the device is using.

Time to Clear: Amount of time it took to clear the alarm.

Recommended Action: Recommended action to resolve the alarm.

Alarms aren't automatically refreshed. To change this behavior, select **Auto-Refresh (On)** on the lower side of the screen so that the display will auto-refresh every 60 seconds.



NOTE

Both the customization and auto refresh changes are persistent for the user account and the new settings are maintained even after logging out.

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

Select **Download** in the bottom left of the screen to download a comma separated (CSV) list of all displayed alarms (meaning the saved file content is filter sensitive).

TCS Events

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

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. As with Performance, 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.

The top of the Events dashboard shows filters for specific data. Selecting each type automatically filters the displayed list. Event types are:

All: 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.

Other Other event types not listed above (not currently used).

Use the search bar on the top to search or filter the list results based on attributes like serial number or hostname.

Serial Number	Hostname	Event Name	Timestamp	Details
S142F1215000176	S142F1215000176	Device Disconnected	07 Aug 2023 13:14:48	bn:radio-reset
S142F1215000176	S142F1215000176	Device Config Set Failed	07 Aug 2023 13:12:44	
S142F1215000176	S142F1215000176	Device Config Set Failed	07 Aug 2023 13:12:39	
S142F1215000176	S142F1215000176	Device Config Set Failed	07 Aug 2023 13:12:34	
S142F1215000176	S142F1215000176	Device Config Set Initiated	07 Aug 2023 13:12:34	
S142F1215000176	S142F1215000176	Device Connected	07 Aug 2023 13:12:34	bn:reboot
S142F1215000176	S142F1215000176	Device Disconnected	04 Aug 2023 19:51:58	bn:admin
S142F1215000176	S142F1215000176	Device Config Set Failed	04 Aug 2023 14:58:19	
S142F1215000176	S142F1215000176	Device Config Set Failed	04 Aug 2023 14:57:39	
S142F1215000176	S142F1215000176	Device Config Set Failed	04 Aug 2023 14:57:19	
S142F1215000176	S142F1215000176	Device Config Set Failed	04 Aug 2023 14:57:09	
S142F1215000176	S142F1215000176	Device Config Set Failed	04 Aug 2023 14:57:03	
S142F1215000176	S142F1215000176	Device Config Set Initiated	04 Aug 2023 14:57:03	
S142F1215000176	S142F1215000176	Device Connected	04 Aug 2023 14:57:03	
S142F1215000176	S142F1215000176	Device Disconnected	04 Aug 2023 14:51:04	bn:admin
S142F1215000176	S142F1215000176	Device Config Set Failed	04 Aug 2023 14:12:48	
S142F1215000176	S142F1215000176	Device Config Set Failed	04 Aug 2023 14:12:08	
S142F1215000176	S142F1215000176	Device Config Set Failed	04 Aug 2023 14:11:47	
S142F1215000176	S142F1215000176	Device Config Set Failed	04 Aug 2023 14:11:37	
S142F1215000176	S142F1215000176	Device Config Set Failed	04 Aug 2023 14:11:32	

To view more items, please change the table size or browse to the next page

Filter Events

To filter events, select the filter icon on the right and select one of the choices:

- Time period: one hour, 24 hours, one week, two weeks, or a custom time period.
- Device hostname
- Device serial number
- User email ID
- Specific event types listed under the drop down

Admin Events

If your role is OP Admin, you can see **Admin** in the middle of the Events pane. Select it to see administrative events in the network. These include user logins, software upgrades, and warnings of upcoming software upgrades.

Event Name	Timestamp	Details
User Logged In	23 Aug 2023 00:08:09	Login IP address: 192.140.152.7
User login failed	23 Aug 2023 00:07:53	Login IP address: 192.140.152.7
User Deleted	21 Aug 2023 03:19:48	Deleted user: mahip neema
User Created	21 Aug 2023 03:19:47	New user: mahip neema
User Resent Signup Details	21 Aug 2023 03:19:47	Resent for user: mahip neema
User Deleted	21 Aug 2023 03:19:47	Deleted user: mahip neema
User Details Updated	21 Aug 2023 03:19:46	[role] modified for the user mahip neema. Due to the sensitivity of the change go to Admin->User Management to see the changed value.
User Created	21 Aug 2023 03:19:45	New user: mahip neema
User Deleted	21 Aug 2023 03:19:12	Deleted user: mahip neema
User Created	21 Aug 2023 03:19:11	New user: mahip neema
User Resent Signup Details	21 Aug 2023 03:19:11	Resent for user: mahip neema
User Deleted	21 Aug 2023 03:19:11	Deleted user: mahip neema
User Details Updated	21 Aug 2023 03:19:09	[retailerId, firstName, lastName, address, role] modified for the user mahip neema. Due to the sensitivity of the change go to Admin->User Management to see the changed ...
User Logged In	18 Aug 2023 02:13:01	Login IP address: 27.107.8.190
User Logged In	18 Aug 2023 01:54:58	Login IP address: 27.107.8.190
User login failed	18 Aug 2023 01:54:55	Login IP address: 27.107.8.190
User login failed	18 Aug 2023 01:54:53	Login IP address: 27.107.8.190
User login failed	18 Aug 2023 01:54:52	Login IP address: 27.107.8.190
User login failed	18 Aug 2023 01:54:50	Login IP address: 27.107.8.190
User Logged In	18 Aug 2023 01:53:58	Login IP address: 27.107.8.190

To view more items, please change the table size or browse to the next page

Admin Events

You can use the Customize icon  on the lower right to choose which fields are displayed.

Options include:

Event Name: The name of the event.

Timestamp: The time and day the event was logged, based on the users time zone selection in their user profile.

Details: Further detailed information about this event.

Category: The event category.

Event Source: The source of the event within the system (base node, remote node, TCS, or User).

Software Version: The version of the software the device is using.

User Email: Email associated with the user account responsible for the event (for example, a configuration change).

Events aren't automatically refreshed. To change this behavior, select Auto-Refresh on the lower side of the screen.



NOTE

Both the customization and auto refresh changes are persistent for your user account and the new settings are maintained even after logging out.

To sort in ascending or descending order, select the column heading. Drag column headings to show them in different order.

Select **Download** in the bottom left of the screen to download a comma separated (CSV) list of all displayed events (meaning the saved file content is filter sensitive).

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
- Alerts Configuration
- User Management
- Software Inventory
- Webhook Management
- API Management

Network Configuration

Network configuration is a key component of TCS that you use to define all deployed networks. One of your first tasks is to define your network entities.

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

Manage Networks

A network entity is defined as a group of base nodes and remote nodes. You must create entities as hierarchies before you can assign equipment. Network 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.

To create or edit a network, select **Admin - Network Configuration** from the main TCS page.

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.

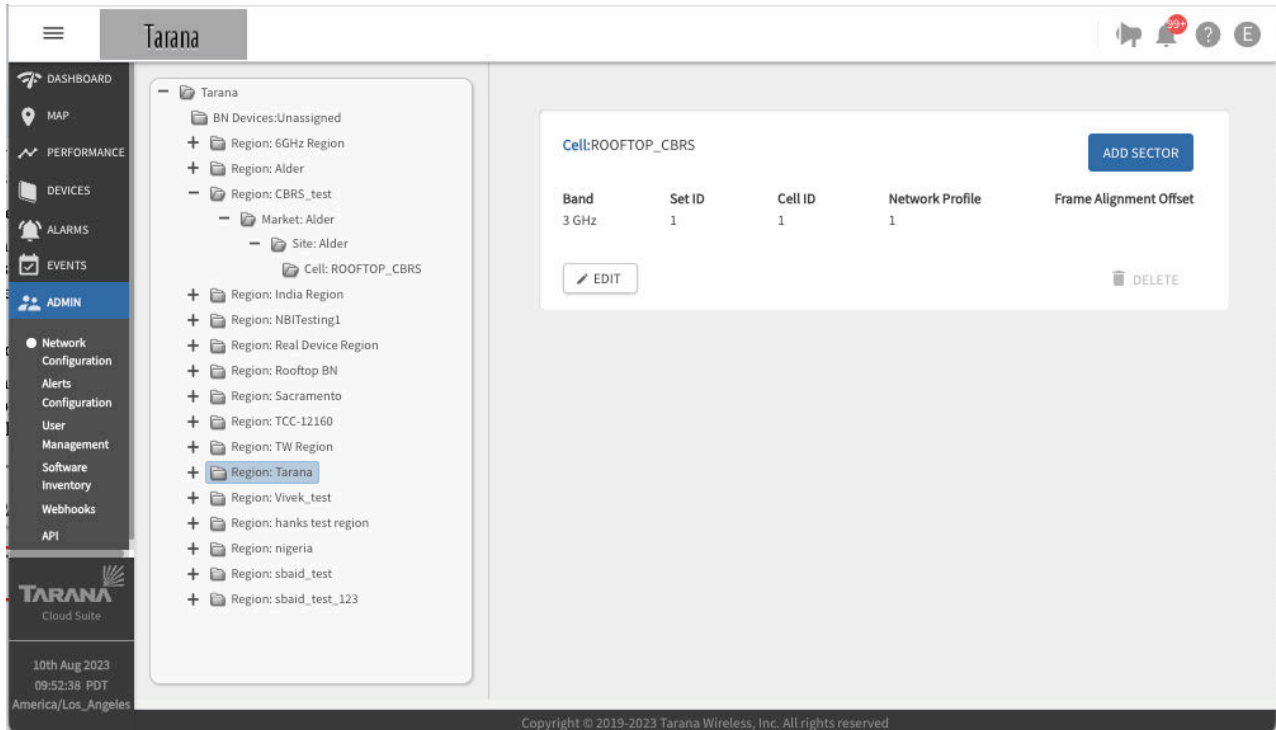


NOTE

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.

This level also includes customer-defined deployment regions.

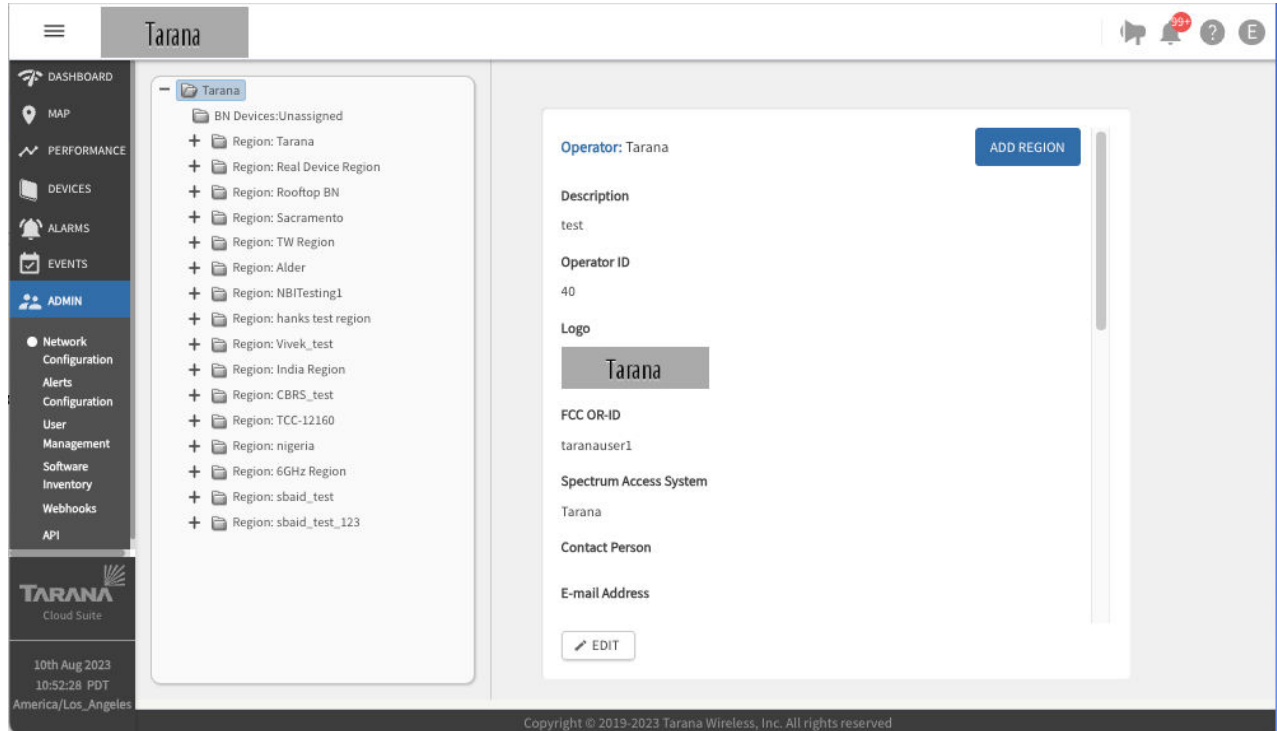
Below that is a hierarchical view of the operator network as defined by the operator that shows configured regions. Select the plus (+) sign to expand each region and show the rest of the hierarchy.



Network Configuration Hierarchy

Manage Operator

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:** A brief description (optional).
- **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.. Select **Guidelines** to see logo image requirements. File must be in PNG, JPG, or GIF format with a maximum size of 500KB. The logo is displayed at 50px high and 145px wide. If you upload a larger or smaller image, it's resized.
- **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.
 - **Spectrum Access Server:** Only required for CBRS operation (supported values are Google or Federated Wireless).
- **Contact Person:** The name of a contact person for this operator (optional).
- **Email Address:** The email address for the contact person (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.
- **Primary BN Settings:** This feature 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 Auto-upgrade Policy:** 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.

- **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.
- **Notification Email:** One or more email addresses (comma separated).
- **Telemetry:** Information for metrics collector end point configuration (optional). Enter the Destination Address and Port, choose a 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.

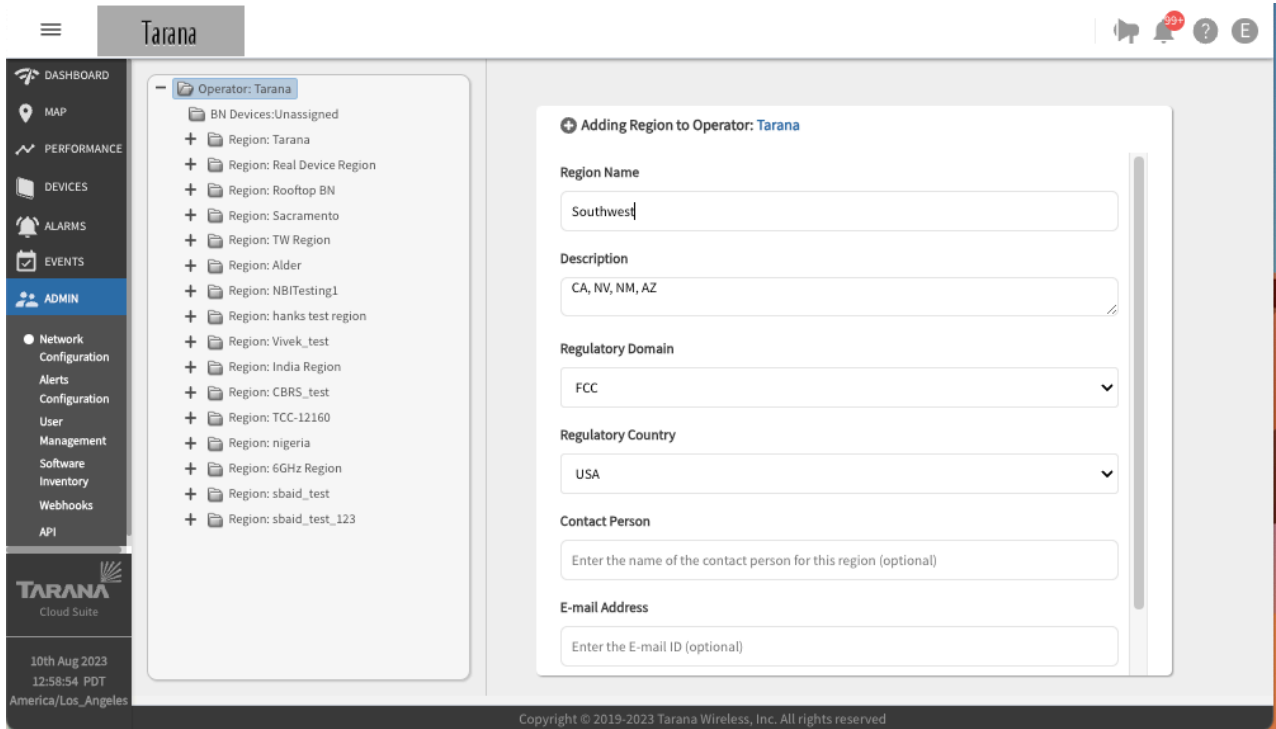
Manage Regions

To create a region, open the Operator on the hierarchy tree and 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 the contact person for the region (optional).
- **E-mail Address:** 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**.



Create a New Region

Manage Markets

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

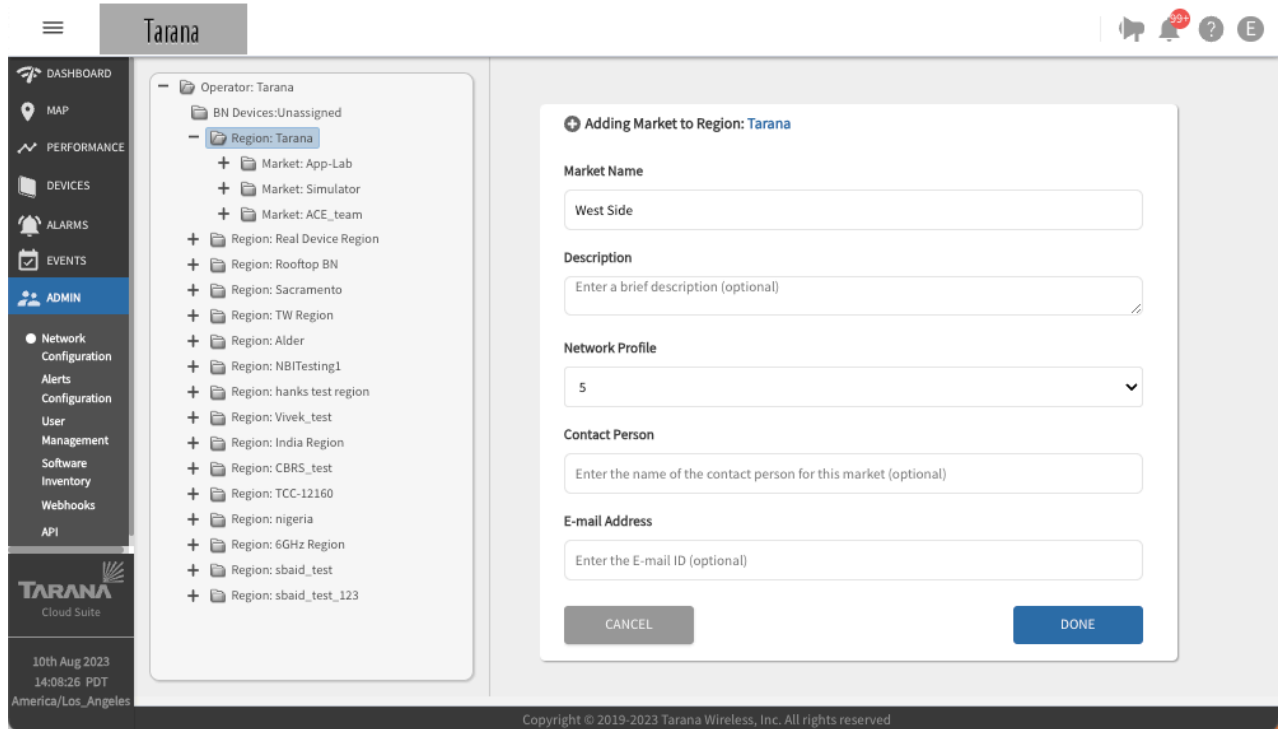
- **Market Name:** Name of the market.
- **Description:** An informative description (optional).
- **Network Profile:** Definition of the maximum distance of the remote node from the base node and the ratio of downlink to uplink throughput. Select a value from the drop down.

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:** Contact person for the market (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**



Create a New Market

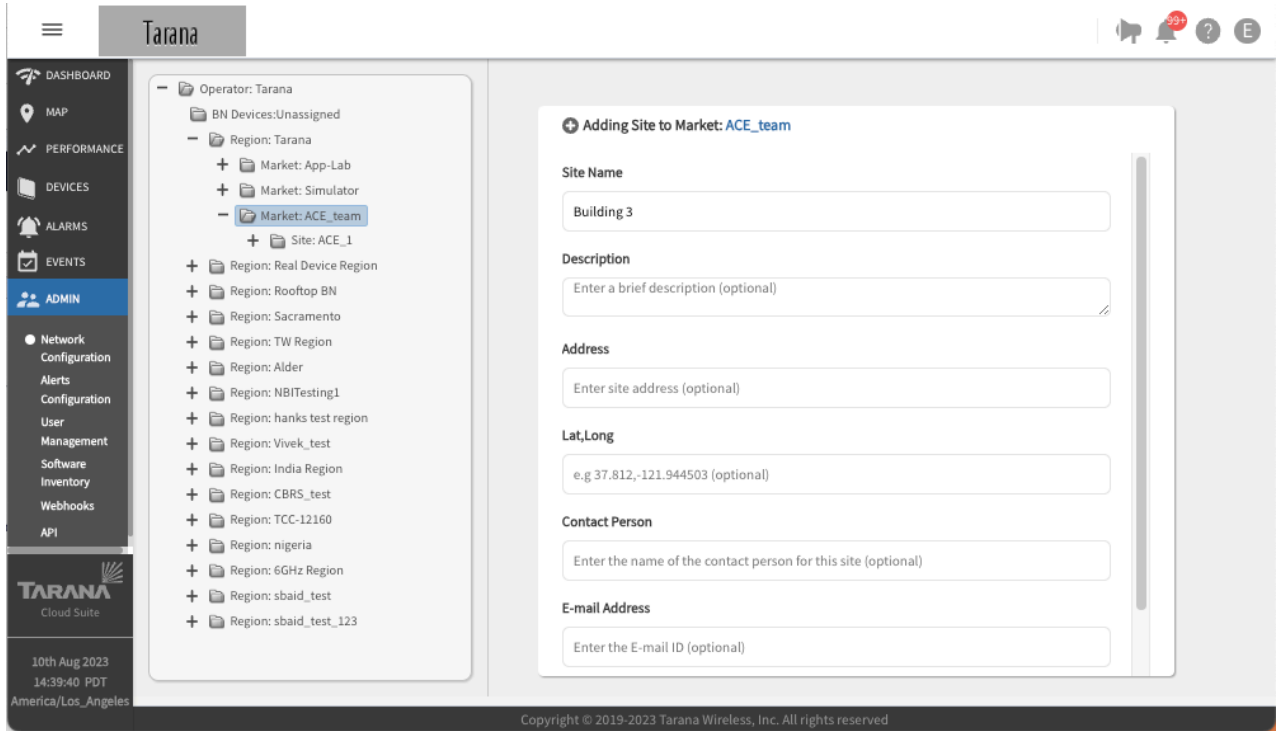
Manage Sites

To create 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:** Contact person for the site (optional).
- **E-mail Address:** 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**.



Create a New Site

Manage Cells

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

- **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.
- **Network Profile:** Defines the maximum distance of the remote node from the base node and the downlink / uplink ratio of the TDD frame. Use the drop down to select a value.

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

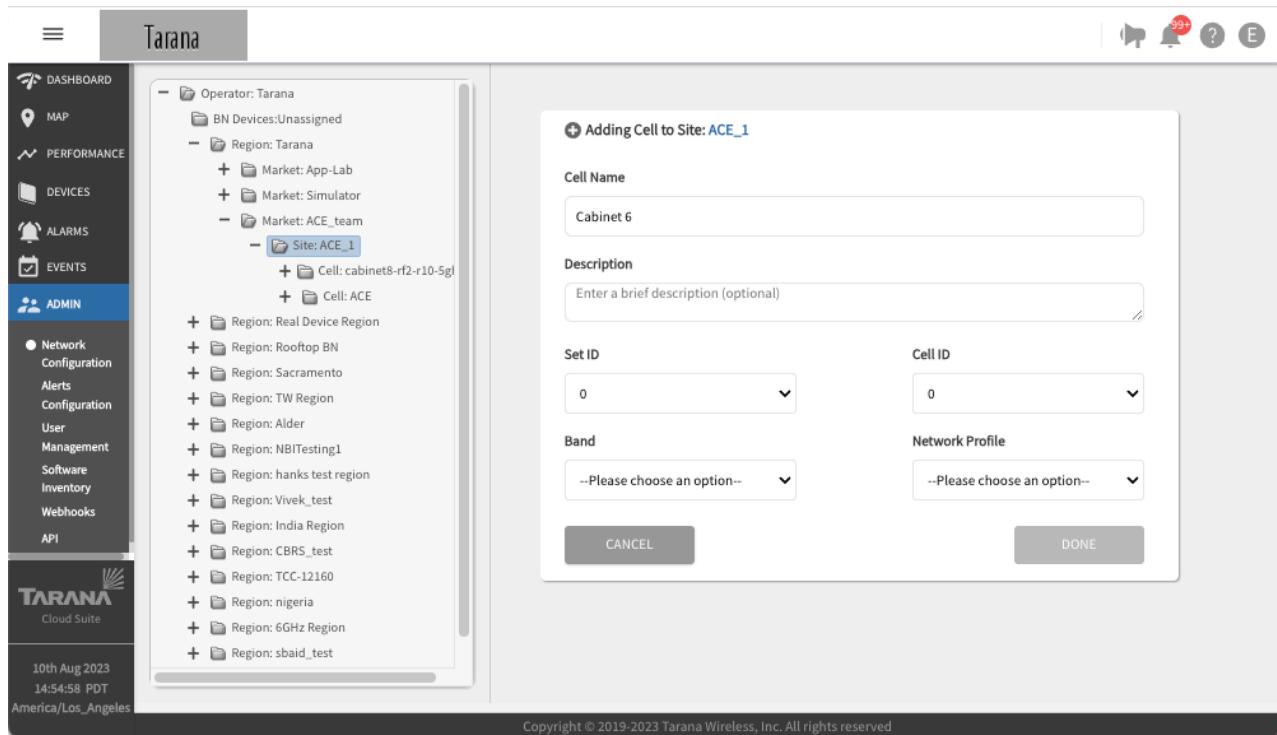


NOTE

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, you can edit the number of microseconds you want to offset the frame. Configuring frame alignment is simple, but determining whether alignment is required and the value of alignment can be complex. If you think that frame alignment might be an issue, you can contact Tarana for guidance.

Manage Sectors

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

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

- **Sector Name:**
- **Description:** An informative description (optional).
- **Carrier 0:** Bandwidth and frequency for the carrier 0 radio of the base node.
- **Carrier 1:** Bandwidth and frequency for the carrier 1 radio of the base node.

You can set a specific center frequency and width for each carrier. When choosing width, be sure the edge of the carrier doesn't overlap with an unavailable grant, or go beyond the CBRS band. Choose the center frequency based on the carrier width. For widths of 10 MHz and 30 MHz, the center frequency should be odd multiples of 5 MHz and for widths of 20 MHz and 40 MHz, it must be even multiples of 5 MHz. You must provide both center frequency and width.

- **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.
 - **DHCP Relay Agent:** Toggle to enable or disable. For details about the DHCP Relay Agent, see [DHCP Option 82 Support \[86\]](#).
 - **Downstream ARP:** Toggle to enable or disable.
- **Primary BN Settings:** Select Inherit Operator Settings or Override. Use the toggle to set a primary base node.
- **Software Auto-upgrade Policy:** Globally, you set this with [Operator Configuration \[72\]](#) but 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.

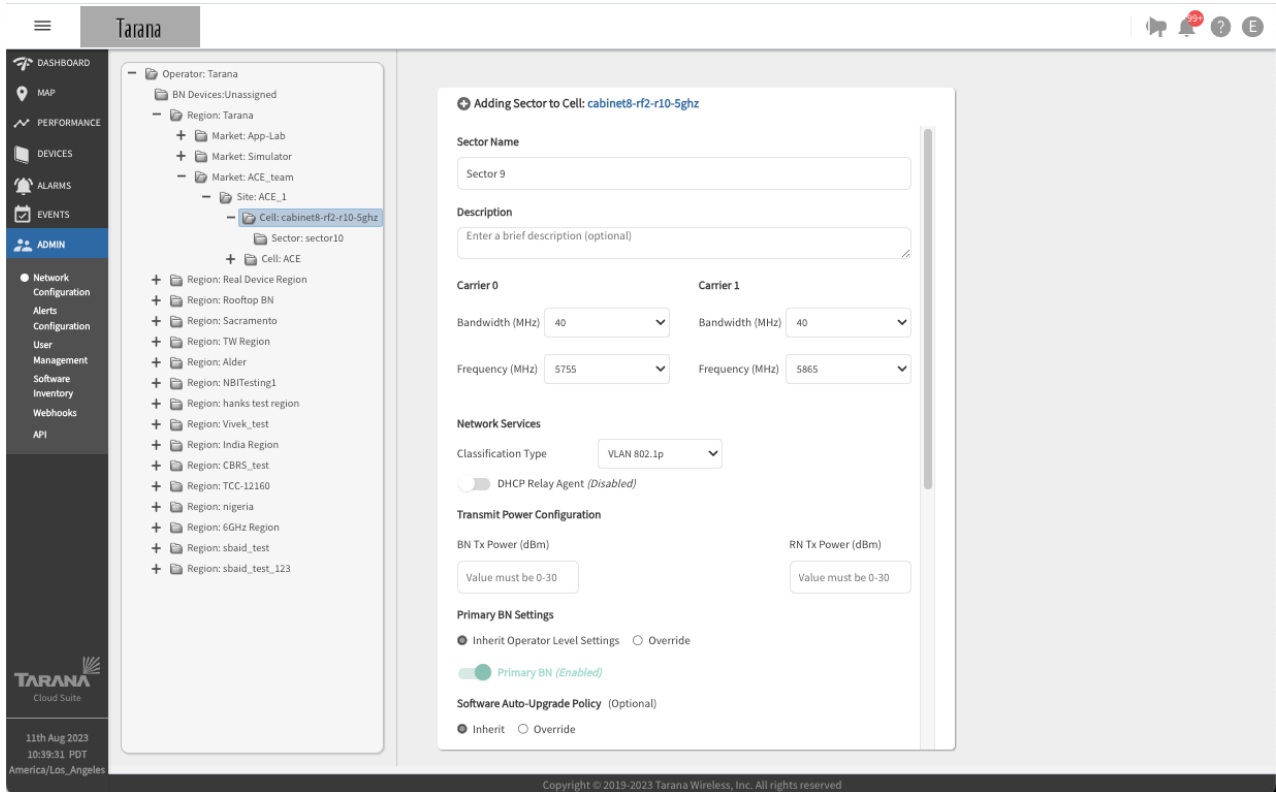
**NOTE**

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.

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** on the main screen.



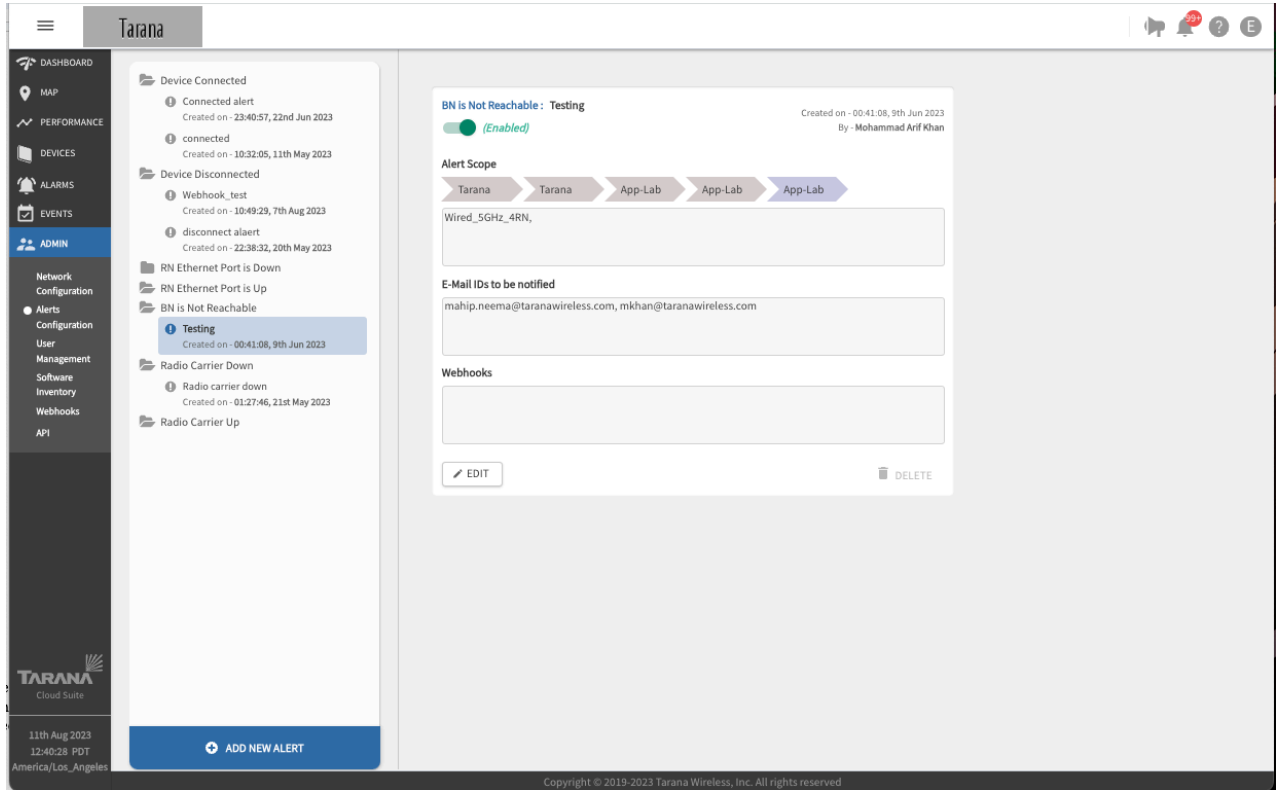
Create a New Sector

Once a sector is created, you can add a base node in the Devices unassigned folder to it.

Alerts Configuration

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 create, with any alerts created for that type. Select an alert to see its details.

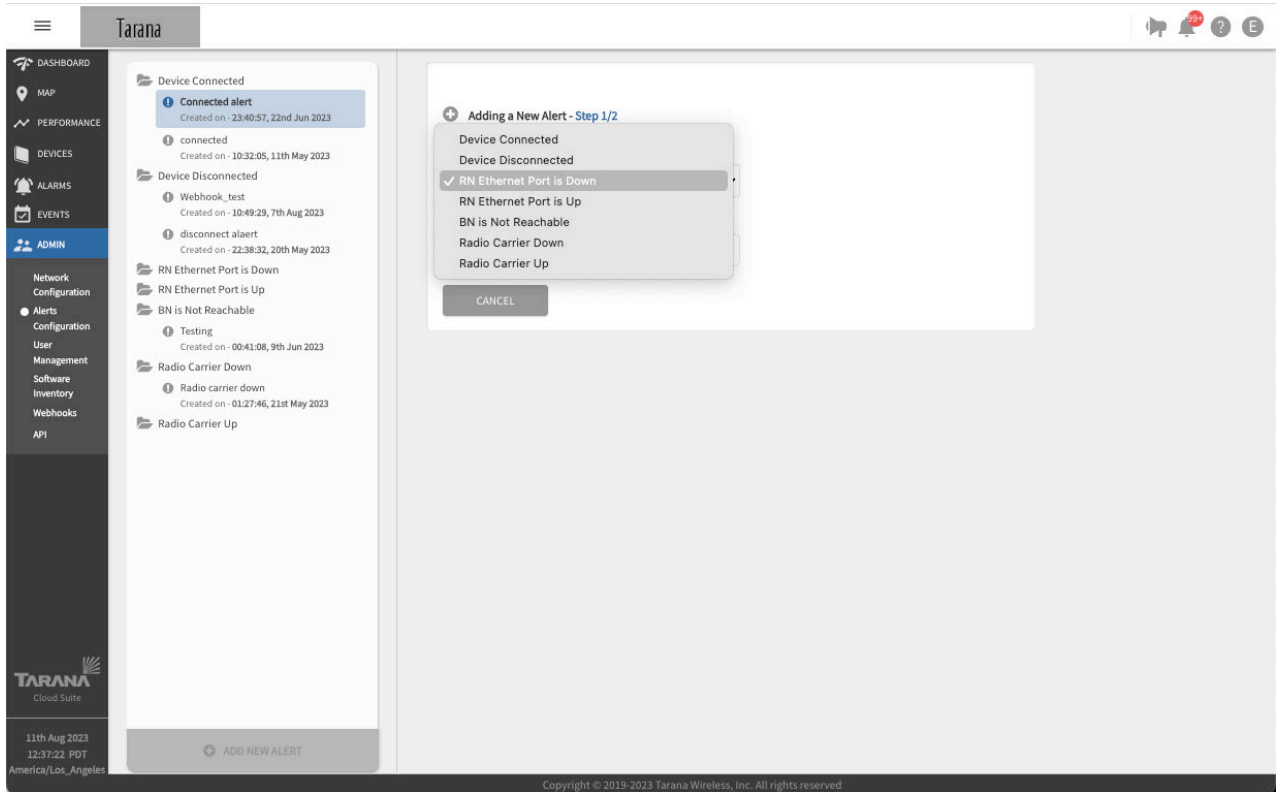


Alerts Configuration

To create an alert, follow these steps:

Select **Add New Alert**.

Select the alert type from the drop down.



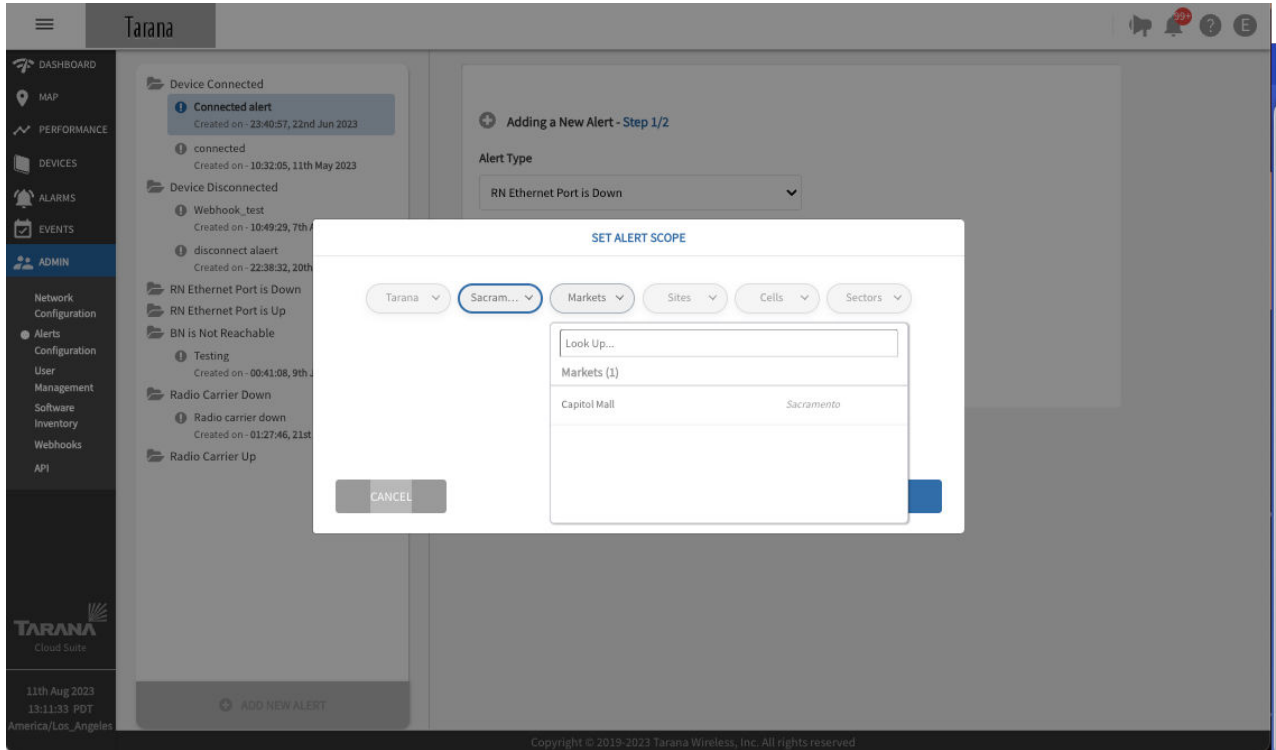
Select Alert Type

Enter a name for the alert.

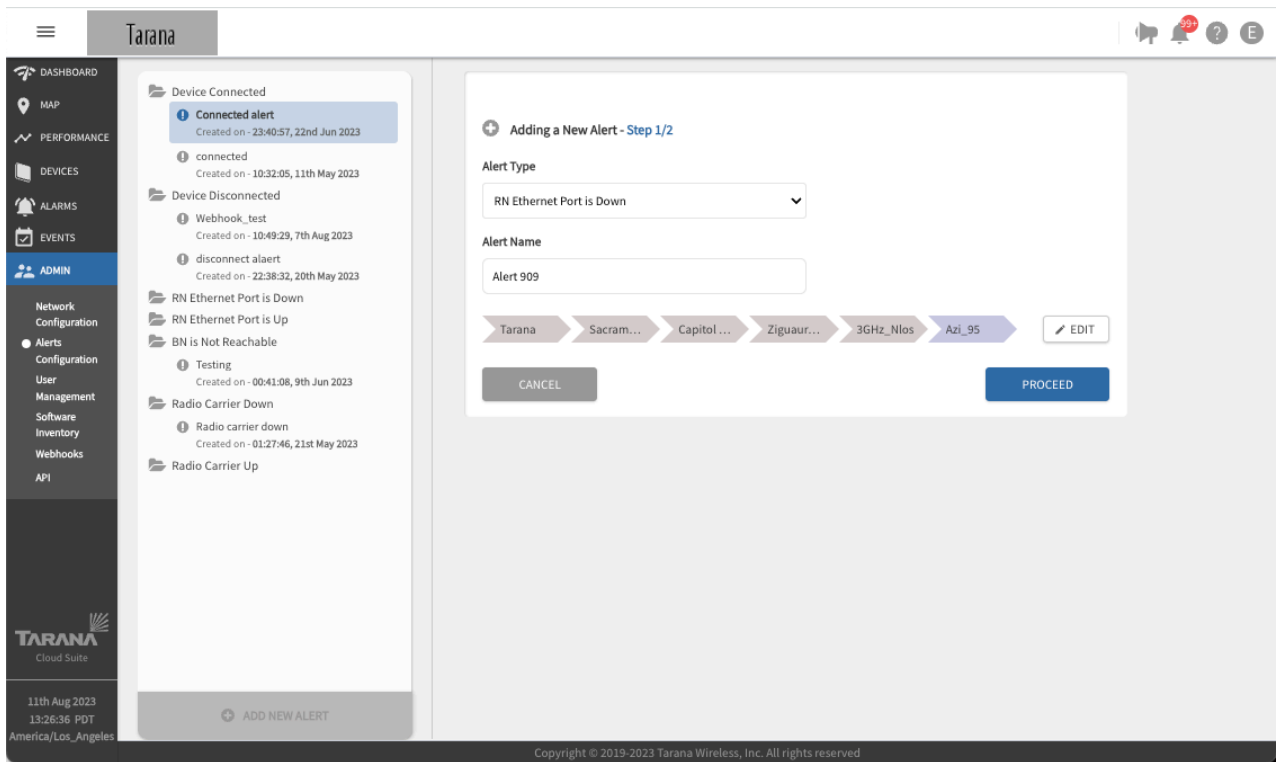
For Device Connected, Device Disconnected, Radio Carrier Down, and Radio Carrier Up, use the radio buttons to select the **Device Type**.

Select **Click to Set Alert Scope**, then define the alarm's scope by selecting the applicable Region, Market, Site, Cell, and Sector. Select **Apply**. The screen shows the scope you've selected. Click **Edit** if you want to change it.

G1 Administration Guide



Select Scope for Alert



Scope for Alert Selected

Select **Proceed**.

Select a link. Enter the email addresses that you want to receive this alert, separated by commas.

Check the boxes for any webhooks you want to receive this alert. Select **Done**.

The screenshot shows the Tarana Cloud Suite interface. On the left is a navigation menu with options like DASHBOARD, MAP, PERFORMANCE, DEVICES, ALARMS, EVENTS, and ADMIN. The main area displays a list of alerts, including 'Connected alert', 'connected', 'Device Disconnected', 'Webhook_test', 'disconnect alaert', 'RN Ethernet Port is Down', 'RN Ethernet Port is Up', 'BN is Not Reachable', 'Testing', 'Radio Carrier Down', and 'Radio Carrier Up'. A modal window titled 'Adding a New Alert - Step 2/2' is open, showing the configuration for a new alert. It includes a dropdown for 'Select Link(s) in Azi_95' with 'S142F1215000176' selected. Below this, there are checkboxes for 'Notify Using' options: 'Email' (checked), 'Webhooks', 'Vivek_Test', 'Test', and 'Webhook Testing'. A text input field contains 'support@help.com'. 'BACK' and 'DONE' buttons are at the bottom of the modal.

Alert is Added

Base Node Telemetry Streaming

Many companies use network management systems that aggregate telemetry from multiple network platforms. 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 either globally 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 sector level, you configure it as an exception to the global configuration, meaning that if you activate telemetry streaming globally, all sectors stream telemetry except those you specifically exclude at the sector level. If you deactivate telemetry streaming globally, no sectors stream telemetry data except those you specifically activate at the 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. Select the global organization name in the network entity tree, shown as Operator <global organization name>, to display global settings.
3. Select **Edit** at the bottom of the settings pane.
4. Enter the metrics collector end point information:
 - **Destination Address:** IP address of the host that receives the telemetry data from the base node.
 - **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 sector level. Follow these steps:

1. Navigate to Admin > Network Configuration.
2. Navigate to the sector in the network entity tree, then select the sector name to display the settings.
3. Select **Edit** at the bottom of the settings pane.

4. In the Metrics Collector End Point Configuration section, select **Override**.
5. Toggle the Streaming switch to activate the feature at the sector level.
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.

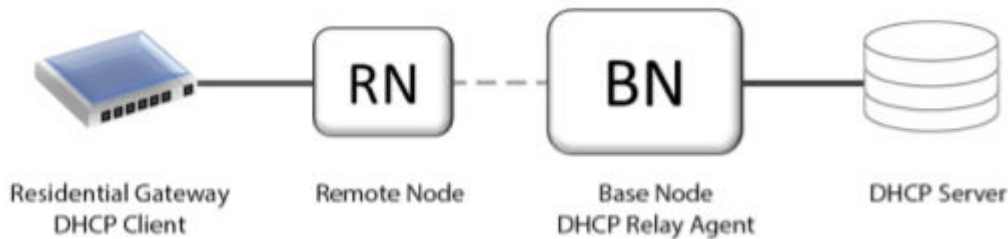
A device operating as an Option 82 relay agent for DHCP clients can enhance network access protection in these ways:

- 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.
- 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 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.



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.

To use the base node WebUI 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 Devices > List, then select BN to display the complete list of base nodes in the table.
3. Select the Serial Number link of the base node you want to configure.
4. Select the WebUI action and log in to the device through the web interface.
5. Navigate to Setup.
6. Enable DHCP Relay Agent.
7. Choose either Serial Number or MAC Address from the Remote / Circuit Identifier Type drop-down list.
8. Select Done to save the changes.

User Management

To create 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:

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.

Use the search bar in the top left-hand corner to search for a user using any field except Last Sign In and Creation Time. To sort in ascending or descending order, select the column heading. You can adjust the width of each column,

The screenshot shows the Tarana G1 Administration interface. The top navigation bar includes a menu icon, the 'Tarana' logo, and notification icons. The left sidebar contains navigation options: DASHBOARD, MAP, PERFORMANCE, DEVICES, ALARMS, EVENTS, and ADMIN (highlighted). Under ADMIN, there are sub-options: Network Configuration, Alerts Configuration, User Management, Software Inventory, Webhooks, and API. The main content area features a search bar 'Look Up Users...' and a table of users. The table has columns: Firstname, Lastname, Role, Email, Mobile, Last Sign In, and Creation Time. The table contains 12 rows of user data. At the bottom right of the table area, there is a 'Customize' button. The footer shows the date '14th Aug 2023 10:57:55 PDT' and the location 'America/Los_Angeles'. Copyright information is visible at the bottom: 'Copyright © 2019-2023 Tarana Wireless, Inc. All rights reserved.'

Firstname	Lastname	Role	Email	Mobile	Last Sign In	Creation Time
arif	khan	NOC L1 User	mkhan+200@taranawireless.com	(844) 601-8960	11 Jun 2023 21:46:14	11 Jun 2023 21:44:32
Vivek	Gupta	OP Admin	vivek.gupta+auth210@taranawireless.com	1234567890	21 May 2023 09:20:13	29 Mar 2023 11:22:29
Tilak	S	Tarana Engineer, TCS A...	Tilaks@taranawireless.com	123456789	10 Aug 2023 07:02:16	26 Apr 2023 19:46:24
Saurabh	Baid	OP Admin	sbaid+opadmin@taranawireless.com	9989740049	10 Aug 2023 09:07:21	18 Apr 2023 02:24:53
Sarang	J	OP Admin	sarang.jlbhakate@taranawireless.com	1234567890	11 Aug 2023 04:53:10	22 May 2023 03:46:11
Romish1	Padalia	OP Admin	rpadalia+1@taranawireless.com	999999999	06 Jul 2023 00:07:39	29 Mar 2023 01:59:29
Ravi	Yadav	OP Admin, Tarana Engi...	Byadav@taranawireless.com	1111111111	11 Jul 2023 10:51:40	09 Jun 2023 12:00:29
Praveen	Jain	Tarana Engineer, NOC ...	pjain@taranawireless.com	1234567890	Unavailable	12 Mar 2023 22:21:32
Prashant	Yadav	OP Admin	pyadav@taranawireless.com	124564563	18 Jun 2023 23:28:21	18 Jun 2023 23:10:50
Pankaj	Bunde	NOC Operator	pbunde@taranawireless.com	1234567890	13 Mar 2023 03:11:53	12 Mar 2023 22:20:48

To view more items, please change the table size or browse to the next page

Table Size: 10 Items 1-10 of 17 Showing Page: 1 of 2 Auto-Refresh (Off) Customize

Display Users

Select **Customize** in the bottom right corner to change the information displayed. Use **Select All** to select all information and **Clear** to deselect all information fields.

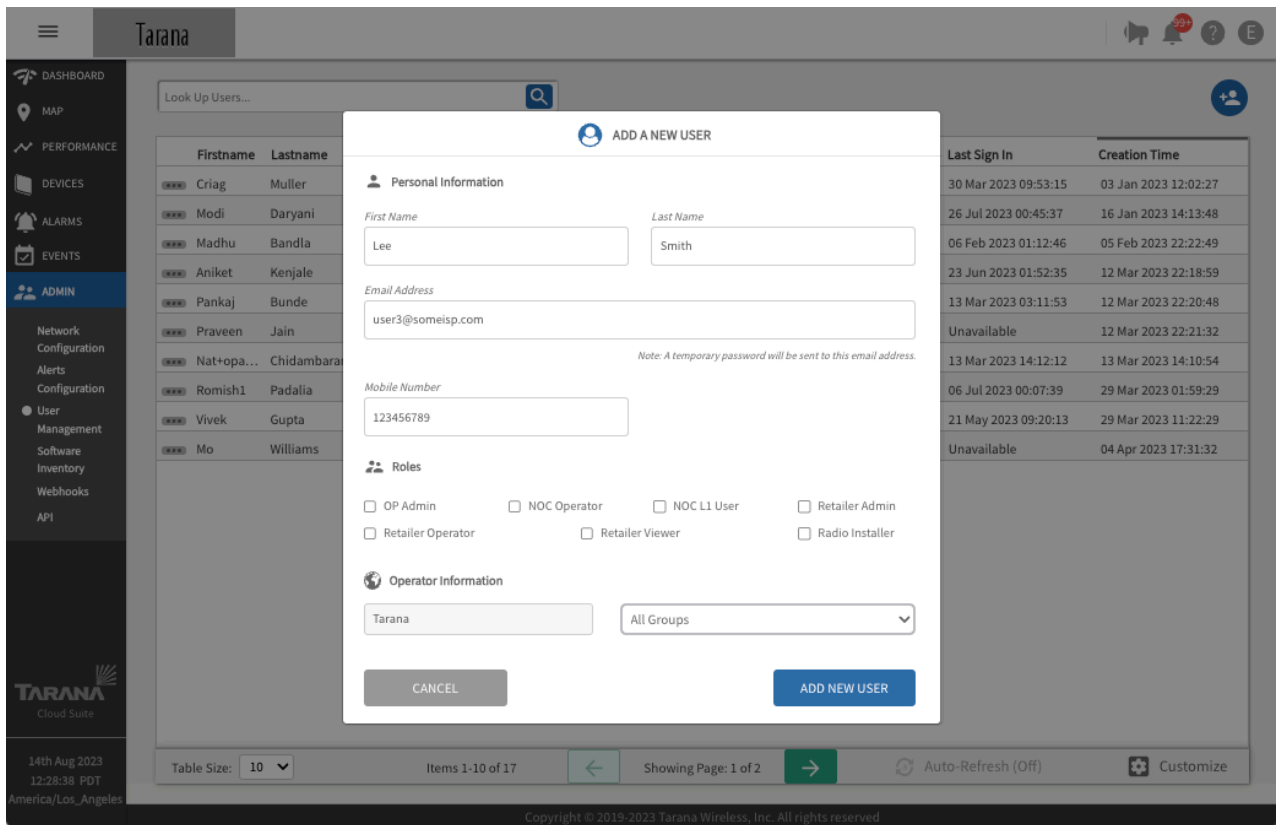
Create User Accounts

To create a new user account, select the **New User** icon (👤) in the top right corner, then enter this 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.
- Check the box for the **Role** you want to assign to this user. Roles assign administrative permission to the new user and are defined as follows:
- **NOC L1 User:** A NOC L1 User has permission to do any of these actions:
 - View Dashboard, Map, Devices, Performance, Alarms, Events, Single Device pages.
 - View or edit their own user profile information and metadata.
- **NOC Operator:** NOC Operator can perform write functions on network devices. Includes all permissions for NOC L1 as well as these device operations:
 - Upgrade software
 - Create snapshots
 - Reboot device
- **OP Admin:** Includes all permissions for NOC Operator as well as these operations:
 - Create or configure networks

- Create or configure users and assign roles
Hover over each checkbox to see a description of the role.
- **Retailer Admin:** Retailer roles have limited view of base nodes and no write permissions for them or for network entities. Includes all permissions for OP Admin as well as these operations:
 - Deny permissions to hide telemetry columns from the BN table
 - Deny permission to not allow launching the BN page
- **Retailer Operator:** Includes all permissions for NOC Operator as well as these operations:
 - Deny permissions to hide telemetry columns from the BN table
 - Deny permission to not allow launching the BN page
- **Retail Viewer:** Includes all permissions for NOC L1 as well as these device operations:
 - Deny permissions to hide telemetry columns from the BN table
 - Deny permission to not allow launching the BN page
- **Radio Installer:** Has mapbox API-related permissions.
- **Operator Information:** Use the drop down list to indicate groups that should include this user.

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



Add User Account

Edit, Delete, or Reset Password for User Accounts

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

To manage a user account, select the three dot menu (⋮) and select one of these options:

Edit Info: Enter the information you want to change and select **Update**. You can't edit the email address. If the address changes you must delete the account and create a new one.

Resend Password: Enter an email address to send a password link and select **Confirm**.

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

The screenshot shows the Tarana administration interface. On the left is a navigation sidebar with options like DASHBOARD, MAP, PERFORMANCE, DEVICES, ALARMS, EVENTS, and ADMIN. The ADMIN section is expanded to show options like Network Configuration, Alerts, Configuration, User Management, Software Inventory, Webhooks, and API. The main area displays a table of users with the following data:

Firstname	Lastname	Role	Email	Mobile	Last Sign In	Creation Time
Saurabh	Baid	OP Admin	sbaid+opadmin@taranawireless.com	9989740049	10 Aug 2023 09:07:21	18 Apr 2023 02:24:53
Tilak	S	Tarana Engineer, TCS ...	Tilaks@taranawireless.com	123456789	10 Aug 2023 07:02:16	26 Apr 2023 19:46:24
Sarang	J	OP Admin	sarang.jibhakate@taranawireless.com	1234567890	11 Aug 2023 04:53:10	22 May 2023 03:46:11
Ravi	Yadav	OP Admin, Tarana Eng...	Ryadav@taranawireless.com	1111111111	11 Jul 2023 10:51:40	09 Jun 2023 12:00:29
arif	khan	NOC L1 User	mkhan+200@taranawireless.com	(844) 601-8960	11 Jun 2023 21:46:14	11 Jun 2023 21:44:32
Prashant	Yadav	OP Admin	pyadav@taranawireless.com	124564563	18 Jun 2023 23:28:21	18 Jun 2023 23:10:50
Elizabeth	Fox	OP Admin	efox@taranawireless.com	1111111111	10 Aug 2023 09:45:15	24 Jul 2023 15:30:21
Lee	Smith	NOC L1 User	user3@someisp.com	123456789	Unavailable	14 Aug 2023 12:33:23

A context menu is open over the last row, showing options: EDIT INFO, RESEND PASSWORD, and DELETE USER. At the bottom of the interface, there are controls for Table Size (10), Items 11-18 of 18, Showing Page: 2 of 2, Auto-Refresh (Off), and a Customize button.

Manage a User Account

Software Inventory

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.

The screenshot displays the Tarana Cloud Suite Software Inventory page. The interface includes a sidebar with navigation options: DASHBOARD, MAP, PERFORMANCE, DEVICES, ALARMS, EVENTS, ADMIN, Network Configuration, Alerts, Configuration, User Management, Software Inventory (selected), Webhooks, and API. The main content area is titled 'Software Inventory' and features a search bar, a table of software images, and a detailed view of a selected image.

Software Image	Tags
SYS.A3.R10.XXX.1.202.017.00	Stable
SYS.A3.B10.XXX.1.202.014.00	Beta
SYS.A3.R10.XXX.1.202.010.00	Beta
SYS.A3.B10.XXX.1.202.010.00	Beta
SYS.A3.R10.XXX.0.997.031.00	Stable
SYS.A3.B10.XXX.0.997.031.00	Stable
SYS.A3.R10.XXX.1.202.004.00	Beta
SYS.A3.B10.XXX.1.202.004.00	Beta
SYS.A3.R10.XXX.1.202.002.00	Beta
SYS.A3.R10.XXX.1.201.029.00	Beta
SYS.A3.B10.XXX.1.201.029.00	Beta
SYS.A3.R10.XXX.1.201.023.00	Beta
SYS.A3.B10.XXX.1.201.023.00	Beta
SYS.A3.R10.XXX.1.201.020.00	Beta

The detailed view for the selected image (SYS.A3.R10.XXX.1.202.017.00) shows the following information:

- File Size: 105.9 MB
- Published on: 03:44 am Aug 14 2023
- Build Date: 10:36 pm Aug 11 2023
- By: mahip.neema@taranawireless.com
- Tags: Stable

At the bottom of the page, the date and time are shown as 14th Aug 2023, 15:14:27 PDT, America/Los_Angeles. The copyright notice reads: Copyright © 2019-2023 Tarana Wireless, Inc. All rights reserved.

Software Inventory

Manage Webhooks and Configure Alerts

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:

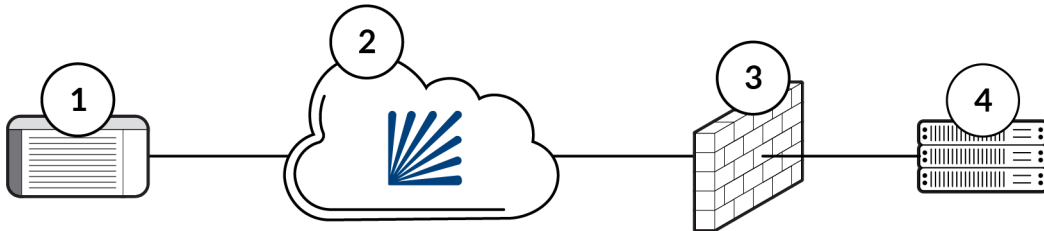
- Device disconnected
- Device reconnected
- Remote node Ethernet port down
- Remote node Ethernet port up
- Base node unreachable
- Radio carrier down
- Radio carrier up

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	Tarana cloud
3	Local router firewall or access control list (ACL). The ACL must allow incoming webhook messages from TCS.
4	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.

To create, edit, or test webhooks, select **Admin > Webhooks** from the navigation pane.

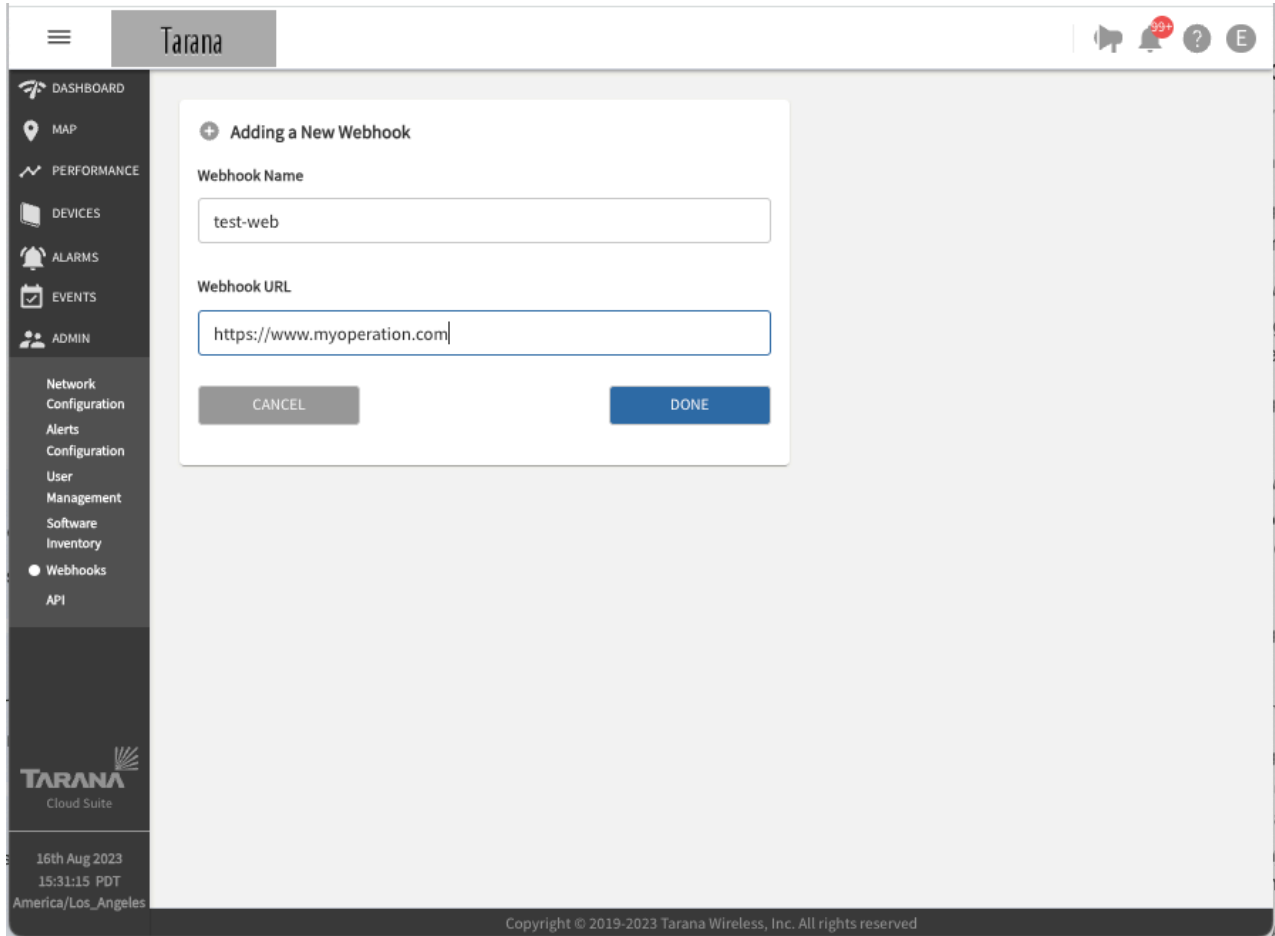
Add a Webhook

To create a new webhook, follow these steps:

1. Select **Add New Webhook**.
2. 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 create a webhook, TCS automatically generates a secure secret, which you can view when you test the webhook.

Test a Webhook

To test a webhook, follow these steps:

1. Choose the webhook that you want to test from the list of available webhooks.
2. Select Test Webhook.
3. 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.

The screenshot shows the Tarana Cloud Suite interface. The left sidebar contains navigation options: DASHBOARD, MAP, PERFORMANCE, DEVICES, ALARMS, EVENTS, ADMIN, Network Configuration, Alerts Configuration, User Management, Software Inventory, Webhooks (selected), and API. The main content area is titled 'Webhooks' and features a table with the following data:

Name	Created On
Webhook Testing	22:16:02 20 May 2023
Test	10:33:25 07 Aug 2023
Vivek_Test	10:46:02 07 Aug 2023

Below the table is a blue button labeled '+ ADD NEW WEBHOOK'. To the right, a detailed view of the 'Webhook Testing' entry is shown, including a 'TEST WEBHOOK' button, creation details (Created on: 22:16:02 20 May 2023, By Mahip Neema), URL (https://webhook.site/29aeb577-e77a-4da4-88ff-1f356a911328), and a masked secret key. There are also 'EDIT' and 'DELETE' buttons.

At the bottom of the interface, the date and time are shown as '16th Aug 2023 15:28:00 PDT America/Los_Angeles' and the copyright notice 'Copyright © 2019-2023 Tarana Wireless, Inc. All rights reserved' is visible.

Test a Webhook

For details about configuring alerts, see [Alerts Configuration \[80\]](#).

API

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.

Tarana Cloud Suite (TCS) supports OpenAPI v3 compliant REST API. Using the Tarana-provided API key, the user can invoke operations that they're authorized to perform.

Tarana NorthBound APIs

This is Tarana Northbound APIs Based on OpenAPI 3.0 specification.

Servers: Authorize

- Operator** Supported operation on Operator
 - GET** /v1/network/operators/custom-attributes Get custom attributes names for operator
 - POST** /v1/network/operators/custom-attributes Set custom attributes names for operator
 - GET** /v1/network/operators/orphans Get Orphan devices
 - GET** /v1/network/operators/devices Get devices
- Region** Supported operation on Region
- Market** Supported operation on Market
- Site** Supported operation on Site
- Cell** Supported operation on Cell
- Sector** Supported operation on Sector
- Retailer** Supported operation on Retailer
- Device** Update Device attributes
- Device Operations** Supported operations on Device
- User** Supported operations on User
- Radio Operations** Supported operations on Radio

API Management

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

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.

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. Swagger documentation is always current because it takes its content from the API.

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

Swagger documentation appears as a collapsed accordion list with only the top-level items visible, as shown above. When you select an item the section expands to review the available API calls. 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.

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, such as Operator or Region, to reveal the individual API call 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.

Each API call has a Try It Out button that you can select to activate the parameter fields and an Execute button, which you 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.
- **Server Response Header:** Indicates the content length and media type.

Device Web UI

The base node has 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. You can't access the remote node web UI except by proxying from TCS once the remote node is deployed.

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 NOC Operator rights in TCS. Web UI login and password information for this device is required.



NOTE

Web UI access for both the base node and remote node is available, but you shouldn't use it for configuration changes once you've completed the initial deployment. 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 Options

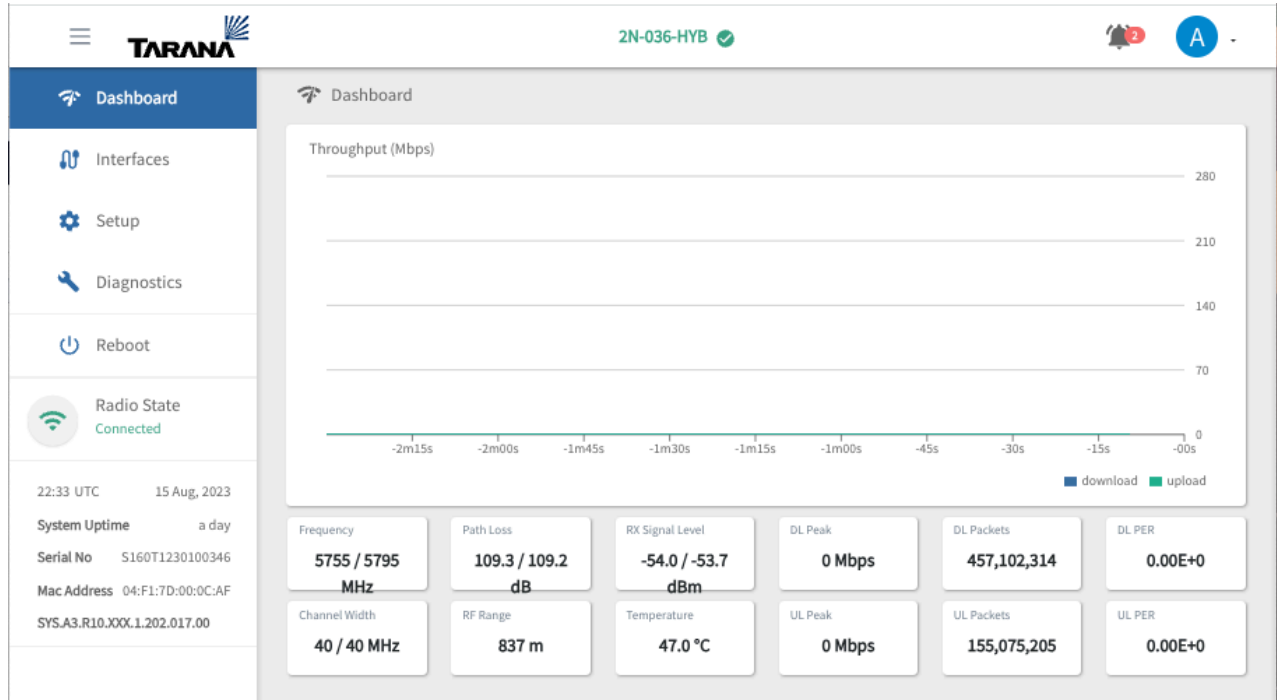
To view or edit Web UI options, select from the navigation pane. Options differ for Base Nodes and Remote Nodes.

Web UI Dashboard (Remote Node Only)

When you log in to the web UI, the device dashboard displays information about the remote 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.

Web UI Base Node Interfaces

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

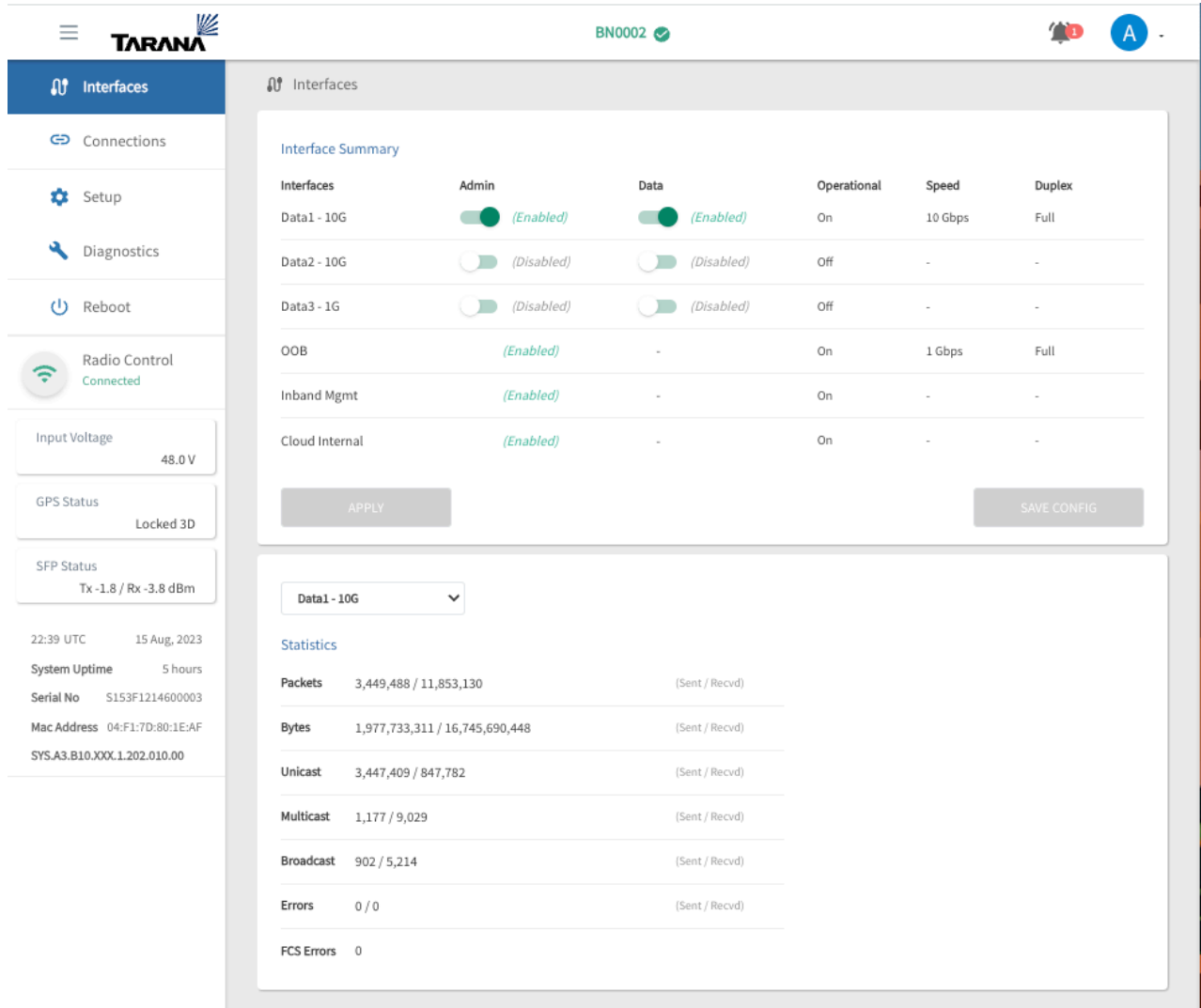
Use the toggles in the top box to switch between different modes on each network interface.

**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 bottom 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)

Web UI 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 bottom box displays MAC addresses and ports.

The screenshot shows the Tarana Web UI interface. The top navigation bar includes the Tarana logo, a user profile icon, and a notification bell. The left sidebar contains navigation links: Dashboard, Interfaces (selected), Setup, Diagnostics, and Reboot. Below the sidebar, there is a 'Radio State' section showing 'Connected' and system information including UTC time, system uptime, serial number, and MAC address.

The main content area is titled 'Interfaces' and contains an 'Interface Summary' table:

Interfaces	Admin	Toggle PHY	Operational	Speed	Duplex
Subscriber - 1G POE	(Enabled)	TOGGLE	On	1 Gbps	Full
Cloud Internal	(Enabled)		On	-	-

Below the summary table, there is a dropdown menu for 'Subscriber - 1G POE' and a 'Statistics' section:

Metric	Value	Direction
Packets	448,618,502 / 153,624,310	(Sent / Recvd)
Bytes	621,901,747,897 / 137,280,412,528	(Sent / Recvd)
Unicast	0 / 153,623,828	(Sent / Recvd)
Multicast	0 / 57	(Sent / Recvd)
Broadcast	0 / 425	(Sent / Recvd)
Errors	0 / 0	(Sent / Recvd)
FCS Errors	0	

At the bottom, there is a table listing MAC addresses and their corresponding ports:

MAC Address	Port
04:f1:7d:00:0c:af	CPU
70:88:6b:82:9d:22	Data
70:88:6b:85:88:9e	Modem
70:88:6b:8b:5a:06	Modem
04:f1:7d:00:00:00	Modem
04:f1:7d:80:29:f4	Modem

The bottom of the page shows pagination controls: 'Items 1-6 of 6', 'Showing Page: 1 of 1', and 'Table Size: 10'.

Web UI Network Interface Summary and Statistics (Remote Node)

Web UI 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).

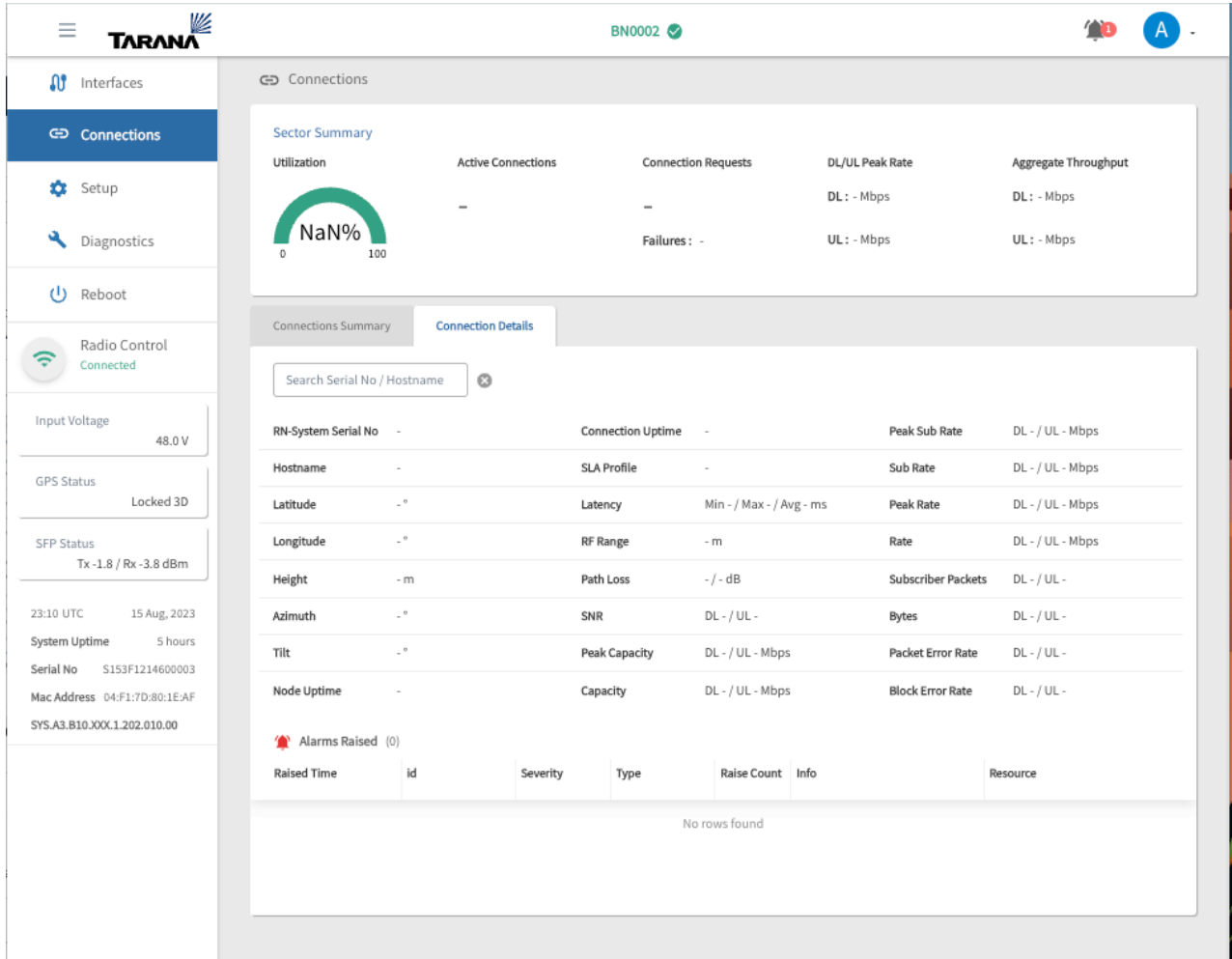
- **Aggregate Throughput:** Amount of data throughput being passed through the base node, by connection direction (download and upload).
- **Failures:** The number of failures.

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

Web UI Base Node Setup

When you log in to the base node web UI, you see the device setup screen. This displays 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.

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 \[129\]](#).
- **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 \[86\]](#).
 - **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):** NTP Server is blank by default and is not used because the base node uses GPS for synchronization. However, if you need this value for lab testing (when the base node doesn't have a view of the sky for GPS synchronization), configure an NTP server using an IP address or FQDN.
 - **DNS Server IP(s):** Domain Name Servers (DNS) used to resolve the TCS URL. Enter servers as IP addresses.

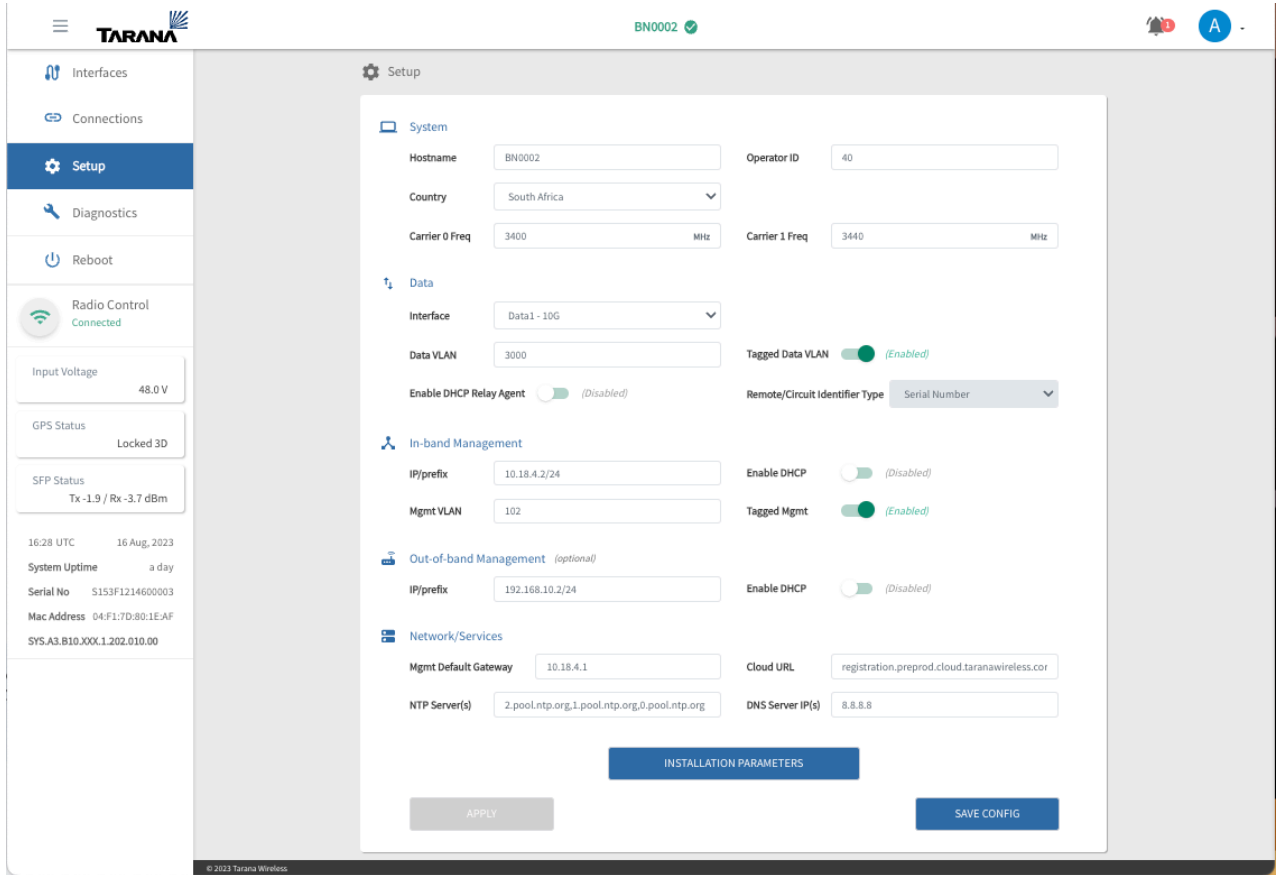
Notes

- These values are reserved on the base node and you can't use them as part of the configuration:
 - Reserved VLANs: 4092, 4093, and 4094
 - Reserved IP subnets: 172.27.0.0/18 and 10.240.0.0/12
- The Data VLAN (optional) 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.
- You can't use DHCP for both In-band and Out-of-band management IP addresses.
- 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)
- 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.
- If you made any changes, select **Save Config**. New configuration settings aren't applied until you select **Apply** or the system is rebooted.



NOTE

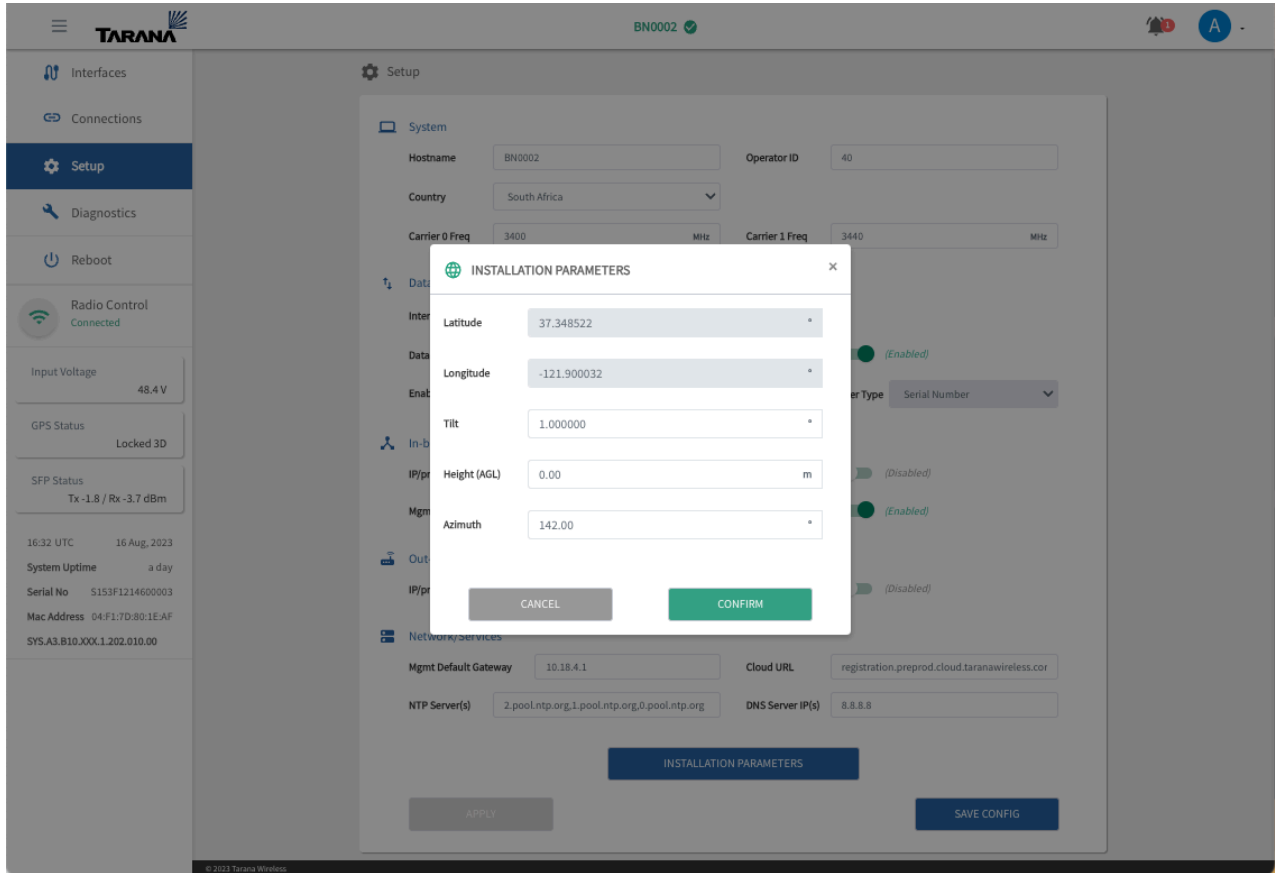
For CBRS installations, change the Cloud URL to:
registration.trial.taranawireless.com:443



Base Node Configuration Setup

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

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



Setup Installation Parameters

Web UI 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 changes to red to indicate active alarms that require attention.

To create or change 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 disconnects and searches for a new base node.



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. 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 \[129\]](#).
- **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 \[44\]](#) 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.

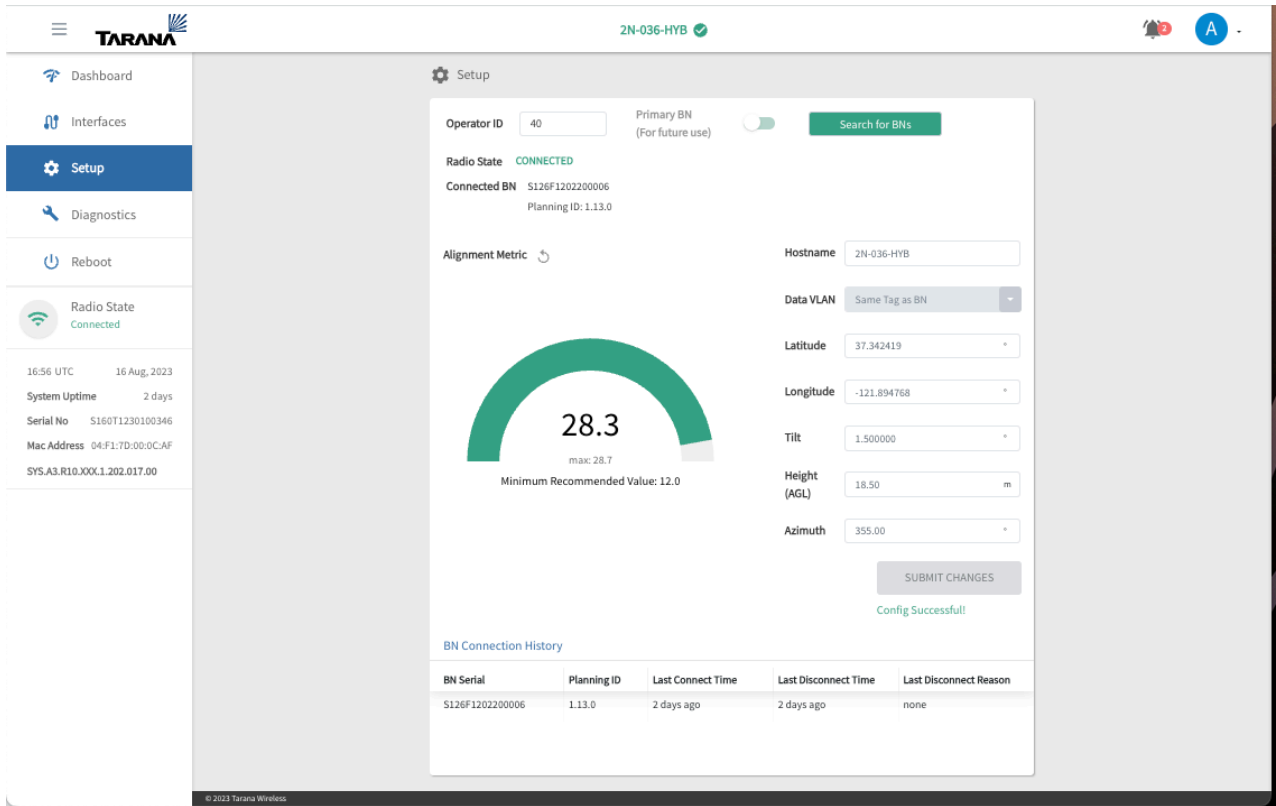
If you made any changes, select **Submit Changes**. For a 5GHz remote node, configuration changes are applied immediately. If this is a CBRS remote node, you see a pop up where you must verify the location metrics and enter the CPI ID.

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.

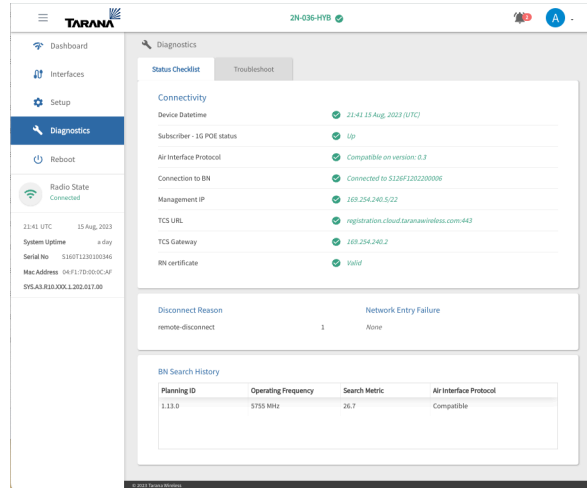
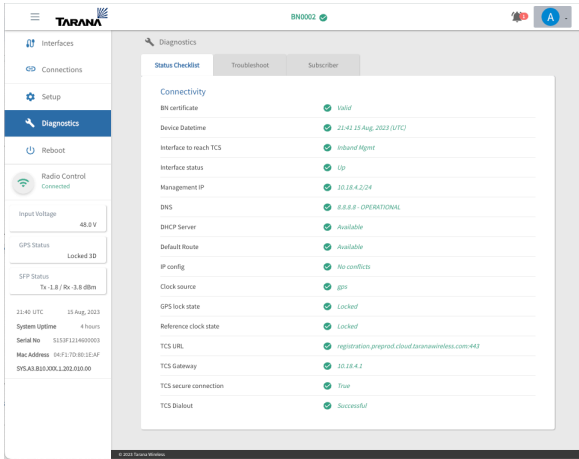


Remote Node Configuration Setup

Web UI Diagnostics

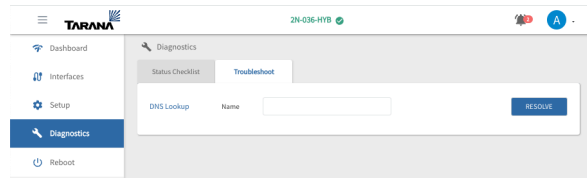
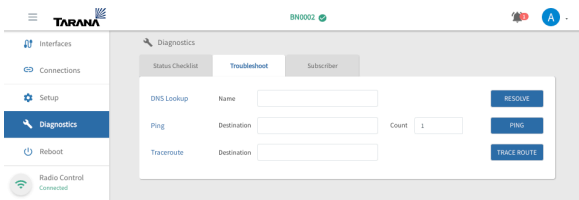
To view a checklist of key system status indicators, select **Diagnostics** from the navigation pane. The base node interface shows three tabs: Status Checklist, Troubleshoot, and Subscriber. The remote node interface shows Status Checklist and Troubleshoot.

G1 Administration Guide



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.

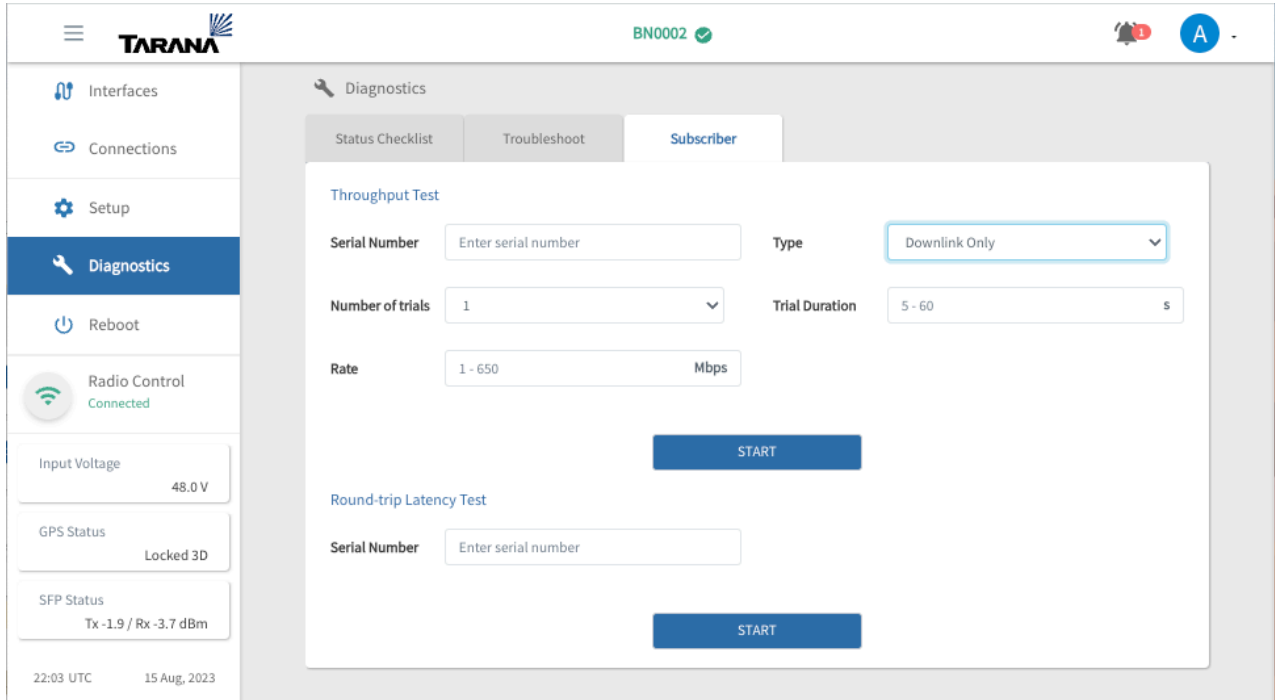


Base Node and Remote Node Diagnostics (Troubleshoot Tab)

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)

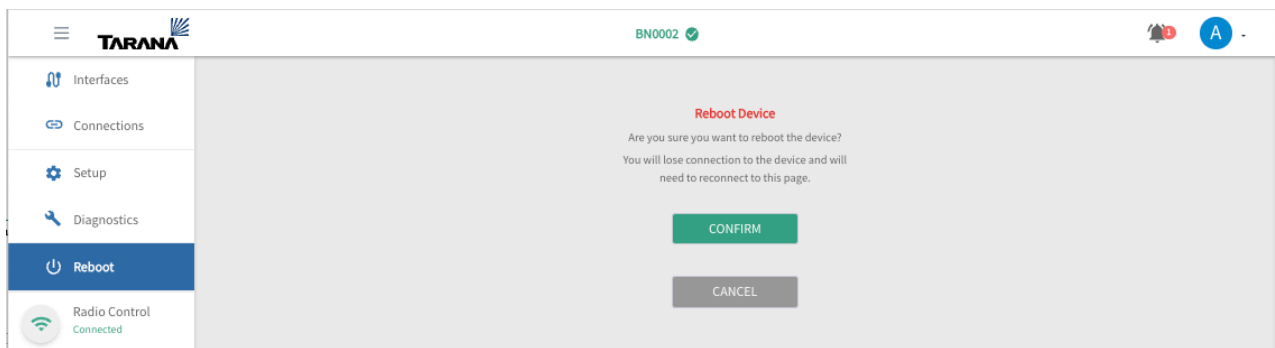
Web UI Device Reboot

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

Web UI Radio Control

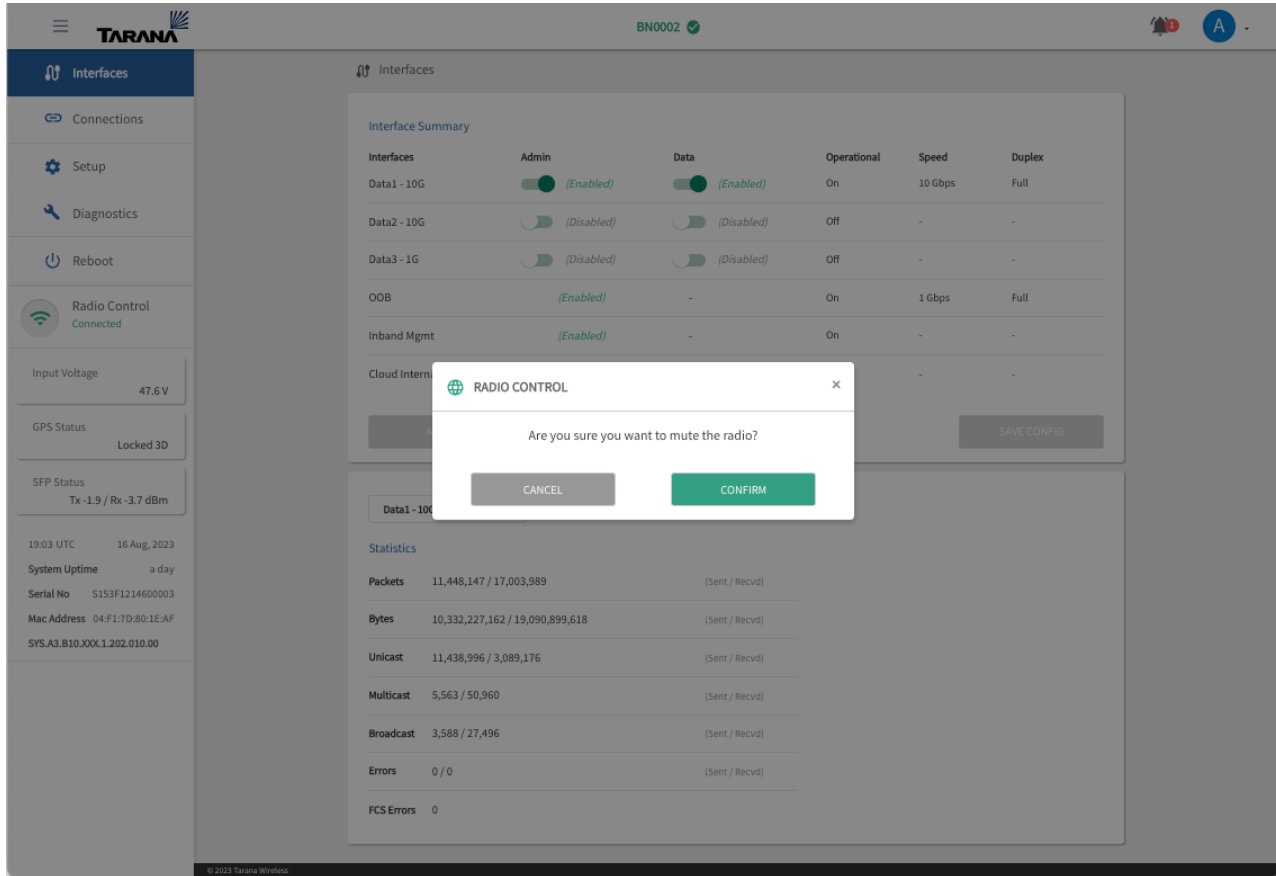
The device's radio state appears in the navigation pane.

To mute or unmute the radio on a base node, select the green **Radio Control** icon (📶) from the navigation pane. TCS asks you to confirm that you want to mute the radio. Select **Cancel** or **Confirm**.



NOTE

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



Mute or Unmute Base Node Radio

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 With TCS, 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.

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 \[124\]](#).

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.

The screenshot shows the Tarana web UI Setup page. The interface includes a sidebar with navigation options: Dashboard, Interfaces, Setup (selected), Diagnostics, Reboot, and Radio State (Connected). The main content area displays the following information:

- Operator ID:** 40
- Primary BN (For future use):**
- Radio State:** CONNECTED
- Connected BN:** S126F1202200006
- Planning ID:** 1.13.0
- Alignment Metric:** 28.3 (max: 28.7, Minimum Recommended Value: 12.0)
- Hostname:** 2N-036-HYB
- Data VLAN:** Same Tag as BN
- Latitude:** 37.342419
- Longitude:** -121.894768
- Tilt:** 1.500000
- Height (AGL):** 18.50 m
- Azimuth:** 355.00

A "SUBMIT CHANGES" button is visible, and a "Config Successful!" message is displayed below it. A "BN Connection History" table is also present:

BN Serial	Planning ID	Last Connect Time	Last Disconnect Time	Last Disconnect Reason
S126F1202200006	1.13.0	2 days ago	2 days ago	none

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.

The screenshot displays the 'Setup' configuration page for a remote node. The interface includes a left-hand navigation menu with options like Dashboard, Interfaces, Setup (highlighted), Diagnostics, Reboot, and Radio State (Connected). The main content area shows the 'Setup' configuration for the node '2N-036-HYB'. Key fields include:

- Operator ID:** 40
- Radio State:** CONNECTED
- Connected BN:** S126F1202200006
- Alignment Metric:** A gauge showing 28.3, with a maximum of 28.7 and a minimum recommended value of 12.0.
- Hostname:** 2N-036-HYB
- Data VLAN:** Same Tag as BN
- Latitude:** 37.342419
- Longitude:** -121.894768
- Tilt:** 1.500000
- Height (AGL):** 18.50 m
- Azimuth:** 355.00

 A 'SUBMIT CHANGES' button is visible, along with a 'Config Successful!' message. Below the configuration fields is a 'BN Connection History' table:

BN Serial	Planning ID	Last Connect Time	Last Disconnect Time	Last Disconnect Reason
S126F1202200006	1.13.0	2 days ago	2 days ago	none

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 Edit icon.

For more information on viewing the SLA for the remote node, see [Remote Node SLA \[51\]](#).

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.

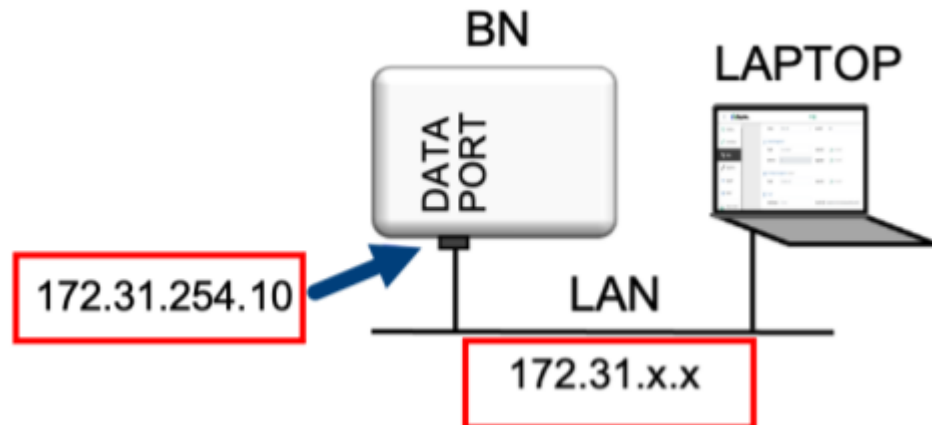
Verify that the input voltage from the base node power supply can compensate for the voltage drop across the cable run to the base node. Proper installation requires calculation of the voltage drop across the entire power cable.

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

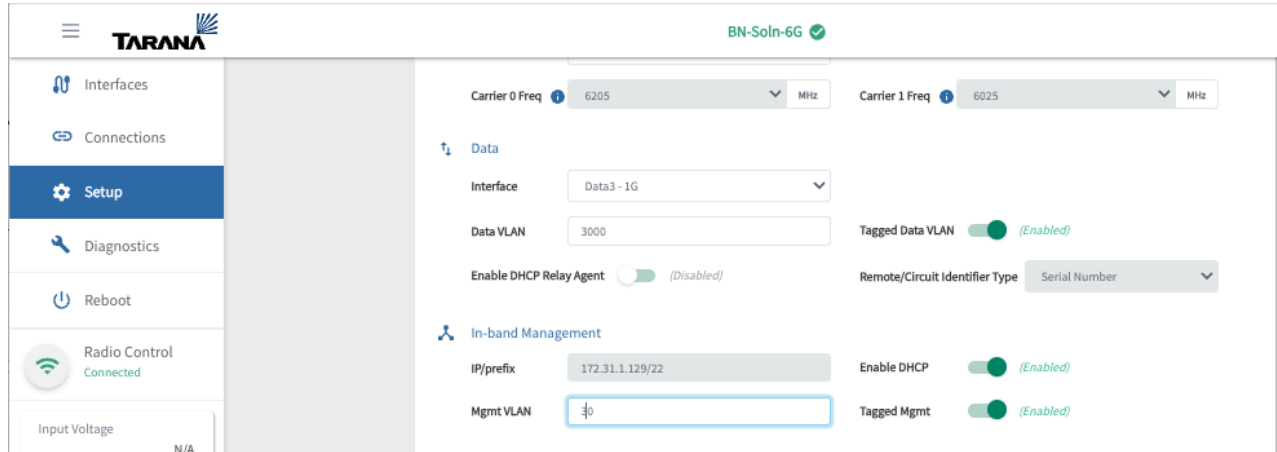
If data traffic is flowing in only one direction across a Tarana RF link (between the base node and remote node), this could be because data traffic coming into the base node is untagged when it should be tagged. Traffic coming into any of the data ports (Data1, Data2, Data3) must be tagged with the 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.

- 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:

- 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://192.168.11.2>
This example uses the default in-band management IP address. If this IP was changed at installation, use the appropriate address.
- After logging into the web UI, select **Setup** from the navigation pane.
- Check the DNS Servers listed under Network Services. Verify the IP address is correct.
- Select **Save Config**.

If the DNS Server information is correct:

- Use ping to check the configured servers are responding.
- 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:

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

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 careful planning is required 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** () > **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**.

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** () > **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 (⚙) > 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**.

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)

^aMay 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)

^aIndicates one or more of the following:

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

^bIndicates 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)

^aMay 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)

^aIndicates one or more of the following:

- Alarm raised

- Lower modulation
- Packet errors above threshold
- Upgrade failed

^bIndicates 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)

TCS 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 type alarms.

G1 Administration Guide

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
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

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 first consideration in Data VLAN configuration is the fact that by default the base node's data ports (DATA1, DATA2, DATA3) require ingressing and egressing data frames to be tagged (802.1q). By default, the base node tags egressing data frames 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 so there's no Data VLAN and traffic is untagged.

The screenshot displays the Tarana web UI for a base node. The left sidebar contains navigation options: Interfaces, Connections, Setup (highlighted), Diagnostics, Upgrade, Reboot, Radio Control (Connected), and Snapshot. The main content area is titled 'Setup' and shows the following configuration sections:

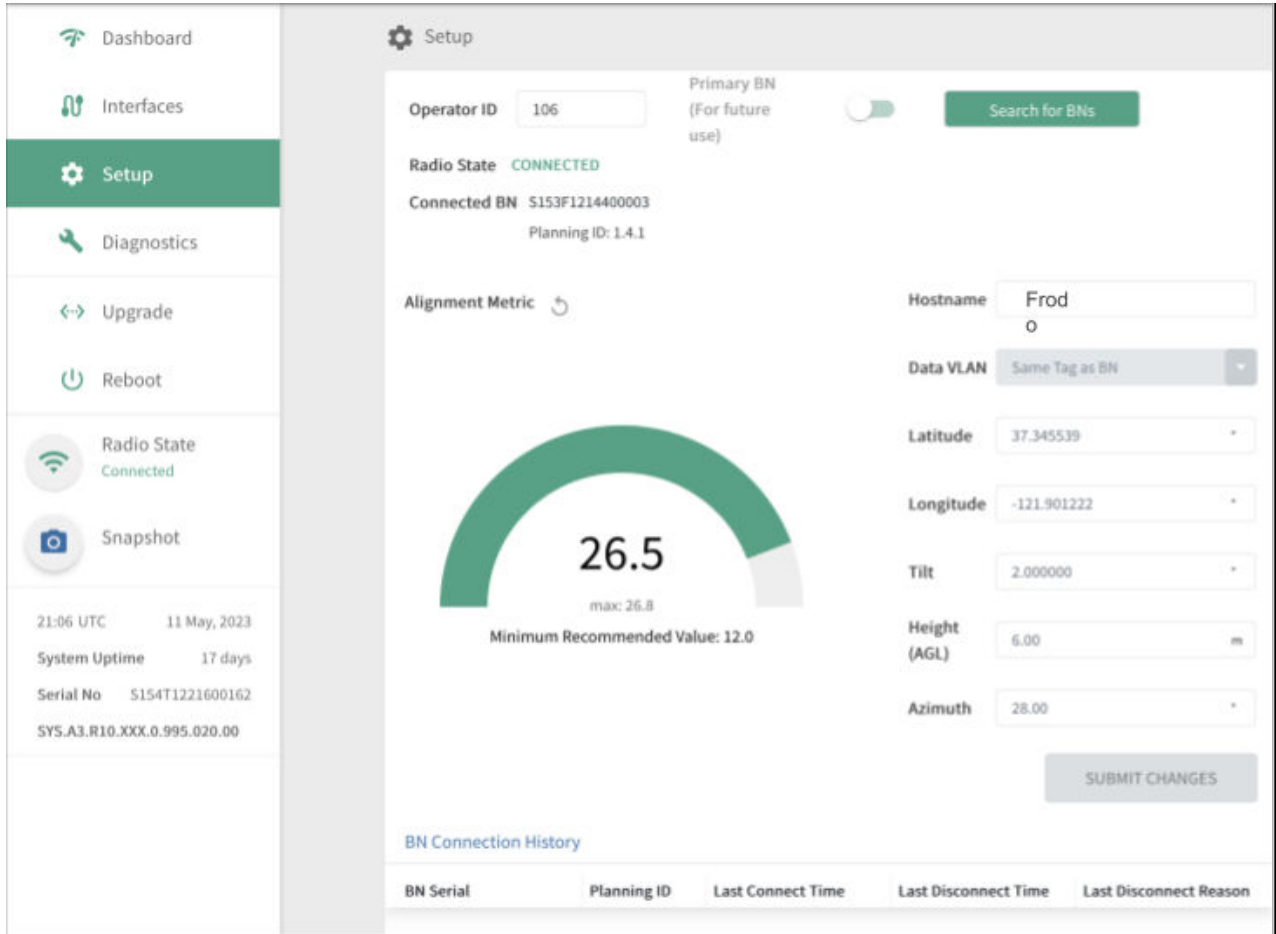
- System:** Hostname (Chamulins_Spaceport_Cantina), Operator ID (106), Carrier 0 Freq (MHz), Carrier 1 Freq (MHz), Country (United States).
- Data:** Interface (Data1 - 10G). The 'Data VLAN' section shows 'Using Untagged Data VLAN' selected and 'Tagged Data VLAN' disabled. 'Enable DHCP Relay Agent' is disabled, and 'Remote/Circuit Identifier Type' is set to 'Serial Number'.
- In-band Management:** IP/prefix (192.168.11.2/24), 'Enable DHCP' is disabled. The 'Mgmt VLAN' section shows 'Using Untagged Mgmt VLAN' selected and 'Tagged Mgmt' disabled.
- Out-of-band Management (optional):** IP/prefix (192.168.10.2/24), 'Enable DHCP' is disabled.
- Network/Services:** Mgmt Default Gateway (192.168.11.1), Cloud URL (registration.cloud.taranawireless.com:443), NTP Server(s), and DNS Server IP(s) (8.8.8.8).

Configure VLANS on the base node Web UI

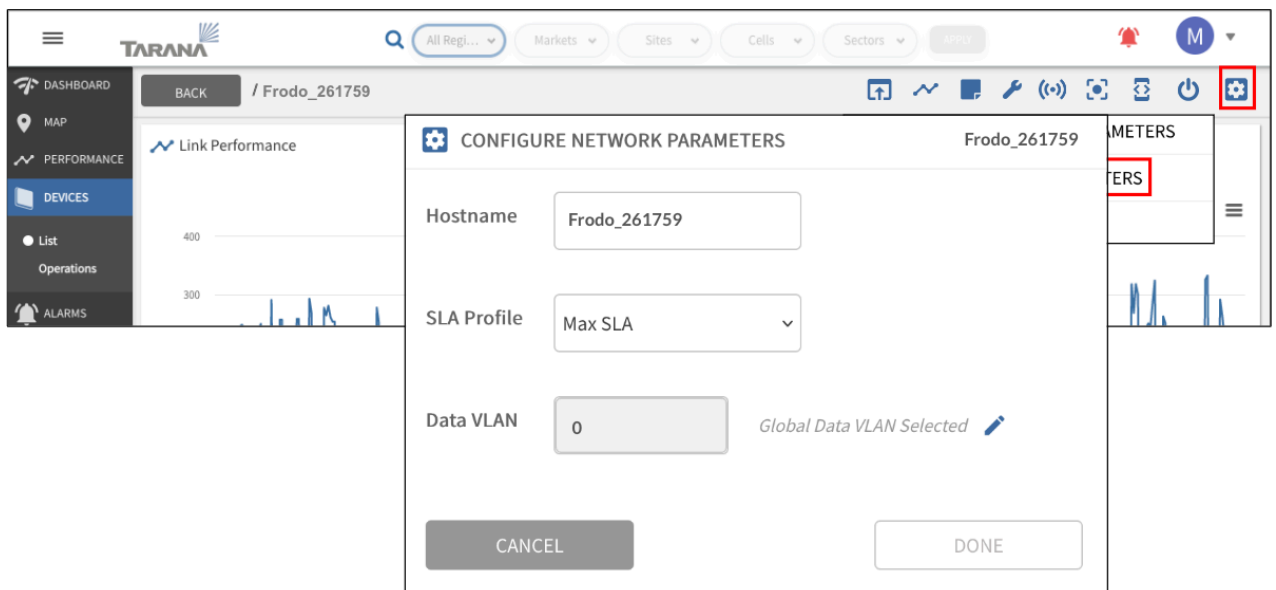
Remote Node VLANS

The second consideration is that 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 Web UI



Configure the Data VLAN on the Remote Node in TCS

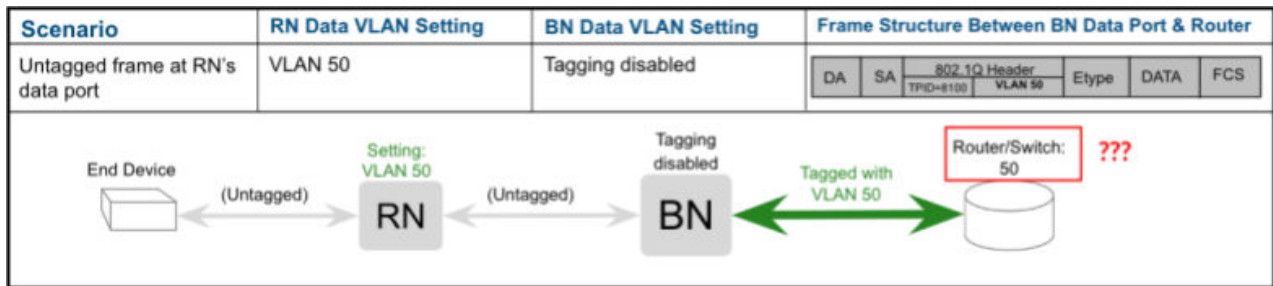
Tarana VLAN Logic

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:

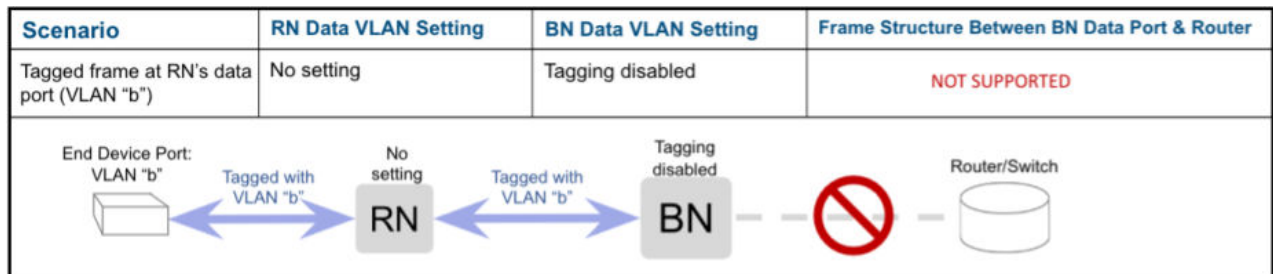
- The Data VLAN between the base node and connected router (or switch) is optional, but enabled by default.
- The optional Data VLAN setting on the remote node doesn't cause the remote to tag frames. Rather, it overrides the Data VLAN setting on the base node.

The remote node's Data VLAN setting (VLAN “a”) 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 RN’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.



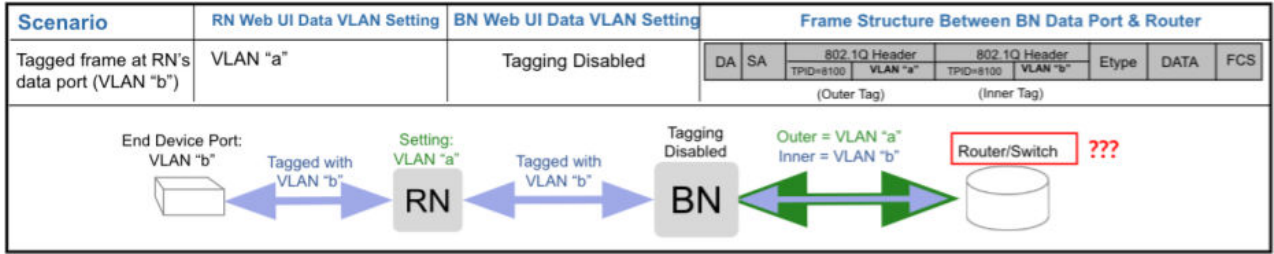
Remote Node VLAN Set, Base Node Untagged

With no Data VLAN settings on the remote node, and “Tagged Data VLAN” disabled on the base node, tagged frames originating from end devices aren't forwarded by the base node.

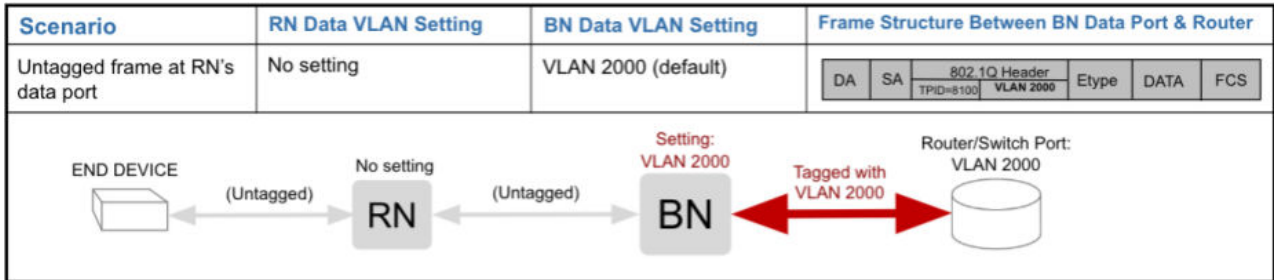


VLAN Set at End Device Port, Remote Node and Base Node Untagged

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.

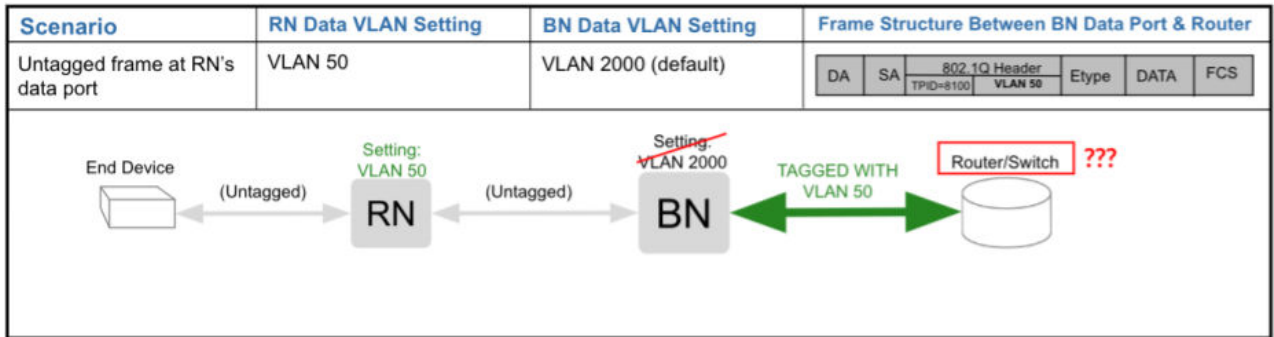


VLAN Set at End Device Port and Remote Node, Base Node Untagged



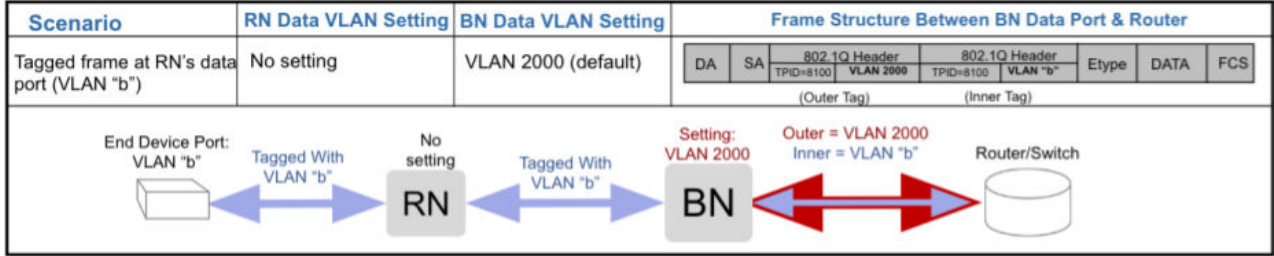
No Data VLAN at End Device Port or Remote Node

The remote node's Data VLAN setting (VLAN "a") overrides the base node's mandatory Data VLAN setting. The remote node doesn't tag or untag frames. You can also set the remote node's VLAN setting with TCS on the remote node's Device page. 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.



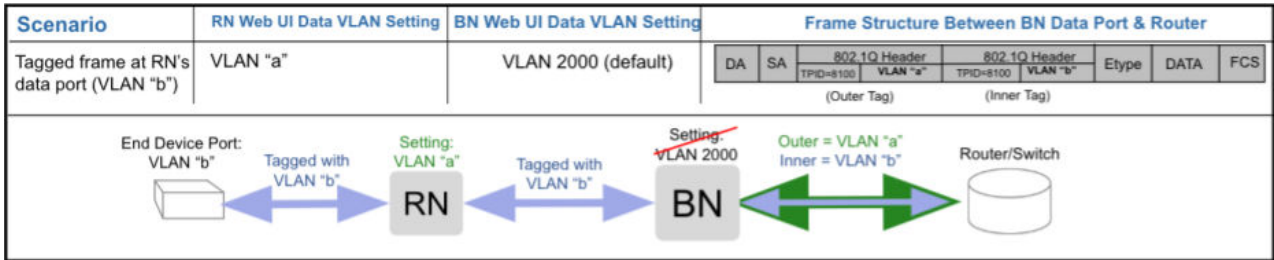
Remote Node VLAN "a"

Tagged frames between the end device and the router are encapsulated between the base node and the router by the base node's mandatory Data VLAN, which is set on the base node's web UI. These frames have an outer tag (VLAN 2000), 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 pass through the remote node's data port.



VLAN Set at End Device Port

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.



VLAN Set at End Device Port and Remote Node

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.

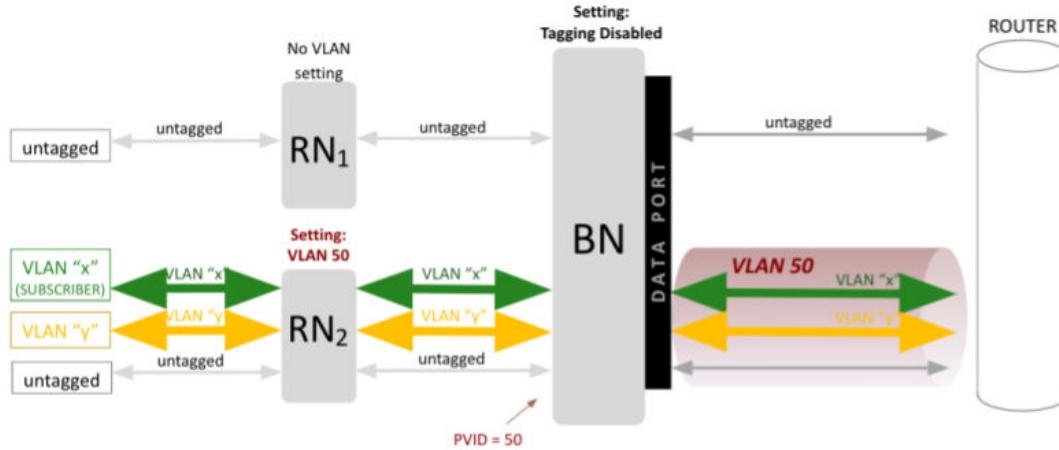
Depending on the desired tag for a frame egressing out of the remote node's data port, you must configure the appropriate tagging at the router.

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)	<table border="1"> <tr> <td colspan="2"></td> <td>(OUTER TAG)</td> <td>(INNER TAG)</td> <td colspan="3"></td> </tr> <tr> <td>DA</td> <td>SA</td> <td>VLAN 2000</td> <td>VLAN "a"</td> <td>Etype</td> <td>DATA</td> <td>FCS</td> </tr> <tr> <td>DA</td> <td>SA</td> <td>VLAN 2000</td> <td>VLAN "b"</td> <td>Etype</td> <td>DATA</td> <td>FCS</td> </tr> <tr> <td>DA</td> <td>SA</td> <td>VLAN 2000</td> <td>Etype</td> <td>DATA</td> <td>FCS</td> <td></td> </tr> <tr> <td>DA</td> <td>SA</td> <td>VLAN 50</td> <td>VLAN "x"</td> <td>Etype</td> <td>DATA</td> <td>FCS</td> </tr> <tr> <td>DA</td> <td>SA</td> <td>VLAN 50</td> <td>VLAN "y"</td> <td>Etype</td> <td>DATA</td> <td>FCS</td> </tr> <tr> <td>DA</td> <td>SA</td> <td>VLAN 50</td> <td>Etype</td> <td>DATA</td> <td>FCS</td> <td></td> </tr> </table>			(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	
		(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

In the scenario above, 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

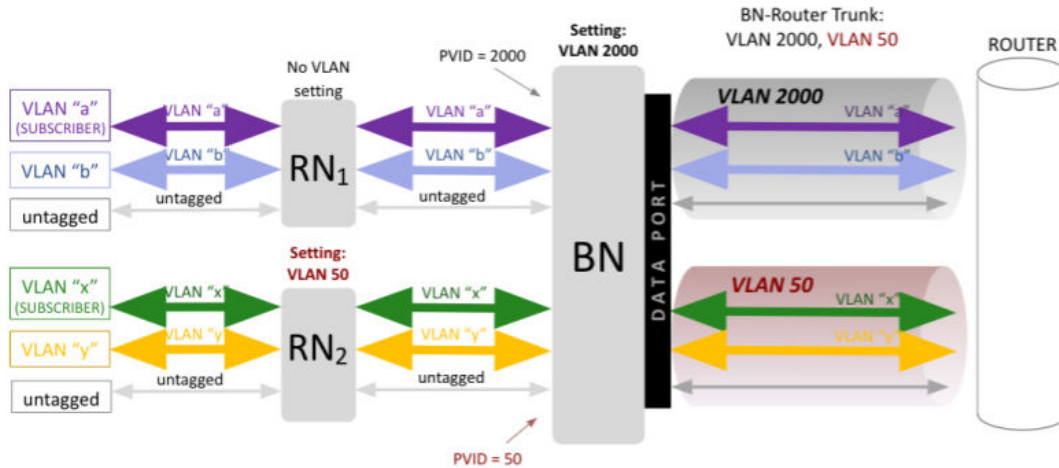
this remote node with Data VLAN 50 between the base node and the router. Tagged frames coming from this remote node will be encapsulated with VLAN 50 as an outer tag between the base node and the router. For “Subscriber” VLANs (VLAN “x” above), note that an appropriate DHCP pool would be needed in order to distribute IPs among the subscribers in this VLAN.



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

Multiple VLAN Scenario, Base Node Untagged

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



In the scenario above, one of the RNs has a VLAN setting (VLAN 50, in this case), and the other does not. This setting overrides the VLAN setting on the BN, therefore, the VLANs passing through this RN get encapsulated between the BN and router in VLAN 50 instead of the default VLAN 2000. For “SUBSCRIBER” VLANs (VLANs “a” and “x” above), please note appropriate DHCP pools would need to be allotted in order to distribute IPs among the subscribers on these VLANs.

Multiple VLAN Scenario

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.

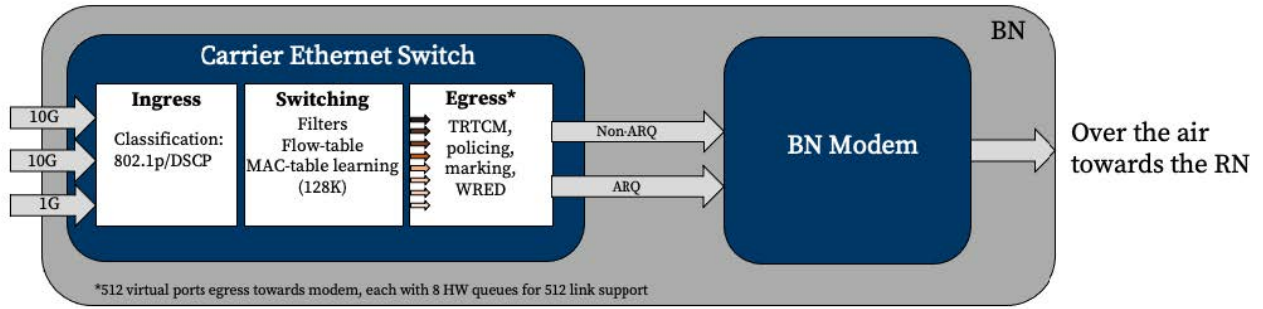
Set the Classification Type parameter on a per-base node basis in Network Configuration > Region > Market > Site > Cell > Sector. The color coding in the charts below shows how traffic is queued in the base node compared to the remote node.

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

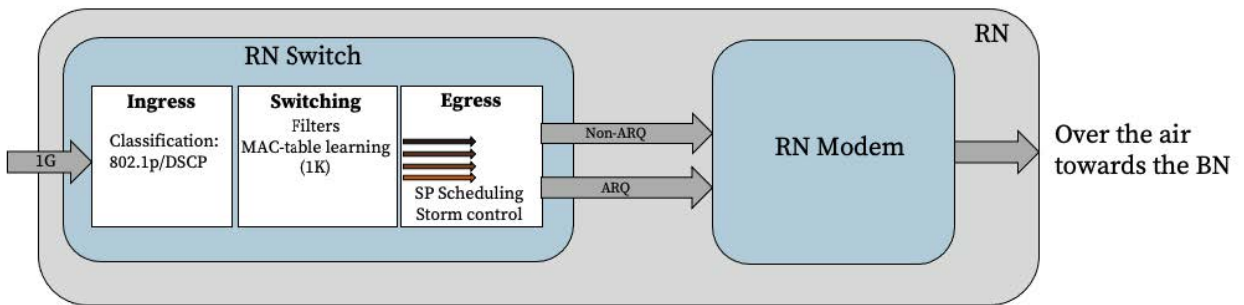
802.1p QoS Queues

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