



TCS Release Notes - 2023-04.1

10-0042-001



Table of Contents

- Intended Audience 3
- New Features and Enhancements 4
 - Base Node Association Management 4
 - Troubleshooting Tool Enhancements 6
 - Visual Alert Indicators 7
 - Usability Enhancements 9
- Known Issues 10
- Fixed Issues 11

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 the 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.

The 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 the TCS.

New Features and Enhancements

This release include the following new features and product enhancements.

Base Node Association Management

When a remote node loses its connection to its base node, the remote node begins to search for another base node so that it can restore a link between the subscriber and the backhaul network. In some cases, maintaining an association with the initial base node is preferred to seeking an alternate. In those cases, you can configure a remote node to connect persistently to a single base node.

Customer Application

Primary base nodes are the base nodes defined in TCS as the preferred connections for remote nodes, and each remote node can have only one primary base node. If a base node becomes unresponsive or restarts, then the remote node loses its connection to the base node. To regain the connection, the remote node can scan for, select, and connect to a different base node.

You can configure remote nodes to seek or ignore alternate base nodes when the link to the primary base node is unavailable. The choice you make can depend on important factors such as seeking alternate base nodes quickly to maintain a subscriber service level agreement (SLA), or maintaining a persistent association to prevent overloading alternate base nodes with too much traffic. Finding the best balance depends on the needs of your network and the needs of your subscribers.

You can filter the list of remote nodes in TCS to view remote nodes that are not connected to their respective primary base node. You can then select one or more of the remote nodes from the list, and then prompt them to re-establish their connection to their primary base node. To reconnect a remote node to its primary base node, both devices must be connected to—and visible in—TCS.

In this release, you can configure a remote node to use a primary base node persistently. When a remote node maintains a persistent association with its primary base node, the remote node does not migrate to another base node when the link is no longer available. Instead, the remote node waits for the primary base to become responsive, and then re-establishes the connection.

Feature Description

The new enhancements to base node association management allow you to configure your network behavior flexibly.

Deactivate Primary Base Node

In cases that do not require a remote node to associate with a specific primary base node, you can disable the feature completely. When the feature is deactivated and the remote node loses its connection to the base node, the remote node immediately searches for a new base node so that it can re-establish a connection to the backhaul. Although the backhaul connection can be re-established quickly, the quality of the connection might be lower, so having other options becomes important.

To deactivate the primary base node feature, do the following:

1. Log in to TCS using Op Admin privileges.
2. Navigate to **Admin > Network Configuration**.

3. To deactivate Primary Base Node Settings at the global level, navigate the network topology tree to the top organization level, otherwise navigate the tree to the sector in which you want to deactivate Primary Base Node Settings.
4. Toggle the **Primary BN** switch to the off position.

**NOTE**

Primary BN is deactivated by default.

Activate Primary Base Node

When a remote node does not have a primary base node defined, the remote node attaches to a base node based on metrics such as signal strength, regardless of whether the base node is intended as the optimal base node as part of the network design. Configuring a primary base node provides an intentional base node to which a remote node establishes its connection. If the remote node becomes disconnected from the primary base node, then the remote node seeks another base node by default; when the primary base node comes back online, the remote node can reconnect to it, returning the network topology to its designed state.

You can return the remote node to its primary base node manually, by prompting the remote node explicitly to reconnect, or automatically, by configuring the remote node to seek the primary base node at specific time intervals.

To activate the primary base node feature, do the following:

1. Log in to TCS using Op Admin privileges.
2. Navigate to **Admin > Network Configuration**.
3. To activate Primary Base Node Settings at the global level, navigate the network topology tree to the top organization level, otherwise navigate the tree to the sector in which you want to activate Primary Base Node Settings.
4. Toggle the **Primary BN** switch to the on position. Additional setting become available.

When you activate the primary base node feature, you must rehome remote nodes manually by default.

Manual Reconnect

To prompt a remote node manually to reconnect to its primary base node, do the following:

1. Log in to TCS using Op Admin privileges.
2. Navigate to **Devices > List**.
3. Select the check box of the device you want to reconnect to its base node. You can also select multiple check boxes to rehome multiple remote nodes.
4. Select **Network Operation (^(u)) > Connect to Primary BN** from the drop-down list.
5. Select **Confirm** in the warning dialog to confirm that the network impact of the action is acceptable.

Automatic Reconnect

With Primary Base Node activated, you can adjust additional settings to customize when and how the affected remote nodes attempt to reconnect to the primary base node.

To rehome remote nodes automatically, do the following:

1. With Primary BN activated, select the **Automatically (Instant)** option in the Reconnect to Primary BN prompt.
2. Select the time frame you want from the Connect to Alternate BN prompt. This is the number of minutes the remote node waits for the primary base node to become available before beginning to search for an alternate base node.
3. Select **Done** to save the changes.



NOTE

When you choose *Immediately* from the Connect to Alternate BN drop-down list, the remote node begins to search for an alternate base node immediately, but normal negotiation and connection times—generally less than five minutes—are required before traffic can flow across the link.



CAUTION

Avoid choosing wait times that are greater than 25 minutes. The remote node remains disconnected from the backhaul network during the wait period, and if a wait time is configured to be greater than 25 minutes, it is possible that the remote node does not seek an alternate base note at all, possibly requiring a truck to be dispatched to solve the issue.

Troubleshooting Tool Enhancements


In this release, some common troubleshooting tools that appeared previously only in the device WebUI now appear in TCS.

The following tools are now located on the single device page:

- Ping (base node only)
- Trace Route (base node only)
- DNS Lookup

Having troubleshooting tools available in TCS without having to log in to the device WebUI makes testing connections easier and more efficient.

To access the troubleshooting tools in TCS, do the following:

1. Log in to TCS using Op Admin privileges.
2. Navigate to **Devices > List**.
3. Select the device from which you want to use the troubleshooting tools. The device must be connected to TCS.
4. Select **Tool () > Troubleshoot**.
5. In the Troubleshoot dialog, select the tool from the Select Test Type drop-down list.

6. Enter any required information the tool requires, and then select **Start Test**.

Each tool has different parameters you must enter.

To perform a DNS lookup in TCS from the Troubleshoot dialog, do the following:

1. Select **DNS Lookup** from the Test Type drop-down list.
2. Enter the fully qualified domain name (FQDN) of the target.
3. Choose **Start Test**.

TCS returns the IP address of the target FQDN in the results section of the dialog.

To perform a network ping in TCS from the Troubleshoot dialog, do the following:

1. Select **Ping** from the Test Type drop-down list.
2. Enter a valid IP address or fully qualified domain name (FQDN) in the Enter IP Address or Domain Name field.
3. Enter the number of ping packets you want to send in the Count field.
4. Select **Start Test**.

The Ping tool sends a number of packets equal to the number entered in the Count field, aggregates the results, and then displays the following aggregated results:

- Average time (in milliseconds)
- Minimum time (in milliseconds)
- Maximum time (in milliseconds)
- Time to live (TTL, in hops)
- Standard deviation (in milliseconds)
- Sequence

If TCS receives no responses, then *No packets received* appears in the dialog results area.

To perform a trace route in TCS from the Troubleshoot dialog, do the following:

1. Select **Trace Route** from the Test Type drop-down list.
2. Enter a fully qualified domain name (FQDN) in the Enter Domain Name field.
3. Select **Start Test**.


TCS reports the trace route results in the results area of the dialog with the following information:

- **Name:** The domain name or IP address of the router at that hop.
- **Address:** The IP address of the router.
- **ICMP Code:** ICMP packets have a type and a code ID. The type refers to the purpose of the packet and is not displayed here. The code refers to the result of the action and is useful for troubleshooting. For example, an ICMP code of 0 indicates that the destination was unreachable.
- **Packet Size:** The size in bytes of the response packet.
- **RTT (round trip time):** The number of milliseconds required for the packet to be sent and a response to be received in a specific hop.
- **Hop:** The sequential order of the hop.

Visual Alert Indicators

This release includes clear visual indications when a device needs attention.

Customer Application

It is important to be able to locate devices that need attention, and to see at a glance what the device needs. This release includes visual indicators that highlight devices that need your attention using an alert icon ().

When you hover over the alert icon, TCS displays up to two alerts in a tooltip. If there are more than two alerts, TCS indicates the number of additional alarms in the tooltip.

The alert indicator provides a shortcut to information about the following non-standard or problematic parameters:

- **Software Policy** [MINOR]: indicated when the software on the devices does not match the valid software versions defined by the customer.
Action: No action is required. The software policy upgrades the devices automatically. You can also clear the alarm by upgrading the device software manually from the Single Device page.
- **Non-primary Base Node** [MINOR]: Indicated when the remote node is not connected to its primary base node.
Action: Ensure that the primary base node is available, and then prompt the remote node to search for the primary base node from the Single Device page.
- **Configuration Mismatch** [CRITICAL]: Indicated when there is a mismatch between TCS and the actual device configuration.
Action: If the device-side configuration is correct, configure TCS to match the device-side configuration. If the TCS configuration is correct and the device is a base node, push the configuration from the base node single device page. If the TCS configuration is correct and the device is a remote node, then reboot the remote node to prompt TCS to upload the current configuration when the RF link is established.
- **Muted Radio** [CRITICAL]: Indicated when a device radio is turned off.
Action: Unmute the radio.
- **Certificate Load Unsuccessful** [CRITICAL]: Indicated when the remote node has a missing or expired certificate.
Action: Contact Tarana Support.
- **Impending Certificate Expiry** [MINOR]: Indicated when the device certificate is within 15 days of expiring.
Action: Contact Tarana Support.
- **Device Unreachable** [MAJOR]: Indicated when the device can detect TCS, but TCS cannot detect the device.
Action: Call Tarana Support.
- **Non-Standard Software Image** [MINOR]: Indicated when the device is running a beta-version of the software.
Action: Upgrade to the latest official version that contains the required features available in your beta or custom build.


Feature Description

You can navigate to the device list and select the alert icon to view alerts associated with a device.

To navigate to the device list, do the following:

1. Log in to TCS using valid credentials.
2. Navigate to **Devices > List**.

3. Select either **RN** or **BN** to display only remote nodes or base nodes, respectively.

To view alerts associated with a specific device from the device list, select the Alert () icon.

Usability Enhancements

The following are minor functional, workflow, and visual enhancements to TCS.

Custom Time Range: The custom range of the performance view is now limited to one month. Ninety days of historical data are still available, but now are only visible in 30-day sets, which you can define in using the date pickers.

Date and Duration Display Formats: TCS now displays dates and durations in the following common standard formats.

- **Date and Time:** dd mmm yyyy hh:mm:ss
For example, 04 Apr 2023 09:56:30
- **Duration:** ad bh cm ds
For example, 3d 14h 22m 49s

Speed Test Packet Size: To optimize the speed test function, the speed test packet size is now 1518 bytes.

Tilt Nomenclature: Previously referred to as downtilt or tilt, this parameter is now consistently referred to as tilt throughout the interface.

Other User Experience and Interfaces Updates: The following minor enhancements are implemented in this release:

- Timestamp columns now contain seconds.
- The appearance time of tooltips are improved.
- The date and time that the device was first detected on the network are now located on the single device information card.

Known Issues

The following issues are known to exist in the current release. Where possible, a workaround appears in the Description column.

ID	Description
N/A	Base nodes cannot accept remote node connections when a grant exists only on Carrier1. Workaround: Set the preferred frequency from Spectrum Management, and then reacquire spectrum.
N/A	Remote nodes cannot connect to the base node if the spectrum provided by the SAS for the remote node is different from the base node spectrum. Workaround: Using Spectrum Management, update base node spectrum to match what is available at the remote node.
N/A	After an administrator attempts to reacquire spectrum, the CBRs Summary card displays old information. Workaround: The card updates when the spectrum reacquisition is completed in about 30 seconds.
N/A	When a remote node disconnects from one base node and connects to another base node on different frequencies, a new grant can take up to 20 minutes. Workaround: Select Reacquire Spectrum to request a new grant immediately.

Fixed Issues

The following issues have been fixed in this release.

ID	Description
TCC-10227	The single device page alternately displayed information for multiple remote nodes without user action.
TCC-9406	The single device page did not display the Tx Power Max value.
TCC-6876	When administrator privileges were changed in TCS, some changes did not propagate correctly.